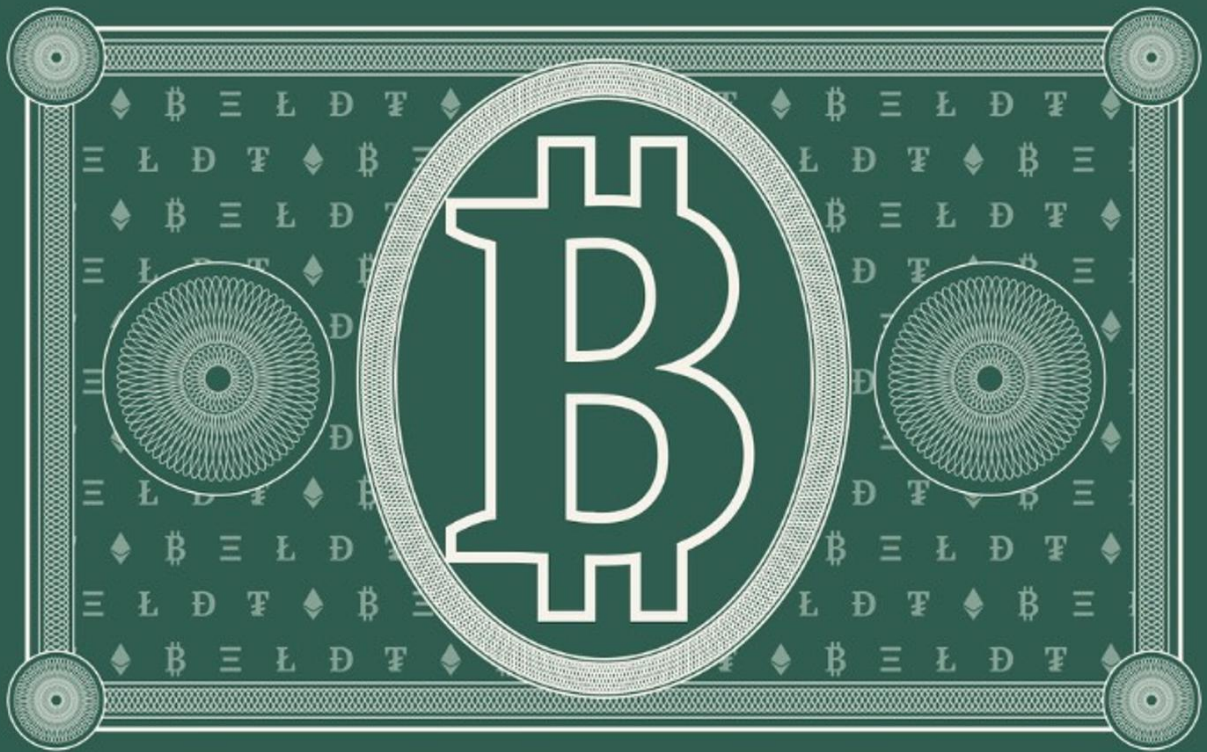
Доверие в долг

Криптовалюты как деньги и кредит: механизм, циклы, правила



АЛЕКСАНДР ЦЕЛЬХЕРТ

Александр Цельхерт

Доверие в долг. Криптовалюты как деньги и кредит: механизм, циклы, правила

«Автор»
2026

Цельхерт А.

Доверие в долг. Криптовалюты как деньги и кредит: механизм, циклы, правила / А. Цельхерт — «Автор», 2026

Если смотреть на криптовалюты только через цену, они так и останутся для вас либо верой, либо пирамидой, потому что цена не объясняет, почему рынок каждые несколько лет растёт в разы, а потом теряет больше половины. Это объясняет механизм. Осенью 2025 года биткоин стоил дороже, чем когда-либо, а через четыре дня биржи за одни сутки принудительно закрыли сделки на заёмные деньги больше чем на 19 млрд долларов. Сам биткоин никто не взламывал (сломались долги, взятые под него), и я покажу, что так устроен каждый большой обвал. Механизм держится на двух вопросах к любым деньгам: кто ведёт запись и кто кому должен. С ними мы пройдём все циклы рынка с 2010 года и в каждом увидим, где сломалось доверие, а где долг. Тогда процент в разы выше банковского не придётся брать на веру: вы сами найдёте, чей долг за ним стоит. Правила в конце книги — о том, сколько вы готовы потерять и кто выбирает день продажи.

Содержание

Александр Цельхерт
Доверие в долг. Криптовалюты как деньги и кредит: механизм, циклы, правила

Данные — на 27 сентября 2026 года. Книга не служит инвестиционной рекомендацией.

Введение. Зачем разбираться в механизме

Осенью 2025 года биткоин стоил дороже, чем когда-либо: 6 октября за него давали около 126 000 долларов[1]. Через четыре дня рынок за одни сутки принудительно закрыл позиций с плечом больше чем на 19 млрд долларов по публичным данным, а на деле, скорее всего, больше, и таких ликвидаций крипторынок ещё не видел[2]. (Плечо — это покупка на заёмные деньги. Когда цена падает, биржа сама продаёт купленное, чтобы вернуть себе долг, и такая продажа называется ликвидацией.) В начале февраля 2026 года цена опускалась примерно до 60 000[3], а самая низкая точка, около 57 700 долларов на бирже Bitstamp, пришлась на 1 июля по всемирному времени и была примерно на 54% ниже вершины[4].[5]

Сам биткоин за эти месяцы никто не взламывал, и сведений об успешной атаке большинства на его запись (попытке переписать её, собрав больше половины вычислительной мощности сети) нет за всё время его работы[6]. Ломалось другое. По оценке Galaxy Research, объём кредитов под залог криптовалют в третьем квартале 2025 года превысил рекорд 2021 года, и оба пика кредита совпали с пиками цены с точностью до квартала[7]. К концу второго квартала 2026 года этот кредит стоял больше чем на четверть ниже вершины[8].[9] Цена поднималась вместе с долгами, взятыми под неё, и падала, пока эти долги гасили или закрывали принудительно.

Эта книга объясняет, почему так происходит. Почти всё, что случается на крипторынке, уже случалось с обычными деньгами и кредитом, и биткоин с его обвалами понятен ровно настолько, насколько понятны они. Новая технология решила одну старую задачу — как вести общую запись о том, кому что принадлежит, так, чтобы у записи не было хозяина. Поверх этой записи люди снова построили посредников, займы и займы под займы, и рынок, выросший на ней, живёт волнами кредита. Подъём раздувается заёмными деньгами, падение расчищает

---

[1] Forbes, 05.10.2025, https://www.forbes.com/sites/digital-assets/2025/10/05/bitcoin-breaks-125000-the-convergence-of-confidence-capital-code/; CoinDesk (многократные упоминания «record high of $126,000 reached last October», напр. 05.02.2026).

[2] CoinDesk Research, «Market Spotlight: Inside Crypto's $19 Billion Liquidation Event», https://www.coindesk.com/research/market-spotlight-the-19-billion-liquidation-that-shook-crypto; CNBC, 22.10.2025, https://www.cnbc.com/2025/10/22/the-biggest-crypto-wipeout-was-led-not-by-bitcoin-but-much-smaller-tokens-heres-what-happened.html.

[3] CoinDesk, 05.02.2026, https://www.coindesk.com/markets/2026/02/05/bitcoin-drops-below-usd65-000-heading-to-worst-one-day-drawdown-since-ftx-blowup; CoinDesk, 06.02.2026, https://www.coindesk.com/markets/2026/02/06/crypto-markets-rebound-from-selloff-that-sent-bitcoin-to-lowest-since-october-2024.

[4] Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=4&start=1759622400; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782691200; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782172800; трёхдневные свечи за январь–март и июль–сентябрь 2026: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1767225600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1782864000.

[5] Пик — 126 272 доллара 06.10.2025, минимум — 57 734,63 доллара в часовой свече 01:00–02:00 UTC 1 июля 2026 года, обе цифры по данным биржи Bitstamp (Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=4&start=1759622400; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782691200; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782172800; трёхдневные свечи за январь–март и июль–сентябрь 2026: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1767225600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1782864000); в СМИ пик обычно округляют до 126 000 (Forbes, 05.10.2025, https://www.forbes.com/sites/digital-assets/2025/10/05/bitcoin-breaks-125000-the-convergence-of-confidence-capital-code/; CoinDesk (многократные упоминания «record high of $126,000 reached last October», напр. 05.02.2026)). До 26.09.2026 ниже цена не опускалась; свежие значения — в приложении Б.

[6] MIT Digital Currency Initiative, «51% Attacks» (трекер реорганизаций PoW-сетей; Г.-Я. Гласберген, Дж. Лавджой, Э. Оуян), http://www.dci.mit.edu/projects/51-percent-attacks.

[7] Galaxy Research, Q3 2025.

[8] Galaxy Research, Q2 2026.

[9] Galaxy Research пересматривает свои ряды: в выпуске за второй квартал 2026 года пик третьего квартала 2025 года указан выше, чем в выпуске за третий квартал 2025 года (78,69 млрд против 73,59 млрд долларов) (Galaxy Research, Q3 2025). Поэтому в тексте сравнение дано по одному выпуску и словами; подробности — в пятой и седьмой главах.

долги (расчисткой я буду называть время, когда накопленные на подъёме долги гасят, списывают или закрывают принудительными продажами). Увидев механизм и цикл, вы сможете судить о новостях, проектах и обещанных доходностях, не опираясь ни на веру, ни на страх.

Почему говорят только «за» и «против»

Разговор о криптовалютах почти всегда сводится к тому, вырастет ли цена. У этого есть простая причина. По опросу Федеральной резервной системы США, в 2025 году криптовалютой пользовались 10% взрослых американцев, почти все они держали её как вложение, а для платежей и переводов её использовали 2%[10].[11] Для большинства владельцев криптовалюта — ставка на цену. О цене же говорят двумя голосами. Один верит, что она вырастет, другой боится, что она упадёт.

Эти два голоса слышны и на книжных полках. Заметные книги о криптовалютах последних лет я бы разложил на три стопки. В первой история денег заканчивается биткоином как ответом на их беды, и даже довольные читатели называют такие книги односторонними[12]. Во второй лежат расследования, авторы которых считают схемой всю отрасль или, по словам рецензентов, сводят её к мошенничеству[13]. В третьей собраны истории людей, от основателей бирж до банкротов, и критики пишут, что устройство крипты там объяснено плохо[14].[15] В каждой стопке есть сильные книги. Книги, которая объясняла бы крипту через механизм денег и цикл кредита, я при подготовке этой не нашёл[16].

Вера и страх плохо помогают по одной и той же причине. Обе отвечают на вопрос о цене, а цена на этом рынке раз за разом подтверждает то одну сторону, то другую. От дна до следующей вершины биткоин дорожал то примерно в 129 раз, то в 22, то в 8[17], а от вершины до следующего дна дешевел на 93% в первом большом цикле, на 78% в последнем завершённом и пока на 54% в нынешнем[18]. Кто верит, каждые несколько лет получает подъём в разы как доказательство своей правоты. Кто боится, получает падение на три четверти. Поэтому спор не кончается, и ни одна сторона не объясняет, почему за подъёмом каждый раз следует падение.

---

[10] Federal Reserve Board, «Economic Well-Being of U.S. Households in 2025» (SHED), май 2026, раздел Banking, https://www.federalreserve.gov/publications/2026-economic-well-being-of-us-households-in-2025-banking.htm; за 2024: https://www.federalreserve.gov/publications/2025-economic-well-being-of-us-households-in-2024-banking-and-credit.htm.

[11] Federal Reserve Board. Economic Well-Being of U.S. Households in 2025, раздел Banking, май 2026: «The 10 percent of adults who used cryptocurrency for either purpose was up 2 percentage points from the prior year.»

[12] сайт автора https://www.lynalden.com/broken-money/; Amazon https://www.amazon.com/Broken-Money-Financial-System-Failing/dp/B0CG8985FR; Goodreads, https://www.goodreads.com/book/show/197566578-broken-money.

[13] Fortune, «Review: ‘Number Go Up’ is a funny if shallow look at the worst people in crypto», 2023, https://fortune.com/crypto/2023/09/12/review-number-go-up-is-a-funny-if-shallow-look-at-the-worst-people-in-crypto/; Kirkus Reviews, https://www.kirkusreviews.com/book-reviews/ben-mckenzie/easy-money-cryptocurrency/.

[14] Wikipedia, «Going Infinite», https://en.wikipedia.org/wiki/Going_Infinite; Ben McKenzie, Slate, 10.2023, https://slate.com/technology/2023/10/michael-lewis-going-infinite-sam-bankman-fried-ben-mckenzie-review.html (в выдаче).

[15] Примеры: в первой стопке — Lyn Alden, «Broken Money» (2023) (сайт автора https://www.lynalden.com/broken-money/; Amazon https://www.amazon.com/Broken-Money-Financial-System-Failing/dp/B0CG8985FR); во второй — Zeke Faux, «Number Go Up» (2023) и Ben McKenzie, Jacob Silverman, «Easy Money» (2023) (Fortune, «Review: ‘Number Go Up’ is a funny if shallow look at the worst people in crypto», 2023, https://fortune.com/crypto/2023/09/12/review-number-go-up-is-a-funny-if-shallow-look-at-the-worst-people-in-crypto/; Kirkus Reviews, https://www.kirkusreviews.com/book-reviews/ben-mckenzie/easy-money-cryptocurrency/); в третьей — Michael Lewis, «Going Infinite» (2023) (Wikipedia, «Going Infinite», https://en.wikipedia.org/wiki/Going_Infinite; Ben McKenzie, Slate, 10.2023, https://slate.com/technology/2023/10/michael-lewis-going-infinite-sam-bankman-fried-ben-mckenzie-review.html (в выдаче)). Раскладка по стопкам моя, оценки — рецензентов и читателей, на которых стоят ссылки.

[16] сайт автора https://www.lynalden.com/broken-money/; Amazon https://www.amazon.com/Broken-Money-Financial-System-Failing/dp/B0CG8985FR; Mark S. Rzepczynski, «Book Review: Boom and Bust», CFA Institute Enterprising Investor, 22.11.2021, https://rpc.cfainstitute.org/blogs/enterprising-investor/2021/book-review-boom-and-bust; Freie Universität Berlin, пресс-релиз, 2025, https://www.fu-berlin.de/en/presse/informationen/fup/2025/fup_25_065-wandel-von-kryptowaehrungen/index.html; статья: https://www.tandfonline.com/doi/full/10.1080/09692290.2025.2476738.

[17] расчёт автора по данным (Bitstamp).

[18] расчёт автора по данным (Bitstamp); для 2011 — V. Ganne (Swissquote), TradingView, 17.11.2025, по данным Glassnode, https://www.tradingview.com/chart/BTC_ATHDRAWDOWN/9AUq2iAG-Bitcoin-What-Historical-Drawdown-in-a-Bear-Market/; CoinDesk, 24.09.2026.

Вера подводит человека ровно тогда, когда объяснение нужнее всего. Тот, кто купил биткоин на вершине 2021 года, пережил падение на 78%[19], и вера в технологию не подсказывала ему, почему в 2022 году одна за другой останавливали вывод денег компании, которые принимали монеты клиентов и платили за них процент[20]. Технология в этих историях как раз работала. Не выдержали обещания посредников.

Страх обходится дешевле, но и он мешает видеть. Запись, на которой всё держится, ведётся с января 2009 года[21]. Стейблкоины, то есть монеты, привязанные к доллару, выросли к весне 2026 года, по данным ФРС, до 317 млрд долларов[22], а взрослые американцы без банковского счёта платят криптовалютой втрое чаще тех, у кого счёт есть (6% против 2%)[23]. Страх хорошо объясняет обвалы. Почему после каждого обвала рынок возвращался и поднимался выше прежней вершины, он объяснить не может.

Механизм отвечает на вопросы, которые не упираются в цену. Возьмём один пример. В начале 2022 года сервис Anchor платил держателям долларового стейблкоина UST стабильные 19,5% годовых, когда по основным стейблкоинам в других кредитных сервисах платили около 2–3%[24]. Верящему здесь легко увидеть новые финансы, боящемуся — пирамиду, и спор между ними идёт о словах. Механизм подсказывает вопрос попроще. Кто должен эти 19,5% и из чего он их заплатит? Когда в мае 2022 года UST и связанная с ним монета LUNA обрушились, инвесторы, по данным американской прокуратуры, потеряли около 40 млрд долларов[25], и ответ стал известен всем, хотя задать вопрос можно было заранее.

Разбираться в этом стоит, даже если вы ничего покупать не собираетесь, потому что крипта за последние годы вошла в обычные финансы. В январе 2024 года американский регулятор рынка ценных бумаг разрешил биржевые фонды, которые держат биткоин, и его председатель в тот же день оговорил, что это не одобрение самого биткоина[26]. В июле 2025 года в США подписан закон о стейблкоинах, по которому под каждый выпущенный доллар нужно держать резервы в ликвидных активах, и заработать он должен не позже января 2027 года[27]. В Евросоюзе единые правила для криптоактивов действуют с 2024 года[28]. Биткоин теперь продаётся в обёртке обычного биржевого фонда, выпуск доллар-токенов переводят под закон, и о том и о другом вы узнаёте из новостей, написанных всё теми же двумя голосами.

---

[19] Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1636329600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1668816000.

[20] CoinDesk, «The Fall of Celsius Network: A Timeline…», 15.07.2022, https://www.coindesk.com/markets/2022/07/15/the-fall-of-celsius-network-a-timeline-of-the-crypto-lenders-descent-into-insolvency; CNBC, 29.06.2022, https://www.cnbc.com/2022/06/29/crypto-hedge-fund-three-arrows-capital-plunges-into-liquidation.html; FSOC 2022, с. 35 (со ссылкой на WSJ, 01.07.2022); Wikipedia, «Voyager Digital» (дата главы 11 — со ссылкой на WSJ, 06.07.2022); SEC, Press Release 2023-7, 12.01.2023, https://www.sec.gov/news/press-release/2023-7.

[21] Bitcoin Wiki, «Genesis block», https://en.bitcoin.it/wiki/Genesis_block (текст поля coinbase воспроизводится любым узлом сети).

[22] Federal Reserve, FEDS Notes, «Stablecoins in 2025: Developments and Financial Stability Implications», 08.04.2026, https://www.federalreserve.gov/econres/notes/feds-notes/stablecoins-in-2025-developments-and-financial-stability-implications-20260408.html.

[23] Federal Reserve Board, «Economic Well-Being of U.S. Households in 2025» (SHED), май 2026, раздел Banking, https://www.federalreserve.gov/publications/2026-economic-well-being-of-us-households-in-2025-banking.htm; за 2024: https://www.federalreserve.gov/publications/2025-economic-well-being-of-us-households-in-2024-banking-and-credit.htm.

[24] NBER WP 31160, с. 3, 19, 21, https://www.nber.org/papers/w31160.

[25] U.S. Attorney's Office SDNY, «Crypto-Enabled Fraudster Sentenced For Orchestrating $40 Billion Fraud», https://www.justice.gov/usao-sdny/pr/crypto-enabled-fraudster-sentenced-orchestrating-40-billion-fraud.

[26] G. Gensler, «Statement on the Approval of Spot Bitcoin Exchange-Traded Products», SEC, 10.01.2024, https://www.sec.gov/newsroom/speeches-statements/gensler-statement-spot-bitcoin-011023.

[27] Covington & Burling, «The GENIUS Act Becomes Law…», 07.2025, https://www.cov.com/news-and-insights/insights/2025/07/the-genius-act-becomes-law-key-provisions-from-the-federal-stablecoin-regulatory-framework; Mayer Brown, 07.2025; The White House, https://www.whitehouse.gov/briefings-statements/2025/07/the-president-signed-into-law-s-1582.

[28] AMF (регулятор Франции), «The European regulation Markets in Crypto-Assets (MiCA)», https://www.amf-france.org/en/news-publications/depth/mica.

Я не собираюсь ни защищать криптовалюты, ни разоблачать их. Где технология работает, я так и скажу, и где она оказалась лишней, тоже. За пределами крипты одна и та же общая запись у одной финансовой компании каждый день проводит сделки, а у другой после нескольких лет стройки ушла в списание[29]. Разницу между такими историями объясняет вопрос о том, кому и зачем понадобилась общая запись без хозяина.

[29] Broadridge, пресс-релиз «Broadridge's Distributed Ledger Repo Platform Processes $368 Billion in Average Daily Trade Volumes in November», 04.12.2025. https://www.broadridge.com/press-release/2025/broadridge-distributed-ledger-repo-platform-november; ASX, «ASX will reassess all aspects of the CHESS replacement project and derecognise capitalised software of $245-255 million pre-tax in 1H23», 17.11.2022, https://www.asx.com.au/content/dam/asx/about/media-releases/2022/60-17-november-2022-CHESS-Replacement-ASX-reassessing-financial-derecognition_.pdf.

Всё это уже было

Если отвлечься от цены и посмотреть, что именно ломалось в каждом обвале, картина окажется знакомой. Токийская биржа Mt. Gox в феврале 2014 года подала на банкротство и сообщила о пропаже около 850 000 биткоинов, из которых примерно 750 000 принадлежали клиентам[30]. Это старая история посредника, которому доверили чужое и который его не сберёг. Криптокредитор Celsius в июне 2022 года заморозил вывод средств, а через месяц подал на банкротство[31], и это паника вкладчиков в банке, у которого нет ни страхования вкладов, ни центрального банка за спиной.

Два других примера ещё ближе к обычным деньгам. В марте 2023 года стейблкоин USDC ненадолго подешевел до 86–87 центов, потому что 3,3 млрд долларов его резервов лежали в обанкротившемся американском банке Silicon Valley Bank. Привязка к доллару вернулась, когда власти гарантировали вкладчикам этого банка их деньги[32]. Криптовалюта в этой истории пострадала от краха самого обычного банка. А октябрьские ликвидации 2025 года — старая продажа заложенного за долги, только исполняли её программы бирж, и уложились они в сутки[33].

Новое во всех четырёх историях одно, и это запись, в которой лежат монеты. Всё, что в них сломалось, люди построили поверх записи, и устроено оно так же, как у обычных денег (хранение чужого, займы под процент, резервы в банке, покупка в долг).

Механику таких поломок экономисты описали задолго до биткоина. Американский экономист Хайман Мински сформулировал её как гипотезу, по которой за долгие периоды процветания экономика сама переходит от финансовых отношений, при которых система устойчива, к отношениям, при которых она неустойчива[34].[35] Историки финансов Уильям Куинн и Джон Тёрнер описали пузырь как треугольник, похожий на треугольник огня, где сторонами служат лёгкость покупки и продажи, деньги и кредит и спекуляция[36]. Заключительную главу своей книги они начинают с того, что этот треугольник объясняет пузырь криптовалют 2017 года[37].[38] Мински писал об экономике вообще, Куинн и Тёрнер — о пузырях за три века. Крипта

---

[30] TechCrunch, 28.02.2014, https://techcrunch.com/2014/02/28/mt-gox-files-for-bankruptcy; NPR, 28.02.2014, https://www.npr.org/sections/thetwo-way/2014/02/28/283863219/mtgox-files-for-bankruptcy-nearly-500m-of-bitcoins-lost.

[31] CoinDesk, «The Fall of Celsius Network: A Timeline…», 15.07.2022, https://www.coindesk.com/markets/2022/07/15/the-fall-of-celsius-network-a-timeline-of-the-crypto-lenders-descent-into-insolvency; CNBC, 29.06.2022, https://www.cnbc.com/2022/06/29/crypto-hedge-fund-three-arrows-capital-plunges-into-liquidation.html.

[32] CNBC, 11.03.2023, https://www.cnbc.com/2023/03/11/stablecoin-usdc-breaks-dollar-peg-after-firm-reveals-it-has-3point3-billion-in-svb-exposure.html; CoinDesk, 13.03.2023, https://www.coindesk.com/business/2023/03/13/usdc-stablecoin-regains-dollar-peg-after-silicon-valley-bank-induced-chaos; разбор ФРС: FEDS Notes, 17.12.2025, https://www.federalreserve.gov/econres/notes/feds-notes/in-the-shadow-of-bank-run-lessons-from-the-silicon-valley-bank-failure-and-its-impact-on-stablecoins-20251217.html.

[33] CoinDesk Research, «Market Spotlight: Inside Crypto's $19 Billion Liquidation Event», https://www.coindesk.com/research/market-spotlight-the-19-billion-liquidation-that-shook-crypto; CNBC, 22.10.2025, https://www.cnbc.com/2025/10/22/the-biggest-crypto-wipeout-was-led-not-by-bitcoin-but-much-smaller-tokens-heres-what-happened.html.

[34] Minsky, 1992, pp. 7–8.

[35] Minsky H. P. The Financial Instability Hypothesis. 1992, pp. 7–8: «…over periods of prolonged prosperity, the economy transits from financial relations that make for a stable system to financial relations that make for an unstable system.»

[36] Cambridge Core, аннотация главы 1 «The Bubble Triangle», с. 1–15, https://www.cambridge.org/core/product/identifier/9781108367677%23CN-bp-1/type/book_part; DOI книги 10.1017/9781108367677.

[37] Cambridge Core, аннотация главы 12, https://www.cambridge.org/core/product/identifier/9781108367677%23CN-bp-12/type/book_part; страницы — Crossref, DOI 10.1017/9781108367677.012.

[38] Quinn W., Turner J. D. Boom and Bust: A Global History of Financial Bubbles. Cambridge University Press, 2020; аннотация главы 12 «Predicting Bubbles»: «The chapter starts by arguing that the bubble triangle can explain why the cryptocurrency bubble occurred in 2017.»

вошла в их схемы без переделки, и для меня это главный довод в пользу того, что её стоит изучать как деньги и кредит.

Раз новое в этих историях только запись, её и стоит понять первой, иначе трудно отличить, где кончается механизм и начинаются люди. У записи биткоина есть свойства, которых нет у банковского счёта, и они меняют цену ошибок. Платёж через банк можно оспорить и отменить, и Накамото прямо писал, что из-за этой возможности продавцам приходится остерегаться собственных покупателей[39]. Перевод в биткоине отменить нельзя. Ошибку в адресе никто не исправит, украденный ключ означает украденные монеты, а правило, записанное в код, исполняется так же неумолимо, как и ошибка в этом коде. Пока вы аккуратны, всё это работает на вас, а стоит ошибиться или отдать ключ не тому, и оно работает против.

[39] Nakamoto, 2008, раздел 1 «Introduction», https://bitcoin.org/bitcoin.pdf.

Что умеет модель

Под моделью я понимаю упрощённое описание механизма, то есть того, из каких частей он состоит и что за чем следует, если изменить одну из них. Модель говорит, что произойдёт, но не говорит когда. У этой книги модель одна, и в ней две половины.

Первая половина — механизм: как устроена общая запись о деньгах, на чём держится доверие к ней и что меняется, когда у записи пытаются совсем убрать хозяина. Её я буду собирать по шагам на игрушечном примере с круглыми числами и каждый раз отмечать, где пример перестаёт быть похожим на настоящие деньги. Вторая половина — цикл кредита. Там, где поверх записи появляются займы, появляется и волна, которая сначала раздувает цены, а потом расчищает долги.

Эта вторая половина и отвечает на вопрос, который спор веры и страха оставляет открытым. Цена растёт, и монеты, лежащие в залоге, дорожают. Под дорогой залог дают больше денег, на эти деньги покупают ещё монеты, и цена растёт снова, выше, чем подняли бы её одни собственные деньги покупателей. На развороте петля крутится в обратную сторону. Залог дешевеет, у кого он опустился ниже порога, у того его продают принудительно, эти продажи опускают цену до порогов следующих заёмщиков, и падение уходит глубже, чем ушло бы без долгов.

Во второй части книги я разложу цикл на шесть этапов: новая история, которая обещает прибыль; приток денег; заёмные деньги и плечо; пик; принудительные продажи; расчистка. Декорации менялись (деньги копились то в кассах первых бирж, то в продажах новых токенов, то у кредитных сервисов, то в биржевых фондах), а порядок этапов оставался прежним. Толкают цикл три слоя сил: деньги снаружи рынка, плечо внутри него и история, которой люди объясняют себе покупку. Экономист Роберт Шиллер предлагал изучать такие истории почти как эпидемии, потому что мозг, по его словам, настроен на рассказы, правдивые или нет, которыми люди оправдывают траты и вложения[40].[41] Пик приходит, когда один из слоёв иссякает, и в разных циклах первым иссякал разный.

Прогноз устроен иначе. Он называет дату или цену и обычно держится на одном рычаге. Самый популярный связан с халвингом, плановым сокращением выпуска новых биткоинов вдвое примерно раз в четыре года. В трёх последних циклах вершина приходила почти через одинаковый срок после халвинга, но трёх точек мало, чтобы назвать причину, а исследования, которое отделило бы действие халвинга от действия дешёвых денег, я не нашёл[42]. Другой прогноз привязывает биткоин к количеству денег в экономике США, но в 2026 году денежная масса там обновляла рекорды, а биткоин дешевел[43].

Модель не обещает ни цены, ни даты. Допустим, вы видите, что за год цена выросла втрое. Прогноз спрашивает, вырастет ли она ещё, и честно ответить на это не может никто. Модель спрашивает, на чьи деньги она поднялась. Если покупали в основном на свои и держат монеты у себя, продавать никого не заставят, и падению почти не на что опереться, чтобы стать обвалом. Если вместе с ценой выросли займы под залог монет и ставки с плечом, у рынка появились продавцы поневоле, и каждый процент падения приближает их к порогу, за которым биржа продаст за них. Цена в обоих случаях одна и та же, а этап цикла и цена ошибки разные.

---

[40] R. J. Shiller, «Narrative Economics», American Economic Review 107(4), April 2017, pp. 967–1004, DOI 10.1257/aer.107.4.967, https://www.aeaweb.org/articles?id=10.1257/aer.107.4.967.

[41] Shiller R. J. Narrative Economics. American Economic Review, 2017, 107(4): «The human brain has always been highly tuned toward narratives, whether factual or not, to justify ongoing actions, even such basic actions as spending and investing.»

[42] расчёт: даты халвингов — (Bitcoin Wiki, mempool.space, The Block); даты пиков — (Bitstamp).

[43] FRED, M2SL, https://fred.stlouisfed.org/graph/fredgraph.csv?id=M2SL&cosd=2024-01-01&coed=2026-09-01; FEDFUNDS; цены — https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=4&start=1759622400.

Я доверяю этой модели по двум причинам. Её звенья описаны на истории обычных денег и кредита, от Компании Южных морей до доткомов, и крипту я в эту схему вписываю, а не строю схему под крипту. И её можно проверить: во второй части мы прогоним через неё все большие циклы рынка с 2010 года до нынешнего, который ещё не закончен. Где модель не справляется, я скажу прямо. В открытом цикле она, например, не может сказать, пройдено ли уже дно, и я этого тоже не знаю.

Как устроена книга

Книга состоит из трёх частей. Первая собирает механизм с нуля. Она начинается с денег, какими они были задолго до компьютеров, и шаг за шагом доходит до блокчейна, до способа, которым тысячи незнакомых участников договариваются об одной записи, до смарт-контрактов и стейблкоинов. Заканчивается она разбором того, где блокчейн прижился за пределами денег и где нет. Вторая часть строит модель криптоцикла и проверяет её на истории рынка, от первых циклов вокруг бирж и продаж токенов через цикл заёмных денег 2020–2022 годов до цикла институтов, который ещё идёт. В каждом цикле у рынка был свой посредник, которому доверили чужие деньги, и вторая часть следит за тем, как от цикла к циклу менялся этот посредник, а вместе с ним и то, где рвалось в первую очередь.

Третья часть переводит понимание в действие. В ней разобрано, как государства отвечают на крипту, как люди теряют криптовалюту и что помогает вам не потерять свою, какие правила помогают участнику рынка пережить расчистку и какие сценарии будущего выглядят правдоподобными. Правила собраны в тринадцатой главе, и там же вся книга сводится к одной схеме из двух вопросов. Первый — кто ведёт запись и кто может её изменить, и на нём держится механизм. Второй — кто кому должен и что случится, когда долг вычеркнут, и на нём держится цикл. Правила опираются на всё, что сказано до них, поэтому читать книгу лучше по порядку. Без первой части вторая превращается в хронику, а без второй правила третьей выглядят произвольными.

Несколько договорённостей помогут при чтении. Условные примеры я всегда называю условными, а числа в них круглые. Каждое проверяемое утверждение опирается на источник, источники собраны в примечаниях, и там же лежат оригиналы цитат, которые в тексте даны в переводе. «Я» в книге значит оценку, мнение или признание того, чего я не знаю. Историй из собственной жизни здесь нет. Главы с практическими выводами заканчиваются короткой выжимкой, у каждой своей формы (в шестой и девятой это вопросы, в седьмой таблица, в двенадцатой чек-лист, в тринадцатой свод правил), а схемы нарисованы так, чтобы их можно было читать и в чёрно-белой печати.

Цифры на этом рынке стареют быстрее всего остального. Данные в книге собраны по состоянию на конец сентября 2026 года, и почти у каждой цифры стоит дата. Свежие значения, статусы законов и судебных дел собраны в приложении Б «Положение на дату», а термины объяснены простыми словами в глоссарии, в приложении А. Механизм от смены цифр не устаревает, и книга построена так, чтобы через несколько лет вы могли подставить в модель новые данные сами.

И последнее. Эта книга не инвестиционная рекомендация. В ней нет советов, какие монеты покупать, и нет прогнозов цены, а о законах и налогах я пишу как об обзоре подходов разных стран, без руководства для какой-то одной. Задача у книги другая. Я хочу, чтобы, прочитав новость о крипте, вы сами могли понять, какая часть механизма в ней задета и на каком этапе цикла это происходит.

Начнём поэтому с денег, какими они были задолго до биткоина, и с вопроса, который можно задать любым деньгам, — кто ведёт запись о долгах и почему этой записи верят.

Часть I. Как это устроено

Глава 1. Деньги — это договорённость о доверии

Если вы не видите, что остаётся от денег, когда из них убраны монеты и банкноты, то и криптовалюты останутся для вас загадкой, потому что они заменяют не бумагу и не металл, а совсем другую часть денег. Эту часть я и хочу показать в первой главе. Сначала мы соберём игрушечную модель денег, потом будем добавлять к ней по одному правилу и следить, как меняется её поведение, пока не дойдём до задачи, которую взялся решить создатель биткоина. Как он её решил, разберём в следующей главе; здесь нужно понять, откуда задача взялась и почему её не смогли решить люди, знавшие криптографию ничуть не хуже.

Начнём с посёлка, которого нет (он условный, и числа в нём круглые для удобства). В посёлке сто дворов и ни одной монеты. Пекарь печёт хлеб, плотник чинит крыши, у доярки есть молоко, и меняться напрямую им неудобно: хлеб плотнику нужен сегодня, а крыша пекарю понадобится только осенью.

Выход находят простой и старый — в посёлке заводят тетрадку. Когда плотник берёт у пекаря десять буханок, туда записывают «плотник должен пекарю 10», а осенью, когда крыша починена, строчку вычёркивают. Если пекарю молоко нужнее крыши, он может отдать доярке своё право на этот долг, и тогда плотник будет должен уже ей.

Обратите внимание на то, что сейчас произошло.

Монет в посёлке по-прежнему нет, а деньги уже появились, и это записи о долгах, которые переходят из рук в руки и которыми можно расплатиться за хлеб, молоко или работу. Монеты, банкноты и цифры на банковском счёте я в этой книге буду считать разными способами вести такую же запись (у каждого способа свои слабости, и мы до них дойдём).

Первое правило понадобится почти сразу. Тетрадка должна быть одна, потому что, если каждый двор ведёт свою, записи быстро разойдутся (у плотника долг вычеркнут, у пекаря нет), и спор решить будет нечем.

С одной тетрадкой у посёлка появляется хранитель, а вместе с ним вопрос, от которого теперь зависит всё: почему хранителю верят? Он может приписать себе лишнюю строчку, стереть чужую или позволить пекарю отдать одно и то же право на долг сразу двоим.

Человек (или группа людей), выступавший под именем Сатоши Накамото, в 2009 году назвал этот вопрос корнем бед обычных денег. Главная их проблема, писал он, во всём том доверии, которое нужно, чтобы они работали. Центральному банку приходится верить, что он не обесценит валюту, а история бумажных денег полна нарушений этого доверия[44].[45] Прежде чем смотреть, чем он предложил доверие заменить, проверим, похож ли наш посёлок на настоящую экономику, и добавим в него ещё несколько правил.

[44] Satoshi Nakamoto, «Bitcoin open source implementation of P2P currency», P2P Foundation, 11.02.2009, 22:27 UTC; архив Satoshi Nakamoto Institute, https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/1/.

[45] Nakamoto S. Bitcoin open source implementation of P2P currency. P2P Foundation, 11.02.2009: «The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust.»

Что остаётся от денег без монет

Посёлок с тетрадкой может показаться удобной выдумкой, подогнанной под нужный вывод. Проверить это проще всего по источнику, который трудно заподозрить в симпатии к криптовалютам, то есть по объяснению самого центрального банка.

В 2014 году три экономиста Банка Англии напечатали в его ежеквартальном бюллетене популярную статью о том, что такое деньги в современной экономике. Их ответ почти совпадает с нашей тетрадкой. Сегодня деньги — это разновидность долговой расписки, и особая она тем, что все в экономике уверены, что её примут другие люди в обмен на товары и услуги[46].[47] Через две страницы та же мысль сказана ещё короче: деньги в современной экономике — всего лишь особая форма расписки[48].

Путь, которым авторы приходят к этому выводу, тоже похож на наш. Они описывают мир, где каждый выписывает собственные расписки и отмечает в общем списке, должен он в итоге или должны ему, и вспоминают средневековых европейских купцов, которые расплачивались расписками и сводили их на ярмарках, большей частью просто погашая долги друг против друга[49]. Слабое место такой системы названо сразу. Она держится на уверенности каждого, что все остальные совершенно надёжны. Деньги, по словам авторов, — общественный институт, который решает проблему недостатка доверия[50].[51]

В посёлке эту разницу легко увидеть. Строчка «плотник должен пекарю 10» годится доярке, только если доярка верит плотнику, ведь он может уехать или слечь до осени. Лесорубу с дальнего края посёлка, который плотника не знает, такая строчка не годится вовсе. Теперь пусть хранитель заменит её своей строчкой «хранитель должен пекарю 10», а с плотника долг спросит сам. Такую строчку возьмут все сто дворов, потому что верить теперь нужно одному хранителю вместо каждого должника по отдельности. Сто частных доверий сжимаются в одно общее, и в этот момент расписка становится деньгами в смысле Банка Англии, то есть распиской, которую примет любой[52].

Как мало деньги зависят от предмета, лучше всего видно на острове Яп в Каролинском архипелаге. В 1910 году о нём выпустил книгу американский путешественник Уильям Фёрнесс[53]. Деньгами там служили большие каменные диски, и после сделки их часто не трогали с

---

[46] Michael McLeay, Amar Radia, Ryland Thomas, «Money in the modern economy: an introduction», Bank of England Quarterly Bulletin 2014 Q1, 14.03.2014, pp. 4–13. https://www.bankofengland.co.uk/quarterly-bulletin/2014/q1/money-in-the-modern-economy-an-introduction; PDF: https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2014/money-in-the-modern-economy-an-introduction.pdf.

[47] McLeay M., Radia A., Thomas R. Money in the modern economy: an introduction. Bank of England Quarterly Bulletin 2014 Q1, p. 4: «Money today is a type of IOU, but one that is special because everyone in the economy trusts that it will be accepted by other people in exchange for goods and services.»

[48] Michael McLeay, Amar Radia, Ryland Thomas, «Money in the modern economy: an introduction», Bank of England Quarterly Bulletin 2014 Q1, 14.03.2014, pp. 4–13. https://www.bankofengland.co.uk/quarterly-bulletin/2014/q1/money-in-the-modern-economy-an-introduction; PDF: https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2014/money-in-the-modern-economy-an-introduction.pdf.

[49] McLeay, Radia, Thomas, «Money in the modern economy: an introduction», BoE QB 2014 Q1, стр. 7, раздел «Why money is special». URL —.

[50] McLeay, Radia, Thomas, «Money in the modern economy: an introduction», BoE QB 2014 Q1, стр. 7, раздел «Why money is special». URL —.

[51] Там же, p. 7: «Money is a social institution that provides a solution to the problem of a lack of trust.»

[52] Michael McLeay, Amar Radia, Ryland Thomas, «Money in the modern economy: an introduction», Bank of England Quarterly Bulletin 2014 Q1, 14.03.2014, pp. 4–13. https://www.bankofengland.co.uk/quarterly-bulletin/2014/q1/money-in-the-modern-economy-an-introduction; PDF: https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2014/money-in-the-modern-economy-an-introduction.pdf.

[53] William Henry Furness 3rd, «The Island of Stone Money: Uap of the Carolines», J. B. Lippincott, Philadelphia & London, 1910, гл. VII «Money and Currency». Текст: Project Gutenberg #72830, https://www.gutenberg.org/ebooks/72830.

места. Новый владелец довольствовался признанием своего права, камень оставался во дворе прежнего хозяина, и на нём даже не ставили никакой отметки[54]. Одна семья, по словам Фёрнесса, считалась богатой благодаря огромному камню, который два или три поколения назад утонул при перевозке и которого с тех пор никто не видел[55].[56]

В той же книге есть эпизод, который я считаю самым точным описанием денег как записи. Вожди нескольких округов раз за разом не выполняли приказ немецкой колониальной администрации починить дороги, и администрация решила их оштрафовать. Вывозить камни никто не стал. На самых ценных нарисовали чёрные кресты в знак того, что теперь они принадлежат правительству[57]. Камни остались на месте, изменилась только общая память о том, чьи они. Когда дороги починили, кресты стёрли, и штраф исчез так же, как появился[58].

Если деньги — запись, то где лежат записи сегодня? Большей частью в банках. В Великобритании на конец 2013 года около 97% денег, находившихся у публики, составляли банковские депозиты, и только остальное приходилось на наличные[59].[60] Сам депозит авторы из Банка Англии определяют без всякой романтики как запись о том, сколько банк должен своему клиенту[61].[62] Остаток на вашем счёте — строчка в тетрадке банка, и в ней написано «банк должен вам столько-то».

С другого конца к той же мысли подошёл экономист Нараяна Кочерлакота. В 1996 году Федеральный резервный банк Миннеаполиса выпустил его работу «Деньги — это память»[63]. Кочерлакота построил формальную модель экономики и сравнил в ней два мира. В первом люди расплачиваются деньгами. Во втором денег нет, зато все помнят все прошлые сделки друг друга. Оказалось, что второй мир может всё, что может первый[64].[65]

Это теорема о модели, а о прошлом она ничего не рассказывает. Работает она к тому же в одну сторону. Память может заменить деньги, а заменить деньгами память, как оговаривает сам автор, удаётся лишь в некоторых моделях. Банк Англии, ссылаясь на эту работу, добавляет к условиям, при которых деньги вообще нужны, ещё одно: в экономике нет записи обо всех

---

[54] William Henry Furness 3rd, «The Island of Stone Money: Uap of the Carolines», J. B. Lippincott, Philadelphia & London, 1910, гл. VII «Money and Currency». Текст: Project Gutenberg #72830, https://www.gutenberg.org/ebooks/72830.

[55] William Henry Furness 3rd, «The Island of Stone Money: Uap of the Carolines», J. B. Lippincott, Philadelphia & London, 1910, гл. VII «Money and Currency». Текст: Project Gutenberg #72830, https://www.gutenberg.org/ebooks/72830.

[56] Furness W. H. The Island of Stone Money: Uap of the Carolines. Philadelphia; London: J. B. Lippincott, 1910, гл. «Money and Currency». Историю утонувшего камня Фёрнесс пересказывает со слов местного знакомого, так что это рассказ, и протоколом его считать не стоит.

[57] William Henry Furness 3rd, «The Island of Stone Money: Uap of the Carolines», J. B. Lippincott, Philadelphia & London, 1910, гл. VII «Money and Currency». Текст: Project Gutenberg #72830, https://www.gutenberg.org/ebooks/72830.

[58] William Henry Furness 3rd, «The Island of Stone Money: Uap of the Carolines», J. B. Lippincott, Philadelphia & London, 1910, гл. VII «Money and Currency». Текст: Project Gutenberg #72830, https://www.gutenberg.org/ebooks/72830.

[59] McLeay, Radia, Thomas, «Money in the modern economy: an introduction», BoE QB 2014 Q1, стр. 5 и сноска 1 («As of December 2013»); повторено в «Money creation in the modern economy», стр. 15 («97% of the amount currently in circulation»).

[60] McLeay, Radia, Thomas. Money in the modern economy: an introduction. Таких же точных цифр по другим странам в моих источниках нет, поэтому британские 97% я на весь мир не переношу.

[61] McLeay, Radia, Thomas, «Money creation in the modern economy», BoE QB 2014 Q1, стр. 16.

[62] McLeay M., Radia A., Thomas R. Money creation in the modern economy. Bank of England Quarterly Bulletin 2014 Q1, p. 16: «Bank deposits are simply a record of how much the bank itself owes its customers.»

[63] Narayana R. Kocherlakota, «Money Is Memory», Federal Reserve Bank of Minneapolis Staff Report 218, 01.10.1996; опубликовано в Journal of Economic Theory 81(2), August 1998, pp. 232–251. https://www.minneapolisfed.org/research/staff-reports/money-is-memory.

[64] Narayana R. Kocherlakota, «Money Is Memory», Federal Reserve Bank of Minneapolis Staff Report 218, 01.10.1996; опубликовано в Journal of Economic Theory 81(2), August 1998, pp. 232–251. https://www.minneapolisfed.org/research/staff-reports/money-is-memory.

[65] Kocherlakota N. Money is Memory. Federal Reserve Bank of Minneapolis, Research Department Staff Report 218, 1996; журнальная версия — Journal of Economic Theory, 1998. В аннотации: «Depending on the environment, the converse may or may not be true.» Банк Англии (McLeay, Radia, Thomas. Money in the modern economy: an introduction, p. 7, сноска 4): «Kocherlakota (1998) points out that a lack of a record of all transactions is another necessary condition».

сделках[66]. Если бы весь посёлок помнил каждую сделку каждого двора, тетрадка с переходящими долгами была бы ему ни к чему.

Отсюда странное положение, в котором окажется биткоин. Его основа — общая запись обо всех переводах, копию которой держит у себя каждый участник (её называют блокчейном). По замыслу это и есть та самая общая память, и при этом создатель назвал свою систему электронными деньгами[67].

Противоречие снимается, если посмотреть, что именно такая запись помнит. Память из модели Кочерлакоты хранит всё: кто кому испёк хлеб, кто кому починил крышу и кто сколько задолжал. Запись биткоина помнит только одно — как переходили из рук в руки её собственные единицы. Хлеб, крыши и обещания остаются за её пределами, поэтому деньги посёлку по-прежнему нужны, и роль денег эта запись берёт на себя сама.

Откуда деньги взялись исторически (из бартера, из ценного товара вроде металла или из учёта долгов), остаётся открытым вопросом, и сам Банк Англии называет его предметом серьёзного спора[68]. Кредитную версию ещё в 1913 году отстаивал британский дипломат и экономист-любитель Альфред Митчелл-Иннес, для которого деньги — это «кредит и только кредит»[69],[70] но решать этот спор нашей модели не нужно, потому что посёлок описывает, как деньги устроены сегодня, и их родословная ему безразлична.

Если хотите проверить модель на себе, откройте выписку по своему счёту и прочитайте её как страницу из тетрадки. Зарплата в ней — строчка, после которой банк должен вам больше. Оплата картой в магазине — строчка, после которой он должен вам меньше[71]. Ни монеты, ни купюры в этой цепочке нет, и держится она только на том, что банк ведёт свою тетрадку правильно и не ошибается ни в вашу пользу, ни против вас. Этого хранителя вы, скорее всего, никогда не видели и в его тетрадку не заглядывали. Вы ему просто верите.

Кто пишет новые строчки

Пока хранитель в нашем посёлке только переносит долги из строчки в строчку. Добавим второе правило: он может давать в долг сам.

Допустим, плотнику нужны доски на 100, а расплатиться с лесорубом ему пока нечем. Хранитель пишет в тетрадку две строчки, «хранитель должен плотнику 100» и «плотник должен хранителю 100». Первой строчкой плотник расплачивается с лесорубом (право требовать с хранителя 100 переходит к лесорубу), а вторая висит на плотнике, пока он не отработает долг. На случай, если плотник не расплатится, хранитель берёт с него залог: пока долг не погашен, сарай плотника записан за хранителем, а если долг так и не вернут, сарай останется хранителю.

Посчитаем, что изменилось. До этих записей в посёлке ходило какое-то количество прав требования, после них стало на 100 больше, хотя никто ничего не добыл, не вырастил и не

---

[66] Narayana R. Kocherlakota, «Money Is Memory», Federal Reserve Bank of Minneapolis Staff Report 218, 01.10.1996; опубликовано в Journal of Economic Theory 81(2), August 1998, pp. 232–251. https://www.minneapolisfed.org/research/staff-reports/money-is-memory.

[67] Satoshi Nakamoto, «Bitcoin P2P e-cash paper», The Cryptography Mailing List, 31.10.2008, 14:10 EDT, https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html.

[68] McLeay, Radia, Thomas, «Money in the modern economy: an introduction», BoE QB 2014 Q1, стр. 6, сноска 1.

[69] A. Mitchell Innes, «What is Money?», The Banking Law Journal, May 1913, pp. 377–408. Текст: http://www.newmoneyhub.com/www/money/mitchell-innes/what-is-money.html.

[70] Mitchell Innes A. What is Money? The Banking Law Journal, May 1913: «Credit and credit alone is money.» Экономисты основного течения долго его не замечали; сейчас на него опираются посткейнсианцы и сторонники современной денежной теории (A. Mitchell Innes, «What is Money?», The Banking Law Journal, May 1913, pp. 377–408. Текст: http://www.newmoneyhub.com/www/money/mitchell-innes/what-is-money.html).

[71] McLeay, Radia, Thomas, «Money creation in the modern economy», BoE QB 2014 Q1, стр. 16.

напечатал. Деньги появились в ту минуту, когда хранитель выдал кредит. Когда плотник рассчитается, обе строчки вычеркнут, и эти 100 исчезнут так же тихо, как появились.

Может показаться, что так бывает только в игрушечном посёлке. Банк Англии в соседней статье того же бюллетеня описывает настоящие банки теми же словами: всякий раз, когда банк выдаёт кредит, он одновременно создаёт на счёте заёмщика соответствующий депозит и тем самым создаёт новые деньги[72].[73] Погашение кредита, наоборот, деньги уничтожает[74]. Там же авторы разбирают две распространённые ошибки. Банки не просто передают в долг деньги, которые принесли вкладчики, и не «умножают» деньги центрального банка по учебной формуле[75].

Отсюда легко сделать вывод, будто банки пишут деньги из воздуха без всяких правил. Это половина картины, и её часто цитируют без второй половины. Создание денег банками ограничено, и Банк Англии перечисляет, чем. Банк должен заработать на кредите в конкуренции с другими банками, его держат правила надзора, а последний предел ставит центральный банк, который в обычное время действует через процентную ставку[76].[77] Чем выше ставка, тем дороже кредит, тем реже за ним приходят и тем меньше новых денег создают банки.

Переведём это на язык посёлка, и получится третье правило. Хранителей в настоящей экономике много (каждый банк ведёт свою тетрадку своих клиентов), а над ними стоит главный хранитель, центральный банк, который решает, сколько будет стоить каждая новая строчка, и тем самым ставит последний предел всей записи[78]. Доверие в таких деньгах двухэтажное. На верхнем этаже вы верите, что главный хранитель не станет обесценивать запись. На нижнем вы верите, что ваш банк ведёт свою тетрадку честно и не раздаёт кредиты сверх меры.

Второе и третье правила вместе дают посёлку новое поведение, которого у него не было, пока хранитель только переписывал долги. Проследим его по шагам. Урожай хороший, настроение в посёлке бодрое, и хранитель охотнее пишет строчки в долг (плотнику на доски, пекарю на новую печь, доярке на вторую корову). Каждая такая строчка — новые деньги[79]. Новые деньги идут к лесорубу, печнику и тому, кто продаёт коров, те тоже чувствуют себя увереннее и сами приходят за кредитом. Цены на доски, коров и сараи растут, вместе с ними дорожают залоги, а под дорогой сарай хранитель охотно даёт в долг больше прежнего, и петля раскручивается.

Теперь представим неурожай. Часть должников не может отработать долг, хранитель пугается и перестаёт писать новые строчки, а старые вычёркиваются по мере погашения, и вместе с ними исчезают деньги[80]. Денег в посёлке становится меньше, цены на доски и коров

---

[72] Michael McLeay, Amar Radia, Ryland Thomas, «Money creation in the modern economy», Bank of England Quarterly Bulletin 2014 Q1, 14.03.2014, pp. 14–27. https://www.bankofengland.co.uk/quarterly-bulletin/2014/q1/money-creation-in-the-modern-economy; PDF: https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2014/money-creation-in-the-modern-economy.pdf.

[73] McLeay, Radia, Thomas. Money creation in the modern economy, p. 14: «Whenever a bank makes a loan, it simultaneously creates a matching deposit in the borrower's bank account, thereby creating new money.»

[74] McLeay, Radia, Thomas, «Money creation in the modern economy», BoE QB 2014 Q1, стр. 16.

[75] Michael McLeay, Amar Radia, Ryland Thomas, «Money creation in the modern economy», Bank of England Quarterly Bulletin 2014 Q1, 14.03.2014, pp. 14–27. https://www.bankofengland.co.uk/quarterly-bulletin/2014/q1/money-creation-in-the-modern-economy; PDF: https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2014/money-creation-in-the-modern-economy.pdf.

[76] McLeay, Radia, Thomas, «Money creation in the modern economy», BoE QB 2014 Q1, стр. 14 (Overview).

[77] Там же, p. 14: «Monetary policy acts as the ultimate limit on money creation.»

[78] McLeay, Radia, Thomas, «Money creation in the modern economy», BoE QB 2014 Q1, стр. 14 (Overview).

[79] Michael McLeay, Amar Radia, Ryland Thomas, «Money creation in the modern economy», Bank of England Quarterly Bulletin 2014 Q1, 14.03.2014, pp. 14–27. https://www.bankofengland.co.uk/quarterly-bulletin/2014/q1/money-creation-in-the-modern-economy; PDF: https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2014/money-creation-in-the-modern-economy.pdf.

[80] McLeay, Radia, Thomas, «Money creation in the modern economy», BoE QB 2014 Q1, стр. 16.

падают, залог дешевеет, и хранитель выдаёт ещё меньше. Та же петля крутится в обратную сторону.

Это игрушка, и настоящая экономика сложнее (центральный банк, например, старается сгладить обе фазы ставкой[81]). Главное она всё же показывает верно. Где хранитель может писать строчки в долг, там запись денег сама собой расширяется и сжимается волнами.

Накамото в том же посте 2009 года прошёлся по обоим этажам. О главном хранителе мы уже говорили. О банках он написал, что им приходится доверять хранение наших денег и их электронный перевод, а они раздают эти деньги в кредит волнами кредитных пузырей, держа в резерве лишь ничтожную долю[82].[83] Слова про «ничтожную долю в резерве» — полемика, и описанием по учебнику их считать нельзя. Как на деле ограничено создание денег, лучше читать у Банка Англии[84]. Зато вторая половина фразы для этой книги главная. Создатель биткоина описал беду обычных денег через кредитные пузыри, и во второй части книги мы увидим, что крипторынок, построенный как ответ на эту беду, живёт теми же волнами кредита. Волны, которые мы только что проследили в посёлке, никуда не денутся и в тетрадке без хозяина, если поверх неё снова начнут выдавать строчки в долг.

Когда хранитель подводит

Хранитель может подвести по-разному, и самый тяжёлый случай проще всего показать на посёлке.

Допустим, за год посёлок производит хлеба, молока и работы на 10 000 условных буханок, и строчек в тетрадке ходит примерно на ту же сумму. Однажды хранитель дописывает себе ещё 10 000. Хлеба, молока и крыш от этого не прибавилось, а прав на них стало вдвое больше, поэтому каждая строчка теперь покупает примерно вдвое меньше (модель грубая, настоящие цены так ровно не делятся, но направление она показывает верно). Пекарь, у которого было право на 100 буханок работы, может получить за него вдвое меньше молока, хотя из его строчки никто ничего не вычеркнул.

Опасен такой сбой тем, что его не видно по отдельной строчке. Каждая запись в тетрадке выглядит так же, как вчера, меняется только то, сколько за неё дают. Если хранитель дописывает раз за разом, люди начинают избавляться от строчек как можно быстрее, пока те не подешевели ещё, и это само ускоряет обесценивание: чем быстрее строчки тратят, тем быстрее растут цены, и тем охотнее от них избавляются. В какой-то момент запись перестают брать совсем.

Что так бывало часто, признают обе стороны спора о криптовалютах. Банк международных расчётов (его называют клубом центральных банков) в главе годового отчёта 2018 года, посвящённой криптовалютам, пишет, что доверие подводило так часто, что история превратилась в кладбище валют. В зале 68 Британского музея, напоминает отчёт, выставлены камни, раковины, табак, монеты и бумажки, которые когда-то были деньгами и перестали ими быть[85].[86] Накамото, как мы видели, говорит о том же самом другими словами. Выводы из одного и того же факта они делают противоположные, и к этой развилке мы придём в конце главы.

---

[81] McLeay, Radia, Thomas, «Money creation in the modern economy», BoE QB 2014 Q1, стр. 14 (Overview).

[82] Nakamoto, P2P Foundation, 11.02.2009, https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/1/.

[83] Nakamoto, P2P Foundation, 11.02.2009: «Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve.»

[84] McLeay, Radia, Thomas, «Money creation in the modern economy», BoE QB 2014 Q1, стр. 14 (Overview).

[85] BIS, Annual Economic Report 2018, ch. V, https://www.bis.org/publ/arpdf/ar2018e5.htm.

[86] BIS. Annual Economic Report 2018, ch. V «Cryptocurrencies: looking beyond the hype»: «Sustained episodes of stable money are historically much more of an exception than the norm. In fact, trust has failed so frequently that history is a graveyard of currencies.»

Самый изученный случай — Германия после Первой мировой войны. По данным Банка Англии, за пять лет после её окончания цены в германских марках удвоились 38 раз[87].[88] Доверие к хранителю к тому времени кончилось, и люди просто ушли в чужую тетрадку. К октябрю 1923 года иностранной валюты в стране ходило, по приблизительным оценкам, которые приводит экономист Томас Сарджент, не меньше, а возможно, в несколько раз больше, чем собственных банкнот, если считать по реальной стоимости[89].

Причинами катастрофы Сарджент называет репарации и дефицит бюджета, оккупацию Рура в 1923 году и то, что «пассивное сопротивление» оккупации оплачивали выпуском денег. К осени 1923 года правительство покрывало выпуском банкнот практически 100% своих расходов[90]. Печатный станок был в этой цепочке последним звеном, через которое дыра в бюджете превращалась в новые строчки.

Для нашей модели интереснее всего, как инфляцию остановили. 15 октября 1923 года декретом объявили новую рентную марку, равную триллиону бумажных марок, но саму смену купюры Сарджент считает мерой косметической[91]. Решающим он считает предел. Декрет жёстко ограничил, сколько всего можно выпустить рентных марок и сколько из них дать в долг правительству, одновременно правительство перестало занимать у центрального банка и свело бюджет к равновесию, и в конце ноября 1923 года цены внезапно перестали расти[92].[93] (Это объяснение Сарджента, признанное, но не единственное, и для нашей модели его достаточно.) На языке посёлка доверие вернуло правило, которое связало хранителю руки: столько строчек и не больше, и в долг самому себе не больше стольких-то.

У биткоина общий выпуск тоже ограничен, только правило записано прямо в коде[94]. Во что обходится такой предел, мы увидим в главе 3.

Германия при этом даже не рекорд. Экономисты Стив Ханке и Николас Крус свели в таблицу больше полусотни эпизодов гиперинфляции[95], и по месячному темпу немецкий пик в ней лишь пятый[96]. В Венгрии летом 1946 года цены удваивались меньше чем за сутки[97], в

---

[87] McLeay, Radia, Thomas, «Money in the modern economy: an introduction», BoE QB 2014 Q1, стр. 5 (со ссылкой на Sargent, 1982).

[88] Ещё три числа для масштаба. То, что в 1918 году стоило одну марку, в 1923 году стоило бы больше 300 млрд марок (McLeay, Radia, Thomas, «Money in the modern economy: an introduction», BoE QB 2014 Q1, стр. 5 (со ссылкой на Sargent, 1982)). В конце октября 1923 года больше 99% банкнот Рейхсбанка в обращении были выпущены за предыдущие 30 дней (Sargent, «The Ends of Four Big Inflations», 1982, стр. 75 и 82 (со ссылкой на Young, 1925)). Курс марки, по таблицам Сарджента, упал с 1,69 американского цента в январе 1920 года до 0,000 000 000 043 цента в ноябре 1923-го (Thomas J. Sargent, «The Ends of Four Big Inflations», in: R. E. Hall (ed.), «Inflation: Causes and Effects», University of Chicago Press / NBER, 1982, pp. 41–98, табл. G1 (стр. 74–75; данные Young, 1925). PDF: https://www.nber.org/system/files/chapters/c11452/c11452.pdf). Sargent T. J. The Ends of Four Big Inflations. In: Hall R. E. (ed.) Inflation: Causes and Effects. University of Chicago Press, 1982.

[89] Sargent, «The Ends of Four Big Inflations», 1982, стр. 75 и 82 (со ссылкой на Young, 1925).

[90] Sargent, «The Ends of Four Big Inflations», 1982, стр. 82–83.

[91] Sargent, «The Ends of Four Big Inflations», 1982, стр. 82–83.

[92] Sargent, «The Ends of Four Big Inflations», 1982, стр. 82–83.

[93] Sargent, 1982, pp. 82–84: «…a new currency unit called the Rentenmark was declared equivalent to 1 trillion (10^{12}) paper marks»; «Simultaneously and abruptly three things happened: additional government borrowing from the central bank stopped, the government budget swung into balance, and inflation stopped». К равновесию бюджет свели повышением налогов и сокращением госслужащих; Сарджент упоминает и облегчение репараций по плану Дауэса. Предел выпуска рентных марок — 3,2 млрд, кредита правительству — 1,2 млрд (Sargent, «The Ends of Four Big Inflations», 1982, стр. 82–83).

[94] The Block, «Bitcoin ushers in fourth halving…», 20.04.2024, https://www.theblock.co/post/289875/bitcoin-ushers-in-fourth-halving-as-miners-block-subsidy-reward-drops-to-3-125-btc; CNBC, 19.04.2024, https://www.cnbc.com/2024/04/19/bitcoin-network-completes-fourth-ever-halving-of-rewards-to-miners.html.

[95] S. H. Hanke, N. Krus, «World Hyperinflations», Cato Working Paper No. 8, 2012 (опубл. в: R. Parker, R. Whaples (eds.), «The Handbook of Major Events in Economic History», Routledge, 2013) — цифры по Wikipedia, «Hyperinflation», https://en.wikipedia.org/wiki/Hyperinflation.

[96] Hanke, Krus, 2012, таблица (копия на Scribd —).

[97] Hanke, Krus, 2012, таблица (копия на Scribd —).

Зимбабве в 2008 году, по модельной оценке Ханке, примерно за сутки[98].[99] Чем кончается такая история, хорошо видно по Зимбабве. Страна перешла на чужие валюты, а в 2015 году её центральный банк выкупал оставшиеся на руках наличные по курсу, при котором самая крупная купюра, номиналом 100 трлн зимбабвийских долларов, стоила 40 американских центов. Банк отдельно оговорил, что это просто обмен и потерю от гиперинфляции он не возмещает[100].[101]

Было бы нечестно выводить из этих историй, что хранителю нельзя верить никогда. Гиперинфляции — крайние случаи. Германия расплачивалась по репарациям после проигранной войны[102], Венгрия проходила через свою в 1945–1946 годах, сразу после Второй мировой[103]. Банк международных расчётов при этом сам признаёт, что долгие периоды стабильных денег в истории скорее исключение, чем правило[104], и всё же выводит из того же кладбища валют противоположное Накамото правило, по которому проверенный способ обеспечить доверие к деньгам в современных условиях — независимый центральный банк[105]. Какая доля хранителей удерживала доверие десятилетиями, надёжной меры у меня нет, поэтому слово «обычно» я здесь не поставлю ни в ту, ни в другую сторону. Для модели достаточно того, что сбои случались больше полусотни раз и по одной схеме: хранитель, которого ничто не ограничивало, писал строчки быстрее, чем их могли покрыть.

В начале главы я назвал три способа, которыми хранитель может подвести (приписать себе строчку, стереть чужую и позволить отдать одно право двоим). Гиперинфляции — первый способ, доведённый до предела. Второй способ в мягком виде можно разглядеть в истории с крестами на Япе, если посмотреть на неё с этой стороны. Администрация без согласия владельцев одной краской переписала строчку «камень принадлежит такой-то семье», и никто не спорил с её записью[106]. Третий в бумажном мире почти не встречался, потому что хранитель видел всю тетрадку сразу. Главным он стал, когда тетрадку перенесли в компьютер.

---

[98] S. H. Hanke, N. Krus, «World Hyperinflations», Cato Working Paper No. 8, 15.08.2012, таблица «The Hyperinflation Table»; оригинал: https://www.cato.org/sites/cato.org/files/pubs/pdf/workingpaper-8.pdf; прочитана копия таблицы: «The Hanke Krus Hyperinflation Table», Scribd, https://www.scribd.com/document/104816500/The-Hanke-Krus-Hyperinflation-Table.

[99] Hanke S. H., Krus N. World Hyperinflations, 2012 (таблица). Венгрия, июль 1946 года: цены удваивались примерно каждые 15 часов (Hanke, Krus, 2012, таблица (копия на Scribd —)). Пик Германии — октябрь 1923 года, 29 500% в месяц, цены удваивались за 3,7 дня; выше в таблице стоят Венгрия, Зимбабве, Югославия и Республика Сербская. Оценка по Зимбабве (удвоение за 24,7 часа в середине ноября 2008 года) модельная, потому что официальная статистика к тому времени перестала публиковаться (S. H. Hanke, N. Krus, «World Hyperinflations», Cato Working Paper No. 8, 15.08.2012, таблица «The Hyperinflation Table»; оригинал: https://www.cato.org/sites/cato.org/files/pubs/pdf/workingpaper-8.pdf; прочитана копия таблицы: «The Hanke Krus Hyperinflation Table», Scribd, https://www.scribd.com/document/104816500/The-Hanke-Krus-Hyperinflation-Table).

[100] Reserve Bank of Zimbabwe, «Press Statement: Demonetization of the Zimbabwe Dollar», Governor J. P. Mangudya, 11.06.2015, https://www.rbz.co.zw/documents/publications/press/demonetisation-press-statement-9-june-2015.pdf.

[101] Reserve Bank of Zimbabwe. Press Statement: Demonetization of the Zimbabwe Dollar, 11.06.2015: «Demonetisation is not compensation for the loss of value of the Z$ due to hyper-inflation. It is an exchange process.» Наличные банкноты серии 2008 года меняли по 250 трлн зимбабвийских долларов за доллар США; крупные остатки на счетах пересчитывали по обменному курсу ООН, 35 квадриллионов за доллар (Reserve Bank of Zimbabwe, «Press Statement: Demonetization of the Zimbabwe Dollar», Governor J. P. Mangudya, 11.06.2015, https://www.rbz.co.zw/documents/publications/press/demonetisation-press-statement-9-june-2015.pdf). На мультивалютную систему, то есть на чужие деньги, Зимбабве перешла в 2009 году (Reserve Bank of Zimbabwe, «Press Statement: Demonetization of the Zimbabwe Dollar», Governor J. P. Mangudya, 11.06.2015, https://www.rbz.co.zw/documents/publications/press/demonetisation-press-statement-9-june-2015.pdf).

[102] Sargent, «The Ends of Four Big Inflations», 1982, стр. 82–83.

[103] Hanke, Krus, 2012, таблица (копия на Scribd —).

[104] BIS, Annual Economic Report 2018, ch. V, https://www.bis.org/publ/arpdf/ar2018e5.htm.

[105] BIS, Annual Economic Report 2018, ch. V, https://www.bis.org/publ/arpdf/ar2018e5.htm.

[106] William Henry Furness 3rd, «The Island of Stone Money: Uap of the Carolines», J. B. Lippincott, Philadelphia & London, 1910, гл. VII «Money and Currency». Текст: Project Gutenberg #72830, https://www.gutenberg.org/ebooks/72830.

Тетрадка в компьютере: проблема двойной траты

До сих пор наша тетрадка была бумажной и лежала в одном месте. Перенесём её в компьютер и посмотрим, что сломается.

Сначала о том, как защищали записи до компьютеров. Английское казначейство с XII до XIX века вело учёт налогов на деревянных бирках[107]. Митчелл-Иннес описывает, как их делали. На ореховой палочке зарубками отмечали сумму, потом палочку раскалывали вдоль, одна половина оставалась у кредитора, другая у должника[108]. Две половины совпадали только друг с другом, поэтому каждая служила проверкой для другой, и защиту записи давала сама физика дерева. (Конец у этой системы вышел мрачный. В 1834 году списанные бирки сожгли в печах под палатой лордов, огонь вышел из-под контроля и уничтожил большую часть средневековых зданий Вестминстерского дворца[109].)

Монету и бумажную купюру защищает похожая физика: у предмета в каждый момент только один владелец. Если я отдал вам банкноту, у меня её больше нет, и отдать её второй раз кому-то ещё я не могу. С цифровой записью это не работает. Файл копируется без потерь, и если электронная монета — просто набор чисел, ничто не мешает отправить одни и те же числа двоим.

Вернёмся в посёлок и добавим четвёртое правило: дворы больше не ходят к хранителю, а пересылают друг другу строчки через сеть. Пекарь пишет на своём компьютере «моё право на 10 с плотника переходит доярке» и отправляет доярке. Через минуту он пишет «моё право на 10 с плотника переходит лесорубу» и отправляет лесорубу. Доярка и лесоруб видят у себя подписанные пекарем записи, и каждая по отдельности выглядит безупречно.

Кто из них получил право?

Цифровые подписи, казалось бы, для того и придуманы. Подпись действительно решает часть задачи, и Накамото прямо так и пишет[110].

Устроена подпись так. У пекаря есть ключ, то есть длинное секретное число, которое знает только он. Из этого числа и текста строчки компьютер вычисляет подпись, а проверить её может любой, не зная самого ключа. Подделать подпись без ключа нельзя, поэтому она доказывает, что строчку составил сам пекарь и что после подписи в ней не изменили ни буквы. Но обе строчки, и для доярки, и для лесоруба, пекарь подписал сам, поэтому обе подписи настоящие. Подпись отвечает на вопрос «кто написал». Двойная трата — вопрос «сколько раз», и на него подпись ответить не может.

---

[107] Caroline Shenton, «Burning the House down: The Fire of 1834», The History of Parliament (блог History of Parliament Trust), 16.10.2013, https://historyofparliament.com/2013/10/16/the-fire-of-1834/; Science Museum Group Collection, «Medieval Exchequer Tally Sticks», https://collection.sciencemuseumgroup.org.uk/objects/co60506/medieval-exchequer-tally-sticks.

[108] A. Mitchell Innes, «What is Money?», 1913 (URL —).

[109] Caroline Shenton, «Burning the House down: The Fire of 1834», The History of Parliament (блог History of Parliament Trust), 16.10.2013, https://historyofparliament.com/2013/10/16/the-fire-of-1834/; Science Museum Group Collection, «Medieval Exchequer Tally Sticks», https://collection.sciencemuseumgroup.org.uk/objects/co60506/medieval-exchequer-tally-sticks.

[110] Satoshi Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System», 2008, https://bitcoin.org/bitcoin.pdf (Abstract).

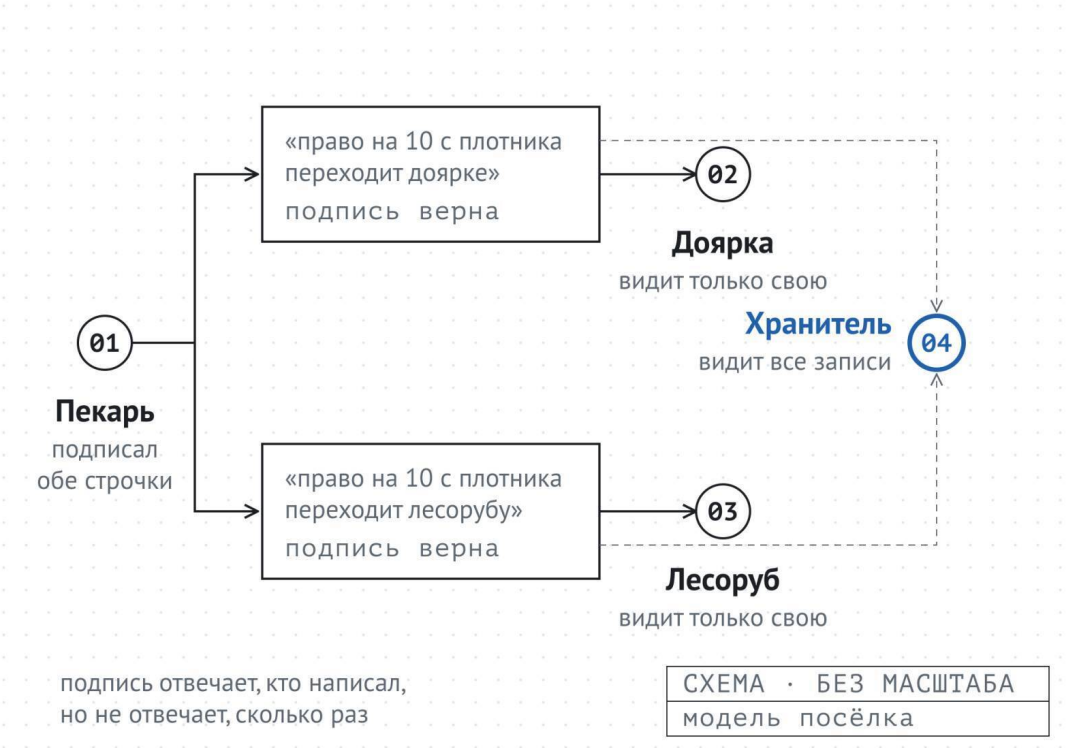


Рисунок 1.1. Двойная трата

Это и называется проблемой двойной траты: как убедиться, что тот, кто платит вам цифровой записью, не отдал её уже кому-то ещё. Создатель биткоина и клуб центральных банков сформулировали её почти одинаково. Накамото в статье 2008 года пишет, что единственный способ убедиться, что транзакции не было, — знать обо всех транзакциях[111].[112] Банк международных расчётов в 2018 году пишет, что для цифровых денег решение проблемы двойной траты требует как минимум, чтобы кто-то вёл запись всех транзакций[113].[114]

Доярка сама не узнает, отдал ли пекарь ту же строчку лесорубу, потому что переписки пекаря с лесорубом она не видит. Проверить может только тот, кто видит все записи сразу, то есть хранитель общей тетрадки. Накамото описывает этот ход прямо. Электронную монету он определяет как цепочку цифровых подписей, каждый владелец передаёт её следующему, подписывая, и тут же признаёт слабость. Получатель не может проверить, не потратил ли один из прежних владельцев монету дважды[115]. Обычное решение — завести центральный монетный двор, через который проходит каждая транзакция, но тогда, пишет он, судьба всей денежной системы зависит от компании, которая ведёт этот двор, и каждая транзакция должна проходить через неё, как через банк[116].[117]

---

[111] Nakamoto, 2008, раздел 2, https://bitcoin.org/bitcoin.pdf.

[112] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, section 2: «The only way to confirm the absence of a transaction is to be aware of all transactions.»

[113] BIS, Annual Economic Report 2018, ch. V, https://www.bis.org/publ/arpdf/ar2018e5.htm.

[114] BIS, Annual Economic Report 2018, ch. V: «For digital money, solving the double-spending problem requires, at a minimum, that someone keep a record of all transactions.»

[115] Nakamoto, 2008, раздел 2 «Transactions», https://bitcoin.org/bitcoin.pdf.

[116] Nakamoto, 2008, раздел 2 «Transactions», https://bitcoin.org/bitcoin.pdf.

[117] Nakamoto, 2008, section 2: «The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.»

Получается петля, из которой долго не могли выбраться. Цифровые деньги нуждаются в общей записи всех транзакций; общую запись кто-то должен вести; тот, кто её ведёт, становится хранителем; хранителю нужно доверять, и мы вернулись к первому правилу посёлка со всеми его рисками.

Эту петлю вы проходите каждый день, не замечая её. Когда вы платите картой или переводите деньги с телефона, вы тоже расплачиваетесь цифровой записью, и двойной траты при этом не боится ни продавец, ни вы. Причина в том, что каждую такую оплату проводит хранитель. Банк видит всю свою тетрадку сразу и не даст списать одну и ту же строчку дважды, то есть делает ровно тот минимум, который Банк международных расчётов считает необходимым[118]. Цифровые деньги с хранителем работают давно и надёжно. Трудность появляется только тогда, когда хранителя хотят убрать.

У каждой попытки был хозяин

Есть расхожее представление, будто биткоин — первая цифровая валюта, придуманная с нуля в 2008 году. Обе части этого представления неверны. Цифровые деньги пытались построить за четверть века до него, и сам Накамото называл своих предшественников по именам. Попыток было много, но их легко разложить на две линии. В первой запись вела компания, и система работала, пока жила компания. Во второй хозяина пытались убрать, и дальше описаний дело не пошло. Ещё одна деталь пришла со стороны, из борьбы со спамом. Обе линии спотыкались об одно и то же место в нашей петле.

Первую линию начал криптограф Дэвид Чаум. В 1982 году он предложил «слепые подписи» (статья вышла в 1983 году), при которых банк подписывает электронную купюру, не видя её номера[119]. Представьте, что банк ставит печать через копирку на запечатанный конверт. Оттиск на купюре внутри остаётся, а что на ней написано, банк не видел. Поэтому и посторонние не могут потом узнать, кому, когда и сколько платил человек[120]. Мотивом Чаума была приватность. Он писал, что знание о получателе, сумме и времени каждого платежа может многое рассказать о том, где человек бывает, с кем водится и как живёт[121].[122] Отказываться от банка он не собирался. От двойной траты его схему защищал банк, который, получив купюру к оплате, проверял подпись, заносил купюру в полный список погашенных и отказывал в оплате, если она там уже была[123].[124]

Самая изощрённая криптография своего времени решала двойную трату одной тетрадкой у одного хранителя. Именно такую конструкцию Накамото позже и назовёт монетным двором, через который проходит каждая транзакция[125].

На этой схеме выросла компания Чаума DigiCash. Первый электронный платёж её системой eCash по компьютерной сети прошёл 27 мая 1994 года. В 1995 году eCash запустил аме-

---

[118] BIS, Annual Economic Report 2018, ch. V, https://www.bis.org/publ/arpdf/ar2018e5.htm.

[119] David Chaum, «Blind Signatures for Untraceable Payments», in: Advances in Cryptology: Proceedings of Crypto 82, Plenum Press, 1983, pp. 199–203. PDF: https://chaum.com/wp-content/uploads/2022/01/Chaum-blind-signatures.pdf.

[120] David Chaum, «Blind Signatures for Untraceable Payments», in: Advances in Cryptology: Proceedings of Crypto 82, Plenum Press, 1983, pp. 199–203. PDF: https://chaum.com/wp-content/uploads/2022/01/Chaum-blind-signatures.pdf.

[121] David Chaum, «Blind Signatures for Untraceable Payments», in: Advances in Cryptology: Proceedings of Crypto 82, Plenum Press, 1983, pp. 199–203. PDF: https://chaum.com/wp-content/uploads/2022/01/Chaum-blind-signatures.pdf.

[122] Chaum D. Blind Signatures for Untraceable Payments. Advances in Cryptology: Proceedings of Crypto 82, 1983, p. 199: «… knowledge by a third party of the payee, amount, and time of payment for every transaction made by an individual can reveal a great deal about the individual's whereabouts, associations and lifestyle.»

[123] Chaum, «Blind Signatures for Untraceable Payments», 1983, стр. 202, шаги протокола (10)–(12).

[124] Там же, p. 202, шаг протокола (11): «Bank adds note to comprehensive list of cleared notes and stops if note already on list.»

[125] Nakamoto, 2008, раздел 2 «Transactions», https://bitcoin.org/bitcoin.pdf.

риканский банк из Сент-Луиса, позже систему пробовали и крупные европейские банки[126]. В начале ноября 1998 года DigiCash подала заявление о банкротстве[127].[128] Отраслевая газета American Banker писала тогда, что банки-партнёры так и не вышли за стадию пилотов, а в интернет-платежах в США победили кредитные карты[129].[130]

Другая судьба у e-gold, цифровой валюты, «обеспеченной золотом», которая работала с 1996 года[131]. В апреле 2007 года Министерство юстиции США предъявило двум компаниям, стоявшим за системой, и трём их владельцам обвинение, среди прочего в отмывании денег и в ведении нелицензированного бизнеса по переводу денег. Для открытия счёта, по словам обвинения, хватало адреса электронной почты[132]. В июле 2008 года обе компании признали вину, и им предписали зарегистрироваться как денежные сервисы, проверять личность клиентов и сообщать о подозрительных операциях[133].[134] У e-gold был хозяин записи, компания с адресом, и государство одним делом заставило этого хозяина вести тетрадку так, как её ведёт банк.

У двух этих историй разные сюжеты, но общая конструкция. И DigiCash, и e-gold держали запись у себя. Одну погубил рынок, другую государство заставило перестроиться, и в обоих случаях решалась судьба одной компании, а вместе с ней и всех её денег.

Вторая линия шла параллельно, и в ней хозяина пытались убрать. В ноябре 1998 года Уэй Дай опубликовал в рассылке шифропанков (так называли сообщество энтузиастов криптографии и приватности) описание b-money. Каждый участник там ведёт собственную базу данных о том, сколько денег принадлежит каждому псевдониму, а новые деньги получает тот, кто решил вычислительную задачу[135]. Схему так и не реализовали, и сам Дай признавал, что

---

[126] chaum.com, «eCash» (хронология), https://chaum.com/ecash/; год основания — Wikipedia, «DigiCash», https://en.wikipedia.org/wiki/DigiCash.

[127] American Banker, «Electronic Commerce: Bankrupt Digicash to Seek Financing, New Allies», 10.11.1998, https://www.americanbanker.com/news/electronic-commerce-bankrupt-digicash-to-seek-financing-new-allies.

[128] Заявление подано по главе 11 американского закона о банкротстве, то есть о защите от кредиторов (American Banker, «Electronic Commerce: Bankrupt Digicash to Seek Financing, New Allies», 10.11.1998, https://www.americanbanker.com/news/electronic-commerce-bankrupt-digicash-to-seek-financing-new-allies). Банк из Сент-Луиса — Mark Twain Bank; среди европейских банков, пробовавших или лицензировавших eCash, — Deutsche Bank и Credit Suisse (chaum.com, «eCash» (хронология), https://chaum.com/ecash/; год основания — Wikipedia, «DigiCash», https://en.wikipedia.org/wiki/DigiCash).

[129] American Banker, «Electronic Commerce: Bankrupt Digicash to Seek Financing, New Allies», 10.11.1998, https://www.americanbanker.com/news/electronic-commerce-bankrupt-digicash-to-seek-financing-new-allies.

[130] American Banker, 10.11.1998: «the licensee group — including Deutsche Bank, Den Norske Bank, Bank Austria, Advance Bank of Australia, and Mark Twain Bank of St. Louis — never got beyond pilot stages»; «credit cards have won the day». Это взгляд журналиста и конкурентов DigiCash (мысль о том, что покупатели доверяют кредитным картам, в статье принадлежит Ричарду Крону из CyberCash). Сам Чаум объяснял провал иначе, но его слов в надёжном источнике у меня нет.

[131] U.S. Department of Justice, «Digital Currency Business E-Gold Indicted for Money Laundering and Illegal Money Transmitting», 27.04.2007, https://www.justice.gov/archive/opa/pr/2007/April/07_crm_301.html; год запуска и основатели — Wikipedia, «E-gold», https://en.wikipedia.org/wiki/E-gold.

[132] U.S. Department of Justice, «Digital Currency Business E-Gold Indicted for Money Laundering and Illegal Money Transmitting», 27.04.2007, https://www.justice.gov/archive/opa/pr/2007/April/07_crm_301.html; год запуска и основатели — Wikipedia, «E-gold», https://en.wikipedia.org/wiki/E-gold.

[133] U.S. Department of Justice, «Digital Currency Business E-Gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges», 21.07.2008, https://www.justice.gov/archive/opa/pr/2008/July/08-crm-635.html; дубль: U.S. Secret Service, 22.07.2008, https://www.secretservice.gov/press/releases/2008/07/us-secret-service-led-investigation-digital-currency-business-e-gold-pleads.

[134] Министерство юстиции США, пресс-релизы 27.04.2007 и 21.07.2008. Обвиняемые компании — E-Gold Ltd. и Gold & Silver Reserve Inc.; обвинение — отмывание денег, сговор и ведение нелицензированного бизнеса по переводу денег. Основатель Дуглас Джексон признал сговор с целью отмывания и ведение нелицензированного бизнеса; компаниям предписали отдать 1,75 млн долларов (U.S. Department of Justice, «Digital Currency Business E-Gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges», 21.07.2008, https://www.justice.gov/archive/opa/pr/2008/July/08-crm-635.html; дубль: U.S. Secret Service, 22.07.2008, https://www.secretservice.gov/press/releases/2008/07/us-secret-service-led-investigation-digital-currency-business-e-gold-pleads).

[135] Wei Dai, «b-money», 1998, http://www.weidai.com/bmoney.txt (сайт при проверке не отвечал — ECONNREFUSED); описание по A. van Wirdum, «The Genesis Files: If Bitcoin Had a First Draft, Wei Dai's B-Money Was It», Bitcoin Magazine, 14.06.2018, https://bitcoinmagazine.com/technical/genesis-files-if-bitcoin-had-first-draft-wei-dais-b-money-was-it.

это ещё не законченный практический проект[136].[137] В посёлке это значило бы, что каждый двор ведёт свою тетрадку, то есть ровно то, от чего нас предостерегало первое правило. Не хватало способа договориться, чья тетрадка верна, если они разошлись. Второй вариант, который Дай описал там же, поручал вести запись группе серверов[138] и тем самым возвращал хранителей, только теперь их было несколько.

Проект bit gold Ник Сабо описал в своём блоге в декабре 2005 года, хотя сама идея, по его словам, пришла ему «давно»[139].[140] Сабо исходил из того, что наши деньги зависят от доверия к третьей стороне, а драгоценные металлы ценны неподделываемой редкостью, потому что их дорого добывать[141].[142] Отсюда его идея создавать «неподделываемо дорогие» цепочки битов, затрачивая на них вычислительную работу, отмечать их время и вносить права на них в распределённый реестр собственности[143], то есть в список владельцев, копии которого хранятся у многих участников сразу. Bit gold тоже остался на бумаге[144].

Последний кирпич принесла задача, к деньгам вроде бы не относящаяся. Адам Бэк придумал Hashcash как защиту от спама, объявил его весной 1997 года в той же рассылке шифропанков, а в 2002 году подробно описал в статье[145]. Отправитель письма тратит немного вычислительной работы и прикладывает доказательство, что он её потратил[146]. Для одного письма это дёшево, для миллиона писем дорого. Эта «цена за запись» потом ляжет в основу того, как биткоин решает, чья версия тетрадки верна. Если совсем коротко, верной считается та версия, в которую вложено больше всего такой работы[147], а почему это защищает от обмана, разберём позже.

---

[136] Wei Dai, «b-money», 1998, http://www.weidai.com/bmoney.txt (сайт при проверке не отвечал — ECONNREFUSED); описание по A. van Wirdum, «The Genesis Files: If Bitcoin Had a First Draft, Wei Dai's B-Money Was It», Bitcoin Magazine, 14.06.2018, https://bitcoinmagazine.com/technical/genesis-files-if-bitcoin-had-first-draft-wei-dais-b-money-was-it.

[137] Со слов историка биткоина Арона ван Вирдума (Wei Dai, «b-money», 1998, http://www.weidai.com/bmoney.txt (сайт при проверке не отвечал — ECONNREFUSED); описание по A. van Wirdum, «The Genesis Files: If Bitcoin Had a First Draft, Wei Dai's B-Money Was It», Bitcoin Magazine, 14.06.2018, https://bitcoinmagazine.com/technical/genesis-files-if-bitcoin-had-first-draft-wei-dais-b-money-was-it).

[138] Wei Dai, «b-money», 1998, http://www.weidai.com/bmoney.txt (сайт при проверке не отвечал — ECONNREFUSED); описание по A. van Wirdum, «The Genesis Files: If Bitcoin Had a First Draft, Wei Dai's B-Money Was It», Bitcoin Magazine, 14.06.2018, https://bitcoinmagazine.com/technical/genesis-files-if-bitcoin-had-first-draft-wei-dais-b-money-was-it.

[139] Nick Szabo, «Bit gold», блог Unenumerated, https://unenumerated.blogspot.com/2005/12/bit-gold.html.

[140] «A long time ago I hit upon the idea of bit gold» (Nick Szabo, «Bit gold», блог Unenumerated, https://unenumerated.blogspot.com/2005/12/bit-gold.html). Дата первой публикации в блоге — 29.12.2005 (Satoshi Nakamoto Institute, «Bit Gold» (библиотека, дата публикации 29.12.2005), https://nakamotoinstitute.org/library/bit-gold/; A. van Wirdum, «The Genesis Files: With Bit Gold, Szabo Was Inches Away From Inventing Bitcoin», Bitcoin Magazine, 12.07.2018, https://bitcoinmagazine.com/culture/genesis-files-bit-gold-szabo-was-inches-away-inventing-bitcoin). Историк биткоина Арон ван Вирдум относит замысел к 1998 году (Satoshi Nakamoto Institute, «Bit Gold» (библиотека, дата публикации 29.12.2005), https://nakamotoinstitute.org/library/bit-gold/; A. van Wirdum, «The Genesis Files: With Bit Gold, Szabo Was Inches Away From Inventing Bitcoin», Bitcoin Magazine, 12.07.2018, https://bitcoinmagazine.com/culture/genesis-files-bit-gold-szabo-was-inches-away-inventing-bitcoin).

[141] Nick Szabo, «Bit gold», блог Unenumerated, https://unenumerated.blogspot.com/2005/12/bit-gold.html.

[142] Szabo N. Bit gold. Unenumerated, 29.12.2005: «Precious metals and collectibles have an unforgeable scarcity due to the costliness of their creation»; «our money currently depends on trust in a third party for its value».

[143] Nick Szabo, «Bit gold», блог Unenumerated, https://unenumerated.blogspot.com/2005/12/bit-gold.html.

[144] Nick Szabo, «Bit gold», блог Unenumerated, https://unenumerated.blogspot.com/2005/12/bit-gold.html.

[145] A. Back, «Hashcash — A Denial of Service Counter-Measure», 01.08.2002, http://www.hashcash.org/papers/hashcash.pdf (ссылка [6] у Накамото, https://bitcoin.org/bitcoin.pdf); дата анонса 1997 — Wikipedia, «Hashcash», https://en.wikipedia.org/wiki/Hashcash (ссылка на http://www.hashcash.org/papers/announce.txt).

[146] A. Back, «Hashcash — A Denial of Service Counter-Measure», 01.08.2002, http://www.hashcash.org/papers/hashcash.pdf (ссылка [6] у Накамото, https://bitcoin.org/bitcoin.pdf); дата анонса 1997 — Wikipedia, «Hashcash», https://en.wikipedia.org/wiki/Hashcash (ссылка на http://www.hashcash.org/papers/announce.txt).

[147] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System», 2008, раздел 4 «Proof-of-Work», https://bitcoin.org/bitcoin.pdf.

Все эти линии сходятся в Накамото, и он сам это признавал. В статье 2008 года среди восьми ссылок есть b-money Уэй Дая и Hashcash Адама Бэка, а также работы о надёжных отметках времени, то есть о том, как доказать, что документ существовал к определённому моменту[148]. Летом 2008 года, ещё до выхода статьи, он написал Даю, что с интересом прочитал страницу о b-money и готовит статью, которая развивает его идеи в полную работающую систему, а на сайт Дая его навёл Бэк[149]. В 2010 году он написал на форуме прямо, что биткоин — реализация предложения b-money Уэй Дая и предложения bit gold Ника Сабо[150].[151]

В феврале 2009 года, отвечая скептикам, Накамото сказал о прошлых неудачах ещё точнее. Многие, по его словам, заранее считают электронные деньги безнадёжным делом из-за всех компаний, прогоревших с 1990-х годов, но их погубила именно централизованность, и биткоин, по его мнению, — первая попытка построить децентрализованную систему, не основанную на доверии[152].[153]

Если разложить всех предшественников по тому, кто у них вёл тетрадку, получится короткий список:

схема Чаума и DigiCash — запись ведёт банк, он же ловит двойную трату[154], а компания обанкротилась в 1998 году[155];

e-gold — запись ведёт компания, и после уголовного дела её обязали работать по правилам денежных сервисов[156];

b-money — каждый ведёт свою копию без способа их согласовать (во втором варианте запись ведёт группа серверов), схема не реализована[157];

bit gold — распределённый реестр прав на «дорогие» биты, не реализован[158];

Hashcash — цена за отправку письма, к деньгам прямого отношения не имеет[159].

В первых двух строчках есть работающая система и хозяин, в следующих двух нет хозяина и нет работающей системы, а последняя даёт недостающую деталь. Накамото понадобилось соединить их так, чтобы получилась работающая система без хозяина.

---

[148] Nakamoto, 2008, «References», https://bitcoin.org/bitcoin.pdf.

[149] переписка Wei Dai — Satoshi Nakamoto, опубликована Уэй Даем (впервые процитирована в The Sunday Times, 2014); архив: https://gwern.net/doc/bitcoin/2008-nakamoto.

[150] Satoshi Nakamoto, «Re: They want to delete the Wikipedia article», bitcointalk.org, 20.07.2010, 18:38:28 UTC; архив: https://satoshi.nakamotoinstitute.org/posts/bitcointalk/249/.

[151] Nakamoto S. Re: They want to delete the Wikipedia article. Bitcointalk, 20.07.2010: «Bitcoin is an implementation of Wei Dai's b-money proposal on Cypherpunks in 1998 and Nick Szabo's Bitgold proposal.»

[152] Satoshi Nakamoto, reply in thread «Bitcoin open source implementation of P2P currency», P2P Foundation, 15.02.2009; архив: https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/2/.

[153] Nakamoto S. Reply. P2P Foundation, 15.02.2009: «A lot of people automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990's. I hope it's obvious it was only the centrally controlled nature of those systems that doomed them. I think this is the first time we're trying a decentralized, non-trust-based system.» Каких именно компаний он имел в виду, Накамото не уточнил; DigiCash и e-gold хорошо подходят под описание, но приписывать ему именно их я не стану.

[154] Chaum, «Blind Signatures for Untraceable Payments», 1983, стр. 202, шаги протокола (10)–(12).

[155] American Banker, «Electronic Commerce: Bankrupt Digicash to Seek Financing, New Allies», 10.11.1998, https://www.americanbanker.com/news/electronic-commerce-bankrupt-digicash-to-seek-financing-new-allies.

[156] U.S. Department of Justice, «Digital Currency Business E-Gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges», 21.07.2008, https://www.justice.gov/archive/opa/pr/2008/July/08-crm-635.html; дубль: U.S. Secret Service, 22.07.2008, https://www.secretservice.gov/press/releases/2008/07/us-secret-service-led-investigation-digital-currency-business-e-gold-pleads.

[157] Wei Dai, «b-money», 1998, http://www.weidai.com/bmoney.txt (сайт при проверке не отвечал — ECONNREFUSED); описание по A. van Wirdum, «The Genesis Files: If Bitcoin Had a First Draft, Wei Dai's B-Money Was It», Bitcoin Magazine, 14.06.2018, https://bitcoinmagazine.com/technical/genesis-files-if-bitcoin-had-first-draft-wei-dais-b-money-was-it.

[158] Nick Szabo, «Bit gold», блог Unenumerated, https://unenumerated.blogspot.com/2005/12/bit-gold.html.

[159] A. Back, «Hashcash — A Denial of Service Counter-Measure», 01.08.2002, http://www.hashcash.org/papers/hashcash.pdf (ссылка [6] у Накамото, https://bitcoin.org/bitcoin.pdf); дата анонса 1997 — Wikipedia, «Hashcash», https://en.wikipedia.org/wiki/Hashcash (ссылка на http://www.hashcash.org/papers/announce.txt).

Тетрадка без хранителя

Цифровая запись должна быть одна, иначе её нельзя проверить. Одну запись до сих пор всегда вёл хранитель, а хранитель мог разориться, попасть под запрет или злоупотребить доверием. Нужна одна общая тетрадка, которую никто в отдельности не ведёт.

31 октября 2008 года Накамото объявил о своей статье в криптографической рассылке, и первая фраза письма гласила, что он работает над новой системой электронных денег, полностью одноранговой, без доверенной третьей стороны[160].[161] Одноранговой называют сеть без центрального сервера, где каждый участник связан с другими напрямую. Дальше в письме шёл короткий список свойств. Двойная трата предотвращается одноранговой сетью; нет ни монетного двора, ни других доверенных сторон; участники могут быть анонимны; новые монеты создаются доказательством работы в стиле Hashcash[162], то есть достаются тому, кто потратил вычислительную работу и может это предъявить. (С анонимностью всё сложнее, чем обещала эта строчка, и в главе 2 мы увидим почему.)

В самой статье задача поставлена в двух фразах. Цифровые подписи решают её часть, но главные преимущества теряются, если для защиты от двойной траты всё равно нужна доверенная третья сторона, а решение предлагается через одноранговую сеть[163]. А во введении сказано, что нужна платёжная система, основанная на криптографическом доказательстве вместо доверия, которая позволит любым двум желающим сторонам рассчитываться напрямую, без доверенного посредника[164].[165] Речь в статье об интернет-платежах и посредниках, через которых они идут, а о центральном банке Накамото писал отдельно, в посте 2009 года[166]. Посредник, объясняет он во введении, обходится дороже своей комиссии, потому что платёж через него можно отменить, и тогда продавцам приходится остерегаться собственных покупателей[167].

Как именно Накамото убрал хранителя, мы будем разбирать дальше, но общий ход виден уже на посёлке. Вспомните формулу из статьи. Чтобы убедиться, что транзакции не было, надо знать обо всех. Без хранителя это значит, что транзакции нужно объявлять открыто, и нужна система, в которой участники договариваются о единой истории того, в каком порядке транзакции поступили[168]. Переведём это в пятое правило посёлка, в котором три части: 1) каждый двор держит у себя полную копию общей тетрадки; 2) каждая новая запись объявляется всем дворам сразу; 3) есть способ, которым дворы, не доверяющие друг другу, приходят к одной версии тетрадки, даже если кто-то из них жульничает.

Посмотрим, как это работает на нашем пекаре. Теперь он не может тайно отправить одну строчку доярке, а другую лесорубу, потому что обе строчки объявляются всем дворам. Каждый

---

[160] Satoshi Nakamoto, «Bitcoin P2P e-cash paper», The Cryptography Mailing List, 31.10.2008, 14:10 EDT, https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html.

[161] Nakamoto S. Bitcoin P2P e-cash paper. The Cryptography Mailing List, 31.10.2008: «I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.»

[162] Satoshi Nakamoto, «Bitcoin P2P e-cash paper», The Cryptography Mailing List, 31.10.2008, 14:10 EDT, https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html.

[163] Satoshi Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System», 2008, https://bitcoin.org/bitcoin.pdf (Abstract).

[164] Nakamoto, 2008, раздел 1 «Introduction», https://bitcoin.org/bitcoin.pdf.

[165] Nakamoto, 2008, section 1: «What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.» Там же: «With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers…»

[166] Satoshi Nakamoto, «Bitcoin open source implementation of P2P currency», P2P Foundation, 11.02.2009, 22:27 UTC; архив Satoshi Nakamoto Institute, https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/1/.

[167] Nakamoto, 2008, раздел 1 «Introduction», https://bitcoin.org/bitcoin.pdf.

[168] Nakamoto, 2008, раздел 2, https://bitcoin.org/bitcoin.pdf.

двор видит, что пекарь пытается отдать одно право дважды, и дело сводится к тому, какая строчка была первой. Первую записывают в тетрадку, вторую отбрасывают.

Но какая из них была первой?

Посмотреть на время отправки не выйдет. Время в строчке ставит сам пекарь, и ничто не мешает ему пометить строчку для лесоруба более ранним часом, а часы на разных компьютерах к тому же расходятся. Поверить чужой отметке времени значит снова поверить тому, кто её поставил. Остаётся порядок, в котором строчки дошли до дворов, но и он у всех свой. Сообщения в сети идут с задержками, и до двора на одном краю посёлка первой дойдёт строчка для доярки, а до двора на другом краю — строчка для лесоруба. Если каждый двор запишет то, что увидел первым, копии тетрадки разойдутся, и мы вернёмся к b-money. Поэтому Накамото и говорит о единой истории порядка, в котором транзакции поступили[169].

Рисунок 1.2. Пять правил посёлка по порядку

Первые две части правила не новы, b-money предлагала почти то же. Вся трудность в третьей, и именно её Накамото решил так, как до него не решал никто. По его собственным словам, он думал над замыслом с 2007 года и в какой-то момент убедился, что это можно сделать вообще без необходимости в доверии; больше всего работы, добавил он, ушло на проектирование, программирование заняло меньше[170].[171]

[169] Nakamoto, 2008, раздел 2, https://bitcoin.org/bitcoin.pdf.

[170] Satoshi Nakamoto, «Re: Transactions and Scripts: DUP HASH160… EQUALVERIFY CHECKSIG», bitcointalk.org, 18.06.2010, 16:17:14 UTC; архив: https://satoshi.nakamotoinstitute.org/posts/bitcointalk/127/.

[171] Nakamoto S. Bitcointalk, 18.06.2010: «Since 2007. At some point I became convinced there was a way to do this without any trust required at all and couldn't resist to keep thinking about it.»

Записи в биткоине собираются в страницы, их называют блоками. Первый блок новой тетрадки датирован 3 января 2009 года, и в него записан заголовок газеты The Times того дня, «Канцлер на грани второго спасения банков»[172].[173] Вписан он затем, чтобы доказать, что блок создан не раньше этой даты, ведь знать заранее, какой заголовок выйдет в газете в этот день, никто не мог. Обычно его читают ещё и как комментарий к спасению банков за счёт государства[174]. Прочтение правдоподобное, но сам Накамото его не подтверждал и не опровергал, так что для меня оно остаётся версией. (У первого блока есть и техническая странность. Вместе с каждым блоком в системе появляются новые монеты; с первым их появилось 50, но из-за особенности кода потратить их нельзя, и намеренно ли так сделано, неизвестно[175].)

На этом месте аналогия с посёлком начинает ломаться, и полезно сказать, где именно. В посёлке тетрадка записывает долги (плотник должен пекарю, банк должен вам). В биткоине за строчкой нет должника. Никто не обещает отдать хлеб, крышу или доллары в обмен на вашу запись, строчка просто говорит, что столько-то единиц теперь принадлежит владельцу такого-то ключа, то есть тому, кто может подписать следующий перевод. Банк Англии ещё в 2014 году отметил, что биткоин тогда не использовался широко для расчётов и был популярен скорее как предмет вложений, и написал, что цифровые валюты вроде биткоина концептуально, возможно, ближе к товарам вроде золота, чем к деньгам[176].[177] Спор о том, деньги это или товар, начался почти одновременно с самим биткоином и не закончен до сих пор. Для этой главы важно, что долг из старой модели биткоин оставляет за бортом и забирает у неё только тетрадку, то есть общую запись о том, кому что принадлежит, и правило, по которому её нельзя тайно переписать.

Куда переходит доверие

Вернёмся к развилке, которую я обещал. Накамото и Банк международных расчётов исходят из одного факта: доверие к хранителям денег подводило много раз. Выводы у них противоположные. Банк международных расчётов пишет, что децентрализованная технология криптовалют, как бы изощрённа она ни была, — плохая замена прочной институциональной опоре денег, а проверенным способом обеспечить доверие к деньгам называет независимый центральный банк[178].[179] Сами деньги он определяет как незаменимую общественную договорённость, за которой стоит подотчётный государственный институт, пользующийся доверием публики[180]. Из этого следует, что хранителей нужно укреплять.

---

[172] Bitcoin Wiki, «Genesis block», https://en.bitcoin.it/wiki/Genesis_block (текст поля coinbase воспроизводится любым узлом сети).

[173] Текст в первом блоке: «The Times 03/Jan/2009 Chancellor on brink of second bailout for banks».

[174] Bitcoin Wiki, «Genesis block», https://en.bitcoin.it/wiki/Genesis_block (текст поля coinbase воспроизводится любым узлом сети).

[175] Bitcoin Wiki, «Genesis block», https://en.bitcoin.it/wiki/Genesis_block (текст поля coinbase воспроизводится любым узлом сети).

[176] McLeay, Radia, Thomas, «Money in the modern economy: an introduction», BoE QB 2014 Q1, стр. 9, врезка «Recent developments in payment technologies and alternative currencies».

[177] McLeay, Radia, Thomas. Money in the modern economy: an introduction, p. 9: «As such they may have more conceptual similarities to commodities, such as gold, than money.»

[178] BIS, Annual Economic Report 2018, ch. V, https://www.bis.org/publ/arpdf/ar2018e5.htm.

[179] BIS, Annual Economic Report 2018, ch. V: «Overall, the decentralised technology of cryptocurrencies, however sophisticated, is a poor substitute for the solid institutional backing of money»; «The tried, trusted and resilient way to provide confidence in money in modern times is the independent central bank.»

[180] BIS, Annual Economic Report 2018, chapter V «Cryptocurrencies: looking beyond the hype», 24.06.2018, https://www.bis.org/publ/arpdf/ar2018e5.htm.

Накамото предлагает убрать нужду в хранителе. Заключение его статьи начинается словами о том, что предложена система электронных транзакций, не полагающаяся на доверие[181].[182]

Кто из них прав, я в этой главе решать не стану. Ответ зависит от того, что держит систему без хранителя и насколько это прочно, а проверить это можно, только разобрав механизм по частям.

Одно я могу сказать уже сейчас. Формулировку Накамото я не считаю точной и дальше в книге буду исходить из более осторожной: доверие в биткоине остаётся, только переходит на другие опоры. В той же статье безопасность системы держится на условии, что честные участники вместе контролируют больше вычислительной мощности (проще говоря, больше компьютеров, занятых той самой работой в стиле Hashcash), чем любая группа нападающих[183]. Кроме того, пользователи доверяют математике подписей, коду, который пишут конкретные люди, и собственной способности не потерять ключ. Одни из этих опор прочнее привычных хранителей, другие слабее, и каждую мы проверим отдельно.

Зачем тогда вся эта конструкция, если доверие всё равно остаётся? Разница в том, кто может изменить запись в одиночку. В посёлке с хранителем для этого хватает одного человека, который допишет строчку, сотрёт чужую или остановит платежи (e-gold, как мы видели, пришлось перестроиться после одного уголовного дела против её хозяев[184]). В тетрадке без хранителя для того же нужно, чтобы сговорились те, у кого большая часть вычислительной мощности сети[185]. Доверие здесь похоже на нагрузку в конструкции. Убрать её нельзя, но можно разнести на много опор, и тогда отказ одной не роняет всё здание. Во что обходится такая распределённость и где она держится хуже, чем обещано, — отдельный вопрос, и до него мы дойдём.

Поэтому к любым деньгам, старым и новым, я в этой книге буду подходить с одним и тем же вопросом: кто ведёт запись и почему ему верят. У денег на вашем банковском счёте ответ двухэтажный (ваш банк и над ним центральный банк, которых ограничивают правила, надзор и денежная политика). У биткоина ответ другой, и из-за него весь спор. Запись ведут все участники сразу, и верить приходится условиям, на которых держится система. Криптовалюта — это попытка сделать тетрадку, которой не нужен хозяин.

Этот вопрос удобно разложить на несколько поменьше, и я советую задавать их себе всякий раз, когда вы читаете о новой монете, платёжной системе или «цифровых деньгах» какого-нибудь банка:

Кто ведёт запись?

Кто может дописать в неё новые строчки, и что его ограничивает?

Кто может стереть или заморозить чужую строчку?

Кто может остановить всю систему одним решением?

Кто выдаёт строчки в долг, и что будет, когда долги начнут вычёркивать?

Для денег на банковском счёте ответы уже есть в этой главе, хотя вы их, скорее всего, никогда не проговаривали. Запись ведёт ваш банк, а над ним центральный банк. Новые строчки пишут банки, выдавая кредиты, и держат их прибыльность, надзор и ставка центрального банка[186]. Стереть, заморозить или остановить может тот, кто ведёт тетрадку, а над ним государ-

---

[181] Nakamoto, 2008, раздел 12 «Conclusion», https://bitcoin.org/bitcoin.pdf.

[182] Nakamoto, 2008, section 12: «We have proposed a system for electronic transactions without relying on trust.»

[183] Satoshi Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System», 2008, https://bitcoin.org/bitcoin.pdf.

[184] U.S. Department of Justice, «Digital Currency Business E-Gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges», 21.07.2008, https://www.justice.gov/archive/opa/pr/2008/July/08-crm-635.html; дубль: U.S. Secret Service, 22.07.2008, https://www.secretservice.gov/press/releases/2008/07/us-secret-service-led-investigation-digital-currency-business-e-gold-pleads.

[185] Satoshi Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System», 2008, https://bitcoin.org/bitcoin.pdf.

[186] McLeay, Radia, Thomas, «Money creation in the modern economy», BoE QB 2014 Q1, стр. 14 (Overview).

ство, которое, как показала история e-gold, способно одним делом перестроить работу хранителя[187]. Строчки в долг выдают те же банки, и когда долги вычёркивают, вместе с ними исчезают деньги[188]. Для биткоина ответы другие, и дальше я постараюсь разобрать механизм так, чтобы вы могли дать их сами, не веря ни сторонникам, ни противникам. Пятый вопрос для этой книги самый важный, и возвращаться к нему я буду чаще, чем к остальным.

Прежде чем судить, стоит увидеть, как эта тетрадка устроена изнутри. В следующей главе мы разберём, почему её нельзя тайно переписать задним числом, что лежит в криптовалютном кошельке и что происходит, когда человек теряет свой ключ.

[187] U.S. Department of Justice, «Digital Currency Business E-Gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges», 21.07.2008, https://www.justice.gov/archive/opa/pr/2008/July/08-crm-635.html; дубль: U.S. Secret Service, 22.07.2008, https://www.secretservice.gov/press/releases/2008/07/us-secret-service-led-investigation-digital-currency-business-e-gold-pleads.

[188] McLeay, Radia, Thomas, «Money creation in the modern economy», BoE QB 2014 Q1, стр. 16.

Глава 2. Реестр без хозяина: как работает блокчейн

Тетрадку без хранителя может прочитать каждый, а тайно переписать не может никто. Если эту фразу разобрать по частям, из неё получится почти всё устройство блокчейна, и в этой главе я хочу собрать его так, чтобы вы могли пересказать его другу без формул и без веры на слово.

В конце первой главы посёлок получил пятое правило: копия тетрадки лежит у каждого двора, каждая новая запись объявляется всем, и есть способ, которым дворы приходят к одной версии. Правило звучит просто, но работать оно начнёт, только когда найдутся ответы на несколько неудобных вопросов. Если копий сто, что мешает пекарю тихо исправить у себя строчку трёхмесячной давности и уверять соседей, что так и было записано? Хранитель знал пекаря в лицо и не принял бы строчку, написанную от его имени чужой рукой, но кто проверяет это теперь? И где лежит богатство пекаря, если у него нет ни счёта, ни хранителя, который этот счёт ведёт?

Из ответов на эти вопросы и складывается блокчейн. Это общая тетрадь, которую нельзя тайно переписать задним числом, а владеть строчкой в ней значит владеть ключом. Из второй половины определения следуют два свойства, которые многих удивляют. Такая тетрадка прозрачна, и анонимности в ней гораздо меньше, чем принято думать. А если ключ потерян, строчку не вернёт никто, потому что возвращать её некому. Детали я везде беру из биткоина, потому что он первый и лучше всего описан, хотя другие блокчейны во многом устроены иначе.

Отпечаток страницы

Представим, что у посёлка есть машинка. В неё кладут любую страницу тетрадки, а она выдаёт короткую строку из цифр и букв, всегда одной и той же длины. Назовём эту строку отпечатком страницы. От машинки нам нужно, чтобы 1) одна и та же страница всегда давала один и тот же отпечаток и любой двор мог проверить это сам; 2) по отпечатку нельзя было восстановить страницу или подобрать страницу под заранее заданный отпечаток иначе как перебором; 3) нельзя было найти две разные страницы с одинаковым отпечатком.

Такая машинка существует. Она называется криптографической хеш-функцией, а её результат — хешем. Наши требования совпадают с теми свойствами, которые справочник «Mastering Bitcoin» называет у неё главными: детерминированность, практическая необратимость и стойкость к коллизиям, то есть к совпадениям отпечатков[189].[190]

Первое свойство позволяет любому двору проверить чужой отпечаток, ни у кого не спрашивая разрешения. Второе превращает поиск отпечатка нужного вида в лотерею, где выигрывают только числом попыток, и из этой лотереи чуть позже получится цена за новую страницу. Третье не даёт подменить страницу другой с тем же отпечатком[191], а будь подмена возможна, отпечаток ничего бы не удостоверял. (Строго говоря, совпадения существуют, ведь страниц бесконечно много, а отпечатков конечное число. Но найти хотя бы одно такое совпадение вычислительно невозможно, и этого достаточно[192].)

Биткоин использует функцию SHA-256. Её результат всегда имеет длину 256 бит, то есть 256 двоичных знаков, нулей и единиц, какой бы длины ни был вход, хоть одна буква, хоть

---

[189] Mastering Bitcoin, 3rd ed., 2023, гл. 12.

[190] Antonopoulos A. M., Harding D. A. Mastering Bitcoin. 3rd ed. O'Reilly, 2023, ch. 12: «It is also virtually impossible to select an input in such a way as to produce a desired digest, other than trying random inputs»; «…it is computationally infeasible to find two different inputs that produce the same digest.»

[191] Mastering Bitcoin, 3rd ed., 2023, гл. 12.

[192] Mastering Bitcoin, 3rd ed., 2023, гл. 12.

целая книга[193]. На экране это 64 знака шестнадцатеричной записи, где кроме цифр от 0 до 9 используются буквы от a до f[194].

Я пропустил через SHA-256 две строчки из нашего посёлка, которые отличаются одной цифрой:

«плотник должен пекарю 10» → 31f1c80ad71f0a47203c0ad31e883c64ae23440b0ee955fb159e3e9982109898

«плотник должен пекарю 11» → e0767f7e15e87062018598fbfc7bb8072327a49b17b995bfdc2ba9c632bb0a5e

Отпечатки не похожи друг на друга ни в одном месте, хотя строчки почти одинаковы. Любое изменение входа, даже одна буква или знак препинания, даёт другой хеш[195].[196] Насколько изменилась страница, по отпечатку понять нельзя, зато любая правка видна сразу.

Ради этого хеш-функции и придуманы. Американский стандарт, в котором описана SHA-256, прямо называет их назначение — обнаруживать, не изменилось ли сообщение с того момента, как для него посчитали отпечаток[197].[198] Стандарт выпустил Национальный институт стандартов и технологий США в августе 2002 года[199], и эта дата полезна против распространённого мифа, будто Накамото изобрёл всю криптографию биткоина. Хеш-функцию он взял из готового правительственного стандарта шестилетней давности[200]. Сцеплять отпечатки в цепочку до него предлагали исследователи Хабер и Сторнетта, на чьи работы он сам ссылается[201], а дерево отпечатков, о котором речь пойдёт ниже, описал Ральф Меркл ещё в конце 1970-х[202]. Сам Накамото соединил эти готовые детали в одну конструкцию, её мы и будем собирать.

С хешем связан и второй миф, будто блокчейн «зашифрован». Хеш — не шифр. Расшифровывать в нём нечего, страница из отпечатка не восстанавливается вовсе[203]. Сами записи в тетрадке биткоина тоже никто не шифрует. Они подписаны и лежат открыто, и к последствиям этого мы придём, когда будем говорить о следах[204].

Проверить отпечаток легко (положил страницу, получил строку, сравнил). Подобрать страницу под нужный отпечаток трудно, потому что остаётся только перебирать варианты[205]. В «Mastering Bitcoin» есть учебный пример. К фразе «Hello, World!» дописывают число и пере-

---

[193] Antonopoulos A. M., Harding D. A. Mastering Bitcoin, 3rd ed., O'Reilly, 2023, гл. 12 «Mining and Consensus»; открытый текст: https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch12_mining.adoc.

[194] Antonopoulos A. M., Harding D. A. Mastering Bitcoin, 3rd ed., O'Reilly, 2023, гл. 12 «Mining and Consensus»; открытый текст: https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch12_mining.adoc.

[195] Mastering Bitcoin, 3rd ed., 2023, гл. 12.

[196] Там же: «Adding a single letter, punctuation mark, or any other character will produce a different hash.» Для любопытных: строка «Плотник должен пекарю 10», отличающаяся от первой только заглавной буквой, даёт отпечаток 799790f8fce2c7cb33c10efc8759c44f735222634cacb948c70e7c0554f21a83 (расчёт автора; повторить может любой).

[197] NIST, FIPS 180-2 «Secure Hash Standard (SHS)», August 2002, https://csrc.nist.gov/pubs/fips/180-2/final; действующая редакция — FIPS 180-4, August 2015, https://csrc.nist.gov/pubs/fips/180-4/upd1/final.

[198] NIST. FIPS 180-4 Secure Hash Standard, 2015, аннотация: хеш-алгоритмы нужны, чтобы «detect whether messages have been changed since the digests were generated». Первая редакция с SHA-256 — FIPS 180-2, август 2002 года: «All four of the algorithms are iterative, one-way hash functions».

[199] NIST, FIPS 180-2 «Secure Hash Standard (SHS)», August 2002, https://csrc.nist.gov/pubs/fips/180-2/final; действующая редакция — FIPS 180-4, August 2015, https://csrc.nist.gov/pubs/fips/180-4/upd1/final.

[200] NIST, FIPS 180-2 «Secure Hash Standard (SHS)», August 2002, https://csrc.nist.gov/pubs/fips/180-2/final; действующая редакция — FIPS 180-4, August 2015, https://csrc.nist.gov/pubs/fips/180-4/upd1/final.

[201] Nakamoto, 2008, раздел 3 «Timestamp Server», https://bitcoin.org/bitcoin.pdf.

[202] Nakamoto, 2008, раздел 7 «Reclaiming Disk Space», https://bitcoin.org/bitcoin.pdf; идея дерева — R. C. Merkle, «Protocols for public key cryptosystems», Proc. 1980 Symposium on Security and Privacy, IEEE, pp. 122–133 (ссылка [7] белой книги).

[203] Mastering Bitcoin, 3rd ed., 2023, гл. 12.

[204] Nakamoto, 2008, раздел 10 «Privacy», https://bitcoin.org/bitcoin.pdf.

[205] Mastering Bitcoin, 3rd ed., 2023, гл. 12.

бирают его, пока хеш не начнётся с нуля, и подходит число 32[206]. Каждый знак отпечатка может быть любым из 16 символов, поэтому отпечаток с одним нулём в начале выпадает в среднем раз на 16 попыток, с двумя нулями — раз на 256, с тремя — раз на 4096 (это чистая арифметика вероятностей). Каждый новый ноль удлиняет перебор ещё в 16 раз, а проверку оставляет такой же мгновенной, и на этой разнице будет держаться цена, которую мы вскоре назначим каждой новой странице.

Страницы, сшитые отпечатками

Вернёмся к пекарю, который хочет тихо поправить старую строчку в своей копии. Добавим в посёлок шестое правило: записи собирают в страницы, и в начале каждой новой страницы пишут отпечаток предыдущей.

Пекарь исправляет строчку на странице 100. Отпечаток страницы 100 от этого меняется, а старый отпечаток записан в начале страницы 101 и больше с ней не сходится. Если пекарь перепишет и начало страницы 101, изменится уже её отпечаток, записанный на странице 102, и так до последней страницы. Любая правка задним числом тянет за собой всю тетрадку до конца. Соседям при этом не нужно перечитывать все страницы, чтобы заметить подлог, им достаточно сравнить отпечаток последней страницы у себя и у пекаря.

Такой двор, со своей копией и привычкой проверять каждую новую страницу, в сети биткоина называется узлом. Узел — это компьютер, на котором лежит полная копия тетрадки и работает программа, проверяющая всё, что в неё добавляют.

Накамото описал цепочку отпечатков в третьем разделе статьи 2008 года и описал её языком меток времени (так называют запись, которая удостоверяет, что документ существовал к определённому моменту). Каждая метка, пишет он, включает в свой хеш предыдущую, так образуется цепочка, и каждая новая метка укрепляет все, что были до неё[207].[208] Там же он предлагает широко публиковать хеш, например в газете[209]. Отпечаток, напечатанный в газете, уже нельзя тихо подменить, а вместе с ним нельзя подменить и страницу, которой он принадлежит.

Цепочка отпечатков доказывает порядок. Страница 101 не могла появиться раньше страницы 100, потому что несёт её отпечаток, а значит, страница 100 существовала к тому моменту, когда писали 101-ю. С другого конца цепочку закрывает первый блок биткоина. В нём, как мы видели в первой главе, записан заголовок The Times от 3 января 2009 года, и поэтому блок не мог появиться раньше этой даты[210]. Каждый следующий блок доказывает, что все предыдущие уже были, и между двумя концами лежит вся история тетрадки, в которой страницы нельзя переставить.

Страницы биткоина, как мы договорились в первой главе, называются блоками, а тетрадь из сшитых отпечатками блоков — цепочкой блоков, по-английски блокчейном. Собирает очередной блок и предлагает его сети майнер (так называют участника, который тратит на это вычислительную работу; в чём она состоит, покажет седьмое правило). У каждого блока есть заголовок, и он совсем маленький, 80 байт и шесть полей[211]:

версия правил;

---

[206] Mastering Bitcoin, 3rd ed., 2023, гл. 12.

[207] Nakamoto, 2008, раздел 3 «Timestamp Server», https://bitcoin.org/bitcoin.pdf.

[208] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, section 3: «Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.» Там же — ссылки на работы Хабера и Сторнетты 1991, 1993 и 1997 годов и предложение публиковать хеш «как в газете или посте Usenet».

[209] Nakamoto, 2008, раздел 3 «Timestamp Server», https://bitcoin.org/bitcoin.pdf.

[210] Bitcoin Wiki, «Genesis block», https://en.bitcoin.it/wiki/Genesis_block (текст поля coinbase воспроизводится любым узлом сети).

[211] Bitcoin Developer Reference, «Block Chain».

хеш заголовка предыдущего блока, то есть отпечаток прошлой страницы;

корень дерева Меркла, общий отпечаток всех записей этой страницы (о нём чуть ниже);

время, которое указал сам майнер; узлы сверяют его только грубо, с допуском примерно в пару часов[212];

закодированная цель сложности, то есть порог, под который должен попасть отпечаток страницы;

число nonce, которое майнеры перебирают.

Второе поле и есть шов между страницами. (Хеш заголовка в биткоине считают дважды, SHA-256 от результата SHA-256[213], но механизма это не меняет.)

Четвёртое поле вызывает законный вопрос. Цепочку только что называли цепочкой меток времени, а время в заголовке ставит сам майнер и может ошибиться или слукавить. В первой главе мы видели, почему нельзя опираться на чужую отметку времени. Здесь опираться на неё и не приходится, потому что порядок страниц доказывают отпечатки. Страница, которая несёт отпечаток предыдущей, написана после неё, что бы ни стояло в поле времени. От поля времени требуется только не уходить далеко от настоящего, и на это хватает грубой сверки, которую делает каждый узел[214].

Самих записей в заголовке нет, там только один отпечаток на все сразу, и получают его хитрее, чем простым хешем страницы. Записи (в биткоине их называют транзакциями) разбивают на пары, каждую пару хешируют, получившиеся хеши снова разбивают на пары и снова хешируют, пока не останется один[215].[216] Получается перевёрнутое дерево, у которого внизу листья-транзакции, наверху один корень, и в заголовок попадает только корень[217].

---

[212] Bitcoin Developer Reference, «Block Chain».

[213] Bitcoin Developer Reference, «Block Chain», https://developer.bitcoin.org/reference/block_chain.html.

[214] Bitcoin Developer Reference, «Block Chain».

[215] Bitcoin Developer Reference, «Block Chain».

[216] Если на каком-то уровне хешей нечётное число, последний идёт в пару с собственной копией (Bitcoin Developer Reference, «Block Chain»). Деревья хешей Меркл описал в 1979 году (диссертация и патентная заявка); Накамото ссылается на его статью 1980 года.

[217] Nakamoto, 2008, раздел 7 «Reclaiming Disk Space», https://bitcoin.org/bitcoin.pdf; идея дерева — R. C. Merkle, «Protocols for public key cryptosystems», Proc. 1980 Symposium on Security and Privacy, IEEE, pp. 122–133 (ссылка [7] белой книги).

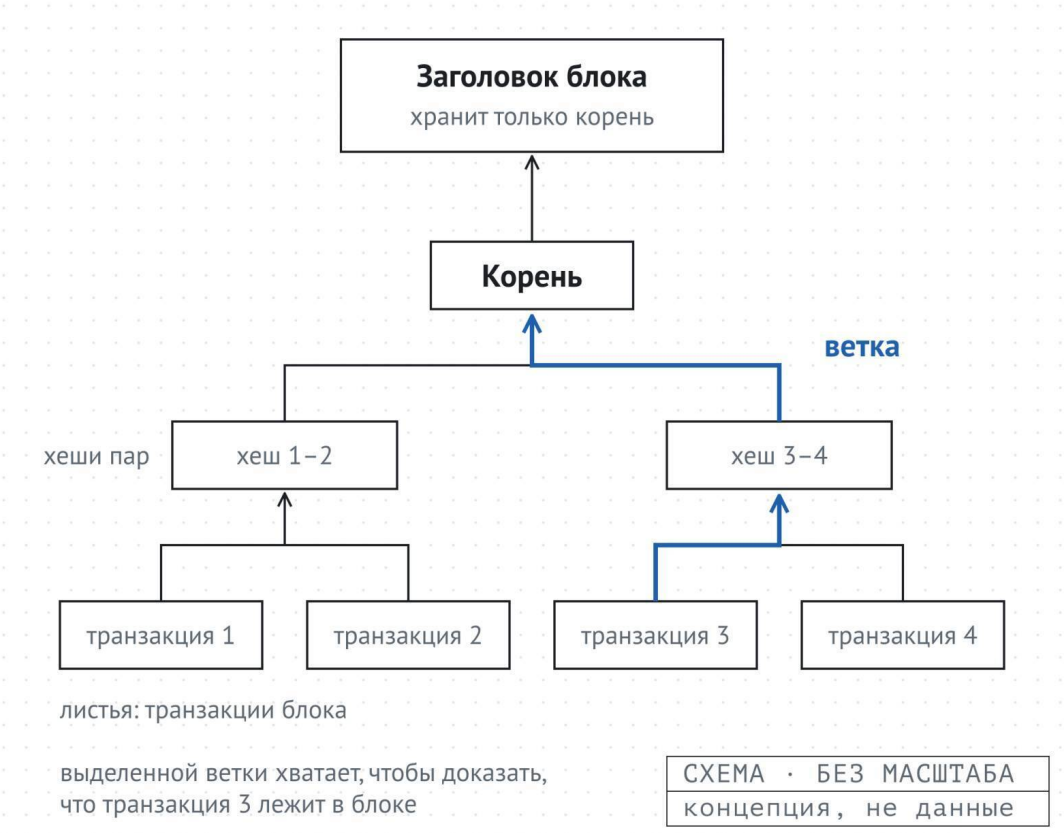


Рисунок 2.1. Дерево Меркла

Зачем такие сложности? Дерево позволяет доказать, что конкретная транзакция лежит в конкретном блоке, не показывая весь блок, потому что для этого хватает ветки хешей от её листа до корня. Каждый уровень дерева вдвое уже предыдущего, и в блоке из нескольких тысяч транзакций такая ветка состоит примерно из дюжины отпечатков (это прямо следует из того, как строится дерево[218]). Накамото извлёк из этого две выгоды. Старые, уже потраченные транзакции можно выбрасывать с диска, не ломая хеш блока[219]. А пользователь, которому не нужна вся тетрадка, может хранить одни заголовки. К таким «лёгким» проверяющим мы вернёмся, когда дойдём до кошелька.

Отпечаток каждого блока зависит от корня дерева, корень зависит от каждой транзакции внутри, а заголовок следующего блока хранит отпечаток предыдущего[220]. Поменяйте одну цифру в одной транзакции тысячу блоков назад, и по цепи изменятся лист, ветка, корень, заголовок, отпечаток блока, заголовок следующего блока и так далее до сегодняшнего дня.

[218] Bitcoin Developer Reference, «Block Chain».

[219] Nakamoto, 2008, раздел 7 «Reclaiming Disk Space», https://bitcoin.org/bitcoin.pdf; идея дерева — R. C. Merkle, «Protocols for public key cryptosystems», Proc. 1980 Symposium on Security and Privacy, IEEE, pp. 122–133 (ссылка [7] белой книги).

[220] Bitcoin Developer Reference, «Block Chain».

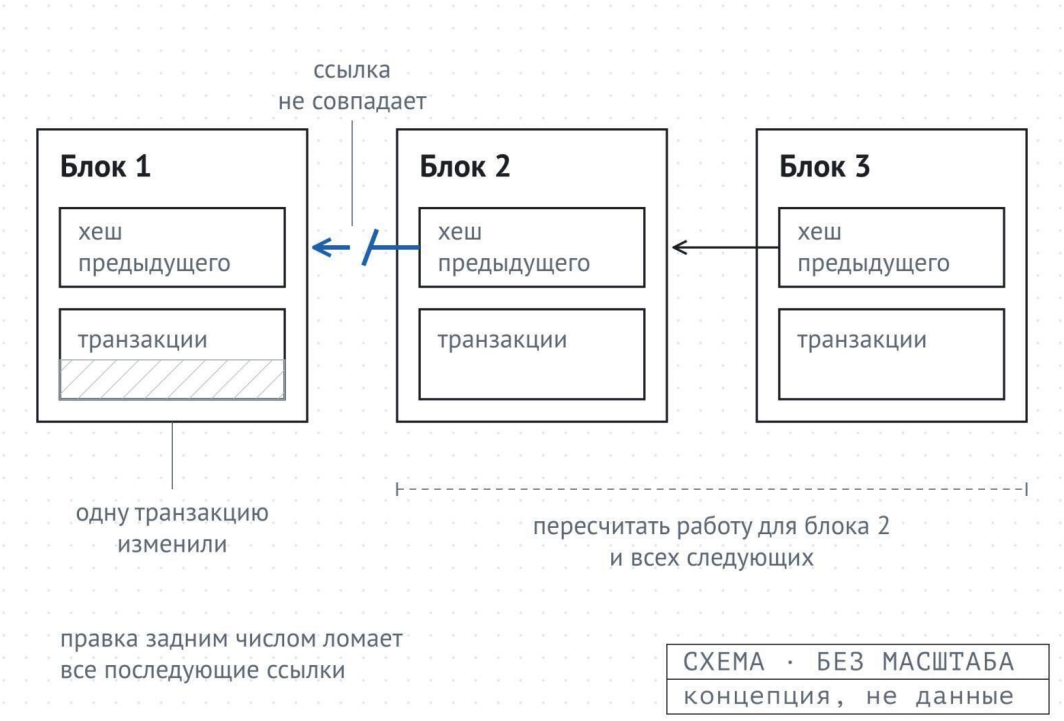


Рисунок 2.2. Цепочка из трёх блоков

У этой защиты есть слабое место. Хешировать дёшево. Если пекарь готов переписать все страницы от сотой до последней, его домашний компьютер пересчитает отпечатки за секунды, и получится новая тетрадка, внутри себя совершенно согласованная. Отпечатки защищают от незаметной правки одной страницы, но того, кто переделал всю тетрадку заново, они не остановят.

Недостающая деталь знакома по первой главе. Это «цена за запись» из Hashcash Адама Бэка, на который Накамото прямо ссылается[221]. Добавим седьмое правило: страницу принимают, только если её отпечаток начинается с заданного числа нулей. Отпечаток нельзя подогнать иначе как перебором[222], поэтому майнер меняет в заголовке число nonce и хеширует заголовок снова и снова, пока не выпадет отпечаток с нужным числом нулей[223]. (Точная формулировка правила — хеш, прочитанный как число, должен быть не больше порога из поля цели сложности, но «начинается с нулей» — слова самого Накамото[224].) Эта работа и называется доказательством работы, а перебор ради неё — майнингом.

За труд майнер получает плату и записывает её себе сам. Первой в каждом блоке идёт его особая транзакция[225], которая выдаёт ему награду за блок и все комиссии из транзакций блока[226]. Размер награды задают правила, и каждый узел его проверяет. В первые годы награда составляла 50 BTC[227], а каждые 210 000 блоков она уменьшается вдвое[228]. Других путей для

[221] Nakamoto, 2008, раздел 4; Bitcoin Developer Reference, «Block Chain».

[222] Mastering Bitcoin, 3rd ed., 2023, гл. 12.

[223] Nakamoto, 2008, раздел 4; Bitcoin Developer Reference, «Block Chain».

[224] Nakamoto, 2008, раздел 4; Bitcoin Developer Reference, «Block Chain».

[225] Bitcoin Developer Reference, «Block Chain».

[226] Nakamoto, 2008, раздел 6 «Incentive»; Mastering Bitcoin, 3rd ed., гл. 6.

[227] Bitcoin Wiki, «Value overflow incident», https://en.bitcoin.it/wiki/Value_overflow_incident; Накамото, архив bitcointalk, посты 16.08.2010 01:00:45 и 12:59:38 UTC.

[228] исходный код Bitcoin Core, src/kernel/chainparams.cpp (CMainParams): nPowTargetSpacing = 10 * 60;

новых монет в тетрадке правила не оставляют. (Расходы майнеров и урезание награды оставим до следующей главы.)

На каждую страницу теперь потрачен труд, и проверить это любой может одним расчётом. Отсюда Накамото вывел главное следствие. Когда на блок затрачена работа, пишет он, его нельзя изменить, не переделав её, а поскольку после него в цепочку добавлены новые блоки, придётся переделать и все последующие[229].[230] Пересчитать отпечатки пекарю теперь мало. Ему нужно заново выполнить всю работу от сотой страницы до последней и успеть это быстрее, чем весь остальной посёлок добавляет новые страницы в честную тетрадку.

Чем глубже страница лежит в тетрадке, тем больше работы накоплено над ней и тем дороже её подделать. В разделе 11 статьи Накамото посчитал, что шанс отстающего атакующего догнать честную цепочку падает экспоненциально с числом блоков, которые ему нужно наверстать[231]. Для того, кто получает платёж, это значит, что свежая запись, над которой ещё нет ни одной страницы, защищена хуже всего, а запись, над которой выросли десятки страниц, почти так же прочна, как вся тетрадка под ней.

Хеш самого первого блока биткоина, от 3 января 2009 года, начинается с 10 нулей. Хеш блока номер 968 721, найденного 26 сентября 2026 года, начинается с 20 нулей[232].[233] Проверить это может любой, кто откроет обозреватель блоков, то есть сайт, который показывает тетрадку биткоина в читаемом виде. Нули показывают, что перебор подорожал, но меряют рост грубо. Для первой страницы правило требовало восьми нулей, и десять ей выпали случайно, а сегодня правило требует почти двадцати. Точную меру даёт показатель сложности, который вычисляется из цели сложности в заголовке. У первого блока он равен единице, у блока 968 721 — около 133 трлн[234].[235] Во столько же раз больше попыток в среднем нужно теперь на одну страницу и во столько же раз дороже её подделать.

Время на страницу задаёт само правило. Целевой интервал между блоками биткоина — 10 минут, и каждые 2016 блоков, то есть примерно раз в две недели, все узлы пересчитывают сложность, чтобы удержать этот темп[236]. Отдельные страницы приходят то через несколько секунд после предыдущей, то через полчаса, и десять минут получаются только в среднем[237].[238]

---

nPowTargetTimespan = 14 * 24 * 60 * 60; nSubsidyHalvingInterval = 210000, https://raw.githubusercontent.com/bitcoin/bitcoin/master/src/kernel/chainparams.cpp; Mastering Bitcoin, 3rd ed., гл. 12.

[229] Nakamoto, 2008, раздел 4 «Proof-of-Work», https://bitcoin.org/bitcoin.pdf.

[230] Nakamoto, 2008, section 4: «Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.»

[231] Nakamoto, 2008, раздел 4 «Proof-of-Work», https://bitcoin.org/bitcoin.pdf.

[232] генезис — исходный код Bitcoin Core, src/kernel/chainparams.cpp (assert hashGenesisBlock), https://raw.githubusercontent.com/bitcoin/bitcoin/master/src/kernel/chainparams.cpp; блок 968 721 — API mempool.space, https://mempool.space/api/block-height/968721 (обращение 2026-09-26).

[233] Хеш первого блока: 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f (исходный код Bitcoin Core). Хеш блока 968 721: 00000000000000000000ed8d95f43f038858adab98f852a40b461624b6825d20 (mempool.space, 26.09.2026). Оба легко найти в любом обозревателе блоков.

[234] Blockstream Explorer API, блок 968 721, поле «difficulty» (https://blockstream.info/api/block/00000000000000000000ed8d95f43f038858adab98f852a40b461624b6825d20); CoinWarz, 132.76T на 26.09.2026 (https://www.coinwarz.com/bitcoin-difficulty); Bitcoin Wiki «Difficulty» (https://en.bitcoin.it/wiki/Difficulty). Внесено по фактчеку 27.09.2026 (reviews/02-factcheck.md, п. 1).

[235] Минимальная сложность, равная 1, соответствует порогу 0x00000000FFFF… — восьми шестнадцатеричным нулям (Bitcoin Wiki, «Difficulty»). Сложность блока 968 721 — 132 757 073 449 487,5 (Blockstream Explorer); сегодняшнему порогу соответствует около 19,7 шестнадцатеричного нуля. Сложность пересчитывается каждые 2016 блоков; свежее значение — в приложении Б.

[236] исходный код Bitcoin Core, src/kernel/chainparams.cpp (CMainParams): nPowTargetSpacing = 10 * 60; nPowTargetTimespan = 14 * 24 * 60 * 60; nSubsidyHalvingInterval = 210000, https://raw.githubusercontent.com/bitcoin/bitcoin/master/src/kernel/chainparams.cpp; Mastering Bitcoin, 3rd ed., гл. 12.

[237] расчёт исследователя по данным: chainparams.cpp (метка генезиса) и API mempool.space, https://mempool.space/api/v1/blocks (метка блока 968 721; обращение 2026-09-26).

Размер страницы тоже ограничен правилами[239], и на момент работы над книгой страницы заполнялись почти до края. Примерно раз в десять минут в тетрадку вшивают страницу около полутора мегабайт и нескольких тысяч строчек[240].[241]

Дворов в посёлке сто, все их знают наперечёт, и любой может обойти соседей и пересчитать. Точного числа узлов биткоина не знает никто. Независимые счётчики видят только узлы, которые принимают входящие соединения (в конце сентября 2026 года их насчитали около 25 тысяч[242]), а на деле узлов больше, и надёжной оценки, насколько больше, у меня нет.[243] Разрешения стать узлом тоже никто не выдаёт. Поэтому правило, по которому участники приходят к одной версии тетрадки, не может опираться на подсчёт голосов по головам, ведь тот, кто считает головы, должен знать, сколько их. Накамото обошёл эту трудность другим способом, и к нему мы придём дальше.

По статье Накамото, сеть работает так: новые транзакции рассылаются всем узлам; майнеры собирают их в блок и ищут для него доказательство работы; найденный блок рассылается всем; узел принимает блок, только если все транзакции в нём действительны и не потрачены раньше, и выражает согласие тем, что начинает собирать следующий блок поверх отпечатка принятого[244].[245]

Узлы не голосуют, каждый проверяет сам.

Блок с приписанными из воздуха монетами честный узел отбросит, сколько бы работы на него ни потратили, потому что сверяет с правилами каждую транзакцию в нём[246]. Этими же проверками ловится двойная трата, из-за которой в первой главе понадобился хранитель. Если строчка пекаря для доярки уже вшита в тетрадку, попытка отдать то же право лесорубу не пройдёт ни у одного честного узла[247]. Открытыми остаются вопросы о правиле согласия: что делать, если две честные страницы найдены почти одновременно и узлы разошлись в том, какая была первой, и можно ли переписать тетрадку, собрав больше половины всей вычислительной мощности сети.

---

[238] От первого блока (3 января 2009 года) до блока 968 721 (26 сентября 2026 года) прошло около 6475 суток, в среднем примерно 9,6 минуты на блок, чуть быстрее цели. 26 сентября 2026 года два соседних блока пришли с разницей в 8 секунд, а между другими проходило по 15–30 минут (расчёт по данным mempool.space).

[239] BIP-141 «Segregated Witness (Consensus layer)», Lombrozo E., Lau J., Wuille P., created 21.12.2015, https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki; дата и блок активации — Trezor Blog, «SegWit and its legacy: Taproot, UASFs and Lightning», https://trezor.io/blog/insights/segwit-and-its-legacy-taproot-uasfs-and-lightning.

[240] API mempool.space, https://mempool.space/api/v1/blocks (обращение 2026-09-26).

[241] До 2017 года блок не мог быть больше миллиона байт; обновление SegWit, активированное в августе 2017 года, заменило этот предел ограничением на «вес» блока в 4 млн единиц (вес — условная мера, в которой разные части транзакции считаются с разными коэффициентами) (BIP-141 «Segregated Witness (Consensus layer)», Lombrozo E., Lau J., Wuille P., created 21.12.2015, https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki; дата и блок активации — Trezor Blog, «SegWit and its legacy: Taproot, UASFs and Lightning», https://trezor.io/blog/insights/segwit-and-its-legacy-taproot-uasfs-and-lightning). Из 15 блоков, найденных подряд 26 сентября 2026 года (968 712–968 726, mempool.space), у 14 вес стоял у самой границы, размер был от 1,44 до 1,73 МБ и в каждом лежало от 2962 до 7256 транзакций; один блок (968 718) был почти пуст — 24 транзакции, 6904 байта. Размер блоков и число узлов меняются каждый день; свежие цифры — в приложении Б.

[242] BTC Nodes (Bitnodes), https://btcnodes.io/; API снимка: https://btcnodes.io/api/v1/snapshots/latest/ (обращение 2026-09-26; старый адрес bitnodes.io перенаправляет туда). Оператор — Rodrigo Martínez.

[243] Краулер BTC Nodes, 26.09.2026: 25 284 достижимых узла, больше всего в США и Германии. Узлы, которые не принимают входящих соединений, в этот счёт не попадают. Свежие цифры — в приложении Б.

[244] Nakamoto, 2008, раздел 5 «Network», https://bitcoin.org/bitcoin.pdf.

[245] Nakamoto, 2008, section 5: «Nodes accept the block only if all transactions in it are valid and not already spent.»

[246] Nakamoto, 2008, раздел 5 «Network», https://bitcoin.org/bitcoin.pdf.

[247] Nakamoto, 2008, раздел 5 «Network», https://bitcoin.org/bitcoin.pdf.

Кто вправе потратить строчку

Половина устройства собрана. Страницы сшиты отпечатками, каждая новая страница стоит работы, и каждый узел сам проверяет каждую запись. Вместе это и делает тайную правку задним числом практически невозможной[248].

Отпечатки защищают тетрадку от переписывания, но ничего не говорят о том, кому принадлежит строчка. В посёлке с хранителем это решал хранитель. Пекарь приходил сам, и хранитель узнавал его в лицо. В тетрадке без хранителя лица нет. Есть только числа.

Эти числа называются ключами, и их всегда два. Закрытый ключ биткоина — это случайно выбранное число от нуля до величины чуть меньше 2^{256}, примерно $1{,}16 \times 10^{77}$[249]. Авторы «Mastering Bitcoin» для сравнения приводят оценку, по которой в видимой Вселенной около 10^{80} атомов[250].[251] Угадать чужое число в таком пространстве невозможно, если оно выбрано действительно случайно. Слабые генераторы случайных чисел и ключи, придуманные «из головы», — отдельная история, и до неё мы дойдём, когда будем говорить о безопасности[252].

Из закрытого ключа по особой формуле вычисляется публичный, и вычисление это работает в одну сторону. Из закрытого ключа публичный получить можно, из публичного закрытый нельзя[253]. «Нельзя» здесь означает, что современным компьютерам на это не хватит никакого разумного времени[254]. (Угроза от квантовых компьютеров — отдельный спор, к нему я вернусь в последней главе.)

Подпись мы разобрали в первой главе. Подписывает владелец закрытого ключа, а проверить подпись может любой, не зная самого ключа. Для тетрадки без хранителя в ней важнее всего две черты. Цифровая подпись своя для каждой записи, потому что подписывают отпечаток самой записи[255]. Подпись под строчкой «10 доярке» не подойдёт к строчке «100 доярке», и перенести её под другую запись нельзя[256] (подпись на бумаге одна на все документы, и умелый человек её перерисует). А проверяют её публичным ключом, в котором нет ничьего имени. Каждый может проверить каждую подпись в каждой транзакции, а создать действительную подпись может только владелец закрытого ключа[257].[258][259]

В первой главе я сказал, что строчка в биткоине принадлежит владельцу ключа. Теперь это можно уточнить. Монета у Накамото — та самая цепочка подписей из первой главы: каждый владелец передаёт её следующему, подписывая перевод на публичный ключ нового вла-

---

[248] Nakamoto, 2008, раздел 4 «Proof-of-Work», https://bitcoin.org/bitcoin.pdf; Nakamoto, 2008, раздел 5 «Network», https://bitcoin.org/bitcoin.pdf.

[249] Mastering Bitcoin, 3rd ed., 2023, гл. 4 «Keys and Addresses», https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch04_keys.adoc.

[250] Mastering Bitcoin, 3rd ed., 2023, гл. 4 «Keys and Addresses», https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch04_keys.adoc.

[251] Mastering Bitcoin, 3rd ed., ch. 4: «The size of Bitcoin's private key space (2^{256}) is an unfathomably large number. It is approximately 10^{77} in decimal. For comparison, the visible universe is estimated to contain 10^{80} atoms.»

[252] Mastering Bitcoin, 3rd ed., 2023, гл. 4 «Keys and Addresses», https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch04_keys.adoc.

[253] Mastering Bitcoin, 3rd ed., 2023, гл. 4.

[254] Mastering Bitcoin, 3rd ed., 2023, гл. 4.

[255] Nakamoto, 2008, раздел 2 «Transactions», https://bitcoin.org/bitcoin.pdf.

[256] Mastering Bitcoin, 3rd ed., 2023, гл. 4.

[257] Mastering Bitcoin, 3rd ed., 2023, гл. 4.

[258] Там же: «…anyone to verify every signature on every transaction, while ensuring that only the owners of private keys can produce valid signatures.»

[259] Технически биткоин долго использовал подписи ECDSA на эллиптической кривой secp256k1; предложение BIP-340 (2020) ввело подписи Шнорра на той же кривой (BIP-340 «Schnorr Signatures for secp256k1», https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki). Для механизма этой главы разница между ними не важна.

дельца[260]. Поэтому строчка в тетрадке биткоина говорит примерно следующее: «10 единиц может потратить тот, кто предъявит подпись, которую проверяет вот этот публичный ключ». Имени в строчке нет. Пекарь в такой тетрадке — просто тот, у кого есть закрытый ключ, и никто, включая сеть, не проверяет, пекарь ли он.

Украсть строчку в такой тетрадке значит скопировать чужой ключ. Кошелёк в кармане пропадает, и вы это замечаете. Скопированный ключ остаётся и у вас, и о краже вы узнаете только тогда, когда вор подпишет перевод, а его подпись сеть примет так же, как вашу, потому что проверяет она только подпись[261]. Отменить такой перевод некому, как некому было бы отменить и ваш собственный.

Публичный ключ в тетрадку обычно тоже не пишут целиком. Туда пишут адрес, короткий отпечаток публичного ключа. «Старые» адреса начинаются с единицы и получаются двойным хешированием ключа с особой кодировкой, а современные начинаются с «bc1»[262]. Адрес можно спокойно раздавать, как номер для переводов, потому что отпечаток обратно не разворачивается и ключа по нему не узнать[263].

Подпись доказывает, кто распорядился строчкой, но ничего не прячет. Транзакцию подписывают и рассылают всем узлам в открытом виде[264], и из этой простой детали вырастает всё, что будет сказано ниже о следах.

Что лежит в кошельке

Если строчки тетрадки принадлежат ключам, то что такое криптовалютный кошелёк? Ответ в «Mastering Bitcoin» короткий. То, что многие называют кошельком биткоина, содержит только ключи, а сами монеты записаны в блокчейне[265].[266] Приложение в телефоне — это связка ключей и программа, которая читает тетрадку, находит в ней строчки, которые эти ключи могут потратить, и подписывает новые.

Откуда такая программа знает, что платёж настоящий? Полный узел, то есть узел со всей тетрадкой, проверяет всё сам, но держать всю тетрадку в телефоне неудобно, и Накамото предусмотрел упрощённую проверку. Пользователь хранит только заголовки самой длинной цепочки и получает ветку дерева Меркла, которая связывает его транзакцию с блоком[267]. Заголовки весят мало. При блоке раз в десять минут их цепочка, по расчёту Накамото, растёт на 4,2 МБ в год, и это помещалось даже в оперативную память компьютера 2008 года[268]. Такая проверка, писал Накамото, надёжна, пока сеть контролируют честные узлы, и уязвимее, если сеть захватил атакующий[269].[270] А предприятия, которые часто принимают платежи, по его словам, скорее всего, всё же захотят держать собственные узлы[271].

---

[260] Nakamoto, 2008, раздел 2 «Transactions», https://bitcoin.org/bitcoin.pdf.

[261] Mastering Bitcoin, 3rd ed., 2023, гл. 4.

[262] Mastering Bitcoin, 3rd ed., 2023, гл. 4.

[263] Mastering Bitcoin, 3rd ed., 2023, гл. 12; Mastering Bitcoin, 3rd ed., 2023, гл. 4.

[264] Nakamoto, 2008, раздел 2 «Transactions», https://bitcoin.org/bitcoin.pdf; Nakamoto, 2008, раздел 10 «Privacy», https://bitcoin.org/bitcoin.pdf.

[265] Mastering Bitcoin, 3rd ed., 2023, гл. 5 «Wallet Recovery», https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch05_wallets.adoc.

[266] Mastering Bitcoin, 3rd ed., ch. 5: «In fact, what many people call a Bitcoin wallet—which we call a wallet database to distinguish it from wallet applications—contains only keys»; «Those keys are associated with bitcoins recorded on the blockchain.»

[267] Nakamoto, 2008, раздел 8 «Simplified Payment Verification», https://bitcoin.org/bitcoin.pdf.

[268] Satoshi Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System», 2008, раздел 7 «Reclaiming Disk Space», https://bitcoin.org/bitcoin.pdf.

[269] Nakamoto, 2008, раздел 8 «Simplified Payment Verification», https://bitcoin.org/bitcoin.pdf.

[270] Nakamoto, 2008, section 8: «As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker.»

Выходит, что владелец лёгкого кошелька снова кому-то доверяет. Хранителя у него нет, зато верить приходится честному большинству узлов и программе, которую он поставил себе в телефон. Из всех способов проверить платёж этот я бы не назвал самым надёжным.

Ещё дальше от тетрадки стоит тот, кто держит монеты на бирже. Ключ в этом случае у биржи, и в тетрадке монеты записаны за её ключами[272]. У клиента остаётся обещание биржи выдать их по первому требованию, то есть строчка в её собственной тетрадке. Биржа в этом случае — держатель чужих ключей, посредник того самого рода, от которого биткоин задумывали избавить, и дальше в книге мы увидим, как такие посредники подводили своих клиентов.

Ключей в кошельке много, и хранить каждый по отдельности неудобно. Поэтому в 2013 году появился стандарт BIP-39 (BIP — так в сообществе биткоина нумеруют предложения по улучшению). Одно случайное число, из которого выводятся все ключи кошелька, записывается последовательностью слов из словаря в 2048 слов: 12 слов для 128 бит случайности и 24 слова для 256 бит[273]. Эти 12–24 слова кошелёк показывает при создании[274]. Вывод отсюда жёсткий. Фраза из слов — это всё, чем вы владеете в этой тетрадке. Кто её знает, тот и владеет, а кто потерял её и не сохранил копии, тот больше не владеет ничем.

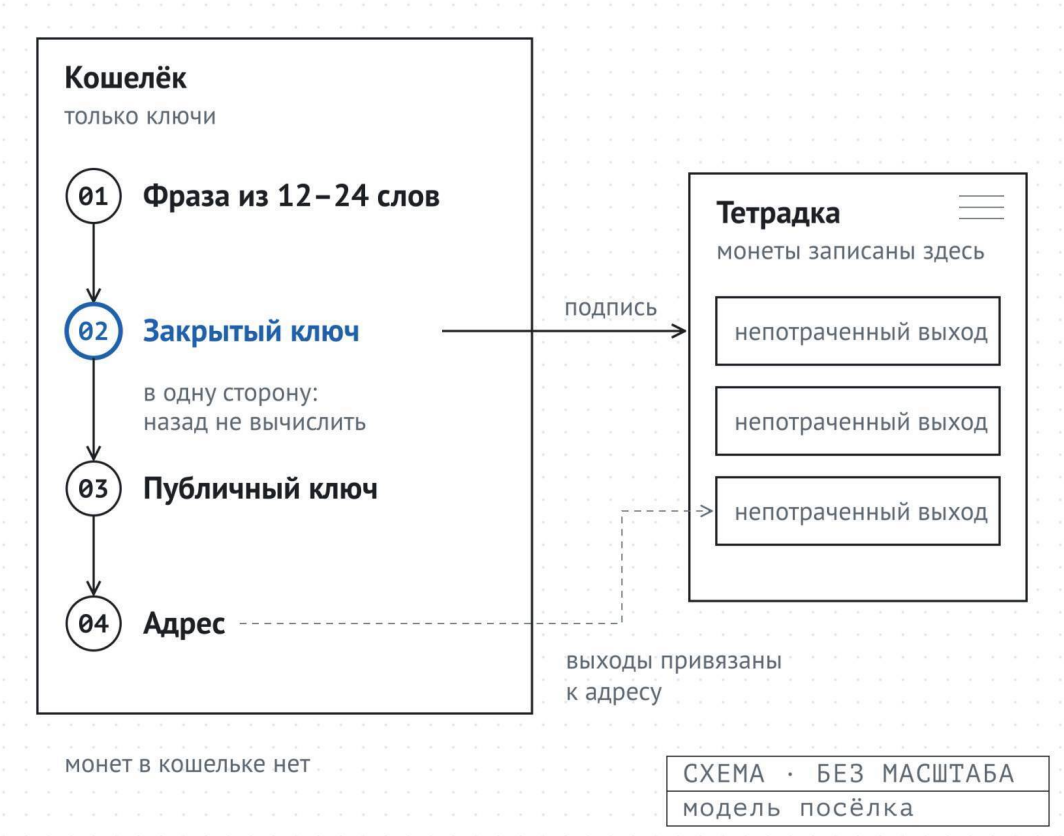


Рисунок 2.3. Что лежит в кошельке

[271] Nakamoto, 2008, раздел 8 «Simplified Payment Verification», https://bitcoin.org/bitcoin.pdf.

[272] Mastering Bitcoin, 3rd ed., 2023, гл. 5 «Wallet Recovery», https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch05_wallets.adoc.

[273] BIP-39 «Mnemonic code for generating deterministic keys», Palatinus M., Rusnak P., Voisine A., Bowe S., created 10.09.2013, https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki; Mastering Bitcoin, 3rd ed., гл. 5.

[274] BIP-39 «Mnemonic code for generating deterministic keys», Palatinus M., Rusnak P., Voisine A., Bowe S., created 10.09.2013, https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki; Mastering Bitcoin, 3rd ed., гл. 5.

С остатком на счёте всё устроено ещё непривычнее. В банковской выписке есть строка «остаток», и хочется думать, что в тетрадке биткоина против адреса тоже написано «1 BTC». Там такой записи нет. Счетов и хранимых остатков в биткоине нет вообще. Каждая транзакция создаёт выходы, то есть строчки с суммой и условием, каким ключом её можно потратить. Каждый полный узел держит перечень непотраченных выходов (по-английски UTXO), а остаток, который показывает приложение, программа вычисляет сама, складывая выходы, которые могут потратить её ключи[275].

В тетрадке посёлка это значит, что строки «у пекаря 16» в ней нет. Есть отдельные строчки, и в каждой написано, сколько единиц и какой ключ может их потратить (здесь 10, там 6), и обе можно потратить ключом пекаря. Когда строчку тратят, её вычёркивают целиком и пишут новые. Такое устройство упрощает главную проверку. Чтобы поймать двойную трату, узлу не нужно пересчитывать ничей остаток, достаточно посмотреть, есть ли выход, на который ссылается транзакция, в перечне непотраченных[276].

Выход проще всего представить как купюру определённого номинала, которая тратится только целиком[277]. Допустим, у вас есть один выход на 1 BTC, а заплатить нужно 0,3 BTC (числа условные и круглые). Ваша транзакция сошлётся на этот выход (такую ссылку называют входом), израсходует его весь и создаст два новых: 0,3 BTC получателю и сдачу вам. Накамото описал это в разделе 9 статьи. Обычно, по его словам, у транзакции либо один крупный вход, либо несколько мелких, а выходов не больше двух, платёж и сдача[278].

Где же комиссия майнеру? Отдельной строкой она нигде не записана. Это разница между суммой входов и суммой выходов транзакции[279]. Если в нашем примере вы создадите выходы на 0,3 BTC и 0,6999 BTC, майнер получит 0,0001 BTC. А если забудете про сдачу и создадите только выход на 0,3 BTC, остальные 0,7 BTC тоже достанутся майнеру, и спросить их будет не с кого[280]. Такую арифметику делает за вас программа кошелька, но знать механизм полезно, потому что в тетрадке без хранителя ошибку в расчёте исполнят так же точно, как правильный расчёт.

Платить комиссию заставляет теснота. Страница ограничена по размеру и заполняется почти до края[281], а майнер получает комиссии со всех строчек, которые включил в свою страницу[282]. Когда желающих больше, чем мест, ему выгоднее взять строчки, за которые оставили больше, и строчка без комиссии рискует ждать своей очереди долго.

Считает программа в целых числах самой мелкой единицы. В одном биткоине 100 млн сатоши, и меньше одного сатоши в транзакции записать нельзя[283]. Эта деталь пригодится нам в последнем разделе.

В Ethereum, для сравнения, есть аккаунты с остатком, похожие на счета, и одними управляет закрытый ключ, другими — программный код[284]. К ним мы придём в главе 4.

---

[275] Mastering Bitcoin, 3rd ed., 2023, гл. 6 «Transactions», https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch06_transactions.adoc.

[276] Mastering Bitcoin, 3rd ed., 2023, гл. 6 «Transactions», https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch06_transactions.adoc; Nakamoto, 2008, раздел 5 «Network», https://bitcoin.org/bitcoin.pdf.

[277] Nakamoto, 2008, раздел 9 «Combining and Splitting Value», https://bitcoin.org/bitcoin.pdf; Mastering Bitcoin, 3rd ed., гл. 6.

[278] Nakamoto, 2008, раздел 9 «Combining and Splitting Value», https://bitcoin.org/bitcoin.pdf; Mastering Bitcoin, 3rd ed., гл. 6.

[279] Nakamoto, 2008, раздел 6 «Incentive»; Mastering Bitcoin, 3rd ed., гл. 6.

[280] Nakamoto, 2008, раздел 6 «Incentive»; Mastering Bitcoin, 3rd ed., гл. 6.

[281] BIP-141 «Segregated Witness (Consensus layer)», Lombrozo E., Lau J., Wuille P., created 21.12.2015, https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki; дата и блок активации — Trezor Blog, «SegWit and its legacy: Taproot, UASFs and Lightning», https://trezor.io/blog/insights/segwit-and-its-legacy-taproot-uasfs-and-lightning; API mempool.space, https://mempool.space/api/v1/blocks (обращение 2026-09-26).

[282] Nakamoto, 2008, раздел 6 «Incentive»; Mastering Bitcoin, 3rd ed., гл. 6.

[283] Mastering Bitcoin, 3rd ed., гл. 6.

[284] ethereum.org, «Ethereum accounts», https://ethereum.org/en/developers/docs/accounts/; «Blocks», https://ethereum.org/en/

Проследим один платёж от начала до конца. Допустим, вы платите знакомому 0,3 BTC с того самого выхода в 1 BTC (пример условный).

Программа кошелька находит в тетрадке выход, который может потратить ваш ключ, и составляет транзакцию: вход ссылается на этот выход, один новый выход на 0,3 BTC ведёт на адрес знакомого, другой, со сдачей, на ваш свежий адрес, а разница между входом и выходами остаётся майнеру[285].

Программа подписывает транзакцию вашим закрытым ключом. Ключ из телефона никуда не уходит, уходит только подпись[286].

Транзакция рассылается всем узлам, и каждый проверяет, что подпись действительна, а выход, на который она ссылается, ещё не потрачен[287].

Майнер включает транзакцию в свой будущий блок. Она становится листом дерева Меркла, её хеш входит в корень, корень — в заголовок[288].

Майнер перебирает nonce, пока отпечаток заголовка не окажется ниже порога, и рассылает найденный блок[289].

Узлы проверяют блок целиком и начинают строить следующий поверх его отпечатка. Ваш выход в 1 BTC исчезает из их перечня непотраченных, а два новых в нём появляются[290].

С каждым следующим блоком переписать вашу транзакцию становится дороже[291].

Ни на одном шаге не участвует никто, кто знал бы ваше имя, и ни на одном шаге биткоины не «переезжают» из одного кошелька в другой. Меняется только перечень выходов в тетрадке, и в нём появляется строчка, которую может потратить ключ вашего знакомого.

Сборку полезно проверить на прочность тем же способом, каким мы собирали посёлок, только в обратную сторону: убирать по одной детали и смотреть, что сломается.

Без отпечатков в заголовках страницы ничем не связаны, и любой двор может тихо поправить свою копию, а спор о том, чья копия верна, решать будет нечем.

Без доказательства работы отпечатки остаются, но пересчитать их после правки стоит секунды, и переписанная тетрадка выглядит не хуже честной.

Без проверки каждым узлом майнер мог бы вшить в страницу строчку, которой не было, или потратить чужой выход, и остальным пришлось бы ему верить. Он стал бы хранителем.

Без подписей любой мог бы составить строчку, которая отдаёт чужие монеты ему, и узнать, кто её написал, было бы нечем.

Каждая деталь закрывает свою дыру, и ни одна не закрывает чужую. Поэтому вопрос «надёжен ли блокчейн» я советую всякий раз уточнять вопросом, о какой детали речь и против чего она защищает.

---

developers/docs/blocks/.

[285] Mastering Bitcoin, 3rd ed., 2023, гл. 6 «Transactions», https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch06_transactions.adoc; Nakamoto, 2008, раздел 9 «Combining and Splitting Value», https://bitcoin.org/bitcoin.pdf; Mastering Bitcoin, 3rd ed., гл. 6; Nakamoto, 2008, раздел 6 «Incentive»; Mastering Bitcoin, 3rd ed., гл. 6.

[286] Mastering Bitcoin, 3rd ed., 2023, гл. 4.

[287] Nakamoto, 2008, раздел 5 «Network», https://bitcoin.org/bitcoin.pdf.

[288] Nakamoto, 2008, раздел 7 «Reclaiming Disk Space», https://bitcoin.org/bitcoin.pdf; идея дерева — R. C. Merkle, «Protocols for public key cryptosystems», Proc. 1980 Symposium on Security and Privacy, IEEE, pp. 122–133 (ссылка [7] белой книги).

[289] Nakamoto, 2008, раздел 4; Bitcoin Developer Reference, «Block Chain»; Nakamoto, 2008, раздел 5 «Network», https://bitcoin.org/bitcoin.pdf.

[290] Mastering Bitcoin, 3rd ed., 2023, гл. 6 «Transactions», https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch06_transactions.adoc; Nakamoto, 2008, раздел 5 «Network», https://bitcoin.org/bitcoin.pdf.

[291] Nakamoto, 2008, раздел 4 «Proof-of-Work», https://bitcoin.org/bitcoin.pdf.

Всё на виду, кроме имён

Анонимен ли биткоин? В первой главе я обещал вернуться к строчке из анонса Накамото, где говорилось, что участники могут быть анонимны.

Статья осторожнее анонса. В разделе о приватности Накамото строит её на том, что публичные ключи не связаны с личностями. Все транзакции объявляются открыто, и посторонние видят, что кто-то отправил сумму кому-то, но не видят, кто и кому[292].[293] Он сравнивает это с лентой фондовой биржи, где время и объём сделок публичны, а стороны нет[294].

Открытость здесь заложена в саму конструкцию, и причина нам знакома по первой главе. Там Накамото объяснял, что убедиться в отсутствии двойной траты можно, только зная обо всех транзакциях, и поэтому транзакции нужно объявлять публично[295]. Хранитель знает всё, а посторонние не знают ничего, и тайна вкладов держится на том, что тетрадку видит только он. Если хранителя убрать, тетрадку должны видеть все, иначе двойную трату ловить некому. Прятать записи стало нельзя, и приватность пришлось перенести с записей на имена.

Там же Накамото называет и слабые места. Он советует заводить новую пару ключей для каждой транзакции и признаёт, что транзакции с несколькими входами всё равно раскрывают общего владельца, а если раскрыт владелец одного ключа, по связям можно раскрыть и другие его транзакции[296]. Так что миф об анонимности биткоина держится скорее на строчке из анонса, чем на самой статье.

Допустим, вы выложили в сеть один адрес для пожертвований и годами получаете на него деньги. Любой, кто откроет этот адрес, увидит каждый платёж, его сумму и время, сложит их и узнает, сколько вы получили, а заодно увидит, куда вы эти деньги потом отправляли[297]. Новый адрес для каждого платежа делает такую картину труднее для чтения, но, как признавал сам Накамото, связать адреса одного владельца всё равно можно[298].

Точное слово для того, что описал Накамото, — псевдонимность: имени в тетрадке нет, но каждый шаг каждого псевдонима записан навсегда и виден всем.

Посёлок показывает, как псевдоним превращается в имя. Допустим, в тетрадке вместо имён стоят номера, и пекарь для каждой строчки берёт новый номер. Однажды ему нужно заплатить 10, а на одном его номере 6 и на другом 4. Он подписывает платёж сразу двумя номерами, и с этой минуты весь посёлок знает, что оба номера принадлежат одному человеку. Сдачу он получает на свежий номер, но соседи могут догадаться, какой из новых номеров — сдача, и приписать пекарю и его, ведь сдача возвращается тому, кто платил. А если однажды он купил молоко у доярки, которая знает его в лицо, то имя получает весь связанный клубок номеров сразу.

В 2013 году группа исследователей, в основном из Калифорнийского университета в Сан-Диего, проделала это на настоящей тетрадке[299].[300] Они взяли все транзакции биткоина к

---

[292] Nakamoto, 2008, раздел 10 «Privacy», https://bitcoin.org/bitcoin.pdf.

[293] Nakamoto, 2008, section 10: «The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone»; «Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner.»

[294] Nakamoto, 2008, раздел 10 «Privacy», https://bitcoin.org/bitcoin.pdf.

[295] Nakamoto, 2008, раздел 2, https://bitcoin.org/bitcoin.pdf.

[296] Nakamoto, 2008, раздел 10 «Privacy», https://bitcoin.org/bitcoin.pdf.

[297] Nakamoto, 2008, раздел 10 «Privacy», https://bitcoin.org/bitcoin.pdf.

[298] Nakamoto, 2008, раздел 10 «Privacy», https://bitcoin.org/bitcoin.pdf.

[299] Meiklejohn S., Pomarole M., Jordan G., Levchenko K., McCoy D., Voelker G. M., Savage S. «A Fistful of Bitcoins: Characterizing Payments Among Men with No Names». IMC '13, 2013. https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf; DOI 10.1145/2504730.2504747.

[300] Meiklejohn S., Pomarole M., Jordan G., Levchenko K., McCoy D., Voelker G. M., Savage S. A Fistful of Bitcoins:

апрелю 2013 года и применили к ним два правила из нашего посёлка: правило общих входов («ключи, подписавшие одну транзакцию, принадлежат одному владельцу») и правило адреса сдачи. Такое склеивание адресов в группы называют кластеризацией, и в этой работе она свела около 12 млн публичных ключей к 3,4 млн групп[301].

Дальше группам нужно было дать имена, и исследователи просто стали покупать. Они платили биржам, онлайн-кошелькам, магазинам и игорным сайтам, заказывали в том числе кофе, серебряные монеты и кепку, и каждая покупка помечала адрес продавца[302]. Кластеризация разнесла эти метки по группам, и в итоге авторы назвали владельцев групп, в которых было больше 1,8 млн адресов[303].

Авторы не скрывают, что метод небезупречен. Правило общих входов следует из самого устройства транзакций и почти не ошибается. Правило сдачи опирается на привычки программ-кошельков: его первая версия дала 13% ложных срабатываний, а после доработки всё равно слепила ложную «сверхгруппу» из 1,6 млн ключей, так что правило пришлось уточнять ещё раз[304]. Главный вывод статьи от этого не меняется. Деньги в биткоине сходятся к крупным сервисам, прежде всего к биржам, и ведомство, которое может затребовать у этих сервисов данные клиентов, сумеет выяснить, кто кому платит; поэтому авторы сочли биткоин непривлекательным для отмывания денег в больших масштабах[305].

След остаётся и в самой сети. В 2014 году исследователи показали, что псевдоним можно связать с IP-адресом компьютера, с которого рассылают транзакции, и для этого хватает нескольких машин[306].[307] Сетевую часть биткоина с тех пор меняли, и я не знаю, работает ли эта атака сегодня[308].

Теми же правилами пользуются и коммерческие аналитики, например компания Chainalysis[309].[310] Надёжность их выводов проверял американский суд. Романа Стерлингова обвиняли в том, что он держал биткоин-миксер Bitcoin Fog, сервис, который перемешивает монеты разных клиентов, чтобы запутать след[311]. Защита называла программу Chainalysis

---

Characterizing Payments Among Men with No Names. IMC '13, 2013 (один из авторов, Д. Маккой, — из Университета Джорджа Мейсона). Данные на 13 апреля 2013 года: 231 207 блоков, 16 086 073 транзакции, 12 056 684 публичных ключа; 5 579 176 групп по правилу общих входов и 3 383 904 — после правила сдачи. Исследователи совершили 344 транзакции (в том числе с Mt. Gox и Silk Road), вручную пометили 1070 адресов и назвали владельцев 2197 групп (Meiklejohn et al., 2013, разделы 3.1 и 4.5). Пользователей биткоина авторы называют «pseudo-anonymous».

[301] Meiklejohn S., Pomarole M., Jordan G., Levchenko K., McCoy D., Voelker G. M., Savage S. «A Fistful of Bitcoins: Characterizing Payments Among Men with No Names». IMC '13, 2013. https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf; DOI 10.1145/2504730.2504747.

[302] Meiklejohn et al., 2013, разделы 3.1 и 4.5.

[303] Meiklejohn et al., 2013, разделы 3.1 и 4.5.

[304] Meiklejohn S., Pomarole M., Jordan G., Levchenko K., McCoy D., Voelker G. M., Savage S. «A Fistful of Bitcoins: Characterizing Payments Among Men with No Names». IMC '13, 2013. https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf; DOI 10.1145/2504730.2504747.

[305] Meiklejohn et al., 2013, разделы 3.1 и 4.5.

[306] Biryukov A., Khovratovich D., Pustogarov I. «Deanonymisation of clients in Bitcoin P2P network». arXiv:1405.7418, 2014 (опубл. ACM CCS 2014). https://arxiv.org/abs/1405.7418.

[307] Biryukov A., Khovratovich D., Pustogarov I. Deanonymisation of clients in Bitcoin P2P network. ACM CCS 2014 (arXiv:1405.7418): «…link user pseudonyms to the IP addresses where the transactions are generated.»

[308] Biryukov A., Khovratovich D., Pustogarov I. «Deanonymisation of clients in Bitcoin P2P network». arXiv:1405.7418, 2014 (опубл. ACM CCS 2014). https://arxiv.org/abs/1405.7418.

[309] Chainalysis, «The Data Accuracy Flywheel: How Chainalysis Consistently Identifies and Verifies Blockchain Entities», 16.01.2024, https://www.chainalysis.com/blog/chainalysis-data-accuracy/.

[310] Chainalysis. The Data Accuracy Flywheel, 16.01.2024: «Co-spend identifies co-ownership of addresses by identifying Unspent Transaction Outputs (UTXOs) that are spent as inputs in the same transaction.» Заявления компании о точности своих выводов — её собственные; методика закрыта.

[311] Cointelegraph, «Founder of Bitcoin Fog crypto mixer sentenced to 12.5 years in jail», 11.2024, https://cointelegraph.com/news/crypto-mixer-bitcoin-fog-roman-sterlingov-founder-prison-sentence-united-states-doj; The Register, 11.11.2024, https://www.theregister.com/2024/11/11/bitcoin_fog_sentencing.

Reactor «лженаукой» без рецензирования и без известного уровня ошибок. В феврале 2024 года судья Рэндолф Мосс признал, что не все правила программы прошли рецензирование и учёта ошибок компания не ведёт, но счёл программу надёжной и допустил её выводы к присяжным[312].[313]

В том же решении судья назвал транзакции биткоина одновременно исключительно анонимными и исключительно публичными и оговорил, что выводы программы можно проверить вручную по открытому блокчейну, с блокнотом, карандашом и несколькими часами работы[314]. Присяжные признали Стерлингова виновным, его приговорили к 12,5 года заключения[315], а 25 сентября 2026 года апелляционный суд оставил приговор в силе и не нашёл ошибок в том, как районный суд допустил экспертные доказательства[316].

Решение судьи касается того, можно ли показывать такие доказательства присяжным. Научной проверкой точности метода не было ни оно, ни апелляция, и сторонники Стерлингова после приговора называли его основанным на лженауке[317]. Суды этот спор решили, а вопрос о том, как часто ошибается кластеризация, остаётся открытым.

Два дела показывают, как след доводит следствие до самих денег. В первом 8 мая 2021 года американская компания Colonial Pipeline заплатила группе вымогателей DarkSide выкуп примерно в 75 BTC[318]. 7 июня Министерство юстиции США объявило, что изъяло из них 63,7 BTC. По тексту заявления, следствие изучило публичный реестр биткоина, проследило несколько переводов и установило, что монеты переведены на адрес, закрытый ключ от которого есть у ФБР[319].[320] Как ФБР получило ключ, не сказано ни в заявлении, ни в документах суда[321].

---

[312] United States v. Sterlingov, Criminal Action No. 21-399 (RDM), Memorandum Opinion and Order, Document 259, filed 29.02.2024, U.S. District Court for the District of Columbia; PDF: https://www.moneylaunderingnews.com/wp-content/uploads/sites/12/2024/03/District_of_Columbia_USA_v._STERLINGOV_Memo_Opinion_and_Order.pdf.

[313] United States v. Sterlingov, No. 21-cr-399 (RDM), Memorandum Opinion and Order, D.D.C., 29.02.2024, p. 3: «…substantial evidence supports the government's submission that the software is highly reliable—and, if anything, conservative—in clustering (and then attributing) bitcoin addresses.» На с. 2: «bitcoin transactions are both uniquely anonymous and uniquely public». По данным обвинения, через Bitcoin Fog с 2011 по 2021 год прошло около 1,2 млн BTC. Присяжные вынесли вердикт 12.03.2024; приговор (ноябрь 2024 года) — по сообщениям СМИ со ссылкой на Министерство юстиции. Апелляция: United States v. Sterlingov, No. 24-3161 (D.C. Cir.), 25.09.2026 — приговор оставлен в силе. Подробности решения и статус возможной петиции в Верховный суд — в приложении Б.

[314] United States v. Sterlingov, Criminal Action No. 21-399 (RDM), Memorandum Opinion and Order, Document 259, filed 29.02.2024, U.S. District Court for the District of Columbia; PDF: https://www.moneylaunderingnews.com/wp-content/uploads/sites/12/2024/03/District_of_Columbia_USA_v._STERLINGOV_Memo_Opinion_and_Order.pdf.

[315] Cointelegraph, «Founder of Bitcoin Fog crypto mixer sentenced to 12.5 years in jail», 11.2024, https://cointelegraph.com/news/crypto-mixer-bitcoin-fog-roman-sterlingov-founder-prison-sentence-united-states-doj; The Register, 11.11.2024, https://www.theregister.com/2024/11/11/bitcoin_fog_sentencing.

[316] Law360, 25.09.2026, «DC Circ. Backs Bitcoin Fog Crypto Mixer Conviction» (https://www.law360.com/appellate/articles/2530252); MLex, 25.09.2026 (https://www.mlex.com/mlex/financial-crime/articles/2530292); карточка решения: https://law.justia.com/cases/federal/appellate-courts/cadc/24-3161/24-3161-2026-09-25.html.

[317] Cointelegraph, «Founder of Bitcoin Fog crypto mixer sentenced to 12.5 years in jail», 11.2024, https://cointelegraph.com/news/crypto-mixer-bitcoin-fog-roman-sterlingov-founder-prison-sentence-united-states-doj; The Register, 11.11.2024, https://www.theregister.com/2024/11/11/bitcoin_fog_sentencing.

[318] U.S. Department of Justice, Office of Public Affairs, «Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside», 07.06.2021, https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside; дубль: https://www.justice.gov/usao-ndca/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists.

[319] U.S. Department of Justice, Office of Public Affairs, «Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside», 07.06.2021, https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside; дубль: https://www.justice.gov/usao-ndca/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists.

[320] U.S. Department of Justice. Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside, 07.06.2021: «By reviewing the Bitcoin public ledger, law enforcement was able to track multiple transfers of bitcoin and identify that approximately 63.7 bitcoins, representing the proceeds of the victim's ransom payment, had been transferred to a specific address, for which the FBI has the „private key"…» Изъятые монеты стоили около 2,3 млн долларов, меньше, чем выкуп в

Проследить деньги позволила открытая тетрадка, а забрать их — ключ. Без ключа следствие видело бы монеты на адресе, но сдвинуть их не смогло бы.

Второе дело длиннее. В 2016 году биржу Bitfinex взломали и вывели с неё 119 754 BTC[322]. Бóльшая часть украденных монет почти шесть лет пролежала в кошельке, адреса которого видел весь мир[323]. Каждый, кто открывал эти адреса в обозревателе блоков, мог убедиться, что монеты на месте, и любой их сдвиг был бы виден так же открыто. В феврале 2022 года Министерство юстиции объявило об аресте Ильи Лихтенштейна и Хизер Морган по обвинению в сговоре с целью отмывания этих денег и об изъятии больше 94 000 BTC[324].[325] Изъятие и здесь прошло через ключ, а файлы с ключами следствие нашло в онлайн-аккаунте Лихтенштейна[326]. Во взломе его тогда не обвиняли, и признал он его сам в августе 2023 года, когда оба признали вину в сговоре с целью отмывания[327].

день оплаты, потому что курс биткоина за месяц упал. По оценке аналитической компании Elliptic, 63,7 BTC были долей исполнителя атаки, около 85% выкупа, а остальное ушло разработчикам программы-вымогателя (Krebs B. «Justice Dept. Claws Back $2.3M Paid by Colonial Pipeline to Ransomware Gang», Krebs on Security, 06.2021, https://krebsonsecurity.com/2021/06/justice-dept-claws-back-2-3m-paid-by-colonial-pipeline-to-ransomware-gang/ (цитирует заявление Минюста); первоисточник — выступление замдиректора ФБР П. Эббейта 7 июня 2021 г., https://www.fbi.gov/news/press-releases/fbi-deputy-director-paul-abbates-remarks-at-press-conference-regarding-the-ransomware-attack-on-colonial-pipeline).

[321] U.S. Department of Justice, Office of Public Affairs, «Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside», 07.06.2021, https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside; дубль: https://www.justice.gov/usao-ndca/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists.

[322] U.S. DOJ / IRS-CI, «Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency», 08.02.2022, копия на сайте IRS: https://www.irs.gov/zh-hant/compliance/criminal-investigation/two-arrested-for-alleged-conspiracy-to-launder-4-point-5-billion-in-stolen-cryptocurrency; оригинал: https://www.justice.gov/archives/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency (не открылся).

[323] U.S. DOJ / IRS-CI, «Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency», 08.02.2022, копия на сайте IRS: https://www.irs.gov/zh-hant/compliance/criminal-investigation/two-arrested-for-alleged-conspiracy-to-launder-4-point-5-billion-in-stolen-cryptocurrency; оригинал: https://www.justice.gov/archives/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency (не открылся).

[324] U.S. DOJ / IRS-CI, «Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency», 08.02.2022, копия на сайте IRS: https://www.irs.gov/zh-hant/compliance/criminal-investigation/two-arrested-for-alleged-conspiracy-to-launder-4-point-5-billion-in-stolen-cryptocurrency; оригинал: https://www.justice.gov/archives/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency (не открылся).

[325] U.S. DOJ / IRS-CI. Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency, 08.02.2022. Монеты вывели с биржи более чем 2000 несанкционированных транзакций; изъятые 94 000 BTC стоили около 3,6 млрд долларов на тот момент, и министерство назвало это крупнейшим финансовым изъятием в своей истории. Около 25 000 BTC к тому времени прошли через сложную схему отмывания, в том числе через обмен на монеты с усиленной анонимностью. Заместитель генерального прокурора Лиза Монако: «Cryptocurrency is not a safe haven for criminals» (U.S. DOJ / IRS-CI, «Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency», 08.02.2022, копия на сайте IRS: https://www.irs.gov/zh-hant/compliance/criminal-investigation/two-arrested-for-alleged-conspiracy-to-launder-4-point-5-billion-in-stolen-cryptocurrency; оригинал: https://www.justice.gov/archives/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency (не открылся)). В ноябре 2024 года Лихтенштейна приговорили к 60 месяцам заключения, Морган — к 18 месяцам (U.S. ICE / HSI (перепубликация релиза Минюста), «Bitfinex Hacker Sentenced in Money Laundering Conspiracy Involving Billions in Stolen Cryptocurrency», 20.11.2024, https://www.ice.gov/news/releases/bitfinex-hacker-sentenced-money-laundering-conspiracy-involving-billions-stolen; оригинал Минюста: https://www.justice.gov/usao-dc/pr/bitfinex-hacker-sentenced-money-laundering-conspiracy-involving-billions-stolen; приговор Морган — CoinDesk, 18.11.2024, https://www.coindesk.com/policy/2024/11/18/bitfinex-hack-launderer-heather-razzlekhan-morgan-sentenced-to-18-months-in-prison).

[326] U.S. DOJ / IRS-CI, «Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency», 08.02.2022, копия на сайте IRS: https://www.irs.gov/zh-hant/compliance/criminal-investigation/two-arrested-for-alleged-conspiracy-to-launder-4-point-5-billion-in-stolen-cryptocurrency; оригинал: https://www.justice.gov/archives/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency (не открылся).

[327] U.S. ICE / HSI (перепубликация релиза Минюста), «Bitfinex Hacker Sentenced in Money Laundering Conspiracy Involving Billions in Stolen Cryptocurrency», 20.11.2024, https://www.ice.gov/news/releases/bitfinex-hacker-sentenced-money-laundering-conspiracy-involving-billions-stolen; оригинал Минюста: https://www.justice.gov/usao-dc/pr/bitfinex-hacker-sentenced-money-laundering-conspiracy-involving-billions-stolen; приговор Морган — CoinDesk, 18.11.2024, https://www.coindesk.com/policy/2024/11/18/bitfinex-hack-launderer-heather-razzlekhan-morgan-sentenced-to-18-months-in-prison.

По материалам Минюста 2024 года, Лихтенштейн стёр с серверов Bitfinex учётные данные и журналы, которые могли его выдать[328]. Журналы на серверах биржи стереть удалось, а строчки в тетрадке биткоина стереть не может никто, в том числе тот, кто их написал.

Биткоин, выходит, псевдонимен. Имени в тетрадке нет, зато каждый платёж каждого псевдонима записан навсегда и доступен любому, и достаточно одной точки, где след касается реального мира (биржи с проверкой личности, покупки с доставкой, IP-адреса), чтобы к псевдониму прикрепилось имя. Если приватность для вас важна, исходить разумнее из того, что каждый ваш платёж будет виден всегда.

Когда ключа больше нет

Обратная сторона той же конструкции видна в деле, которое в январе 2025 года рассмотрел Высокий суд Англии и Уэльса. Джеймс Хауэллс добивался от городского совета Ньюпорта доступа к свалке, куда в 2013 году попал его жёсткий диск. На диске, по словам истца, лежал ключ от 8000 BTC, намайненных им в начале 2009 года. Суд дело прекратил, потому что по британскому закону всё, что доставлено на свалку, становится собственностью совета[329].[330] Попутно суд написал, что биткоины — не материальное имущество и ни на жёстком диске, ни на свалке их быть не может[331]. Сам того не добиваясь, он дал лучшее определение кошелька, какое я знаю. Монеты лежат в тетрадке, доступной каждому, а на диске под слоем мусора лежит только возможность ими распорядиться.

Если вы забыли пароль от банка, вы идёте в отделение, показываете паспорт, и хранитель восстанавливает вам доступ, потому что он знает вас и ведёт вашу строчку сам. В тетрадке биткоина пойти не к кому. Сеть не знает, кто вы, и признаёт только подпись, а подписать без ключа нельзя[332]. На этом же правиле держится и то, что в обычное время вашу строчку никто не может заморозить (исключение появится в последнем разделе).

Пусть ключ потерял пекарь. Его строчки по-прежнему стоят в каждой копии тетрадки, их видят все сто дворов, но воспользоваться ими не может ни один двор, включая самого пекаря. Никому другому строчки тоже не переходят и так и стоят в тетрадке, пока она существует.

Защита от этого в тетрадке без хранителя одна, и это копия ключа, которую вы храните сами. Фраза из 12–24 слов, о которой шла речь выше, восстанавливает все ключи кошелька, если её копия записана и сохранена отдельно от телефона[333]. У Хауэллса такой фразы быть не могло, потому что стандарт появился только в 2013 году[334], через четыре года после того,

---

[328] U.S. ICE / HSI (перепубликация релиза Минюста), «Bitfinex Hacker Sentenced in Money Laundering Conspiracy Involving Billions in Stolen Cryptocurrency», 20.11.2024, https://www.ice.gov/news/releases/bitfinex-hacker-sentenced-money-laundering-conspiracy-involving-billions-stolen; оригинал Минюста: https://www.justice.gov/usao-dc/pr/bitfinex-hacker-sentenced-money-laundering-conspiracy-involving-billions-stolen; приговор Морган — CoinDesk, 18.11.2024, https://www.coindesk.com/policy/2024/11/18/bitfinex-hack-launderer-heather-razzlekhan-morgan-sentenced-to-18-months-in-prison.

[329] James Howells v Newport City Council [2025] EWHC 22 (Ch), 09.01.2025, https://caselaw.nationalarchives.gov.uk/ewhc/ch/2025/22.

[330] James Howells v Newport City Council [2025] EWHC 22 (Ch), 09.01.2025, судья Кизер; основание — Control of Pollution Act 1974: «Bitcoin are not tangible property and cannot be on the Hard Drive or in the Landfill.» Что на диске был ключ, — версия истца; суд её не проверял и решил дело по праву собственности на сам диск. Подробнее о деле — в главе 12.

[331] James Howells v Newport City Council [2025] EWHC 22 (Ch), 09.01.2025, https://caselaw.nationalarchives.gov.uk/ewhc/ch/2025/22.

[332] Mastering Bitcoin, 3rd ed., 2023, гл. 4.

[333] BIP-39 «Mnemonic code for generating deterministic keys», Palatinus M., Rusnak P., Voisine A., Bowe S., created 10.09.2013, https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki; Mastering Bitcoin, 3rd ed., гл. 5.

[334] BIP-39 «Mnemonic code for generating deterministic keys», Palatinus M., Rusnak P., Voisine A., Bowe S., created 10.09.2013, https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki; Mastering Bitcoin, 3rd ed., гл. 5.

как он, по его словам, намайнил свои монеты[335]. Хранение такой копии и её слабые места я подробно разберу в главе 12.

Точного счёта строчкам, оставшимся без ключа, нет ни у кого. Одну из известных оценок сделала в 2020 году компания Chainalysis. По её подсчёту, около 3,72 млн BTC к тому времени не двигались пять лет и дольше, и компания сочла их, скорее всего, потерянными[336]. У этой оценки есть слабое место. Потерянной монету делает отсутствие ключа у владельца, а извне этого не проверить, поэтому на деле считали монеты, которые давно не двигались[337]. Часть давно лежащих монет, вероятно, намайнил в самом начале работы сети сам Накамото[338], и никто не знает, лежат они или потеряны. Поэтому, когда вы читаете, что количество биткоинов строго ограничено, помните, что это предел записи в тетрадке, а сдвинуться с места из записанного может заметно меньше.

Ночь, когда тетрадку переписали

До сих пор я описывал тетрадку, которую нельзя тайно переписать. Осталось показать случай, когда её переписали открыто.

15 августа 2010 года, в 19:04 по всемирному времени, пользователь форума биткоина под ником lfm сообщил, что блок 74 638, судя по всему, использовал ошибку в сети: через переполнение целого числа в нём получена отрицательная общая сумма транзакции[339].[340] В блоке оказалась транзакция, которая создала 184 467 440 737,095 516 16 BTC на три адреса. Два адреса получили примерно по 92,2 млрд BTC, а майнер, нашедший блок, — лишние 0,01 BTC, которых до этой транзакции не существовало[341]. Всего же биткоинов по правилам выпуска будет чуть меньше 21 млн[342].

Причина была в арифметике. Программа, как мы видели, считает в целых сатоши[343], а целое число в компьютере занимает ограниченное число разрядов. Код, проверявший транзакции, не учитывал случая, когда выходы так велики, что при сложении переполняют это число[344]. Получившаяся сумма ровно равна 2^{64} сатоши, а каждый из двух огромных выходов близок к 2^{63}, то есть к самому большому числу, которое помещается в 64-разрядную ячейку со знаком[345]. Похоже на механический счётчик пробега, который после последней девятки перескакивает на ноль. Сумма двух гигантских выходов «проворачивалась» в маленькое (по пер-

---

[335] James Howells v Newport City Council [2025] EWHC 22 (Ch), 09.01.2025, https://caselaw.nationalarchives.gov.uk/ewhc/ch/2025/22.

[336] Chainalysis, «60% of Bitcoin is Held Long Term as Digital Gold. What About the Rest?», 18.06.2020, https://www.chainalysis.com/blog/bitcoin-market-data-exchanges-trading/; цифры и формулировки — по The Daily Hodl, 22.06.2020, https://dailyhodl.com/2020/06/22/staggering-35000000000-in-bitcoin-btc-is-forever-lost-reports-chainalysis/ и Decrypt.

[337] Chainalysis, «60% of Bitcoin is Held Long Term as Digital Gold. What About the Rest?», 18.06.2020, https://www.chainalysis.com/blog/bitcoin-market-data-exchanges-trading/; цифры и формулировки — по The Daily Hodl, 22.06.2020, https://dailyhodl.com/2020/06/22/staggering-35000000000-in-bitcoin-btc-is-forever-lost-reports-chainalysis/ и Decrypt.

[338] Lerner S. D. «The Well Deserved Fortune of Satoshi Nakamoto, Bitcoin creator, Visionary and Genius», Bitslog, 17.04.2013, https://bitslog.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/.

[339] Satoshi Nakamoto Institute, архив bitcointalk: тема «overflow bug SERIOUS», https://satoshi.nakamotoinstitute.org/posts/bitcointalk/threads/185/; тема «Version 0.3.10 - block 74638 overflow PATCH!», https://satoshi.nakamotoinstitute.org/posts/bitcointalk/threads/186/.

[340] Архив форума bitcointalk (Satoshi Nakamoto Institute), тема «overflow bug SERIOUS», 15.08.2010, 19:04 UTC: «seems a block at height 74638 has expoited a bug in the net. It uses an integer overflow to make a negative total transaction.» Орфография оригинала сохранена.

[341] Bitcoin Wiki, «Value overflow incident» (CVE-2010-5139), https://en.bitcoin.it/wiki/Value_overflow_incident.

[342] Bitcoin Wiki, «Controlled supply», https://en.bitcoin.it/wiki/Controlled_supply.

[343] Mastering Bitcoin, 3rd ed., гл. 6.

[344] Bitcoin Wiki, «Value overflow incident» (CVE-2010-5139), https://en.bitcoin.it/wiki/Value_overflow_incident.

[345] Bitcoin Wiki, «Value overflow incident» (CVE-2010-5139), https://en.bitcoin.it/wiki/Value_overflow_incident.

вому сообщению, отрицательное) число и проходила проверку, что выходы не больше входов[346].

Дальше события шли быстро, и все они сохранились в архиве форума[347]. В 20:59 Накамото выложил первые проверки кода. В 21:06 он попросил участников остановиться: будет полезно, если люди перестанут генерировать блоки, потому что, вероятно, придётся заново построить ветку вокруг текущей, и чем меньше они генерируют, тем быстрее это получится[348].[349] Логика просьбы понятна из той же фразы. Каждый новый блок на ошибочной ветке удлинял её, и исправленной ветке пришлось бы догонять больше. Чем меньше блоков строилось поверх ошибки, тем быстрее её можно было обойти. В 21:40 исправление было в хранилище кода, а в 23:17 вышли готовые сборки версии 0.3.10[350]. От первого сообщения до исправления прошло около двух часов сорока минут, до готовой программы — около четырёх с четвертью[351].

Новая версия добавила правило, по которому узлы отвергали транзакции с переполнением, а заодно и транзакции с выходом больше 21 млн BTC[352]. После этого тетрадка разветвилась. Узлы со старой программой продолжали строить на ошибочной ветке, а узлы с новой отвергали блок с ошибкой и строили другую. Когда исправленная ветка обогнала ошибочную (по вики сообщества, на блоке 74 691, примерно через пятьдесят блоков), её приняли все узлы[353].[354] Обычные транзакции из ошибочной ветки вошли в исправленную, и пострадали только те, кто успел намайнить блоки в ошибочной ветке после 74 638, потому что их награды по 50 BTC исчезли[355].[356]

Представим то же самое в посёлке. Однажды утром в тетрадке обнаруживается страница, на которой кто-то приписал себе строчек больше, чем может быть во всём посёлке. Часть дворов уже подшила её и пишет следующие страницы поверх. Вырвать страницу из чужой копии никто не может. Тогда дворы договариваются о новом правиле, по которому такая страница

---

[346] Bitcoin Wiki, «Value overflow incident» (CVE-2010-5139), https://en.bitcoin.it/wiki/Value_overflow_incident; Satoshi Nakamoto Institute, архив bitcointalk: тема «overflow bug SERIOUS», https://satoshi.nakamotoinstitute.org/posts/bitcointalk/threads/185/; тема «Version 0.3.10 - block 74638 overflow PATCH!», https://satoshi.nakamotoinstitute.org/posts/bitcointalk/threads/186/.

[347] Satoshi Nakamoto Institute, архив bitcointalk: тема «overflow bug SERIOUS», https://satoshi.nakamotoinstitute.org/posts/bitcointalk/threads/185/; тема «Version 0.3.10 - block 74638 overflow PATCH!», https://satoshi.nakamotoinstitute.org/posts/bitcointalk/threads/186/.

[348] Satoshi Nakamoto Institute, архив bitcointalk: тема «overflow bug SERIOUS», https://satoshi.nakamotoinstitute.org/posts/bitcointalk/threads/185/; тема «Version 0.3.10 - block 74638 overflow PATCH!», https://satoshi.nakamotoinstitute.org/posts/bitcointalk/threads/186/.

[349] Там же, 21:06 UTC: «It would help if people stop generating. We will probably need to re-do a branch around the current one, and the less you generate the faster that will be.»

[350] Satoshi Nakamoto Institute, архив bitcointalk: тема «overflow bug SERIOUS», https://satoshi.nakamotoinstitute.org/posts/bitcointalk/threads/185/; тема «Version 0.3.10 - block 74638 overflow PATCH!», https://satoshi.nakamotoinstitute.org/posts/bitcointalk/threads/186/.

[351] Satoshi Nakamoto Institute, архив bitcointalk: тема «overflow bug SERIOUS», https://satoshi.nakamotoinstitute.org/posts/bitcointalk/threads/185/; тема «Version 0.3.10 - block 74638 overflow PATCH!», https://satoshi.nakamotoinstitute.org/posts/bitcointalk/threads/186/.

[352] Bitcoin Wiki, «Value overflow incident», https://en.bitcoin.it/wiki/Value_overflow_incident; Накамото, архив bitcointalk, посты 16.08.2010 01:00:45 и 12:59:38 UTC.

[353] Bitcoin Wiki, «Value overflow incident», https://en.bitcoin.it/wiki/Value_overflow_incident; Накамото, архив bitcointalk, посты 16.08.2010 01:00:45 и 12:59:38 UTC.

[354] Сам Накамото 16 августа писал «около 74 689»; разница — в его оценке на глаз. Вики сообщества относит исправление к «мягким» изменениям правил, то есть к ужесточению того, что считается допустимым.

[355] Bitcoin Wiki, «Value overflow incident», https://en.bitcoin.it/wiki/Value_overflow_incident; Накамото, архив bitcointalk, посты 16.08.2010 01:00:45 и 12:59:38 UTC.

[356] Накамото, bitcointalk, 16.08.2010, 01:00 UTC: «It's only if you generated a block in the bad chain after block 74638 that the 50 BTC from that will disappear.»

недействительна, и продолжают тетрадку с последней честной страницы. Дворов с новым правилом больше, их версия растёт быстрее, и в какой-то момент отставшие переходят на неё.

Само исправление опиралось на то же правило, которое делает тетрадку трудной для подделки. Исправленная ветка стала настоящей потому, что оказалась длиннее и узлы перешли на неё[357]. Приказывать им было некому.

Для биткоина уже можно ответить на три из пяти вопросов, которые я в первой главе советовал задавать любым деньгам. Кто ведёт запись? Каждый узел держит полную копию и сам проверяет каждую новую страницу[358]. Кто может дописать новые строчки? Только майнер, нашедший блок, только себе и только в размере, который задают правила и проверяет каждый узел[359]. Кто может стереть или заморозить чужую строчку? Никто, у кого нет ключа (а у кого ключ есть, тот и владеет строчкой; изъятия по делам Colonial Pipeline и Bitfinex тоже прошли через ключ[360]). Исключение одно, и мы его только что видели: большинство сети по общему согласию, как в 2010 году, когда исчезли награды за блоки ошибочной ветки[361]. Четвёртый вопрос, кто может остановить всю систему, упирается в правило согласия, а пятый, о строчках в долг, станет главным во второй части книги.

Ночь 2010 года показывает, где у «неизменяемости» проходит граница. Код биткоина ошибся всерьёз, и одна пропущенная проверка позволила создать из ничего почти в девять тысяч раз больше монет, чем их может существовать вообще[362], хотя математика отпечатков и подписей в ту ночь сработала безупречно. Ошибку за несколько часов заметили и исправили люди: участник форума, Накамото и владельцы узлов, которые поставили новую версию[363]. А около пятидесяти страниц, уже вшитых в цепочку, заменили другими[364]. Поэтому в определении, с которого началась глава, и стоит слово «тайно». Тайно и в одиночку переписать тетрадку задним числом практически невозможно, потому что для этого пришлось бы заново выполнить работу, вложенную во все последующие страницы[365]. Открыто и по согласию большинства участников это возможно, и в 2010 году это было сделано[366]. Значит, вся защита тетрадки держится на том, кто в такой сети считается большинством и во что обходится его собрать.

---

[357] Bitcoin Wiki, «Value overflow incident», https://en.bitcoin.it/wiki/Value_overflow_incident; Накамото, архив bitcointalk, посты 16.08.2010 01:00:45 и 12:59:38 UTC.

[358] Nakamoto, 2008, раздел 5 «Network», https://bitcoin.org/bitcoin.pdf.

[359] Bitcoin Developer Reference, «Block Chain»; исходный код Bitcoin Core, src/kernel/chainparams.cpp (CMainParams): nPowTargetSpacing = 10 * 60; nPowTargetTimespan = 14 * 24 * 60 * 60; nSubsidyHalvingInterval = 210000, https://raw.githubusercontent.com/bitcoin/bitcoin/master/src/kernel/chainparams.cpp; Mastering Bitcoin, 3rd ed., гл. 12; Nakamoto, 2008, раздел 5 «Network», https://bitcoin.org/bitcoin.pdf.

[360] U.S. DOJ / IRS-CI, «Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency», 08.02.2022, копия на сайте IRS: https://www.irs.gov/zh-hant/compliance/criminal-investigation/two-arrested-for-alleged-conspiracy-to-launder-4-point-5-billion-in-stolen-cryptocurrency; оригинал: https://www.justice.gov/archives/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency (не открылся); U.S. Department of Justice, Office of Public Affairs, «Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside», 07.06.2021, https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside; дубль: https://www.justice.gov/usao-ndca/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists.

[361] Bitcoin Wiki, «Value overflow incident», https://en.bitcoin.it/wiki/Value_overflow_incident; Накамото, архив bitcointalk, посты 16.08.2010 01:00:45 и 12:59:38 UTC.

[362] Bitcoin Wiki, «Value overflow incident» (CVE-2010-5139), https://en.bitcoin.it/wiki/Value_overflow_incident; Bitcoin Wiki, «Controlled supply», https://en.bitcoin.it/wiki/Controlled_supply.

[363] Satoshi Nakamoto Institute, архив bitcointalk: тема «overflow bug SERIOUS», https://satoshi.nakamotoinstitute.org/posts/bitcointalk/threads/185/; тема «Version 0.3.10 - block 74638 overflow PATCH!», https://satoshi.nakamotoinstitute.org/posts/bitcointalk/threads/186/; Bitcoin Wiki, «Value overflow incident», https://en.bitcoin.it/wiki/Value_overflow_incident; Накамото, архив bitcointalk, посты 16.08.2010 01:00:45 и 12:59:38 UTC.

[364] Bitcoin Wiki, «Value overflow incident», https://en.bitcoin.it/wiki/Value_overflow_incident; Накамото, архив bitcointalk, посты 16.08.2010 01:00:45 и 12:59:38 UTC.

[365] Nakamoto, 2008, раздел 4 «Proof-of-Work», https://bitcoin.org/bitcoin.pdf.

[366] Bitcoin Wiki, «Value overflow incident», https://en.bitcoin.it/wiki/Value_overflow_incident; Накамото, архив bitcointalk,

посты 16.08.2010 01:00:45 и 12:59:38 UTC.

Глава 3. Кто ведёт запись: консенсус и его цена

Если вы видите в майнинге только расход электричества, а в споре о нём только спор о климате, то так и не узнаете, за что сеть этим электричеством платит, а платит она за вполне определённую вещь. Тысячи участников, которые не знают друг друга и не обязаны друг другу верить, должны раз за разом соглашаться, какая версия общей тетрадки настоящая, и никто не может утвердить эту версию своей властью. Такое согласие стоит дорого. Платят за него либо электричеством, либо деньгами, запертыми в залоге, в обоих случаях ещё и скоростью, и вся эта плата есть цена отказа от посредника.

Способ, которым участники сети приходят к одной версии записи, называют консенсусом. В первой главе он появился как третья часть пятого правила посёлка: дворы, не доверяющие друг другу, приходят к одной версии тетрадки, даже если кто-то из них жульничает. Вторая глава закончилась вопросом, который из этого правила вытекает. Если две версии тетрадки разошлись, кто решает, какая настоящая, и что мешает тому, кто соберёт больше половины вычислительной мощности сети, навязать свою?

Генералы у вражеского города

Задачу согласия сформулировали задолго до криптовалют, причём в виде притчи. В 1982 году Лесли Лэмпорт и двое его соавторов опубликовали статью «Задача византийских генералов»[367]. Несколько отрядов византийской армии стоят лагерем у вражеского города, у каждого отряда свой генерал, и сообщаться друг с другом генералы могут только через гонцов[368].[369] Им нужно принять общий план, а часть генералов может оказаться предателями. Авторы сразу переводят притчу на язык машин: сломанная или злонамеренная деталь системы может рассылать разным её частям противоречивые сведения[370].

Перенести притчу в посёлок несложно. Генералы — это дворы с копиями тетрадки, гонцы — сообщения по сети, предатели — дворы, которые жульничают или просто сломались[371]. Пекарь из первой главы, который отправил одну и ту же строчку доярке и лесорубу, и есть такой предатель, потому что рассказывает разным соседям разное.

Главный результат статьи неприятен. Если генералы обмениваются только устными сообщениями, которые можно переврать при пересказе, согласие достижимо тогда и только тогда, когда верны больше двух третей из них. При трёх генералах одного предателя хватает, чтобы два верных так и не договорились[372].[373]

---

[367] L. Lamport, R. Shostak, M. Pease, «The Byzantine Generals Problem», ACM Transactions on Programming Languages and Systems, vol. 4, no. 3, July 1982, pp. 382–401, https://lamport.azurewebsites.net/pubs/byz.pdf.

[368] L. Lamport, R. Shostak, M. Pease, «The Byzantine Generals Problem», ACM Transactions on Programming Languages and Systems, vol. 4, no. 3, July 1982, pp. 382–401, https://lamport.azurewebsites.net/pubs/byz.pdf.

[369] Lamport L., Shostak R., Pease M. The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems, vol. 4, no. 3, July 1982, pp. 382–401. Авторы работали в SRI International. «We imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals can communicate with one another only by messenger.»

[370] L. Lamport, R. Shostak, M. Pease, «The Byzantine Generals Problem», ACM Transactions on Programming Languages and Systems, vol. 4, no. 3, July 1982, pp. 382–401, https://lamport.azurewebsites.net/pubs/byz.pdf.

[371] L. Lamport, R. Shostak, M. Pease, «The Byzantine Generals Problem», ACM Transactions on Programming Languages and Systems, vol. 4, no. 3, July 1982, pp. 382–401, https://lamport.azurewebsites.net/pubs/byz.pdf.

[372] Lamport, Shostak, Pease, 1982, аннотация и раздел 2 «Impossibility results», https://lamport.azurewebsites.net/pubs/byz.pdf.

[373] Там же, аннотация: «It is shown that, using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so a single traitor can confound two loyal generals.»

Допустим, генералов трое: командующий и двое подчинённых. Командующий приказал наступать, а один из подчинённых оказался предателем и передаёт второму, что приказ был отступать. Верный генерал держит в руках два противоречащих сообщения и не знает, кто лжёт, командующий или сосед. Теперь пусть предателем окажется сам командующий и отдаст двоим разные приказы. Верный генерал увидит ровно ту же картину. Два разных мира выглядят для него одинаково, и выбрать между ними ему нечем.

В той же статье есть и утешение. С письменными сообщениями, которые нельзя подделать, задача решается при любом числе генералов и предателей[374].[375] Такое сообщение нам уже знакомо: это цифровая подпись из второй главы. Предатель может молчать или врать от своего имени, но переврать чужой подписанный приказ он не может.

Можно подумать, что для биткоина задача на этом решена, ведь подписи в нём есть. Но в классической постановке спрятано допущение, которое легко пропустить: генералы известны, число их задано, и каждый знает, от кого пришло письмо[376]. В открытой сети всё иначе. Полного числа узлов биткоина не знает никто, и разрешения стать узлом никто не выдаёт[377]. Подпись доказывает, что приказ написан владельцем ключа, но ключей любой может завести сколько угодно. Предателю, которому нужно большинство, достаточно нарисовать себе тысячу генералов.

Для закрытого круга задачу довели до практики к концу девяностых. В 1999 году Мигель Кастро и Барбара Лисков описали алгоритм практической византийской отказоустойчивости (по-английски его сокращают до PBFT)[378]. Он работает в сетях вроде интернета, где сообщения идут с задержками, и выдерживает сбойных или злонамеренных участников, пока их меньше трети[379].[380] Защита обошлась почти даром. Сетевая файловая система, которую авторы построили на своём алгоритме, в обычной работе оказалась всего примерно на 3% медленнее стандартной, где никакой защиты от предателей не было[381].[382]

Условие, при котором это работает, авторы записали прямо: все участники знают открытые ключи друг друга[383].[384] Получается клуб с закрытым списком членов. Кто в списке, тот голосует, кого в списке нет, того не слушают, и голоса считать легко, потому что известно, сколько

---

[374] Lamport, Shostak, Pease, 1982, аннотация, https://lamport.azurewebsites.net/pubs/byz.pdf.

[375] Там же: «With unforgeable written messages, the problem is solvable for any number of generals and possible traitors.»

[376] Lamport, Shostak, Pease, 1982, аннотация, https://lamport.azurewebsites.net/pubs/byz.pdf.

[377] BTC Nodes (Bitnodes), https://btcnodes.io/; API снимка: https://btcnodes.io/api/v1/snapshots/latest/ (обращение 2026-09-26; старый адрес bitnodes.io перенаправляет туда). Оператор — Rodrigo Martínez.

[378] M. Castro, B. Liskov, «Practical Byzantine Fault Tolerance», Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, February 1999; PDF (зеркало курса MIT 6.824): https://css.csail.mit.edu/6.824/2014/papers/castro-practicalbft.pdf.

[379] M. Castro, B. Liskov, «Practical Byzantine Fault Tolerance», Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, February 1999; PDF (зеркало курса MIT 6.824): https://css.csail.mit.edu/6.824/2014/papers/castro-practicalbft.pdf.

[380] Castro M., Liskov B. Practical Byzantine Fault Tolerance. Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI '99), New Orleans, February 1999: «…it works in asynchronous environments like the Internet…» Точная граница: алгоритм выдерживает не более $\lfloor (n-1)/3 \rfloor$ неисправных участников из n, то есть при f злонамеренных участников нужно не меньше 3f+1 участников всего (M. Castro, B. Liskov, «Practical Byzantine Fault Tolerance», Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, February 1999; PDF (зеркало курса MIT 6.824): https://css.csail.mit.edu/6.824/2014/papers/castro-practicalbft.pdf).

[381] Castro, Liskov, 1999 (по пересказу: Colyer, The Morning Paper, 2015, https://blog.acolyer.org/2015/05/18/practical-byzantine-fault-tolerance/).

[382] Сравнение шло со стандартной нереплицированной NFS, во введении — со стандартным демоном NFS в ядре Digital Unix при нормальной работе, без сбоев (Castro, Liskov, 1999 (по пересказу: Colyer, The Morning Paper, 2015, https://blog.acolyer.org/2015/05/18/practical-byzantine-fault-tolerance/)).

[383] M. Castro, B. Liskov, «Practical Byzantine Fault Tolerance», Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, February 1999; PDF (зеркало курса MIT 6.824): https://css.csail.mit.edu/6.824/2014/papers/castro-practicalbft.pdf.

[384] Castro, Liskov, 1999, p. 2: «All replicas know the others' public keys.»

их. (К тому же в таком алгоритме каждый обменивается сообщениями с каждым, поэтому он хорош для десятков участников и плохо подходит для тысяч[385].)

В закрытом кругу согласие почти бесплатно, дорогим его делает открытость[386]. Посёлок из ста дворов, где все знают друг друга, мог бы договариваться по правилам Кастро и Лисков. Посёлок, куда может записаться кто угодно под любым числом имён и откуда можно уйти не попрощавшись, так договориться не может.

В посёлке первой главы с хранителями так и было устроено. Хранители известны, над ними стоит главный хранитель, и спор о том, чья запись верна, есть кому решить, поэтому тратить электричество на согласие такому посёлку незачем. Биткоин отказался и от главного хранителя, и от закрытого списка, и всё, что описано дальше в этой главе, так или иначе оказывается платой за этот отказ.

Голос по работе

Накамото решил задачу тем, что поменял, чем голосуют. В четвёртом разделе статьи 2008 года он рассуждает так. Если бы голос давался каждому IP-адресу (сетевому адресу компьютера), то голосов было бы больше у того, кто может завести много адресов. Поэтому голосует вычислительная мощность, и доказательство работы, по его словам, — это «один процессор, один голос»[387]. Решение большинства — самая длинная цепочка, точнее, цепочка, в которую вложено больше всего работы[388].[389]

Голос теперь нельзя нарисовать. Тысячу ключей можно завести бесплатно, а тысячу машин, которые перебирают отпечатки, нужно купить и кормить электричеством. Голос стоит столько, сколько стоит работа, которую за ним можно предъявить, а проверить эту работу может любой одним расчётом[390]. (Расхожее выражение «майнеры решают сложные математические задачи» сбивает с толку. Задача в майнинге механическая, она сводится к перебору числа nonce, пока отпечаток не окажется ниже порога[391]. Трудна она только объёмом перебора.)

Мысль платить вычислениями за доступ к общему ресурсу старше биткоина на полтора десятка лет. В 1992 году криптографы Синтия Дворк и Мони Наор предложили заставлять отправителя письма вычислять умеренно трудную функцию, чтобы массовая рассылка спама стала дорогой[392].[393] Адам Бэк, чей Hashcash мы встречали в первой главе, пришёл к той же

---

[385] M. Castro, B. Liskov, «Practical Byzantine Fault Tolerance», Proceedings of OSDI '99, 1999, https://www.usenix.org/conference/osdi-99/practical-byzantine-fault-tolerance (карточка), http://pmg.csail.mit.edu/papers/osdi99.pdf; содержание сверено по обзору A. Colyer, «Practical Byzantine Fault Tolerance», The Morning Paper, 18.05.2015, https://blog.acolyer.org/2015/05/18/practical-byzantine-fault-tolerance/.

[386] Castro, Liskov, 1999 (по пересказу: Colyer, The Morning Paper, 2015, https://blog.acolyer.org/2015/05/18/practical-byzantine-fault-tolerance/).

[387] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System», 2008, раздел 4 «Proof-of-Work», https://bitcoin.org/bitcoin.pdf.

[388] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System», 2008, раздел 4 «Proof-of-Work», https://bitcoin.org/bitcoin.pdf.

[389] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, section 4: «Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it.»

[390] Nakamoto, 2008, раздел 4, https://bitcoin.org/bitcoin.pdf.

[391] Nakamoto, 2008, раздел 4, https://bitcoin.org/bitcoin.pdf.

[392] C. Dwork, M. Naor, «Pricing via Processing or Combatting Junk Mail», Advances in Cryptology — CRYPTO '92, Lecture Notes in Computer Science, vol. 740, Springer, 1993, pp. 139–147, DOI 10.1007/3-540-48071-4_10, https://link.springer.com/chapter/10.1007/3-540-48071-4_10; карточка IACR: https://iacr.org/cryptodb/data/paper.php?pubkey=1268.

[393] Dwork C., Naor M. Pricing via Processing or Combatting Junk Mail. Advances in Cryptology — CRYPTO '92, LNCS 740, Springer, 1993, pp. 139–147. Термина proof-of-work в этой работе нет, его популяризовали позже (C. Dwork, M. Naor, «Pricing via Processing or Combatting Junk Mail», Advances in Cryptology — CRYPTO '92, Lecture Notes in Computer Science, vol. 740, Springer, 1993, pp. 139–147, DOI 10.1007/3-540-48071-4_10, https://link.springer.com/chapter/10.1007/3-540-48071-4_10; карточка IACR: https://iacr.org/cryptodb/data/paper.php?pubkey=1268).

мысли весной 1997 года, не зная об их работе[394]. В его объявлении есть фраза, в которой уместилось всё доказательство работы: такие вычисления можно сделать сколь угодно дорогими, а проверить мгновенно[395].[396] Накамото взял эту асимметрию за основу и прямо сослался на Бэка[397].

Добавим восьмое правило посёлка: если у дворов оказались две разные версии тетрадки, верной считается та, в которую вложено больше работы[398]. Каждый двор, увидев более тяжёлую версию, переходит на неё сам, ни у кого не спрашивая.

Со второй главы остался вопрос, что будет, если две страницы найдены почти одновременно. Допустим, страница А дошла до одной половины посёлка раньше, чем страница Б, а до другой половины раньше дошла Б. Обе честные, на обе потрачена правильная работа, и каждый двор начинает писать следующую страницу поверх той, которую увидел первой (так узел и выражает согласие[399]). Тетрадка ненадолго раздваивается.

Следующая страница найдётся на одной из ветвей раньше, чем на другой, эта ветвь станет тяжелее, и по восьмому правилу на неё перейдут все. Так эту ничью разрешает и Накамото[400].[401] Перевод, записанный только на проигравшей странице, обычно не пропадает: узлы возвращают его в очередь ожидающих записей, и он дожидается места на одной из следующих страниц выигравшей ветви[402]. Пропадает он, только если на выигравшей ветви уже лежит другой перевод тех же монет. Этим и пользуется атакующий, о котором речь ниже.

---

[394] Aaron van Wirdum, «The Genesis Files: Hashcash or How Adam Back Designed Bitcoin's Motor Block», Bitcoin Magazine, 04.06.2018, https://bitcoinmagazine.com/technical/genesis-files-hashcash-or-how-adam-back-designed-bitcoins-motor-block; статья Бэка: A. Back, «Hashcash — A Denial of Service Counter-Measure», 01.08.2002, http://www.hashcash.org/hashcash.pdf (не открылась — ошибка SSL); Bitcoin Annotated, «Hashcash», https://bitcoinannotated.com/entries/hashcash/; архив рассылки: https://cypherpunks.venona.com/date/1997/03/msg00774.html (при проверке — ошибка 522, не открыт); ср. van Wirdum.

[395] Aaron van Wirdum, «The Genesis Files: Hashcash or How Adam Back Designed Bitcoin's Motor Block», Bitcoin Magazine, 04.06.2018, https://bitcoinmagazine.com/technical/genesis-files-hashcash-or-how-adam-back-designed-bitcoins-motor-block; статья Бэка: A. Back, «Hashcash — A Denial of Service Counter-Measure», 01.08.2002, http://www.hashcash.org/hashcash.pdf (не открылась — ошибка SSL).

[396] Слова Бэка в пересказе историка биткоина Арона ван Вирдума: «the idea of using partial hashes is that they can be made arbitrarily expensive to compute, and yet can be verified instantly» (Aaron van Wirdum, «The Genesis Files: Hashcash or How Adam Back Designed Bitcoin's Motor Block», Bitcoin Magazine, 04.06.2018, https://bitcoinmagazine.com/technical/genesis-files-hashcash-or-how-adam-back-designed-bitcoins-motor-block; статья Бэка: A. Back, «Hashcash — A Denial of Service Counter-Measure», 01.08.2002, http://www.hashcash.org/hashcash.pdf (не открылась — ошибка SSL)). Объявление в рассылке шифропанков два независимых пересказа датируют 28 марта 1997 года, а в статье самого Бэка 2002 года, как её цитируют, сказано «in May 1997» (Bitcoin Annotated, «Hashcash», https://bitcoinannotated.com/entries/hashcash/; архив рассылки: https://cypherpunks.venona.com/date/1997/03/msg00774.html (при проверке — ошибка 522, не открыт); ср. van Wirdum); отсюда «весной 1997 года».

[397] Nakamoto, 2008, раздел 4, https://bitcoin.org/bitcoin.pdf.

[398] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System», 2008, раздел 4 «Proof-of-Work», https://bitcoin.org/bitcoin.pdf.

[399] Nakamoto, 2008, раздел 5 «Network», https://bitcoin.org/bitcoin.pdf.

[400] Nakamoto S., Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, section 5, https://bitcoin.org/bitcoin.pdf (стр. 3).

[401] Nakamoto, 2008, section 5: «The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.» О переводах с проигравшей страницы у Накамото ничего не сказано; так их обрабатывает программа Bitcoin Core: «Transactions which are mined into blocks that later become stale blocks may be added back into the memory pool» (Bitcoin Developer Guide, P2P Network) (Bitcoin Developer Guide, P2P Network, раздел Memory Pool, https://developer.bitcoin.org/devguide/p2p_network.html).

[402] Bitcoin Developer Guide, P2P Network, раздел Memory Pool, https://developer.bitcoin.org/devguide/p2p_network.html.

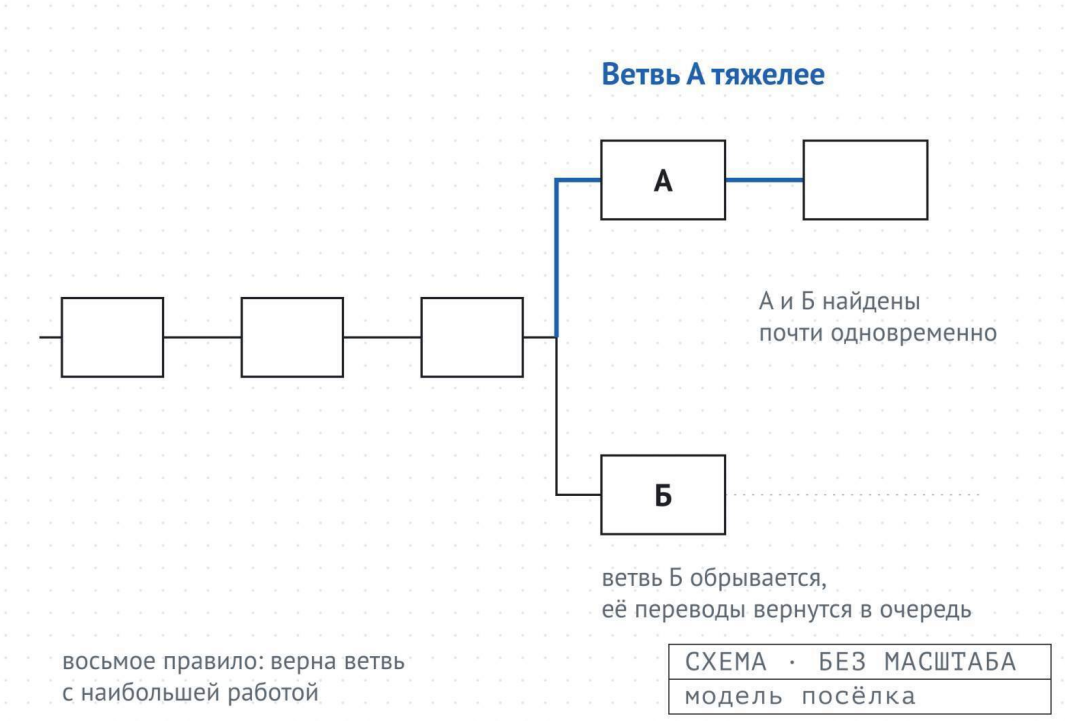


Рисунок 3.1. Развилка

Из этого выросла привычка ждать. Свежая страница может оказаться на проигравшей ветви, поэтому получатель крупного платежа ждёт, пока над его записью вырастет несколько страниц. Каждая страница сверху — ещё одна порция работы, которую пришлось бы переделать тому, кто захочет запись отменить[403]. Сколько страниц ждать, решает сам получатель.

На восьмом правиле держится и главная угроза, атака большинства, которую обычно называют атакой 51%. Безопасность биткоина, по статье Накамото, держится на условии, что честные узлы вместе контролируют больше вычислительной мощности, чем любая группа нападающих[404]. Когда условие нарушено, у нападающего появляется возможность, которой нет у пекаря-одиночки: тайно строить свою ветвь быстрее, чем посёлок строит общую, а потом выложить её. Его ветвь окажется тяжелее, и дворы перейдут на неё сами. Нужно только переделать работу всех страниц над той, которую он хочет изменить, и обогнать честную сеть[405].[406]

Допустим, в посёлке сто одинаковых машин для перебора, и 30 из них у атакующего. В среднем из каждых десяти новых страниц три найдёт он, а семь найдут все остальные. Если ему нужно отменить перевод, над которым уже лежат шесть страниц, он стартует с отставанием в шесть страниц, и в среднем оно только растёт. Догнать честную ветвь он может лишь за счёт везения, долгой серии удачных попыток подряд, а чем глубже лежит запись, тем длиннее нужна серия. Поэтому шанс отстающего и падает с каждой новой страницей так быстро[407].

---

[403] Nakamoto, 2008, раздел 4, https://bitcoin.org/bitcoin.pdf.

[404] Satoshi Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System», 2008, https://bitcoin.org/bitcoin.pdf.

[405] Nakamoto, 2008, раздел 4, https://bitcoin.org/bitcoin.pdf.

[406] Nakamoto, 2008, section 4: «To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes.» Шанс отстающего атакующего догнать честную цепочку, по расчёту Накамото, падает экспоненциально с каждым новым блоком (Nakamoto, 2008, раздел 4, https://bitcoin.org/bitcoin.pdf).

[407] Nakamoto, 2008, раздел 4, https://bitcoin.org/bitcoin.pdf.

Теперь дадим атакующему 60 машин из ста. Он в среднем быстрее всех остальных вместе, его отставание сокращается, и рано или поздно его ветвь станет тяжелее; глубина записи только оттягивает этот момент. Граница проходит по половине мощности.

(У генералов с устными сообщениями порог был выше: там верных должно быть больше двух третей[408], а у Накамото честным достаточно контролировать больше мощности, чем любая группа нападающих[409].)

Что он сможет сделать с такой ветвью?

Меньше, чем принято думать. Каждый узел по-прежнему сам проверяет каждую запись, поэтому монеты из воздуха не пройдут и на ветви атакующего[410]. Подписать перевод чужих монет без чужого ключа он тоже не сможет[411]. Зато он может убрать из истории собственные переводы[412], а заодно не пускать на свои страницы чужие. Первое и есть двойная трата, от которой в первой главе понадобился хранитель.

Почему с биткоином этого не случается каждый день? Накамото ответил экономикой. Тот, кто собрал больше мощности, чем все честные узлы вместе, может либо обманывать людей, отменяя свои платежи, либо получать новые монеты по правилам. Второе, писал Накамото, должно быть ему выгоднее, чем подрывать систему, а вместе с ней ценность собственного богатства[413].[414] Для большой сети, где атакующему пришлось бы купить и запустить больше машин, чем у всех остальных вместе, расчёт работает. Для маленькой сети, где нужную мощность можно собрать со стороны[415], он может сломаться, и дальше мы увидим, как это выглядело.

Для вас как получателя платежа отсюда следует простое правило. Чем меньше мощности охраняет сеть, тем дешевле переписать её недавнюю историю и тем больше страниц разумно ждать, прежде чем считать крупный платёж окончательным. Сколько именно, одной формулой не скажешь (это зависит и от суммы, и от того, во что обходится мощность сети), но направление у правила одно для всех сетей с доказательством работы: маленькая сеть требует больше терпения, чем большая.

Кто держит темп и кто пишет страницы

Мощность в сети биткоина всё время меняется, потому что машины подключают и выключают, одни майнеры приходят в отрасль, а другие разоряются и уходят. Если бы порог для отпечатка стоял на месте, страницы то сыпались бы каждую минуту, то не выходили бы часами. Поэтому в правила встроен регулятор темпа, который я буду называть термостатом. Каждые 2016 блоков все узлы пересчитывают сложность, чтобы страница выходила в среднем раз в десять минут[416]. Если за прошедший период блоки шли быстрее, сложность растёт, если медленнее, падает[417].

---

[408] Lamport, Shostak, Pease, 1982, аннотация и раздел 2 «Impossibility results», https://lamport.azurewebsites.net/pubs/byz.pdf.

[409] Satoshi Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System», 2008, https://bitcoin.org/bitcoin.pdf.

[410] Nakamoto, 2008, раздел 5 «Network», https://bitcoin.org/bitcoin.pdf.

[411] Mastering Bitcoin, 3rd ed., 2023, гл. 4.

[412] Nakamoto, 2008, раздел 5 «Network», https://bitcoin.org/bitcoin.pdf.

[413] Nakamoto, 2008, раздел 6 «Incentive», https://bitcoin.org/bitcoin.pdf.

[414] Nakamoto, 2008, section 6: «He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.»

[415] Bitcoin Gold, «Responding to Attacks», 24.05.2018, http://www.bitcoingold.org/responding-to-attacks/.

[416] исходный код Bitcoin Core, src/kernel/chainparams.cpp (CMainParams): nPowTargetSpacing = 10 * 60; nPowTargetTimespan = 14 * 24 * 60 * 60; nSubsidyHalvingInterval = 210000, https://raw.githubusercontent.com/bitcoin/bitcoin/master/src/kernel/chainparams.cpp; Mastering Bitcoin, 3rd ed., гл. 12.

[417] Bitcoin Wiki, «Difficulty», https://en.bitcoin.it/wiki/Difficulty; принцип — Nakamoto, 2008, раздел 4 («the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour»).

Если мощность сети разом удвоится, страницы начнут выходить в среднем раз в пять минут, потому что перебор идёт вдвое быстрее, а порог прежний. Очередные 2016 блоков наберутся не за две недели, а примерно за одну, узлы это увидят и поднимут сложность примерно вдвое[418]. Дальше страницы снова пойдут раз в десять минут, только каждая будет стоить вдвое больше перебора.

Поэтому новые майнеры не ускоряют ни ваши переводы, ни выпуск монет: у выпуска своё расписание, и от числа машин оно не зависит. Вся добавленная мощность уходит в одно: подделать тетрадку становится дороже, потому что атакующему приходится перегонять больше работы[419].

Мощность сети измеряют числом попыток перебора, которое все майнеры вместе делают за секунду (эту величину называют хешрейтом). Посчитать её напрямую нельзя, поэтому её выводят из сложности и темпа блоков, и разные сервисы получают немного разные числа[420]. В конце сентября 2026 года она составляла около миллиарда триллионов попыток в секунду[421].[422]

Однажды термостат проверили в деле, и проверка вышла жёсткой. 21 мая 2021 года комитет Госсовета КНР по финансовой стабильности поставил задачу «пресечь майнинг и торговлю биткоином»[423].[424] Майнерам в Китае пришлось выключать машины и переезжать[425]. 3 июля 2021 года сложность снизилась на 27,9%, и это было самое большое снижение за всю историю сети[426].[427]

Из сети за несколько недель ушло больше четверти мощности. Страницы при этом продолжали выходить, после пересчёта снова примерно раз в десять минут, и никакого решения

---

[418] Bitcoin Wiki, «Difficulty», https://en.bitcoin.it/wiki/Difficulty; принцип — Nakamoto, 2008, раздел 4 («the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour»).

[419] Bitcoin Wiki, «Difficulty», https://en.bitcoin.it/wiki/Difficulty; принцип — Nakamoto, 2008, раздел 4 («the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour»).

[420] mempool.space, API «mining/hashrate/1m» и «mining/pools/1m», запрос 26.09.2026: https://mempool.space/api/v1/mining/hashrate/1m (currentHashrate ≈ $9{,}34 \cdot 10^{20}$ H/s; дневные средние 24–26.09.2026: 837, 933, 880 ЭХ/с); https://mempool.space/api/v1/mining/pools/1m (оценка за месяц ≈ $1{,}02 \cdot 10^{21}$ H/s).

[421] mempool.space, API «mining/hashrate/1m» и «mining/pools/1m», запрос 26.09.2026: https://mempool.space/api/v1/mining/hashrate/1m (currentHashrate ≈ $9{,}34 \cdot 10^{20}$ H/s; дневные средние 24–26.09.2026: 837, 933, 880 ЭХ/с); https://mempool.space/api/v1/mining/pools/1m (оценка за месяц ≈ $1{,}02 \cdot 10^{21}$ H/s).

[422] Оценка mempool.space на 26.09.2026: около $9{,}34 \times 10^{20}$ хешей в секунду, дневные средние 24–26 сентября — от 837 до 933 эксахешей в секунду; оценка за месяц — около $1{,}02 \times 10^{21}$. Хешрейт не измеряется, а выводится, поэтому дневные значения скачут примерно на ±10%, и разные сервисы дают разные цифры. Последняя корректировка перед этой датой, 19.09.2026 на блоке 967 680, подняла сложность на 4,2% (mempool.space, API «mining/hashrate/1m» и «mining/pools/1m», запрос 26.09.2026: https://mempool.space/api/v1/mining/hashrate/1m (currentHashrate ≈ $9{,}34 \cdot 10^{20}$ H/s; дневные средние 24–26.09.2026: 837, 933, 880 ЭХ/с); https://mempool.space/api/v1/mining/pools/1m (оценка за месяц ≈ $1{,}02 \cdot 10^{21}$ H/s)). Свежие цифры — в приложении Б.

[423] сайт правительства КНР gov.cn, сообщение о 51-м заседании Комитета, 21.05.2021, https://www.gov.cn/xinwen/2021-05/21/content_5610192.htm.

[424] Сообщение о 51-м заседании Комитета по финансовой стабильности и развитию Госсовета КНР, gov.cn, 21.05.2021: «##########». Общий запрет операций с криптовалютой последовал 24.09.2021 (сайт правительства КНР gov.cn, сообщение о 51-м заседании Комитета, 21.05.2021, https://www.gov.cn/xinwen/2021-05/21/content_5610192.htm).

[425] A. de Vries, U. Gallersdörfer, L. Klaaßen, C. Stoll, «Revisiting Bitcoin's carbon footprint», Joule 6(3), 2022, pp. 498–502, DOI 10.1016/j.joule.2022.02.005; цифры по Euronews, «Bitcoin mining was actually worse for the environment since China banned it, a new study says», 26.02.2022, https://www.euronews.com/next/2022/02/26/bitcoin-mining-was-actually-worse-for-the-environment-since-china-banned-it-a-new-study-sa; библиография — репозиторий VU Amsterdam, https://research.vu.nl/en/publications/revisiting-bitcoins-carbon-footprint/.

[426] mempool.space, история корректировок сложности, https://mempool.space/api/v1/mining/difficulty-adjustments/all (запись: метка 1625294046, высота 689472, коэффициент 0,720573).

[427] Блок 689 472; сложность умножена на 0,7206 (mempool.space) (mempool.space, история корректировок сложности, https://mempool.space/api/v1/mining/difficulty-adjustments/all (запись: метка 1625294046, высота 689472, коэффициент 0,720573)). По данным Кембриджского центра альтернативных финансов, мощность сети после запрета упала до 57,47 эксахешей в секунду, а к февралю 2022 года поднялась до рекордных 248,11 (Cambridge Judge Business School / CCAF, «Bitcoin mining – an (un)surprising resurgence?», 17.05.2022, https://www.jbs.cam.ac.uk/2022/bitcoin-mining-new-data-reveal-a-surprising-resurgence/).

сверху для этого не понадобилось. К концу июля сложность опять пошла вверх[428], а к февралю 2022 года мощность сети достигла нового рекорда[429].

Запрет к тому же не выгнал майнинг из Китая целиком. По данным Кембриджского центра альтернативных финансов, летом 2021 года доля Китая в мощности сети упала почти до нуля, но к январю 2022 года вернулась к 21%, второму месту после США; авторы объясняют это заметным подпольным майнингом[430].[431] Государство может запретить майнинг на своей территории и выгнать часть майнеров, а тетрадку остановить ему нечем, потому что работу ушедших термостат перераспределяет между оставшимися. Эту проверку я считаю самой наглядной из всех, что прошла тетрадка без хранителя: правило сработало само, ровно так, как было задумано[432].

Расписание выпуска держит и урезание награды за страницу, которое называют халвингом. Примерно раз в четыре года награда уменьшается вдвое, поэтому общее число биткоинов приближается к 21 млн[433]. Четыре халвинга уже прошли, и за страницу теперь дают 3,125 BTC вместо первоначальных 50[434].[435] Уже выпущенных монет халвинг не касается, он сокращает только выпуск новых[436].

---

[428] mempool.space, история корректировок сложности, https://mempool.space/api/v1/mining/difficulty-adjustments/all (запись: метка 1625294046, высота 689472, коэффициент 0,720573).

[429] Cambridge Judge Business School / CCAF, «Bitcoin mining – an (un)surprising resurgence?», 17.05.2022, https://www.jbs.cam.ac.uk/2022/bitcoin-mining-new-data-reveal-a-surprising-resurgence/.

[430] Cambridge Judge Business School / CCAF, «Bitcoin mining – an (un)surprising resurgence?», 17.05.2022, https://www.jbs.cam.ac.uk/2022/bitcoin-mining-new-data-reveal-a-surprising-resurgence/; CoinDesk (James Van Straten), «China Returns as Third Largest BTC Mining Hub With a 14% Share: Reuters», 24.11.2025, https://www.coindesk.com/markets/2025/11/24/china-returns-as-third-largest-bitcoin-mining-hub-with-a-14-share-reuters.

[431] Cambridge Judge Business School / CCAF. Bitcoin mining – an (un)surprising resurgence? 17.05.2022: доля Китая в январе 2022 года — 21,11%, США — 37,84%, далее Казахстан (13,22%), Канада (6,48%), Россия (4,66%); «…significant underground mining activity has formed in the country…» Данные только от четырёх пулов, геолокация по IP может обманываться VPN и прокси (Cambridge Judge Business School / CCAF, «Bitcoin mining – an (un)surprising resurgence?», 17.05.2022, https://www.jbs.cam.ac.uk/2022/bitcoin-mining-new-data-reveal-a-surprising-resurgence/). В октябре 2025 года на Китай, по отраслевым оценкам (Hashrate Index в пересказе CoinDesk со ссылкой на Reuters), приходилось около 14% мощности; компания CryptoQuant оценивала долю Китая в 15–20% (CoinDesk (James Van Straten), «China Returns as Third Largest BTC Mining Hub With a 14% Share: Reuters», 24.11.2025, https://www.coindesk.com/markets/2025/11/24/china-returns-as-third-largest-bitcoin-mining-hub-with-a-14-share-reuters). Свежие цифры — в приложении Б.

[432] Bitcoin Wiki, «Difficulty», https://en.bitcoin.it/wiki/Difficulty; принцип — Nakamoto, 2008, раздел 4 («the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour»); mempool.space, история корректировок сложности, https://mempool.space/api/v1/mining/difficulty-adjustments/all (запись: метка 1625294046, высота 689472, коэффициент 0,720573).

[433] Bitcoin Wiki, «Controlled supply», https://en.bitcoin.it/wiki/Controlled_supply.

[434] Bitcoin Wiki, «Halving day 2012», https://en.bitcoin.it/wiki/Halving_day_2012; таблица эпох: https://en.bitcoin.it/wiki/Controlled_supply; The Block, «Bitcoin ushers in fourth halving as miners' block subsidy reward drops to 3.125 BTC», 20.04.2024, https://www.theblock.co/post/289875/bitcoin-ushers-in-fourth-halving-as-miners-block-subsidy-reward-drops-to-3-125-btc; перенесено из https://www.theblock.co/post/289875/bitcoin-ushers-in-fourth-halving-as-miners-block-subsidy-reward-drops-to-3-125-btc (там же CNBC, 19.04.2024).

[435] Награда уменьшается вдвое каждые 210 000 блоков; последняя монета при нынешнем темпе появится около 2140 года (Bitcoin Wiki, «Controlled supply», https://en.bitcoin.it/wiki/Controlled_supply). Первый халвинг — блок 210 000, 28.11.2012, награда 50 → 25 BTC (Bitcoin Wiki, «Halving day 2012», https://en.bitcoin.it/wiki/Halving_day_2012; таблица эпох: https://en.bitcoin.it/wiki/Controlled_supply); второй — блок 420 000, 09.07.2016, 25 → 12,5 BTC (данные блокчейна через mempool.space: https://mempool.space/api/block-height/420000 → блок 000000000000000002cce816c0ab2c5c269cb081896b7dcb34b8422d6b74ffa1, метка времени 1468082773 (09.07.2016, 16:46 UTC); The Block, 20.04.2024 (перечень прошлых халвингов), https://www.theblock.co/post/289875/bitcoin-ushers-in-fourth-halving-as-miners-block-subsidy-reward-drops-to-3-125-btc); третий — блок 630 000, 11.05.2020, 12,5 → 6,25 BTC (mempool.space, https://mempool.space/api/block-height/630000 → блок 000000000000000000024bead8df69990852c202db0e0097c1a12ea637d7e96d, метка времени 1589225023 (11.05.2020, 19:23 UTC); The Block, 20.04.2024 («the last halving on May 11, 2020»)); четвёртый — блок 840 000, 20.04.2024 по всемирному времени, 6,25 → 3,125 BTC, дневная добыча сократилась примерно с 900 до 450 BTC (The Block, «Bitcoin ushers in fourth halving as miners' block subsidy reward drops to 3.125 BTC», 20.04.2024, https://www.theblock.co/post/289875/bitcoin-ushers-in-fourth-halving-as-miners-block-subsidy-reward-drops-to-3-125-btc; перенесено из https://www.theblock.co/post/289875/bitcoin-ushers-in-fourth-halving-as-miners-block-subsidy-reward-drops-to-3-125-btc (там же CNBC, 19.04.2024)). Пятый ожидается на блоке 1 050

В первой главе я обещал показать, во что обходится предел выпуска. Награда за страницу служит главной платой майнерам за охрану тетрадки, и по правилам она сжимается к нулю. После этого майнерам останутся только комиссии, которые платят сами пользователи; так было задумано ещё в статье 2008 года[437]. Сегодня до этого далеко. С осени 2025 года комиссии дают майнерам меньше процента дохода, и, по данным аналитической компании Glassnode, это минимум за десять лет[438].[439]

Бывало и по-другому. 20 апреля 2024 года, в день четвёртого халвинга, заработала новая надстройка для выпуска собственных монет поверх биткоина, и желающих записаться на страницы стало так много, что в отдельных блоках комиссии дали до трёх четвертей дохода майнеров[440]. К началу 2025 года ажиотаж схлынул, и на комиссии снова приходилось чуть больше процента[441]. Один день показал, как могла бы выглядеть охрана, оплаченная пользователями, и тут же выяснилось, что такой спрос сам по себе не держится.

Хватит ли комиссий, когда новых монет почти не станет, — открытый вопрос, и у него есть две известные постановки. Группа исследователей из Принстона показала в 2016 году на модели, что сеть, где майнеров кормят одни комиссии, становится неустойчивой: доход от страницы сильно зависит от везения, и майнеру выгоднее переписать чужую «богатую» страницу, чтобы забрать её комиссии себе[442].[443] Экономист Эрик Будиш из Чикагского университета смотрит шире. Чтобы атака не окупалась, постоянные выплаты майнерам должны быть

000, около 2028 года; точная дата зависит от темпа блоков (Bitcoin Wiki, «Controlled supply» («next expected around 2028»), https://en.bitcoin.it/wiki/Controlled_supply).

[436] Bitcoin Wiki, «Controlled supply», https://en.bitcoin.it/wiki/Controlled_supply.

[437] Bitcoin Wiki, «Controlled supply», https://en.bitcoin.it/wiki/Controlled_supply.

[438] J. Butterfill (CoinShares), «Bitcoin Mining Report — Q1 2026», 25.03.2026, https://coinshares.com/insights/research-data/bitcoin-mining-report-q1-2026/; W. Suberg, «Bitcoin Miner Squeeze In Focus As Fees Make Up Under 0.7% Of Revenue», Cointelegraph, 12.08.2026, https://cointelegraph.com/markets/bitcoin-miners-earn-under-07-of-revenue-from-fees-in-new-10-year-low.

[439] По данным Glassnode в пересказе Cointelegraph (12.08.2026), в августе 2026 года комиссии давали около 0,69% дохода майнеров, ниже 1% доля держалась почти год; сооснователь Glassnode Рафаэль Шульце-Крафт: «Bitcoin was below $400 the last time fee share was this low» (W. Suberg, «Bitcoin Miner Squeeze In Focus As Fees Make Up Under 0.7% Of Revenue», Cointelegraph, 12.08.2026, https://cointelegraph.com/markets/bitcoin-miners-earn-under-07-of-revenue-from-fees-in-new-10-year-low). По отчёту CoinShares, в четвёртом квартале 2025 года комиссии составляли «consistently below 1% of total block rewards», в среднем около 0,018 BTC на блок при награде 3,125 BTC (J. Butterfill (CoinShares), «Bitcoin Mining Report — Q1 2026», 25.03.2026, https://coinshares.com/insights/research-data/bitcoin-mining-report-q1-2026/). 20.04.2024, в день запуска протокола Runes, средняя комиссия достигла рекордных 127,97 доллара, а доля комиссий в доходе за блок — 75% (CoinDesk по данным BitInfoCharts и YCharts; это пик по отдельным блокам, а не среднее за день) (B. Keoun, «Bitcoin Miners Reap Windfall as ‘Runes’ Debut Sends Transaction Fees to Record Highs», CoinDesk, 21.04.2024, https://www.coindesk.com/tech/2024/04/21/bitcoin-miners-reap-windfall-as-runes-debut-sends-transaction-fees-to-record-highs). Coin Metrics: в первом квартале 2025 года на комиссии пришлось 1,33% дохода майнеров, около 3,6 млрд долларов (T. Ved, «Q1 2025 Bitcoin Data Special», Coin Metrics’ State of the Network, Issue 304, 25.03.2025, https://coinmetrics.substack.com/p/state-of-the-network-issue-304). Свежие цифры — в приложении Б.

[440] B. Keoun, «Bitcoin Miners Reap Windfall as ‘Runes’ Debut Sends Transaction Fees to Record Highs», CoinDesk, 21.04.2024, https://www.coindesk.com/tech/2024/04/21/bitcoin-miners-reap-windfall-as-runes-debut-sends-transaction-fees-to-record-highs.

[441] T. Ved, «Q1 2025 Bitcoin Data Special», Coin Metrics’ State of the Network, Issue 304, 25.03.2025, https://coinmetrics.substack.com/p/state-of-the-network-issue-304.

[442] M. Carlsten, H. Kalodner, S. M. Weinberg, A. Narayanan, «On the Instability of Bitcoin Without the Block Reward», Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS ’16), pp. 154–167, DOI 10.1145/2976749.2978408; PDF: https://www.cs.princeton.edu/~smattw/CKWN-CCS16.pdf; популярное изложение — A. Narayanan, CITP Blog, 21.10.2016, https://blog.citp.princeton.edu/2016/10/21/bitcoin-is-unstable-without-the-block-reward/.

[443] Carlsten M., Kalodner H., Weinberg S. M., Narayanan A. On the Instability of Bitcoin Without the Block Reward. ACM CCS ’16, pp. 154–167. В изложении Нараянана: «with only transaction fees, the variance of the miner reward is very high due to the randomness of the block arrival time, and it becomes attractive to fork a „wealthy“ block to „steal“ the rewards therein» (M. Carlsten, H. Kalodner, S. M. Weinberg, A. Narayanan, «On the Instability of Bitcoin Without the Block Reward», Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS ’16), pp. 154–167, DOI 10.1145/2976749.2978408; PDF: https://www.cs.princeton.edu/~smattw/CKWN-CCS16.pdf; популярное изложение — A. Narayanan, CITP Blog, 21.10.2016, https://blog.citp.princeton.edu/2016/10/21/bitcoin-is-unstable-without-the-block-reward/).

велики по сравнению с разовой выгодой от атаки, поэтому охрана дорожает вместе с ценностью, которую сеть хранит[444].[445]

Обе работы — модели, а не наблюдения, и до последней монеты больше века[446], поэтому прогноз в любую сторону я считал бы гаданием. Сам расчёт прозрачен. Предел выпуска защищает держателей от хранителя, который пишет лишние строчки, а оплачивать эту защиту со временем придётся тем, кто пользуется тетрадкой.

В популярном описании биткоина тетрадку ведут тысячи равных участников. Узлов, которые хранят копию и проверяют каждую запись, действительно десятки тысяч[447]. Страницы же пишут майнеры, и среди них картина другая.

В сутки выходит около 144 страниц (по одной в десять минут). Если ваши машины дают одну стотысячную мощности сети, вы в среднем будете находить одну страницу примерно раз в 700 дней. Среднее здесь обманчиво. Страница может выпасть завтра, а может не выпасть и за пять лет, и всё это время счета за электричество придётся оплачивать каждый месяц. Поэтому майнеры объединяются в пулы и складывают мощность.

Крупнейший из них платит участнику за каждую сданную порцию перебора по средней ожидаемой цене, независимо от того, нашёл ли пул в этот день страницу, а риск невезения берёт на себя за комиссию[448].[449] Каждый получает свою долю небольшими, зато регулярными порциями. Пул, как правило, служит координатором и машинами участников не владеет (бывают исключения: один из крупных пулов добывает на машинах собственной компании[450]). Зато он собирает черновик страницы, то есть решает, какие записи в неё войдут, и раздаёт участникам перебор, а участники могут уйти в другой пул за часы[451].

Право решать, какие записи войдут в страницу, и есть главная власть пула. Пул, который откажется включать чьи-то переводы, задержит их, но навсегда не остановит, потому что их включит в свою страницу другой пул (если только отказ не станет общим для большинства мощности, а это уже знакомая нам атака большинства).

За месяц до 26 сентября 2026 года три крупнейших пула нашли около 60% всех блоков биткоина[452].[453] Трёх координаторов хватило бы, чтобы собрать больше половины мощности

---

[444] E. Budish, «The Economic Limits of Bitcoin and the Blockchain», NBER Working Paper 24717, June 2018, https://www.nber.org/papers/w24717; журнальная версия — E. Budish, «Trust at Scale: The Economic Limits of Cryptocurrencies and Blockchains», The Quarterly Journal of Economics 140(1), 2025, https://academic.oup.com/qje/article/140/1/1/7824430.

[445] Budish E. The Economic Limits of Bitcoin and the Blockchain. NBER Working Paper 24717, 2018: «the recurring, „flow", payments to miners for running the blockchain must be large relative to the one-off, „stock", benefits of attacking it. This is very expensive!» Журнальная версия — The Quarterly Journal of Economics, 2025. Сумму, которую сеть платит майнерам за охрану, в отрасли называют «бюджетом безопасности»; у Будиша этого выражения нет (E. Budish, «The Economic Limits of Bitcoin and the Blockchain», NBER Working Paper 24717, June 2018, https://www.nber.org/papers/w24717; журнальная версия — E. Budish, «Trust at Scale: The Economic Limits of Cryptocurrencies and Blockchains», The Quarterly Journal of Economics 140(1), 2025, https://academic.oup.com/qje/article/140/1/1/7824430).

[446] Bitcoin Wiki, «Controlled supply», https://en.bitcoin.it/wiki/Controlled_supply.

[447] BTC Nodes (Bitnodes), https://btcnodes.io/; API снимка: https://btcnodes.io/api/v1/snapshots/latest/ (обращение 2026-09-26; старый адрес bitnodes.io перенаправляет туда). Оператор — Rodrigo Martínez.

[448] Foundry USA Pool, FAQ «What is Foundry USA Pool's Payout Methodology?», https://pool-faq.foundrydigital.com/what-is-foundry-usa-pools-payout-methodology.

[449] Foundry USA Pool, FAQ: «Foundry USA Pool pays out to all pool members according to the Full-Pay-Per-Share (FPPS) payout scheme»; доход участника считается по принятым долям работы, а не по найденным блокам (Foundry USA Pool, FAQ «What is Foundry USA Pool's Payout Methodology?», https://pool-faq.foundrydigital.com/what-is-foundry-usa-pools-payout-methodology). Исключение из правила «пул не владеет машинами» — MARA Pool: «MARA Pool is the only self-owned and operated mining pool among public miners» (MARA, пресс-релиз за май 2025 года) (MARA, пресс-релиз о добыче за май 2025 года, https://ir.mara.com/news-events/press-releases/detail/1396/mara-announces-bitcoin-production-and-mining-operation-updates-for-may-2025).

[450] MARA, пресс-релиз о добыче за май 2025 года, https://ir.mara.com/news-events/press-releases/detail/1396/mara-announces-bitcoin-production-and-mining-operation-updates-for-may-2025.

[451] mempool.space, https://mempool.space/api/v1/mining/pools/1m (4 546 блоков за месяц; запрос 26.09.2026).

[452] mempool.space, https://mempool.space/api/v1/mining/pools/1m (4 546 блоков за месяц; запрос 26.09.2026).

сети. Надёжного способа оценить, насколько вероятен такой сговор, я не знаю и судить о нём не возьмусь.

Доли эти подвижны. Весной 2026 года у крупнейшего пула было около трети мощности, к осени около четверти[454]. На подвижности и строится главный довод тех, кто считает концентрацию пулов неопасной. Пул, который начнёт злоупотреблять, быстро потеряет майнеров.

Есть довод и в обратную сторону. В 2024 году независимый исследователь под ником b10c сравнил черновики страниц, которые рассылают участникам разные пулы, и выделил девять пулов с подозрительно похожими черновиками. Вместе эти девять пулов нашли за месяц около 37,6% блоков, больше, чем крупнейший пул по официальным данным[455].[456] Сам автор оговаривает, что контроля одного лица это не доказывает[457]. Но официальные доли пулов могут занижать настоящую концентрацию, потому что за разными вывесками может стоять один координатор.

Часть отрасли пытается это исправить. В мае 2026 года крупнейшие пулы, у которых вместе было около трёх четвертей мощности, вступили в рабочую группу открытого стандарта Stratum V2, который позволяет самим майнерам собирать черновик страницы[458].

Сосредоточена и география. В декабре 2022 года, во время зимнего шторма «Эллиотт», майнеры в Северной Америке выключили столько машин, что сеть в тот день лишилась примерно 38% мощности[459]. Авторы, которые это посчитали, вывели отсюда, что не меньше 38% майнинга биткоина к концу 2022 года находилось в США и Канаде[460].[461] Среди крупных ком-

---

[453] mempool.space, 4546 блоков за месяц до 26.09.2026: Foundry USA — 25,4%, AntPool — 19,4%, F2Pool — 15,0%, ViaBTC — 8,7%, SpiderPool — 8,4%, MARA Pool — 5,3%; два крупнейших — около 45%, пять — около 77%. Принадлежность блоков определяется по самоназванию пулов, часть блоков остаётся неизвестной (mempool.space, https://mempool.space/api/v1/mining/pools/1m (4 546 блоков за месяц; запрос 26.09.2026)). Весной 2026 года, по данным Hashrate Index, доля Foundry составляла 34,2% (CoinDesk (Shaurya Malwa), «Bitcoin mining pools with 75% of BTC hashrate join open standard for block construction», 11.05.2026, https://www.coindesk.com/markets/2026/05/11/bitcoin-mining-pools-with-75-of-btc-hashrate-join-open-standard-for-block-construction). Свежие доли — в приложении Б.

[454] CoinDesk (Shaurya Malwa), «Bitcoin mining pools with 75% of BTC hashrate join open standard for block construction», 11.05.2026, https://www.coindesk.com/markets/2026/05/11/bitcoin-mining-pools-with-75-of-btc-hashrate-join-open-standard-for-block-construction; mempool.space, https://mempool.space/api/v1/mining/pools/1m (4 546 блоков за месяц; запрос 26.09.2026).

[455] b10c, «Block Template Similarities between Mining Pools», 16.09.2024, https://b10c.me/observations/12-template-similarity/.

[456] b10c. Block Template Similarities between Mining Pools, 16.09.2024. Черновики AntPool, Poolin и BTC.com совпадали попарно на 98–99%, у остальных пулов из девяти сходство ниже; часть из них временами пересылала задания других пулов. Крупнейшим по официальным данным в тот месяц был Foundry с 31,3% (b10c, «Block Template Similarities between Mining Pools», 16.09.2024, https://b10c.me/observations/12-template-similarity/). В рабочую группу Stratum V2 в мае 2026 года вступили Foundry, AntPool, F2Pool, SpiderPool, MARA Pool, а также Block Inc и DMND — не пулы в обычном смысле (CoinDesk (Shaurya Malwa), «Bitcoin mining pools with 75% of BTC hashrate join open standard for block construction», 11.05.2026, https://www.coindesk.com/markets/2026/05/11/bitcoin-mining-pools-with-75-of-btc-hashrate-join-open-standard-for-block-construction).

[457] b10c, «Block Template Similarities between Mining Pools», 16.09.2024, https://b10c.me/observations/12-template-similarity/.

[458] CoinDesk (Shaurya Malwa), «Bitcoin mining pools with 75% of BTC hashrate join open standard for block construction», 11.05.2026, https://www.coindesk.com/markets/2026/05/11/bitcoin-mining-pools-with-75-of-btc-hashrate-join-open-standard-for-block-construction.

[459] C. Stoll, L. Klaaßen, U. Gallersdörfer, A. Neumüller, «Climate Impacts of Bitcoin Mining in the U.S.», MIT CEEPR Working Paper 2023-11, June 2023, https://ceepr.mit.edu/wp-content/uploads/2023/06/MIT-CEEPR-WP-2023-11.pdf.

[460] C. Stoll, L. Klaaßen, U. Gallersdörfer, A. Neumüller, «Climate Impacts of Bitcoin Mining in the U.S.», MIT CEEPR Working Paper 2023-11, June 2023, https://ceepr.mit.edu/wp-content/uploads/2023/06/MIT-CEEPR-WP-2023-11.pdf.

[461] Stoll C., Klaaßen L., Gallersdörfer U., Neumüller A. Climate Impacts of Bitcoin Mining in the U.S. MIT CEEPR Working Paper 2023-11, June 2023: «This number provides empirical evidence that at least 38% of all Bitcoin mining activity was located in the U.S. and Canada by December 2022.» Сокращение — около 100 эксахешей в секунду. Это рабочий доклад без рецензирования и нижняя граница доли (C. Stoll, L. Klaaßen, U. Gallersdörfer, A. Neumüller, «Climate Impacts of Bitcoin Mining in the U.S.», MIT CEEPR Working Paper 2023-11, June 2023, https://ceepr.mit.edu/wp-content/uploads/2023/06/MIT-CEEPR-WP-2023-11.pdf). Кембриджский опрос: на США пришлось 75,4% добычи внутри выборки из 49 компаний, на Канаду — 7,1%; это доля выборки, и на весь мир её переносить нельзя (Cambridge Judge Business School, «Cambridge study: sustainable energy rising in Bitcoin mining», 28.04.2025, https://www.jbs.cam.ac.uk/2025/cambridge-study-sustainable-energy-rising-in-bitcoin-mining/; отчёт: https://www.jbs.cam.ac.uk/wp-content/uploads/2025/04/2025-04-cambridge-digital-mining-industry-report.pdf).

паний, согласившихся ответить на кембриджский опрос 2025 года, три четверти мощностей стояли в США[462].

Тысяч равных участников в этой картине нет. Есть десятки тысяч узлов, которые проверяют, несколько пулов, которые пишут, и несколько стран, где стоят машины. Защиты, о которой шла речь выше, это не отменяет. Узлы по-прежнему отбрасывают любую недействительную страницу, кто бы её ни написал[463]. Меняется другое. Условие Накамото о честном большинстве мощности на деле держится на независимости небольшого числа пулов.

Во что обходится электричество

Работа, на которой держится голос, — это электричество, и о том, сколько его уходит, спорят по меньшей мере с 2018 года[464]. Считают его двумя способами. Кембриджский центр альтернативных финансов считает от оборудования: берёт мощность сети и характеристики машин, которыми её, вероятно, набирают, и получает потребление[465]. Индекс Digiconomist аналитика Алекса де Вриса считает от денег. Он берёт доход майнеров, предполагает, какую его долю они тратят на электричество, и делит эту сумму на цену киловатт-часа[466].

Кембриджский центр в отчёте, опубликованном в апреле 2025 года, оценил годовое потребление примерно в 138 тераватт-часов (тераватт-час — это миллиард киловатт-часов), около полупроцента мирового потребления электроэнергии[467]. Индекс Digiconomist 26 сентября 2026 года показывал около 204 тераватт-часов[468].[469] Числа относятся к разным датам, и сравнивать их напрямую нельзя.

---

[462] Cambridge Judge Business School, «Cambridge study: sustainable energy rising in Bitcoin mining», 28.04.2025, https://www.jbs.cam.ac.uk/2025/cambridge-study-sustainable-energy-rising-in-bitcoin-mining/; отчёт: https://www.jbs.cam.ac.uk/wp-content/uploads/2025/04/2025-04-cambridge-digital-mining-industry-report.pdf.

[463] Nakamoto, 2008, раздел 5 «Network», https://bitcoin.org/bitcoin.pdf.

[464] Semantic Scholar API, метаданные DOI 10.1016/j.joule.2018.04.016 и 10.1016/j.joule.2022.02.005, https://api.semanticscholar.org/graph/v1/paper/DOI:10.1016/j.joule.2022.02.005.

[465] CCAF, «CBECI — Methodology», https://ccaf.io/cbnsi/cbeci/methodology.

[466] Digiconomist, «Bitcoin Energy Consumption Index», https://digiconomist.net/bitcoin-energy-consumption (обращение 26.09.2026).

[467] Cambridge Judge Business School, 28.04.2025, https://www.jbs.cam.ac.uk/2025/cambridge-study-sustainable-energy-rising-in-bitcoin-mining/ (перенесено из https://www.jbs.cam.ac.uk/2025/cambridge-study-sustainable-energy-rising-in-bitcoin-mining/, перепроверено).

[468] Digiconomist, «Bitcoin Energy Consumption Index», https://digiconomist.net/bitcoin-energy-consumption (обращение 26.09.2026).

[469] Оценки годового потребления биткоина: Кембриджский центр альтернативных финансов, отчёт от апреля 2025 года, — около 138 ТВт·ч (около 0,54% мирового потребления) и 39,8 Мт CO2-экв. (Cambridge Judge Business School, 28.04.2025, https://www.jbs.cam.ac.uk/2025/cambridge-study-sustainable-energy-rising-in-bitcoin-mining/ (перенесено из https://www.jbs.cam.ac.uk/2025/cambridge-study-sustainable-energy-rising-in-bitcoin-mining/, перепроверено)); Университет ООН за 2020–2021 годы — 173,42 ТВт·ч (United Nations University, пресс-релиз «UN Study Reveals the Hidden Environmental Impacts of Bitcoin: Carbon is Not the Only Harmful By-product», 24.10.2023, https://unu.edu/press-release/un-study-reveals-hidden-environmental-impacts-bitcoin-carbon-not-only-harmful-product; статья: S. Chamanara, S. A. Ghaffarizadeh, K. Madani, «The environmental footprint of Bitcoin mining across the globe: Call for urgent action», Earth's Future 11, e2023EF003871, https://agupubs.onlinelibrary.wiley.com/doi/10.1029/2023EF003871); Digiconomist на 26.09.2026 — около 204 ТВт·ч и 114 Мт CO2 (Digiconomist, «Bitcoin Energy Consumption Index», https://digiconomist.net/bitcoin-energy-consumption (обращение 26.09.2026)). Кембриджская оценка, судя по данным публикации (рост на 17% за год, характеристики машин на июнь 2024 года), относится к 2024 году; получена ли она живой моделью или расчётом по опросу компаний, в публикации не сказано (Cambridge Judge Business School, 28.04.2025, https://www.jbs.cam.ac.uk/2025/cambridge-study-sustainable-energy-rising-in-bitcoin-mining/ (перенесено из https://www.jbs.cam.ac.uk/2025/cambridge-study-sustainable-energy-rising-in-bitcoin-mining/, перепроверено)). Сам кембриджский индекс называет свой подход «гибридным сверху вниз» (по методу Марка Бевана), даёт три оценки (нижнюю, верхнюю и наиболее вероятную) и принимает цену электричества в 5 центов за кВт·ч (CCAF, «CBECI — Methodology», https://ccaf.io/cbnsi/cbeci/methodology). Digiconomist на дату обращения закладывал, что на электричество уходит около 73,6% дохода майнеров (Digiconomist, «Bitcoin Energy Consumption Index», https://digiconomist.net/bitcoin-energy-consumption (обращение 26.09.2026)). Для сравнения, в 2019 году опубликованные оценки лежали в диапазоне примерно 20–80 ТВт·ч (G. Kamiya, «Bitcoin energy use — mined the gap», IEA Commentary, 04.07.2019, https://www.iea.org/commentaries/

Но и на одну дату два способа не обязаны совпасть. Авторы кембриджской оценки сами называют слабые места своего счёта: настоящий состав парка машин неизвестен, а цена электричества принята одинаковой для всех[470]. Счёт от денег упрекают в завышении. Исследователь энергопотребления Джонатан Куми писал, что оценки индекса стабильно примерно вдвое выше более надёжных[471].[472] (Куми опубликовал это у некоммерческой организации, которая защищает интересы криптоиндустрии, так что заинтересованы в споре обе стороны[473].)

Вот условный расчёт от денег с круглыми числами. Майнеры за год заработали 10 млрд долларов; если 60% этой суммы ушло на электричество по 5 центов за киловатт-час, получается 6 млрд долларов, то есть 120 тераватт-часов. Возьмите вместо 60% тридцать, и оценка упадёт вдвое, хотя в сети не изменилась ни одна машина. А если майнеры на деле платят за киловатт-час меньше 5 центов, та же сумма покупает больше энергии, и оценка вырастет. Спор между методами во многом сводится к тому, каким из этих допущений верить[474].

Одну метрику из этого спора стоит отбросить сразу — энергию на одну транзакцию (у Digiconomist около 804 киловатт-часов[475]). Аналитик Международного энергетического агентства называл такие сравнения для сетей с доказательством работы бессмысленными, потому что энергия, которая нужна сети, от числа транзакций не зависит[476].[477] Это видно и по нашей модели: термостат держит темп страниц, сколько бы записей на них ни лежало[478]. Если записей на каждой странице станет вдвое больше, счёт за электричество не изменится, а «энергия на транзакцию» упадёт вдвое.

Второй спор — о том, из чего это электричество. Доля возобновляемой энергии в оценках лежит между неполной четвертью и двумя пятыми, а вместе с атомной самая высокая оценка превышает половину. Низкие получены по географии майнинга: у Университета ООН за 2020–2021 годы возобновляемых около 23%[479], у де Вриса и соавторов около четверти в августе 2021 года, когда после китайского запрета майнеры лишились гидроэнергии южных провинций и переехали в Казахстан, где много угля, и в США, где много газа[480].[481] Самая высокая —

---

bitcoin-energy-use-mined-the-gap). Свежие цифры — в приложении Б.

[470] CCAF, «CBECI — Methodology», https://ccaf.io/cbnsi/cbeci/methodology.

[471] J. Koomey, «Estimating Bitcoin Electricity Use: A Beginner's Guide», Coin Center, май 2019, https://www.coincenter.org/estimating-bitcoin-electricity-use-a-beginners-guide/; G. Kamiya, «Bitcoin energy use — mined the gap», IEA Commentary, 04.07.2019, https://www.iea.org/commentaries/bitcoin-energy-use-mined-the-gap.

[472] Koomey J. Estimating Bitcoin Electricity Use: A Beginner's Guide. Coin Center, May 2019: «consistently about a factor of two higher than the more credible estimates». Критика, которую пересказывает МЭА (Kamiya, 2019), касалась допущения, что майнеры тратят на электричество 60% дохода: «These key assumptions have been criticised to overestimate electricity consumption» (G. Kamiya, «Bitcoin energy use — mined the gap», IEA Commentary, 04.07.2019, https://www.iea.org/commentaries/bitcoin-energy-use-mined-the-gap).

[473] J. Koomey, «Estimating Bitcoin Electricity Use: A Beginner's Guide», Coin Center, май 2019, https://www.coincenter.org/estimating-bitcoin-electricity-use-a-beginners-guide/.

[474] CCAF, «CBECI — Methodology», https://ccaf.io/cbnsi/cbeci/methodology; G. Kamiya, «Bitcoin energy use — mined the gap», IEA Commentary, 04.07.2019, https://www.iea.org/commentaries/bitcoin-energy-use-mined-the-gap.

[475] Digiconomist, «Bitcoin Energy Consumption Index», https://digiconomist.net/bitcoin-energy-consumption (обращение 26.09.2026).

[476] G. Kamiya, «Bitcoin energy use — mined the gap», IEA Commentary, 04.07.2019, https://www.iea.org/commentaries/bitcoin-energy-use-mined-the-gap.

[477] Kamiya G. Bitcoin energy use — mined the gap. IEA Commentary, 04.07.2019: «comparisons on a per-transaction basis are not meaningful in the context of PoW blockchains, particularly because the energy required for the networks to function is independent of the number of processed transactions.»

[478] API mempool.space, https://mempool.space/api/v1/blocks (обращение 2026-09-26).

[479] United Nations University, пресс-релиз «UN Study Reveals the Hidden Environmental Impacts of Bitcoin: Carbon is Not the Only Harmful By-product», 24.10.2023, https://unu.edu/press-release/un-study-reveals-hidden-environmental-impacts-bitcoin-carbon-not-only-harmful-product; статья: S. Chamanara, S. A. Ghaffarizadeh, K. Madani, «The environmental footprint of Bitcoin mining across the globe: Call for urgent action», Earth's Future 11, e2023EF003871, https://agupubs.onlinelibrary.wiley.com/doi/10.1029/2023EF003871.

[480] A. de Vries, U. Gallersdörfer, L. Klaaßen, C. Stoll, «Revisiting Bitcoin's carbon footprint», Joule 6(3), 2022, pp. 498–

самоотчёт 49 компаний в кембриджском опросе 2025 года. Эти компании, в основном крупные западные, покрывают примерно половину мирового майнинга, а как обстоят дела у другой половины, не знает никто[482].[483]

Число о биткоине и электричестве без года, метода и предмета счёта мало что говорит,[484] а прогноз — ещё и без объяснения, почему нынешний рост должен продолжаться. Сам я держусь порядка величины, в котором сходятся серьёзные оценки, то есть около полупроцента мирового электричества[485]. В сравнительной таблице на сайте Ethereum (оценки на июль 2023 года) рядом с биткоином стоят добыча золота и все дата-центры мира, и у всех трёх числа одного порядка[486].[487]

502, DOI 10.1016/j.joule.2022.02.005; цифры по Euronews, «Bitcoin mining was actually worse for the environment since China banned it, a new study says», 26.02.2022, https://www.euronews.com/next/2022/02/26/bitcoin-mining-was-actually-worse-for-the-environment-since-china-banned-it-a-new-study-sa; библиография — репозиторий VU Amsterdam, https://research.vu.nl/en/publications/revisiting-bitcoins-carbon-footprint/.

[481] Де Врис и соавторы (Joule, 2022): доля возобновляемых источников упала с 41,6% в 2020 году до 25,1% в августе 2021 года (A. de Vries, U. Gallersdörfer, L. Klaaßen, C. Stoll, «Revisiting Bitcoin's carbon footprint», Joule 6(3), 2022, pp. 498–502, DOI 10.1016/j.joule.2022.02.005; цифры по Euronews, «Bitcoin mining was actually worse for the environment since China banned it, a new study says», 26.02.2022, https://www.euronews.com/next/2022/02/26/bitcoin-mining-was-actually-worse-for-the-environment-since-china-banned-it-a-new-study-sa; библиография — репозиторий VU Amsterdam, https://research.vu.nl/en/publications/revisiting-bitcoins-carbon-footprint/). Сам де Врис заключил, что добровольные климатические обещания отрасли не работают; в статье Euronews от 26.02.2022: «It clearly is not working because the network actually got less green during the year». Авторы оценивали и выбросы сети после переезда — около 65,4 Мт CO2 в год, сопоставимо с выбросами Греции (A. de Vries, U. Gallersdörfer, L. Klaaßen, C. Stoll, «Revisiting Bitcoin's carbon footprint», Joule 6(3), 2022, pp. 498–502, DOI 10.1016/j.joule.2022.02.005; цифры по Euronews, «Bitcoin mining was actually worse for the environment since China banned it, a new study says», 26.02.2022, https://www.euronews.com/next/2022/02/26/bitcoin-mining-was-actually-worse-for-the-environment-since-china-banned-it-a-new-study-sa; библиография — репозиторий VU Amsterdam, https://research.vu.nl/en/publications/revisiting-bitcoins-carbon-footprint/).

[482] Cambridge Judge Business School, «Cambridge study: sustainable energy rising in Bitcoin mining», 28.04.2025, https://www.jbs.cam.ac.uk/2025/cambridge-study-sustainable-energy-rising-in-bitcoin-mining/; отчёт: https://www.jbs.cam.ac.uk/wp-content/uploads/2025/04/2025-04-cambridge-digital-mining-industry-report.pdf; Cambridge Judge Business School, 28.04.2025, https://www.jbs.cam.ac.uk/2025/cambridge-study-sustainable-energy-rising-in-bitcoin-mining/ (перенесено из https://www.jbs.cam.ac.uk/2025/cambridge-study-sustainable-energy-rising-in-bitcoin-mining//https://www.jbs.cam.ac.uk/wp-content/uploads/2025/04/2025-04-cambridge-digital-mining-industry-report.pdf, перепроверено).

[483] Университет ООН за 2020–2021 годы: уголь — 45%, газ — 21%, гидроэнергия — 16%, атомная — 9%, ветер — 5%, солнце — 2% (United Nations University, пресс-релиз «UN Study Reveals the Hidden Environmental Impacts of Bitcoin: Carbon is Not the Only Harmful By-product», 24.10.2023, https://unu.edu/press-release/un-study-reveals-hidden-environmental-impacts-bitcoin-carbon-not-only-harmful-product; статья: S. Chamanara, S. A. Ghaffarizadeh, K. Madani, «The environmental footprint of Bitcoin mining across the globe: Call for urgent action», Earth's Future 11, e2023EF003871, https://agupubs.onlinelibrary.wiley.com/doi/10.1029/2023EF003871). Кембриджский опрос 2025 года: 52,4% из «устойчивых» источников (42,6% — возобновляемые, 9,8% — атомная энергия), газ — 38,2%, уголь — 8,9%; в 2022 году угля было 36,6% (Cambridge Judge Business School, 28.04.2025, https://www.jbs.cam.ac.uk/2025/cambridge-study-sustainable-energy-rising-in-bitcoin-mining/ (перенесено из https://www.jbs.cam.ac.uk/2025/cambridge-study-sustainable-energy-rising-in-bitcoin-mining//https://www.jbs.cam.ac.uk/wp-content/uploads/2025/04/2025-04-cambridge-digital-mining-industry-report.pdf, перепроверено)). Снимки сделаны разными методами для разных лет и выборок, поэтому сравнивать их как один ряд нельзя. Группа, которая считала последствия шторма «Эллиотт», оценила, что электричество тринадцати публичных майнеров США было примерно таким же «грязным», как в среднем по американской энергосистеме; вывод получен по средним коэффициентам выбросов энергосистемы (C. Stoll, L. Klaaßen, U. Gallersdörfer, A. Neumüller, «Climate Impacts of Bitcoin Mining in the U.S.», MIT CEEPR Working Paper 2023-11, June 2023, https://ceepr.mit.edu/wp-content/uploads/2023/06/MIT-CEEPR-WP-2023-11.pdf).

[484] Даже государственная статистика даёт широкую вилку. U.S. EIA. Tracking electricity consumption from U.S. cryptocurrency mining operations, 01.02.2024: «annual electricity use from cryptocurrency mining probably represents from 0.6% to 2.3% of U.S. electricity consumption», то есть нижняя и верхняя оценки различаются почти вчетверо. Ведомство выявило 137 майнинговых объектов (U.S. EIA, «Tracking electricity consumption from U.S. cryptocurrency mining operations», Today in Energy, 01.02.2024, https://www.eia.gov/todayinenergy/detail.php?id=61364).

[485] Cambridge Judge Business School, 28.04.2025, https://www.jbs.cam.ac.uk/2025/cambridge-study-sustainable-energy-rising-in-bitcoin-mining/ (перенесено из https://www.jbs.cam.ac.uk/2025/cambridge-study-sustainable-energy-rising-in-bitcoin-mining/, перепроверено); ethereum.org, «Ethereum energy consumption», https://ethereum.org/en/energy-consumption/ (обращение 26.09.2026).

[486] ethereum.org, «Ethereum energy consumption», https://ethereum.org/en/energy-consumption/ (обращение 26.09.2026).

[487] ethereum.org, «Ethereum energy consumption»: биткоин — 149 ТВт·ч в год, мировые дата-центры — 190, добыча золота — 131. Сайт — заинтересованная сторона; оценки собраны в июле 2023 года, источники даны ссылками в таблице (ethereum.org, «Ethereum energy consumption», https://ethereum.org/en/energy-consumption/ (обращение 26.09.2026)).

Много это или мало, зависит от того, за что платят. В начале главы предатель мог нарисовать себе тысячу генералов, потому что ключи ничего не стоят. Электричество делает каждого генерала дорогим, и подделать эту цену нельзя, ведь работу любой проверяет одним расчётом[488]. Если бы охрану можно было удешевить, ничего не отдав взамен, атакующий удешевил бы её для себя тем же способом. Поэтому вопрос, может ли биткоин тратить меньше, я бы ставил иначе: какой частью своей безопасности сеть готова за это заплатить и чем эту часть заменит.

Оправдана ли такая плата за охрану тетрадки без хранителя — спор о ценностях, и арифметика его не решит. Сторонники доказательства работы говорят, что энергия и есть стена, которую нужно проломить для атаки, и подделать её нельзя[489]. Критики отвечают, что сравнимую защиту можно получить почти без электричества[490].

Когда за согласие платят мало

Если безопасность держится на том, что атака дороже честной игры, то у маленькой сети и безопасность маленькая. Это можно проверить на истории, потому что атаки большинства случались не раз.

Сначала о том, как атаку превращают в деньги. Допустим, у атакующего 1000 монет небольшой сети. Он переводит их на биржу, продаёт за другие деньги и выводит выручку. Одновременно, втайне от всех, он строит собственную ветвь тетрадки, в которой перевода на биржу нет. Когда биржа выплатила выручку, атакующий выкладывает свою ветвь. Она тяжелее общей, по восьмому правилу узлы переходят на неё, и в новой истории 1000 монет снова лежат у атакующего. Выручка тоже у него, а биржа осталась и без монет, и без денег[491].

---

[488] Nakamoto, 2008, раздел 4, https://bitcoin.org/bitcoin.pdf.

[489] Nakamoto, 2008, раздел 4, https://bitcoin.org/bitcoin.pdf; Nakamoto, 2008, раздел 6 «Incentive», https://bitcoin.org/bitcoin.pdf.

[490] ethereum.org, «The Merge», https://ethereum.org/en/roadmap/merge/; «Ethereum energy consumption», https://ethereum.org/en/energy-consumption/ (перенесено из https://ethereum.org/en/roadmap/merge//https://ethereum.org/energy-consumption/, перепроверено 26.09.2026).

[491] Coinbase, «Coinbase's perspective on the recent Ethereum Classic (ETC) double spend incidents», 2020, https://www.coinbase.com/blog/coinbases-perspective-on-the-recent-ethereum-classic-etc-double-spend (перенесено из https://www.coinbase.com/blog/coinbases-perspective-on-the-recent-ethereum-classic-etc-double-spend).

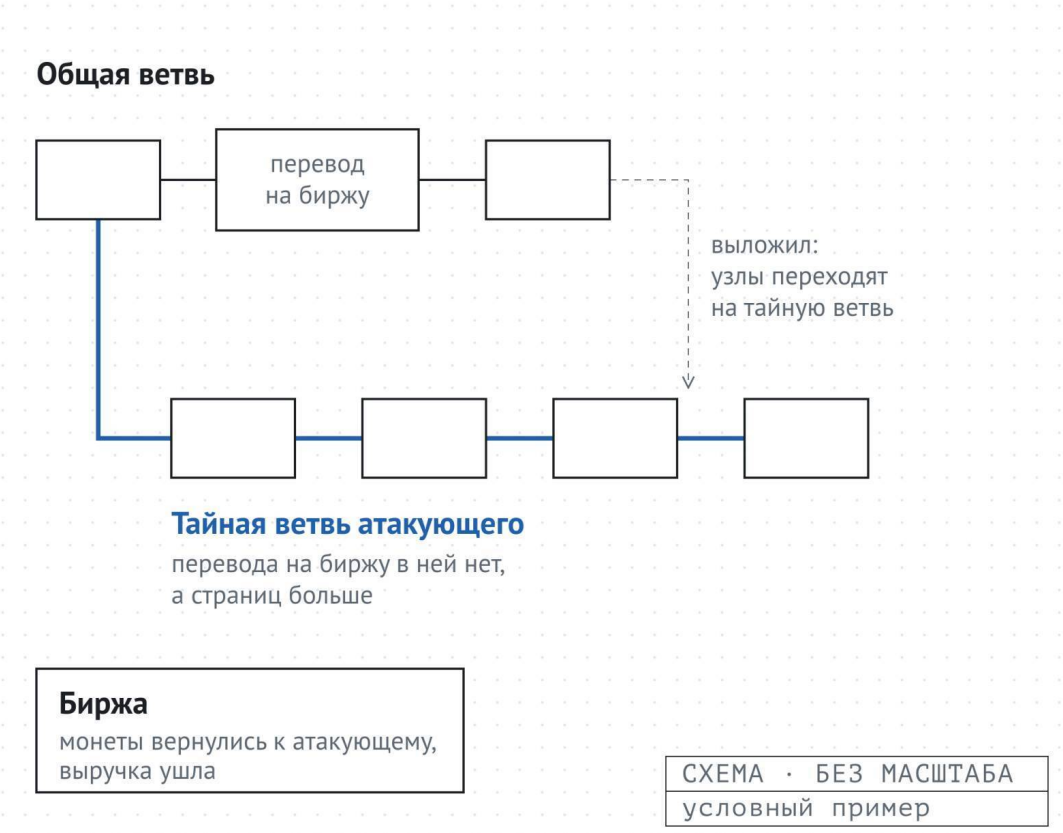


Рисунок 3.2. Атака большинства

Ethereum Classic — отдельная сеть, продолжение старой ветви Ethereum, которая осталась после раскола 2016 года (и об Ethereum, и о расколе речь пойдёт в главе 4)[492]. В августе 2020 года её атаковали трижды за месяц, и последняя атака, 29 августа, переписала больше 7000 блоков, около двух суток работы сети[493].[494] Биржа Coinbase заметила первую атаку по характерному признаку: её узлы перестали видеть новые блоки с ожидаемой частотой[495].[496] В

[492] CoinDesk (Zack Voell), «Ethereum Classic Hit by Third 51% Attack in a Month», 29.08.2020, https://www.coindesk.com/markets/2020/08/29/ethereum-classic-hit-by-third-51-attack-in-a-month (по отчётам майнинговой компании Bitfly); ethereum.org, «Ethereum Fork Timeline» (DAO fork), https://ethereum.org/en/ethereum-forks/.

[493] CoinDesk (Zack Voell), «Ethereum Classic Hit by Third 51% Attack in a Month», 29.08.2020, https://www.coindesk.com/markets/2020/08/29/ethereum-classic-hit-by-third-51-attack-in-a-month (по отчётам майнинговой компании Bitfly).

[494] Первая атака (1 августа) перестроила 3693 блока, вторая — около 4,2 тыс. блоков (CoinDesk (Zack Voell), «Ethereum Classic Hit by Third 51% Attack in a Month», 29.08.2020, https://www.coindesk.com/markets/2020/08/29/ethereum-classic-hit-by-third-51-attack-in-a-month (по отчётам майнинговой компании Bitfly); CoinDesk, «Ethereum Classic Attacker Successfully Double-Spends $1.68M in Second Attack: Report», 07.08.2020, https://www.coindesk.com/markets/2020/08/07/ethereum-classic-attacker-successfully-double-spends-168m-in-second-attack-report). Оценка «около двух суток майнинга» для третьей атаки — майнинговой компании Bitfly в пересказе CoinDesk (CoinDesk (Zack Voell), «Ethereum Classic Hit by Third 51% Attack in a Month», 29.08.2020, https://www.coindesk.com/markets/2020/08/29/ethereum-classic-hit-by-third-51-attack-in-a-month (по отчётам майнинговой компании Bitfly)).

[495] Coinbase, «Coinbase's perspective on the recent Ethereum Classic (ETC) double spend incidents», 08.2020, https://www.coinbase.com/blog/coinbases-perspective-on-the-recent-ethereum-classic-etc-double-spend; цитаты — по Crowdfund Insider, «Coinbase Clarifies It Wasn't Targeted By "Any Of The Attack Transactions" On Etherem Classic (ETC) During 51% Attack And Didn't Lose Funds», 08.2020, https://www.crowdfundinsider.com/2020/08/165589-coinbase-clarifies-it-wasnt-targeted-by-any-of-the-attack-transactions-on-etherem-classic-etc-during-51-attack-and-didnt-lose-funds/.

[496] Coinbase, разбор атак 2020 года, в цитате Crowdfund Insider: «At 11:10 PM PST 7/31/2020, Coinbase Blockchain Security was alerted that Coinbase's ETC nodes were not seeing new blocks at the expected interval.» (Coinbase, «Coinbase's perspective on the recent Ethereum Classic (ETC) double spend incidents», 08.2020, https://www.coinbase.com/

посёлке это выглядело бы так, будто страницы вдруг стали приходить реже, потому что часть мощности ушла писать тайную ветвь.

Сколько атакующий заработал, считают по-разному, и расхождение поучительно. Coinbase считала все транзакции двойной траты, то есть попытки, и для второй атаки получила около 460 тыс. ETC, примерно 3,2 млн долларов[497]. Аналитическая компания Bitquery посчитала для той же атаки только удавшиеся двойные траты и получила около 1,7 млн долларов, примерно половину[498].[499] За долларами в новости об атаке может стоять любое из этих чисел. Сама Coinbase подчёркивала, что целью атакующих не была и денег не потеряла[500].

Уже после второй атаки Coinbase стала ждать подтверждений для депозитов ETC около двух недель[501].[502] Правило терпения для маленьких сетей здесь дошло до крайности.

Команда другой небольшой сети, Bitcoin Gold, после атак на биржи в мае 2018 года объяснила, почему маленькую сеть так легко перегнать: тот же алгоритм перебора используют и другие монеты, поэтому мощность для атаки можно собрать со стороны[503]. Если рядом с маленьким посёлком стоит большой, где машины для перебора такие же, одному крупному двору оттуда достаточно на несколько часов перевести машины на чужую тетрадку, чтобы собрать в ней большинство.

Исследователи из MIT, которые вели учёт таких атак, фиксировали их и на других небольших сетях[504].[505] Об успешной атаке большинства на сам биткоин сведений нет[506].

---

blog/coinbases-perspective-on-the-recent-ethereum-classic-etc-double-spend; цитаты — по Crowdfund Insider, «Coinbase Clarifies It Wasn't Targeted By "Any Of The Attack Transactions" On Etherem Classic (ETC) During 51% Attack And Didn't Lose Funds», 08.2020, https://www.crowdfundinsider.com/2020/08/165589-coinbase-clarifies-it-wasnt-targeted-by-any-of-the-attack-transactions-on-etherem-classic-etc-during-51-attack-and-didnt-lose-funds/)

[497] Coinbase, «Coinbase's perspective on the recent Ethereum Classic (ETC) double spend incidents», 08.2020, https://www.coinbase.com/blog/coinbases-perspective-on-the-recent-ethereum-classic-etc-double-spend; цитаты — по Crowdfund Insider, «Coinbase Clarifies It Wasn't Targeted By "Any Of The Attack Transactions" On Etherem Classic (ETC) During 51% Attack And Didn't Lose Funds», 08.2020, https://www.crowdfundinsider.com/2020/08/165589-coinbase-clarifies-it-wasnt-targeted-by-any-of-the-attack-transactions-on-etherem-classic-etc-during-51-attack-and-didnt-lose-funds/.

[498] CoinDesk, «Ethereum Classic Attacker Successfully Double-Spends $1.68M in Second Attack: Report», 07.08.2020, https://www.coindesk.com/markets/2020/08/07/ethereum-classic-attacker-successfully-double-spends-168m-in-second-attack-report.

[499] По Coinbase, транзакции двойной траты в первой атаке — около 800 тыс. ETC (≈5,8 млн долларов), во второй — около 460 тыс. ETC (≈3,2 млн долларов) (Coinbase, «Coinbase's perspective on the recent Ethereum Classic (ETC) double spend incidents», 08.2020, https://www.coinbase.com/blog/coinbases-perspective-on-the-recent-ethereum-classic-etc-double-spend; цитаты — по Crowdfund Insider, «Coinbase Clarifies It Wasn't Targeted By "Any Of The Attack Transactions" On Etherem Classic (ETC) During 51% Attack And Didn't Lose Funds», 08.2020, https://www.crowdfundinsider.com/2020/08/165589-coinbase-clarifies-it-wasnt-targeted-by-any-of-the-attack-transactions-on-etherem-classic-etc-during-51-attack-and-didnt-lose-funds/). По Bitquery, во второй атаке (6 августа 2020 года по UTC) атакующий пытался дважды потратить 465 444 ETC (≈3,3 млн долларов), а удалось ему 238 306 ETC (≈1,68 млн долларов) (CoinDesk, «Ethereum Classic Attacker Successfully Double-Spends $1.68M in Second Attack: Report», 07.08.2020, https://www.coindesk.com/markets/2020/08/07/ethereum-classic-attacker-successfully-double-spends-168m-in-second-attack-report).

[500] Coinbase, «Coinbase's perspective on the recent Ethereum Classic (ETC) double spend incidents», 08.2020, https://www.coinbase.com/blog/coinbases-perspective-on-the-recent-ethereum-classic-etc-double-spend; цитаты — по Crowdfund Insider, «Coinbase Clarifies It Wasn't Targeted By "Any Of The Attack Transactions" On Etherem Classic (ETC) During 51% Attack And Didn't Lose Funds», 08.2020, https://www.crowdfundinsider.com/2020/08/165589-coinbase-clarifies-it-wasnt-targeted-by-any-of-the-attack-transactions-on-etherem-classic-etc-during-51-attack-and-didnt-lose-funds/.

[501] CoinDesk, 29.08.2020, https://www.coindesk.com/markets/2020/08/29/ethereum-classic-hit-by-third-51-attack-in-a-month.

[502] Биржа OKEx тогда же рассматривала исключение ETC из торговли из-за «серьёзного недостатка безопасности» (CoinDesk, 29.08.2020, https://www.coindesk.com/markets/2020/08/29/ethereum-classic-hit-by-third-51-attack-in-a-month).

[503] Bitcoin Gold, «Responding to Attacks», 24.05.2018, http://www.bitcoingold.org/responding-to-attacks/.

[504] MIT Digital Currency Initiative, «51% Attacks» (трекер реорганизаций PoW-сетей; Г.-Я. Гласберген, Дж. Лавджой, Э. Оуян), http://www.dci.mit.edu/projects/51-percent-attacks.

[505] MIT Digital Currency Initiative, трекер «51% Attacks»: Expanse, Litecoin Cash (июль 2019 года), Vertcoin (декабрь 2019 года), повторная атака на Bitcoin Gold в январе 2020 года с двойными тратами больше чем на 72 тыс. долларов (MIT Digital Currency Initiative, «51% Attacks» (трекер реорганизаций PoW-сетей; Г.-Я. Гласберген, Дж. Лавджой, Э. Оуян), http://www.dci.mit.edu/projects/51-percent-attacks).

[506] MIT Digital Currency Initiative, «51% Attacks» (трекер реорганизаций PoW-сетей; Г.-Я. Гласберген, Дж. Лавджой, Э. Оуян), http://www.dci.mit.edu/projects/51-percent-attacks.

Самый показательный случай с биткоином был вообще не атакой.

В марте 2013 года сеть случайно раскололась на две цепочки, потому что версии программы 0.7 и 0.8 по-разному судили об одном большом блоке (новая его принимала, старая отвергала)[507]. Раскол устранили люди. Два крупных пула, BTC Guild и Slush, добровольно откатили свои узлы на старую версию, чтобы их мощность тоже отвергала спорный блок, и большинство мощности вернулось на старую цепочку[508].[509]

Восьмое правило при этом никто не нарушал. Люди просто перенесли работу на ту ветвь, которую решили сделать тяжелее. За время раскола случилась как минимум одна крупная двойная трата, по описанию разработчиков экспериментальная, без злого умысла[510].

После этого случая можно ответить и на четвёртый из пяти вопросов, которые я в первой главе советовал задавать любым деньгам: кто может остановить всю систему одним решением? Государство, которое выгнало со своей территории часть майнеров, тетрадку не остановило[511]. Несколько крупнейших пулов, если сговорятся, смогут отменять собственные переводы и не пускать в тетрадку чужие, но ни создать монеты из воздуха, ни потратить чужие не смогут[512]. В одиночку остановить тетрадку не может никто. А в трудную минуту, как в 2010 и в 2013 году, какую историю считать настоящей, решали люди, и решали быстро[513]. Пятый вопрос, о строчках в долг, остаётся для второй части книги.

Залог вместо электричества

Сделать голос дорогим можно и без электричества. Вернёмся в посёлок и заменим восьмое правило девятым. Право написать следующую страницу разыгрывается по жребию между дворами, которые заперли часть своих строчек в залог, и чем больше залог, тем больше у двора шансов. Строчка залога записана за самой тетрадкой, как сарай плотника в первой главе был записан за хранителем, и вернётся к двору, только если тот не жульничал. Кто пойман на обмане (например, подписал две разные страницы на одно и то же место), теряет залог. Голос по-прежнему дорог, только платят за него теперь деньгами, которые лежат в залоге и которыми нельзя пользоваться.

Такой способ называют доказательством доли, а внесение залога — стейкингом (от английского stake, «ставка»). Возьмём Ethereum; его монета называется эфиром, ETH. Чтобы стать проверяющим, которого там называют валидатором, нужно внести 32 ETH на особый депозитный счёт в самой сети и запустить у себя три программы[514]. Время в сети поделено на слоты по 12 секунд. В каждом слоте случайно выбранный валидатор предлагает страницу, а комитет из других случайно выбранных валидаторов голосует за то, что она правильная[515].[516]

---

[507] BIP 50, «March 2013 Chain Fork Post-Mortem», https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki.

[508] BIP 50, «March 2013 Chain Fork Post-Mortem», https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki.

[509] BIP 50. March 2013 Chain Fork Post-Mortem: «BTCGuild and Slush downgraded their Bitcoin 0.8 nodes to 0.7 so their pools would also reject the larger block.»

[510] BIP 50, «March 2013 Chain Fork Post-Mortem», https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki.

[511] mempool.space, история корректировок сложности, https://mempool.space/api/v1/mining/difficulty-adjustments/all (запись: метка 1625294046, высота 689472, коэффициент 0,720573).

[512] mempool.space, https://mempool.space/api/v1/mining/pools/1m (4 546 блоков за месяц; запрос 26.09.2026); Nakamoto, 2008, раздел 5 «Network», https://bitcoin.org/bitcoin.pdf.

[513] Bitcoin Wiki, «Value overflow incident», https://en.bitcoin.it/wiki/Value_overflow_incident; Накамото, архив bitcointalk, посты 16.08.2010 01:00:45 и 12:59:38 UTC; BIP 50, «March 2013 Chain Fork Post-Mortem», https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki.

[514] ethereum.org, «Proof-of-stake (PoS)», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

[515] ethereum.org, «Proof-of-stake (PoS)», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

[516] ethereum.org, «Proof-of-stake»: «Time in proof-of-stake Ethereum is divided into slots (12 seconds) and epochs (32 slots).» Три программы — клиент исполнения, клиент консенсуса и клиент валидатора (ethereum.org, «Proof-of-stake (PoS)», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/).

Здесь возвращается задача генералов. Валидаторов можно пересчитать, потому что каждый внёс залог и его ключ записан в самой тетрадке. Список членов клуба снова известен, только вход в клуб теперь стоит 32 ETH, и поэтому снова работает старое правило двух третей[517]. Страница в Ethereum становится окончательной, когда за неё проголосовали валидаторы, у которых вместе не меньше двух третей всего залога[518].

Такое свойство называют финальностью. Чтобы отменить окончательную страницу, нападающему придётся пожертвовать не меньше чем третью всего залога сети: протокол сожжёт её штрафами[519]. В биткоине финальности нет. Там запись с каждой новой страницей сверху становится всё надёжнее, но окончательной её не объявляет никто[520].

Наказание за обман называют слэшингом. Ethereum наказывает за три нарушения: подписать две разные страницы на один слот, проголосовать сразу за двух кандидатов и проголосовать так, чтобы фактически переписать прежний голос[521]. Устроено наказание в два шага. Первый штраф маленький (для залога в 32 ETH это меньше сотой доли эфира), но на 18-й день начисляется второй, и он тем больше, чем больше залога наказано одновременно, вплоть до всего залога[522].[523]

Допустим, валидаторов миллион, и один из них из-за сбоя в настройках подписал две страницы на один слот. Он заплатит маленький первый штраф, второй окажется почти нулевым, потому что одновременно с ним никого не наказали, и из сети его выведут. Теперь допустим, что сговорились валидаторы, у которых вместе треть всего залога, и все они подписали две версии истории сразу. Первый штраф у каждого будет тем же маленьким, но второй рассчитают на треть залога сети, и сговорившиеся лишатся залогов целиком[524].

Атакующий с долей залога больше трети может задерживать финальность, а если сумеет управлять задержками сообщений в сети, то и добиться двух противоречащих окончательных версий, заплатив за это всем своим залогом. С половиной залога он может цензурировать транзакции и управлять выбором будущих страниц, с двумя третями — переписывать уже окончательную историю[525].[526] Так эти пороги перечисляет сайт самого Ethereum, и последней защитой

---

[517] ethereum.org, «Gasper», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/gasper/; «Proof-of-stake», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

[518] ethereum.org, «Gasper», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/gasper/; «Proof-of-stake», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

[519] ethereum.org, «Gasper», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/gasper/; «Proof-of-stake», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

[520] Nakamoto, 2008, раздел 4, https://bitcoin.org/bitcoin.pdf.

[521] ethereum.org, «Proof-of-stake rewards and penalties», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/rewards-and-penalties/.

[522] ethereum.org, «Proof-of-stake rewards and penalties», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/rewards-and-penalties/.

[523] Для залога в 32 ETH начальный штраф — 0,007 812 5 ETH; валидатор принудительно выводится из сети за 36 дней. Второй штраф растёт с суммой залога всех валидаторов, наказанных за предыдущие 36 дней: «scales with the total staked ether of all slashed validators». Если сеть больше четырёх эпох не доходит до финальности, залоги неактивных валидаторов постепенно тают, пока у активных не наберётся две трети (ethereum.org, «Proof-of-stake rewards and penalties», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/rewards-and-penalties/).

[524] ethereum.org, «Proof-of-stake rewards and penalties», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/rewards-and-penalties/.

[525] ethereum.org, «Proof-of-stake attack and defense», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/attack-and-defense/.

[526] ethereum.org, «Proof-of-stake attack and defense»: «Assuming that the Ethereum network is asynchronous… an attacker controlling 34% of the total stake could cause double finality»; «The attacker would necessarily destroy their entire stake…» (ethereum.org, «Proof-of-stake attack and defense», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/attack-and-defense/).

он называет «социальный слой»: если атака всё-таки удалась, сообщество может договориться и перейти на честную ветвь[527].

С биткоином это сравнение выходит двояким. Майнер, проигравший атаку, сохраняет свои машины и может попробовать снова или вернуться к честной работе, а у валидатора протокол сожжёт залог[528]. Зато «социальный слой» прямо признаёт, что в крайнем случае решают люди. К этому признанию мы вернёмся в главе 4, где людям однажды пришлось решать, какую историю Ethereum считать настоящей.

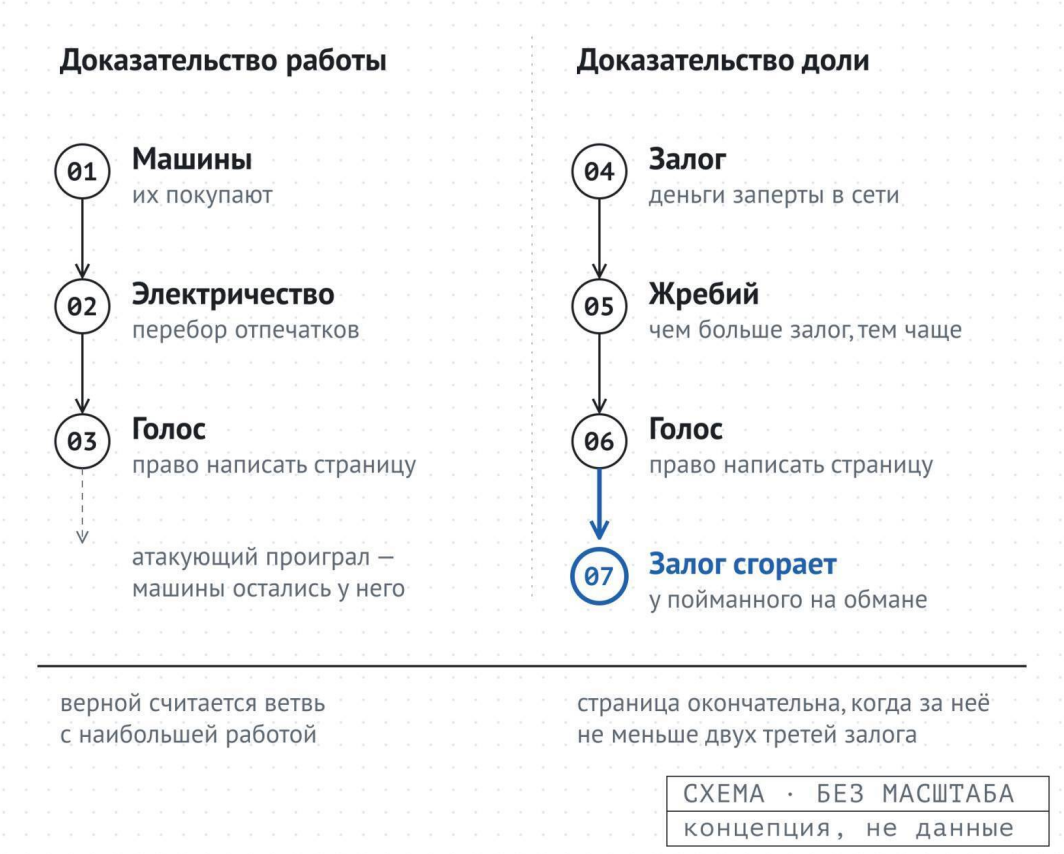


Рисунок 3.3. Два способа сделать голос дорогим

Ethereum сам начинал с доказательства работы и перешёл на залог 15 сентября 2022 года; этот переход назвали The Merge. По оценке, на которую ссылается сайт проекта, годовое потребление электричества сетью упало больше чем на 99,9%[529].[530] Источник заинтересованный, но порядок величины сомнений не вызывает.

---

[527] ethereum.org, «Proof-of-stake attack and defense», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/attack-and-defense/.

[528] ethereum.org, «Proof-of-stake attack and defense», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/attack-and-defense/.

[529] ethereum.org, «The Merge», https://ethereum.org/en/roadmap/merge/; «Ethereum energy consumption», https://ethereum.org/en/energy-consumption/ (перенесено из https://ethereum.org/en/roadmap/merge//https://ethereum.org/energy-consumption/, перепроверено 26.09.2026).

[530] ethereum.org, страница об энергопотреблении: снижение «более чем на 99,988%», до примерно 0,0026 ТВт·ч в год, по оценке CCRI; страница The Merge пишет «примерно на 99,95%». Оценки потребления до перехода — от ~21 до ~94 ТВт·ч в год (ethereum.org, «The Merge», https://ethereum.org/en/roadmap/merge/; «Ethereum energy consumption», https://ethereum.org/en/energy-consumption/ (перенесено из https://ethereum.org/en/roadmap/merge//https://ethereum.org/energy-consumption/, перепроверено 26.09.2026)).

Переход не прибавил пропускной способности и снижать комиссии не был призван: он заменил способ согласия, а страницы стали выходить примерно на 10% чаще, и только[531].[532] Цена согласия и скорость тетрадки — разные вещи, и это понадобится нам в конце главы.

Зато замороженный капитал здесь виден в прямом смысле. Эфир, внесённый в залог, нельзя было забрать до обновления 12 апреля 2023 года, то есть ещё семь месяцев после перехода, а те, кто вносил залог раньше, ждали дольше[533]. В конце сентября 2026 года в залоге лежала примерно треть всего эфира, а очередь желающих его внести растянулась примерно на месяц[534].[535] Доход у залога есть (около 2,6% годовых на ту же дату), но есть и риск потерять часть залога или весь залог за нарушения[536]. Расхожая мысль, будто при доказательстве доли богатые просто богатеют без риска, верна только наполовину.

Концентрация у залога своя. Крупнейший посредник здесь — протокол Lido, который принимает эфир от многих владельцев и распределяет его между операторами валидаторов[537]. В конце 2023 года на Lido приходилось 32,3% всего эфира в залоге, а исследователи Ethereum считают тревожным порогом 33%[538]. Порог выбран не случайно, потому что больше трети залога позволяет задерживать финальность[539]. С тех пор доля снизилась и осенью 2026 года составляла почти четверть[540].[541] Насколько опасен такой посредник, спорят до сих пор[542].

Пересчитать людей по валидаторам тоже больше нельзя. После обновления 2025 года один валидатор может держать до 2048 ETH[543], так что число валидаторов не показывает, сколько за ними стоит владельцев.

---

[531] ethereum.org, «The Merge», раздел о заблуждениях, https://ethereum.org/en/roadmap/merge/ (перенесено из https://ethereum.org/en/roadmap/merge/, перепроверено).

[532] ethereum.org, «The Merge»: «The Merge was a change of consensus mechanism, not an expansion of network capacity, and was never intended to lower gas fees.»

[533] ethereum.org, «The Merge» (про вывод), https://ethereum.org/en/roadmap/merge/; ethereum.org, «Pectra», https://ethereum.org/en/roadmap/pectra/; дата Shanghai — https://ethereum.org/en/ethereum-forks/ (ethereum.org, Fork Timeline).

[534] Validator Queue (данные beaconcha.in), https://www.validatorqueue.com/ (обращение 26.09.2026).

[535] Validator Queue (данные beaconcha.in) на 26.09.2026: около 43,3 млн ETH в залоге, примерно 35,5% всего предложения; около 892 тыс. активных валидаторов; в очереди на вход — около 1,66 млн ETH (Validator Queue (данные beaconcha.in), https://www.validatorqueue.com/ (обращение 26.09.2026)). Свежие цифры — в приложении Б.

[536] Validator Queue (данные beaconcha.in), https://www.validatorqueue.com/ (обращение 26.09.2026); ethereum.org, «Proof-of-stake rewards and penalties», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/rewards-and-penalties/.

[537] CoinDesk (Margaux Nijkerk), «Figment outpaces rivals in ether staking growth; Lido's decline eases dominance concerns», 14.08.2025, https://www.coindesk.com/tech/2025/08/14/figment-outpaces-rivals-in-ether-staking-growth-lido-s-decline-eases-dominance-concerns (данные Dune, дашборд hildobby) — перенесено из «Спорных моментов» RC, перепроверено.

[538] CoinDesk (Margaux Nijkerk), «Figment outpaces rivals in ether staking growth; Lido's decline eases dominance concerns», 14.08.2025, https://www.coindesk.com/tech/2025/08/14/figment-outpaces-rivals-in-ether-staking-growth-lido-s-decline-eases-dominance-concerns (данные Dune, дашборд hildobby) — перенесено из «Спорных моментов» RC, перепроверено.

[539] ethereum.org, «Proof-of-stake attack and defense», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/attack-and-defense/.

[540] Lido, API статистики stETH, https://eth-api.lido.fi/v1/protocol/steth/stats (поле totalStaked = 9 797 125,47; обращение 26.09.2026); общий стейкинг — Validator Queue, https://www.validatorqueue.com/.

[541] Около 9,80 млн ETH по API Lido на 26.09.2026, то есть примерно 22,6% от 43,3 млн ETH в залоге; точность — до процента (Lido, API статистики stETH, https://eth-api.lido.fi/v1/protocol/steth/stats (поле totalStaked = 9 797 125,47; обращение 26.09.2026); общий стейкинг — Validator Queue, https://www.validatorqueue.com/). В августе 2025 года доля была 24,4% (по данным Dune в пересказе CoinDesk) (CoinDesk (Margaux Nijkerk), «Figment outpaces rivals in ether staking growth; Lido's decline eases dominance concerns», 14.08.2025, https://www.coindesk.com/tech/2025/08/14/figment-outpaces-rivals-in-ether-staking-growth-lido-s-decline-eases-dominance-concerns (данные Dune, дашборд hildobby) — перенесено из «Спорных моментов» RC, перепроверено). Свежая доля — в приложении Б.

[542] CoinDesk (Margaux Nijkerk), «Figment outpaces rivals in ether staking growth; Lido's decline eases dominance concerns», 14.08.2025, https://www.coindesk.com/tech/2025/08/14/figment-outpaces-rivals-in-ether-staking-growth-lido-s-decline-eases-dominance-concerns (данные Dune, дашборд hildobby) — перенесено из «Спорных моментов» RC, перепроверено.

[543] ethereum.org, «The Merge» (про вывод), https://ethereum.org/en/roadmap/merge/; ethereum.org, «Pectra», https://ethereum.org/en/roadmap/pectra/; дата Shanghai — https://ethereum.org/en/ethereum-forks/ (ethereum.org, Fork Timeline).

Если вы когда-нибудь отдадите эфир в залог через биржу или через такой протокол, полезно понимать, кому вы при этом верите. Ключи валидаторов будут у операторов, а у вас останется их обещание вернуть эфир с доходом, то есть строчка в чужой тетрадке, как в посёлке с хранителем[544]. Советовать, делать так или нет, я не стану. Мне важно, чтобы этот посредник не остался для вас незамеченным.

В обоих способах тетрадку пишет меньше участников, чем обещает слово «распределённый». При доказательстве работы большую часть страниц собирают несколько пулов, при доказательстве доли заметная доля залога проходит через один протокол.

Если сравнить два способа по устройству, у каждого найдётся своё слабое место. При доказательстве работы голос покупают снаружи сети. Машины и электричество продаются за обычные деньги, и новичок может получить голос, ничего не покупая у нынешних участников, зато платить приходится непрерывно, а машины сами собой скапливаются там, где дешевле электричество и крупнее пулы. При доказательстве доли голос покупают внутри сети. Чтобы его получить, нужно купить монеты у тех, у кого они уже есть, зато, раз заплатив, валидатор почти ничего не тратит на поддержание голоса, кроме возможности пользоваться своими деньгами.

Сарай плотника в первой главе имел цену сам по себе, и если плотник не расплатится, хранитель получит вещь, которую можно продать кому угодно. Залог валидатора сделан из монет той самой тетрадки, которую он охраняет. Если тетрадке перестанут верить, подешевеет и залог, а вместе с ним и наказание за обман; у сарая такой зависимости нет, и модель посёлка её не передаёт. У майнера похожая зависимость, только слабее: его машины годятся лишь для перебора, и их ценность тоже держится на цене монет, которые ими добывают (на этом Накамото и строил расчёт, что атакующий не захочет подрывать ценность собственного богатства[545]).

Скорость как цена согласия

Последняя цена согласия — скорость. Каждую страницу должны получить и проверить все узлы (иначе проверка, на которой всё держится, станет делом немногих), поэтому страницы делают небольшими и выпускают редко, а открытая тетрадка в итоге пропускает мало записей. С конца августа по конец сентября 2026 года сеть биткоина подтверждала в среднем около 8 транзакций в секунду[546]. Visa за год до 30 сентября 2025 года обрабатывала в среднем около 10 400 транзакций в секунду[547]. Разница больше чем в тысячу раз.[548] (Сравнение грубое,

---

[544] CoinDesk (Margaux Nijkerk), «Figment outpaces rivals in ether staking growth; Lido's decline eases dominance concerns», 14.08.2025, https://www.coindesk.com/tech/2025/08/14/figment-outpaces-rivals-in-ether-staking-growth-lido-s-decline-eases-dominance-concerns (данные Dune, дашборд hildobby) — перенесено из «Спорных моментов» RC, перепроверено.

[545] Nakamoto, 2008, раздел 6 «Incentive», https://bitcoin.org/bitcoin.pdf.

[546] Blockchain.com, график «Confirmed Transactions Per Day», API: https://api.blockchain.info/charts/n-transactions?timespan=30days&format=json (обращение 26.09.2026).

[547] Visa, «Visa Fact Sheet» (FY26), https://corporate.visa.com/content/dam/VCOM/corporate/documents/about-visa-factsheet.pdf.

[548] Visa Fact Sheet: 329 млрд транзакций за 12 месяцев до 30.09.2025, включая платежи и снятие наличных; среднее в секунду посчитано делением на число секунд в году (Visa, «Visa Fact Sheet» (FY26), https://corporate.visa.com/content/dam/VCOM/corporate/documents/about-visa-factsheet.pdf). Биткоин: около 696 тыс. подтверждённых транзакций в сутки с 27 августа по 25 сентября 2026 года (Blockchain.com) (Blockchain.com, график «Confirmed Transactions Per Day», API: https://api.blockchain.info/charts/n-transactions?timespan=30days&format=json (обращение 26.09.2026)). Популярные цифры «пика Visa» (47 000, 56 000 или 65 000 в секунду) относятся к разным годам и замерам, а последнюю в документах Visa найти не удалось (J. Poon, T. Dryja, «The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments», DRAFT Version 0.5.9.2, 14.01.2016, https://lightning.network/lightning-network-paper.pdf; Visa, «Visa Fact Sheet» (FY26), https://corporate.visa.com/content/dam/VCOM/corporate/documents/about-visa-factsheet.pdf). Свежие цифры — в приложении Б.

потому что одна транзакция биткоина может содержать много платежей, но порядок разрыва оно передаёт верно[549].)

Почему у Visa выходит в тысячу раз больше? Visa — хранитель в смысле первой главы. Платежи через её сеть идут по правилам одной компании, а остатки на счетах ведут банки, которым клиенты и так доверяют. Никому не нужно, чтобы каждую строчку проверили тысячи посторонних людей, каждый на своём компьютере. Соглашаться о версии записи приходится только внутри своего круга, а в закрытом кругу согласие, как мы видели на примере Кастро и Лисков, почти бесплатно[550].

У открытой тетрадки каждую страницу должны получить и проверить десятки тысяч независимых узлов[551]. Тысячекратный разрыв в скорости — та же цена открытости, о которой шла речь в начале главы.

Почему бы просто не сделать страницы больше?

В 2016 году группа исследователей посчитала, что это быстро упирается в сеть. Если страница будет больше нескольких мегабайт, заметная часть узлов перестанет успевать её получать, и тетрадку смогут вести немногие[552]. Авторы заключили, что для настоящего роста без потери распределённости устройство блокчейна нужно пересматривать целиком[553].[554] Авторы Lightning Network в том же году прикинули крайний случай. Чтобы сравняться с Visa прямо в тетрадке, понадобились бы страницы почти по 8 ГБ каждые десять минут, больше 400 ТБ данных в год, а это, по словам самих авторов, привело бы к крайней централизации узлов[555].[556]

Виталик Бутерин, один из создателей Ethereum, называет это трилеммой масштабируемости. Блокчейн хочет сразу трёх свойств: пропускать больше, чем может проверить обычный ноутбук; не зависеть от небольшой группы крупных участников; выдерживать атаку большой доли участников. Простыми средствами, пишет он, можно получить только два свойства из трёх[557].[558] Доказательства у трилеммы нет, это наблюдение инженера[559], но обе попытки ускорения, о которых дальше, обходят её одинаково, унося часть работы за пределы общей тетрадки.

---

[549] Blockchain.com, график «Confirmed Transactions Per Day», API: https://api.blockchain.info/charts/n-transactions?timespan=30days&format=json (обращение 26.09.2026).

[550] Castro, Liskov, 1999 (по пересказу: Colyer, The Morning Paper, 2015, https://blog.acolyer.org/2015/05/18/practical-byzantine-fault-tolerance/).

[551] BTC Nodes (Bitnodes), https://btcnodes.io/; API снимка: https://btcnodes.io/api/v1/snapshots/latest/ (обращение 2026-09-26; старый адрес bitnodes.io перенаправляет туда). Оператор — Rodrigo Martínez.

[552] Croman et al., 2016, раздел 1, https://www.comp.nus.edu.sg/~prateeks/papers/Bitcoin-scaling.pdf.

[553] Croman et al., 2016, раздел 1, https://www.comp.nus.edu.sg/~prateeks/papers/Bitcoin-scaling.pdf.

[554] Croman K. et al. On Scaling Decentralized Blockchains (A Position Paper). Financial Cryptography 2016 Workshops: «fundamental protocol redesign is needed for blockchains to scale significantly while retaining their decentralization». По расчёту авторов, чтобы 90% узлов успевали получать блоки, при десятиминутном интервале блок не должен превышать 4 МБ (не больше 27 транзакций в секунду), а интервал между блоками не может быть короче 12 секунд (Croman et al., 2016, раздел 1, https://www.comp.nus.edu.sg/~prateeks/papers/Bitcoin-scaling.pdf). Тогдашний предел биткоина авторы оценивали в 7 транзакций в секунду (K. Croman et al., «On Scaling Decentralized Blockchains (A Position Paper)», Financial Cryptography 2016 Workshops (BITCOIN'16), https://www.comp.nus.edu.sg/~prateeks/papers/Bitcoin-scaling.pdf).

[555] J. Poon, T. Dryja, «The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments», DRAFT Version 0.5.9.2, 14.01.2016, https://lightning.network/lightning-network-paper.pdf.

[556] Poon J., Dryja T. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. Draft 0.5.9.2, 14.01.2016: «The payment network Visa achieved 47,000 peak transactions per second (tps) on its network during the 2013 holidays… Currently, Bitcoin supports less than 7 transactions per second with a 1 megabyte block limit.»

[557] V. Buterin, «Why sharding is great: demystifying the technical properties», 07.04.2021, https://vitalik.eth.limo/general/2021/04/07/sharding.html; та же формулировка — ethereum.org, «Layer 2», https://ethereum.org/en/layer-2/learn/.

[558] Buterin V. Why sharding is great: demystifying the technical properties, 07.04.2021: «if you stick to „simple" techniques, you can only get two of those three». Когда Бутерин впервые употребил это слово, установить не удалось (V. Buterin, «Why sharding is great: demystifying the technical properties», 07.04.2021, https://vitalik.eth.limo/general/2021/04/07/sharding.html; та же формулировка — ethereum.org, «Layer 2», https://ethereum.org/en/layer-2/learn/).

[559] V. Buterin, «Why sharding is great: demystifying the technical properties», 07.04.2021, https://vitalik.eth.limo/general/2021/04/07/sharding.html; та же формулировка — ethereum.org, «Layer 2», https://ethereum.org/en/layer-2/learn/.

Добавим десятое правило посёлка. Два двора, которые часто рассчитываются друг с другом, могут вести свою маленькую тетрадку расчётов, а в общую вносить только открытие счёта и итог. Пока они согласны, общая тетрадка их не касается. Если один попробует жульничать, второй понесёт в общую последнюю подписанную запись, и общая тетрадка рассудит[560].

Так устроена Lightning Network, предложенная в 2016 году. Это сеть платёжных каналов, в которой платежи идут вне блокчейна, а в основную сеть попадают только открытие и закрытие канала или спор[561].[562] Пока это ниша. В конце августа 2026 года в публичных каналах Lightning лежало около 3800 BTC, порядка сотых долей процента всех биткоинов[563].[564]

У Ethereum свой путь, сети второго уровня (они работают поверх основной сети), которые называют роллапами (от английского roll up, «сворачивать»). Роллап собирает сотни транзакций, выполняет их у себя, а в основную тетрадку записывает одну сводную транзакцию и данные, по которым её можно проверить[565]. Одни роллапы считают записи верными, пока кто-нибудь не оспорит их, предъявив доказательство обмана, другие прикладывают к каждой пачке криптографическое доказательство правильности[566].

На языке посёлка роллап похож на двор, который ведёт расчёты за многих соседей сразу и вносит в общую тетрадку только итог. В первом варианте итог считается верным, пока кто-нибудь из соседей не докажет обман. Во втором двор прикладывает к итогу доказательство, которое любой проверит сам, не пересчитывая всех расчётов.

С марта 2024 года для данных роллапов в основной сети отведено отдельное дешёвое место[567]. Удешевление, которого не дал переход на залог, пришло с этой стороны: обновление удешевило работу сетей второго уровня[568]. По данным аналитического проекта L2BEAT, 26 сентября 2026 года сети второго уровня вместе выполняли примерно в 80 раз больше операций, чем основная сеть Ethereum[569].[570]

Скорость здесь тоже покупается, и платят за неё доверием. L2BEAT делит такие сети на стадии. На нулевой сеть полностью контролирует небольшой круг лиц. На первой последнее слово остаётся за советом безопасности из нескольких участников, и, чтобы заблокировать вывод денег, нужно подчинить три четверти совета. На второй сетью управляет код, а при нежелательном обновлении у пользователей есть не меньше 30 дней, чтобы уйти[571]. Осенью 2026 года ни один из 17 крупнейших роллапов до второй стадии не дошёл: шесть стояли на

---

[560] Poon, Dryja, 14.01.2016, аннотация, https://lightning.network/lightning-network-paper.pdf.

[561] Poon, Dryja, 14.01.2016, аннотация, https://lightning.network/lightning-network-paper.pdf.

[562] Авторы — Джозеф Пун и Таддеус Дрийя. Poon, Dryja, 2016, аннотация: «A decentralized system is proposed whereby transactions are sent over a network of micropayment channels (a.k.a. payment channels or transaction channels) whose transfer of value occurs off-blockchain.»

[563] mempool.space, «Lightning statistics», API: https://mempool.space/api/v1/lightning/statistics/latest (запись от 2026-08-25; обращение 26.09.2026).

[564] mempool.space, запись от 25.08.2026: около 16,4 тыс. узлов, 33,3 тыс. каналов, суммарная ёмкость около 3843 BTC. Учитываются только публично объявленные каналы (mempool.space, «Lightning statistics», API: https://mempool.space/api/v1/lightning/statistics/latest (запись от 2026-08-25; обращение 26.09.2026)). Свежие цифры — в приложении Б.

[565] ethereum.org, «Layer 2», https://ethereum.org/en/layer-2/learn/.

[566] ethereum.org, «Layer 2», https://ethereum.org/en/layer-2/learn/.

[567] ethereum.org, «Ethereum Fork Timeline», https://ethereum.org/en/ethereum-forks/ (перенесено из https://ethereum.org/en/ethereum-forks/).

[568] ethereum.org, «Ethereum Fork Timeline», https://ethereum.org/en/ethereum-forks/ (перенесено из https://ethereum.org/en/ethereum-forks/); ethereum.org, «The Merge», раздел о заблуждениях, https://ethereum.org/en/roadmap/merge/ (перенесено из https://ethereum.org/en/roadmap/merge/, перепроверено).

[569] L2BEAT, «Activity», https://l2beat.com/scaling/activity (обращение 26.09.2026, данные за последние сутки).

[570] L2BEAT, «Activity», данные за сутки на 26.09.2026: основная сеть — около 26 пользовательских операций в секунду, сети второго уровня вместе — около 2120. Метрика считает операции пользователей по методике L2BEAT, а распределение по проектам быстро меняется (L2BEAT, «Activity», https://l2beat.com/scaling/activity (обращение 26.09.2026, данные за последние сутки)). Свежие цифры — в приложении Б.

[571] L2BEAT, «Stages», https://l2beat.com/stages; L2BEAT, «Stages», https://l2beat.com/stages (обращение 27.09.2026).

первой, одиннадцать на нулевой[572].[573] Ускоряя тетрадку, её отчасти снова отдают в руки немногих, которым приходится верить.

Отсюда три вопроса к любой сети, которая обещает быть в тысячу раз быстрее и дешевле биткоина. Чем в ней платят за голос: электричеством, залогом или ничем (последнее, если следовать логике этой главы, означает закрытый список, как у Кастро и Лисков)? Сколько участников на деле пишут её страницы, и может ли кто-нибудь со стороны их пересчитать? Кто решает, какую историю считать настоящей, если что-то пойдёт не так? Пока ответов нет, к обещанной скорости разумно относиться как к рекламе.

За главу у посёлка прибавилось три правила:

восьмое — из двух версий тетрадки верна та, в которую вложено больше работы[574];

девятое, другой путь вместо восьмого, — право писать страницу разыгрывается между теми, кто внёс залог, обманщик теряет залог, а страница становится окончательной, когда за неё проголосовали владельцы двух третей залога[575];

десятое — двое соседей ведут расчёты в своей маленькой тетрадке, вносят в общую только открытие и итог, а общая служит судьёй при споре[576].

Каждый раз, когда цену согласия пытаются снизить, в каком-то месте снова появляется тот, кому нужно верить: пул, который собирает страницы, протокол, через который идёт залог, совет безопасности сети второго уровня, «социальный слой» на крайний случай. Я не считаю это провалом замысла. Это счёт, который приходит за отказ от посредника, и видеть его стоит целиком.

Пока в тетрадке лежали только переводы, люди вмешивались в неё редко, в аварийных случаях. Стоит записать в неё программы, которые исполняются сами, и вопрос, кто решает, когда правила нужно изменить, аварийным быть перестаёт: Ethereum столкнулся с ним меньше чем через год после запуска[577].

---

[572] L2BEAT, «Scaling — Summary», https://l2beat.com/scaling/summary (обращение 27.09.2026).

[573] L2BEAT, «Stages»: на первой стадии «the only way (other than bugs) for a rollup to indefinitely block an L2→L1 message or push an invalid L2→L1 message is by compromising ≥75% of the Security Council»; обновления в обход совета допустимы, если у пользователей есть не меньше 7 дней на выход (L2BEAT, «Stages», https://l2beat.com/stages (обращение 27.09.2026)). L2BEAT, «Scaling — Summary», 27.09.2026: на первой стадии — Base, Arbitrum One, OP Mainnet, Starknet, Ink, Unichain; три крупнейших по защищаемой стоимости (Base, Arbitrum One, OP Mainnet) — все на первой; на нулевой — среди прочих Mantle, Linea, ZKsync Era, Scroll, Taiko. Всего L2BEAT относит к роллапам 23 проекта, из них 17 крупнейших по защищаемой стоимости разобраны в тексте; кроме них учитываются ещё десятки проектов, которые не дотягивают и до нулевой стадии (L2BEAT, «Scaling — Summary», https://l2beat.com/scaling/summary (обращение 27.09.2026)). Стадии проектов меняются; свежие данные — в приложении Б.

[574] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System», 2008, раздел 4 «Proof-of-Work», https://bitcoin.org/bitcoin.pdf.

[575] ethereum.org, «Proof-of-stake (PoS)», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/; ethereum.org, «Gasper», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/gasper/; «Proof-of-stake», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/; ethereum.org, «Proof-of-stake rewards and penalties», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/rewards-and-penalties/.

[576] Poon, Dryja, 14.01.2016, аннотация, https://lightning.network/lightning-network-paper.pdf.

[577] ethereum.org, «Ethereum Fork Timeline», https://ethereum.org/en/ethereum-forks/; ethereum.org, «Ethereum Fork Timeline» (DAO fork), https://ethereum.org/en/ethereum-forks/.

Глава 4. Программируемые деньги: смарт-контракты и цена ошибки

17 июня 2016 года из The DAO начали уходить деньги. The DAO была программой в сети Ethereum. Незадолго до этого она продала свои токены всем желающим и собрала за них эфир[578]. Неизвестный человек или группа людей выводили этот эфир, и около 3,6 млн ETH, треть собранного, ушли на адрес, которым распоряжался атакующий[579]. В тот же день Виталик Бутерин, автор первоначального описания Ethereum, написал в блоге фонда Ethereum, что в The DAO нашли уязвимость и уже её используют, что сам Ethereum «совершенно безопасен» и что забрать выведенное атакующий не сможет ещё около 27 дней[580].[581] Столько держал деньги код самой The DAO[582]. Кто стоял за атакой, неизвестно до сих пор.

Сайт The DAO обещал, что она будет действовать исключительно «несгибаемой железной волей неостановимого кода»[583].[584] 20 июля, через тридцать три дня после атаки, большинство майнеров Ethereum перешли на версию сети, в которой один блок единственным внеочередным изменением переложил эфир The DAO на контракт возврата, откуда вкладчики могли забрать свои деньги[585]. Меньшинство отказалось и осталось на прежней цепочке[586].

Неостановимый код остановили люди, и сеть при этом разделилась надвое.

Смарт-контракт — правило, которое исполняет себя само, и ошибку оно исполняет так же неумолимо, как правильное условие. Когда ошибка обходится в сотню миллионов долларов и больше, у системы без хозяина находятся люди, которые решают, что делать, и каждый раз решают по-своему.

Автомат с монетоприёмником

Само слово появилось раньше первого блокчейна. В 1994 году Ник Сабо (тот самый, что позже описал bit gold, одну из попыток из первой главы) назвал смарт-контрактом компьютерный протокол транзакций, который исполняет условия договора[587].[588] Цели он перечислил

---

[578] SEC, отчёт о The DAO, 2017, с. 2–3 (перенос https://www.sec.gov/files/litigation/investreport/34-81207.pdf, перепроверено); SEC, отчёт о The DAO, 2017, с. 6.

[579] SEC, отчёт о The DAO, 2017, с. 9 (перенос , перепроверено).

[580] Vitalik Buterin, «CRITICAL UPDATE Re: DAO Vulnerability», Ethereum Foundation Blog, 17.06.2016, https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability.

[581] Buterin V. CRITICAL UPDATE Re: DAO Vulnerability. Ethereum Foundation Blog, 17.06.2016: «An attack has been found and exploited in the DAO, and the attacker is currently in the process of draining the ether contained in the DAO into a child DAO»; «This is an issue that affects the DAO specifically; Ethereum itself is perfectly safe.»

[582] SEC, отчёт о The DAO, 2017, с. 9 (перенос , перепроверено).

[583] SEC, отчёт о The DAO, 2017, с. 5 (цитата с сайта daohub.org, сноска 18).

[584] Цитата с сайта daohub.org по отчёту SEC: SEC. Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO. Release No. 81207, 25.07.2017, p. 5: «To blaze a new path in business for the betterment of its members, existing simultaneously nowhere and everywhere and operating solely with the steadfast iron will of unstoppable code.»

[585] Jeffrey Wilcke, «To fork or not to fork», Ethereum Foundation Blog, 15.07.2016, https://blog.ethereum.org/2016/07/15/to-fork-or-not-to-fork; ethereum.org, «Ethereum Fork Timeline», https://ethereum.org/ethereum-forks/ (перенос https://ethereum.org/en/ethereum-forks/, перепроверено); Vitalik Buterin, «Hard Fork Completed», Ethereum Foundation Blog, 20.07.2016, https://blog.ethereum.org/2016/07/20/hard-fork-completed.

[586] SEC, отчёт о The DAO, 2017, с. 9–10 и сноска 32 (перенос , перепроверено).

[587] Nick Szabo, «Smart Contracts», 1994 (копия текста с пометкой «Copyright (c) 1994 by Nick Szabo»), https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html; тот же текст с датой 1994 цитирует SEC в отчёте о The DAO (2017), сноска 3, https://www.sec.gov/files/litigation/investreport/34-81207.pdf.

[588] Szabo N. Smart Contracts, 1994: «A smart contract is a computerized transaction protocol that executes the terms of a contract.» Исходный адрес текста больше не работает; копия сохранена на сайте Амстердамского университета, тот же текст с датой 1994

тогда же: выполнять обычные условия договора вроде оплаты или залога, свести к минимуму исключения, как злонамеренные, так и случайные, и уменьшить нужду в доверенных посредниках[589].[590] Последняя цель знакома. Накамото потом искал способ обойтись без хранителя тетрадки, а Сабо — способ реже нуждаться в посредниках и удешевить арбитраж и принуждение к исполнению договора[591].

В 1996 году Сабо дал определение, более близкое к юридическому: смарт-контракт — это набор обещаний в цифровой форме вместе с протоколами, по которым стороны эти обещания исполняют[592]. В той же статье появился пример, которым смарт-контракт объясняют до сих пор. «Примитивным предком» смарт-контрактов Сабо назвал обычный торговый автомат. Автомат принимает монеты и через простой механизм честно выдаёт сдачу и товар, а защищён ровно настолько, чтобы взлом обходился дороже, чем лежит денег в кассе[593].[594] (Часто пишут, что автомат был уже в тексте 1994 года. Там его нет, там речь идёт о платёжных терминалах и электронном обмене документами[595].)

Общую идею Сабо можно пересказать так. Условия договора встраивают в железо и программы, чтобы нарушить договор стало для нарушителя дорого[596]. Суд при этом никуда не девается, но, если следовать этой логике, дело до него доходит реже. Для автомата это очевидно, ведь заплатить за шоколадку проще, чем ломать дверцу.

Посмотрим на автомат как на договор. Условие у него одно: опусти нужную сумму, нажми кнопку, получи шоколадку. Продавца рядом нет, и никто не решает, достоин ли покупатель шоколадки и стоит ли ему верить. Условие исполняет механизм, одинаково для всех. В статье 1997 года Сабо назвал автомат договором с предъявителем, потому что участвовать в обмене может любой, у кого есть монеты[597].[598] Официальный сайт Ethereum сегодня объясняет смарт-контракт тем же автоматом (определённые входы гарантируют заранее заданный результат) и признаёт авторство термина за Сабо[599].

Первая черта автомата — «любой, у кого есть монеты». Автомат не знает покупателя и не хочет знать. Он исполняет условие для каждого, кто его выполнил, в том числе для того, кто нашёл способ выполнить его непредусмотренным образом. Вторая черта — соразмерность. По

года цитирует SEC в отчёте о The DAO (сноска 3).

[589] Szabo, «Smart Contracts», 1994, в цитате SEC: отчёт о The DAO, Release No. 81207, 25.07.2017, с. 2, сноска 3, https://www.sec.gov/files/litigation/investreport/34-81207.pdf.

[590] Там же, в цитате SEC (отчёт о The DAO, с. 2, сноска 3): «…minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries.» Экономические цели, по Сабо, — снизить потери от мошенничества, издержки арбитража и принуждения к исполнению, прочие транзакционные издержки.

[591] Szabo, «Smart Contracts», 1994, в цитате SEC: отчёт о The DAO, Release No. 81207, 25.07.2017, с. 2, сноска 3, https://www.sec.gov/files/litigation/investreport/34-81207.pdf.

[592] Nick Szabo, «Smart Contracts: Building Blocks for Digital Markets», 1996 (пометка: «Extropy #16», частичная переработка; «Copyright (c) 1996 by Nick Szabo»), https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

[593] Szabo, «Smart Contracts: Building Blocks for Digital Markets», 1996.

[594] Szabo N. Smart Contracts: Building Blocks for Digital Markets. Extropy #16, 1996: «A canonical real-life example, which we might consider to be the primitive ancestor of smart contracts, is the humble vending machine. Within a limited amount of potential loss (the amount in the till should be less than the cost of breaching the mechanism), the machine takes in coins, and via a simple mechanism… dispense change and product fairly.» Определение 1996 года: «A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises.»

[595] Szabo, «Smart Contracts: Building Blocks for Digital Markets», 1996.

[596] Szabo, «Smart Contracts: Building Blocks for Digital Markets», 1996.

[597] Nick Szabo, «Formalizing and Securing Relationships on Public Networks», First Monday, vol. 2, no. 9, 1 September 1997, DOI 10.5210/fm.v2i9.548, https://firstmonday.org/ojs/index.php/fm/article/view/548; текст: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/formalize.html.

[598] Szabo N. Formalizing and Securing Relationships on Public Networks. First Monday, vol. 2, no. 9, 01.09.1997: «The vending machine is a contract with bearer: anybody with coins can participate in an exchange with the vendor.»

[599] ethereum.org, «Introduction to smart contracts», https://ethereum.org/smart-contracts/; ethereum.org, «Introduction to smart contracts» (developers), https://ethereum.org/developers/docs/smart-contracts/.

Сабо, в кассе должно лежать меньше, чем стоит вскрытие[600]. Автомат охраняет арифметика, потому что вскрывать его невыгодно.

Если перенести автомат в компьютер, возникает вопрос, знакомый по первой главе. Чья это программа? Программа на чьём-то сервере исполняется так, как решит владелец сервера, и мы снова зависим от хранителя, только теперь хранитель следит за автоматом. Автомату нужна тетрадка, которую никто не может тихо переписать и в которой нет хозяина, а первая такая тетрадка заработала в январе 2009 года[601].

Тетрадка, которая помнит

В биткоине условие уже есть в каждой строчке. Как мы видели во второй главе, строчка говорит, какой ключ может её потратить. Условия в биткоине записывают на простом языке, и Бутерин в своём описании Ethereum перечислил, чего этому языку не хватает. На нём нельзя записать любое вычисление. Условие не может тонко управлять суммой, которую снимают. Условие не видит данных самого блока. И у него нет памяти: выход либо потрачен, либо нет, и ничего больше[602].[603]

Без памяти не обходится даже простое общее дело. Представим, что двадцать дворов посёлка хотят новый колодец, а работа плотника стоит 100 (числа условные). Нужна строчка, которая скажет: «Принимать взносы от любого двора. Если к первому сентября набралось 100, отдать их плотнику. Если не набралось, вернуть каждому его взнос». Строчка биткоина так не умеет, потому что для этого нужно помнить, кто сколько внёс, и следить за датой. В посёлке такую работу поручили бы казначею, и казначей стал бы маленьким хранителем со всеми его слабостями.

По воспоминаниям Бутерина, в октябре 2013 года он много общался с командой Mastercoin, протокола поверх биткоина, и предлагал им новые функции. А в ноябре, на долгой прогулке по Сан-Франциско, понял, что смарт-контракты можно сделать полностью универсальными[604].[605] Мотив он описывал так: вместо того чтобы добавлять в протокол функции по одной, сделать протокол общим, чтобы он поддерживал больше типов контрактов без большого и сложного набора функций[606]. Описание Ethereum разошлось по рукам в конце 2013 года[607].[608] Цель в нём названа прямо — блокчейн со встроенным языком программирования,

---

[600] Szabo, «Smart Contracts: Building Blocks for Digital Markets», 1996.

[601] генезис — исходный код Bitcoin Core, src/kernel/chainparams.cpp (assert hashGenesisBlock), https://raw.githubusercontent.com/bitcoin/bitcoin/master/src/kernel/chainparams.cpp; блок 968 721 — API mempool.space, https://mempool.space/api/block-height/968721 (обращение 2026-09-26).

[602] V. Buterin, «Ethereum Whitepaper», https://ethereum.org/whitepaper/.

[603] Buterin V. Ethereum Whitepaper: «UTXO can either be spent or unspent; there is no opportunity for multi-stage contracts or scripts which keep any other internal state beyond that.» Четыре ограничения в описании называются так: неполнота по Тьюрингу, «слепота к стоимости», отсутствие состояния и «слепота к блокчейну».

[604] Vitalik Buterin, «A Prehistory of the Ethereum Protocol», 14.09.2017, https://vitalik.eth.limo/general/2017/09/14/prehistory.html.

[605] Buterin V. A Prehistory of the Ethereum Protocol, 14.09.2017: «…a long walk through San Francisco I took in November once I realized that smart contracts could potentially be fully generalized.» Воспоминания написаны через четыре года после событий.

[606] Vitalik Buterin, «A Prehistory of the Ethereum Protocol», 14.09.2017, https://vitalik.eth.limo/general/2017/09/14/prehistory.html.

[607] ethereum.org, «Ethereum Fork Timeline», https://ethereum.org/ethereum-forks/; ethereum.org, «Ethereum Whitepaper», https://ethereum.org/whitepaper/ (перенос https://ethereum.org/en/ethereum-forks/, обе страницы перепроверены).

[608] Дата описания расходится даже на сайте Ethereum: хронология форков называет 27 ноября 2013 года, страница самого описания — «опубликовано в 2014 году» (ethereum.org, «Ethereum Fork Timeline», https://ethereum.org/ethereum-forks/; ethereum.org, «Ethereum Whitepaper», https://ethereum.org/whitepaper/ (перенос https://ethereum.org/en/ethereum-forks/, обе страницы перепроверены)). Формальную спецификацию Ethereum («Yellow Paper») написал Гэвин Вуд, первая версия — 2014 год (G. Wood, «Ethereum: A Secure Decentralised Generalised Transaction Ledger», https://ethereum.github.io/yellowpaper/paper.pdf (перенос https://ethereum.github.io/yellowpaper/paper.pdf, не перепроверялся)).

на котором можно записать «контракт» с произвольными правилами[609].[610] Сеть запустили 30 июля 2015 года[611].[612]

Добавим в посёлок одиннадцатое правило: в тетрадку можно записать правило-автомат, то есть строчку, которой распоряжается не ключ, а записанный в ней порядок действий. Когда кто-то обращается к автомату, каждый двор выполняет этот порядок у себя и получает один и тот же результат.

Двенадцатое правило добавляет память. У автомата есть своя страница, где он сам ведёт записи (кто сколько внёс, какая сегодня дата по тетрадке, сколько осталось до сотни) и сам их меняет.

С этими двумя правилами колодец обходится без казначея. Проследим по шагам. Дворы один за другим присылают автомату по 5, и после каждого взноса автомат делает запись на своей странице («пекарь — 5, доярка — 5» и так далее), а внизу держит сумму. Допустим, к первому сентября пришло 95. Условие «набралось 100» не выполнено, и каждый двор может обратиться к автомату и забрать своё. Автомат найдёт на странице его строчку, отдаст 5 и вычеркнет её. Если бы набралось 100, первое же обращение после первого сентября запустило бы другую ветку, и автомат перевёл бы всю сотню плотнику.

Сам автомат первого сентября не просыпается. Он выполняет свой код, только когда к нему кто-то обращается, и это свойство ещё понадобится нам в истории The DAO. Плотнику не нужно бояться, что казначей сбежит с деньгами, дворам не нужно бояться, что казначей отдаст деньги своему родственнику. Одна вещь автомату при этом недоступна. Он не знает, выкопан ли колодец, потому что знает только то, что записано в тетрадке. К этому мы тоже вернёмся.

---

[609] Buterin, «Ethereum Whitepaper», https://ethereum.org/whitepaper/ (перенос https://ethereum.org/en/ethereum-forks/, цитата перепроверена).

[610] Buterin V. Ethereum Whitepaper: «What Ethereum intends to provide is a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create „contracts“ that can be used to encode arbitrary state transition functions». «Полный по Тьюрингу» — язык, на котором можно записать любое вычисление, какое вообще можно записать программой.

[611] ethereum.org, «Ethereum Fork Timeline», https://ethereum.org/ethereum-forks/ (перенос https://ethereum.org/en/ethereum-forks/, перепроверено).

[612] ethereum.org, Ethereum Fork Timeline: 30.07.2015, 15:26:13 UTC, выпуск Frontier — «живая, но минимальная» версия сети.

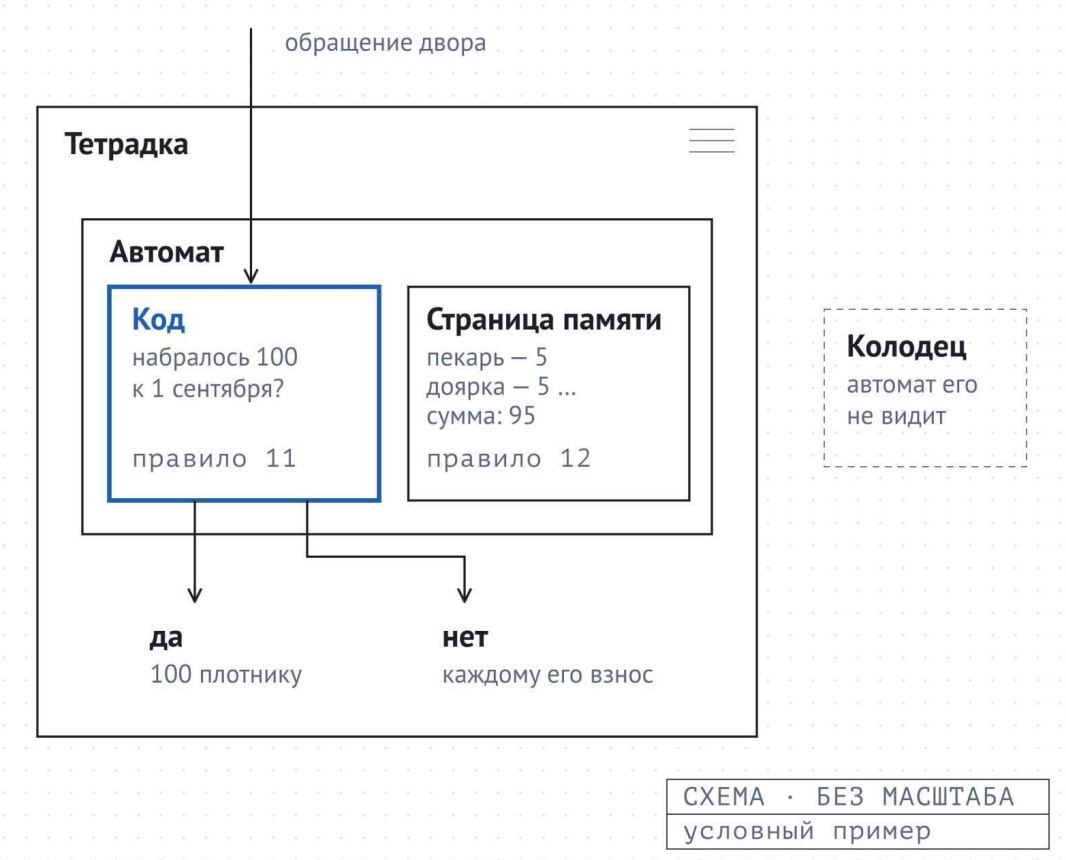


Рисунок 4.1. Автомат колодца

Документация Ethereum описывает то же самое без посёлка. Смарт-контракт — это обычная программа, которая хранится в блокчейне по определённому адресу: набор кода (функций) и данных (состояния)[613].[614] Во второй главе я обещал вернуться к счетам Ethereum, которыми управляет код. Это они и есть. Одними счетами в Ethereum распоряжается закрытый ключ, другими — программа[615]. Особый депозитный счёт, на который валидаторы вносят залог (о нём шла речь в прошлой главе), тоже контракт[616].

Биткоин можно представить как тетрадь записей о том, кто кому что передал. Ethereum описывает себя иначе, как «машину состояний». Его состояние — одна большая структура со всеми счетами, остатками и памятью всех контрактов, и от блока к блоку она меняется по заранее заданным правилам[617]. Исполняет их виртуальная машина Ethereum (EVM), программа, которая одинаково работает на каждом узле[618].[619] При одной и той же памяти и одном и том

[613] ethereum.org, «Introduction to smart contracts», https://ethereum.org/developers/docs/smart-contracts/.

[614] ethereum.org, Introduction to smart contracts: «A „smart contract“ is simply a program that runs on the Ethereum blockchain. It's a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereum blockchain.»

[615] ethereum.org, «Ethereum accounts», https://ethereum.org/en/developers/docs/accounts/; «Blocks», https://ethereum.org/en/developers/docs/blocks/.

[616] ethereum.org, «Proof-of-stake (PoS)», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

[617] ethereum.org, «Ethereum Virtual Machine (EVM)», https://ethereum.org/developers/docs/evm/.

[618] ethereum.org, «Ethereum Virtual Machine (EVM)», https://ethereum.org/developers/docs/evm/.

[619] ethereum.org, Ethereum Virtual Machine (EVM): «The Ethereum Virtual Machine (EVM) is a decentralized virtual environment that executes code consistently and securely across all Ethereum nodes.» Технически EVM — стековая машина глубиной 1024 элемента по 256 бит; код контракта — последовательность простых операций (сложение, вычитание, логические операции) и особых операций блокчейна (адрес, баланс, хеш блока) (ethereum.org, «Ethereum Virtual Machine (EVM)», https://

же обращении все узлы обязаны получить один и тот же результат, иначе они не договорятся о том, какое состояние теперь верно[620].

Слово «контракт» вводит в заблуждение, и сам Бутерин предупреждал об этом. В описании Ethereum сказано, что «контракты» не стоит понимать как нечто, что «исполняют» или «соблюдают». Это скорее «автономные агенты», которые живут внутри Ethereum и выполняют свой код, когда их «толкнёт» сообщение[621], как наш автомат у колодца.[622] Юридического договора с подписями сторон и судом, который его толкует, здесь нет. Есть программа, и она делает ровно то, что в ней написано. Дальше я буду говорить «смарт-контракт» или просто «контракт», потому что так принято, но держать в голове стоит слово «программа».

Счётчик и необратимость

Язык, на котором можно записать любое вычисление, позволяет записать и такое, которое никогда не кончится. Допустим, кто-то записывает в тетрадку автомат, который по кругу прибавляет к числу единицу и никогда не останавливается, и все сто дворов, обязанные выполнить его у себя, садятся считать до бесконечности. Злой умысел для этого не нужен, хватит ошибки в условии остановки.

Ethereum отвечает на это газом. Газ — единица, которой меряют объём вычислительной работы, нужной для операции[623].[624] Каждая транзакция обязана заранее указать, сколько шагов вычислений она готова оплатить, и Бутерин прямо объяснял это защитой от случайных и враждебных бесконечных циклов[625].[626] Добавим тринадцатое правило: каждый шаг автомата стоит платы; кто обращается к автомату, заранее говорит, сколько шагов оплачивает; если плата кончилась посреди работы, все изменения отменяются, а заплаченное всё равно списывается[627].

Проще всего представить газ как счётчик в такси, который останавливает поездку, когда кончились деньги. Разница в том, что пассажира высаживают там, откуда он выехал, а за километры, которые счётчик уже насчитал, всё равно берут плату[628]. Отмена изменений нужна, чтобы автомат не застрял на полпути с наполовину переписанной памятью. Плата не возвращается, потому что дворы свою работу уже проделали. У страницы тетрадки тоже есть предел газа, то есть предел работы, которую можно уложить в один блок[629], и эта деталь понадобится нам в истории The DAO.

---

ethereum.org/developers/docs/evm/).

[620] ethereum.org, «Oracles», https://ethereum.org/developers/docs/oracles/.

[621] Buterin, «Ethereum Whitepaper», https://ethereum.org/whitepaper/.

[622] Buterin V. Ethereum Whitepaper: «Note that „contracts“ in Ethereum should not be seen as something that should be „fulfilled“ or „complied with“; rather, they are more like „autonomous agents“…»

[623] ethereum.org, «Gas and fees», https://ethereum.org/developers/docs/gas/.

[624] ethereum.org, Gas and fees: «Gas refers to the unit that measures the amount of computational effort required to execute specific operations on the Ethereum network.» Цену газа указывают в gwei, одной миллиардной эфира (ethereum.org, «Gas and fees», https://ethereum.org/developers/docs/gas/). После обновления EIP-1559 (2021) цена состоит из двух частей: «The base fee is set by the protocol» (пересчитывается по тому, насколько предыдущий блок заполнен относительно целевого размера) и «The priority fee is a tip that you add to the base fee to make your transaction attractive to validators» (ethereum.org, «Gas and fees», https://ethereum.org/developers/docs/gas/). Базовая часть «сжигается», то есть выводится из обращения (ethereum.org, «Gas and fees», https://ethereum.org/developers/docs/gas/). В 2016 году, о котором идёт речь дальше, цену газа целиком назначал отправитель.

[625] Buterin, «Ethereum Whitepaper», https://ethereum.org/whitepaper/; ethereum.org, «Gas and fees», https://ethereum.org/developers/docs/gas/.

[626] Buterin V. Ethereum Whitepaper: «In order to prevent accidental or hostile infinite loops or other computational wastage in code, each transaction is required to set a limit to how many computational steps of code execution it can use.» В описании для этого служат поля STARTGAS и GASPRICE (Buterin, «Ethereum Whitepaper», https://ethereum.org/whitepaper/; ethereum.org, «Gas and fees», https://ethereum.org/developers/docs/gas/).

[627] ethereum.org, «Gas and fees», https://ethereum.org/developers/docs/gas/.

[628] ethereum.org, «Gas and fees», https://ethereum.org/developers/docs/gas/.

[629] Péter Szilágyi, «DAO Wars: Your voice on the soft-fork dilemma», Ethereum Foundation Blog, 24.06.2016, https://

Из предела следует и цена. Место на странице ограничено, как в биткоине во второй главе, и цена газа (её считают в миллиардных долях эфира) зависит от того, сколько желающих[630]. Основную её часть сеть назначает сама: когда страницы переполнены, цена растёт, когда пустеют, падает. Сверху отправитель может добавить чаевые, чтобы пройти быстрее[631]. Поэтому, если вы обратитесь к тому же автомату в день ажиотажа, вы заплатите больше, чем в спокойный день, хотя работы в вашем обращении столько же.

Сложим это с правилами, записанными раньше. Тетрадку нельзя тайно переписать (шестое и седьмое правила), а автомат исполняет себя сам и одинаково у всех (одиннадцатое). Значит, то, что автомат сделал, сделано навсегда.

Документация Ethereum говорит то же самое. По умолчанию смарт-контракт нельзя удалить, а взаимодействия с ним необратимы[632].[633] Там же названо ещё одно свойство. Контракты публичны и могут обращаться друг к другу, как детали, из которых собирают более сложные механизмы[634]. Это удобно, пока детали исправны. Если одна деталь сломана, могут сломаться все механизмы, в которые её встроили.

Здесь контракт и торговый автомат расходятся, и это различие важнее сходства. У автомата в магазине есть хозяин. У него есть ключ от дверцы, он может открыть её, вынуть деньги, заменить сломанный механизм или увезти автомат совсем. У контракта в тетрадке такого хозяина по умолчанию нет[635]. Если у кого-то есть особые права, они записаны в самом коде, и распорядиться ими может тот, кого код признаёт хозяином (как мы увидим, это не всегда тот, кого имели в виду авторы). Касса автомата в магазине невелика, а в кассу контракта можно положить столько, сколько готовы принести все желающие. Соразмерность, на которую рассчитывал Сабо, никто не гарантирует.

Автомат, который исполняет правильное условие без участия людей, так же без участия людей исполняет и ошибочное. Ему всё равно, что имели в виду авторы, он делает то, что записано, для любого, кто к нему обратился, и отменить сделанное нельзя. Если в обычном договоре есть ошибка, стороны идут с ней в суд. Ошибкой в контракте первым пользуется тот, кто нашёл её раньше других, и суд, если дело до него дойдёт, разбирает уже сделанное.

Касса на 150 миллионов

The DAO придумали в немецкой компании Slock.it. В ноябре 2015 года её сооснователь Кристоф Йенч представил идею на конференции разработчиков Ethereum в Лондоне как «коммерческую DAO»[636].[637] (DAO — сокращение от английского decentralized autonomous organization, «децентрализованная автономная организация». Так, по определению SEC, называют «виртуальную» организацию, воплощённую в компьютерном коде и исполняемую в

---

blog.ethereum.org/2016/06/24/dao-wars-youre-voice-soft-fork-dilemma.

[630] ethereum.org, «Gas and fees», https://ethereum.org/developers/docs/gas/.

[631] ethereum.org, «Gas and fees», https://ethereum.org/developers/docs/gas/; ethereum.org, «Gas and fees», https://ethereum.org/developers/docs/gas/.

[632] ethereum.org, «Introduction to smart contracts», https://ethereum.org/developers/docs/smart-contracts/.

[633] ethereum.org, Introduction to smart contracts: контракты «cannot be deleted by default, and interactions with them are irreversible.»

[634] ethereum.org, «Introduction to smart contracts», https://ethereum.org/developers/docs/smart-contracts/.

[635] ethereum.org, «Introduction to smart contracts», https://ethereum.org/developers/docs/smart-contracts/.

[636] SEC, Report of Investigation… The DAO, Release No. 81207, 25.07.2017, с. 3–5 и сноски 7, 12, https://www.sec.gov/files/litigation/investreport/34-81207.pdf.

[637] Сооснователи Slock.it — Кристоф Йенч, Симон Йенч и Штефан Туаль; конференция — Devcon1 (Лондон, ноябрь 2015 года). Финальный черновик описания The DAO — около 23 марта 2016 года (SEC, отчёт о The DAO, с. 3–5) (SEC, Report of Investigation… The DAO, Release No. 81207, 25.07.2017, с. 3–5 и сноски 7, 12, https://www.sec.gov/files/litigation/investreport/34-81207.pdf).

блокчейне[638].)[639] Устройство было такое. Участники платят эфир и получают токены, то есть строчки на странице памяти контракта, где записано, сколько единиц принадлежит какому адресу. Токены дают голос при выборе проектов, которые фонд будет финансировать, и право на «вознаграждения», а сам Йенч сравнивал это с покупкой акций компании и получением дивидендов[640].

Код развернули в сети около 29 апреля 2016 года, а с 30 апреля по 28 мая The DAO продала около 1,15 млрд токенов примерно за 12 млн ETH[641].[642] Купить мог любой, у кого был эфир, без ограничений по числу покупателей и их опыту[643]. Это тот же «договор с предъявителем», что у автомата Сабо, только в кассе на момент закрытия продажи лежало, по оценке SEC, около 150 млн долларов[644].

Децентрализованной эта организация была не вполне. Какие предложения попадут на голосование, решали «кураторы», одиннадцать человек, отобранных Slock.it, и один из них публично говорил, что у кураторов «огромная власть»[645].[646] Люди, которые принимают решения, были в The DAO с первого дня, задолго до всякой аварии. О безопасности кода Slock.it сообщала, что его проверила одна из ведущих компаний по аудиту и что за «пять полных дней анализа безопасности» не осталось ни одного неперевёрнутого камня[647].[648]

Тревога появилась ещё до атаки. 26 мая Slock.it внесла предложение о безопасности DAO, 27 мая группа исследователей призвала к временному мораторию на The DAO (их статья разбирала в основном устройство голосования), а 3 июня Йенч предложил приостановить все предложения до исправления уязвимостей[649]. 10 июня в блоге фонда Ethereum вышла статья о безопасности смарт-контрактов, где разбирался как раз этот класс ошибок[650]. Статья разбирала общий случай и не говорила, что такая ошибка есть в The DAO[651], но лекарство в ней было названо.

---

[638] SEC, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Release No. 81207, 25.07.2017, с. 1, https://www.sec.gov/files/litigation/investreport/34-81207.pdf (страница прочитана фактчекером 27.09.2026).

[639] SEC, отчёт о The DAO, с. 1: «The DAO is one example of a Decentralized Autonomous Organization, which is a term used to describe a „virtual" organization embodied in computer code and executed on a distributed ledger or blockchain.» (SEC, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Release No. 81207, 25.07.2017, с. 1, https://www.sec.gov/files/litigation/investreport/34-81207.pdf (страница прочитана фактчекером 27.09.2026))

[640] SEC, Report of Investigation… The DAO, Release No. 81207, 25.07.2017, с. 3–5 и сноски 7, 12, https://www.sec.gov/files/litigation/investreport/34-81207.pdf.

[641] SEC, Report of Investigation… The DAO, Release No. 81207, 25.07.2017, с. 3–5 и сноски 7, 12, https://www.sec.gov/files/litigation/investreport/34-81207.pdf; SEC, отчёт о The DAO, 2017, с. 2–3 (перенос https://www.sec.gov/files/litigation/investreport/34-81207.pdf, перепроверено).

[642] Цена во время продажи колебалась примерно от 1 до 1,5 ETH за 100 токенов DAO (SEC, отчёт о The DAO, 2017, с. 6). В пересказах встречаются «12,7 млн ETH» и «около 14% всего эфира» (Mastering Ethereum); здесь и дальше — цифры SEC: «approximately 12 million» (SEC, отчёт о The DAO, 2017, с. 2–3 (перенос https://www.sec.gov/files/litigation/investreport/34-81207.pdf, перепроверено)).

[643] SEC, отчёт о The DAO, 2017, с. 6.

[644] SEC, отчёт о The DAO, 2017, с. 2–3 (перенос https://www.sec.gov/files/litigation/investreport/34-81207.pdf, перепроверено).

[645] SEC, отчёт о The DAO, 2017, с. 7–8, сноски 25–26.

[646] SEC, отчёт о The DAO, с. 7–8: «…noting that „curators have tremendous power."» Многие кураторы были связаны с фондом Ethereum (SEC, отчёт о The DAO, 2017, с. 7–8, сноски 25–26).

[647] SEC, отчёт о The DAO, 2017, с. 5, сноска 19 (ссылка на пост С. Туаля в блоге Slock.it от 05.04.2016).

[648] SEC, отчёт о The DAO, с. 5, сноска 19 (со ссылкой на пост С. Туаля в блоге Slock.it от 05.04.2016): «…no stone was left unturned during those five whole days of security analysis.»

[649] SEC, отчёт о The DAO, 2017, с. 7 (сноска 24: Dino Mark et al., «A Call for a Temporary Moratorium on The DAO», Hacking, Distributed, 27.05.2016) и с. 9 (сноски 28–29).

[650] Christian Reitwiessner, «Smart Contract Security», Ethereum Foundation Blog, 10.06.2016, https://blog.ethereum.org/2016/06/10/smart-contract-security.

[651] Christian Reitwiessner, «Smart Contract Security», Ethereum Foundation Blog, 10.06.2016, https://blog.ethereum.org/2016/06/10/smart-contract-security.

Сама ошибка описывается в двух фразах, и лучше всего её понять на условном примере. Представим банкомат, который, получив запрос «снять всё», сначала выдаёт купюры и только потом списывает сумму со счёта, а пока купюры идут из лотка, позволяет нажать «снять всё» ещё раз. Каждое новое нажатие банкомат проверяет по счёту, который ещё не уменьшился, и каждое проходит. Никакой банкомат так не устроен, пример условный. Но функция вывода в The DAO была устроена именно так. Две строки кода стояли не в том порядке, и контракт сначала отправлял эфир, а потом обнулял баланс[652].[653]

Почему получатель мог нажать ещё раз? Получателем эфира может быть другой контракт, и, пока отправка ещё не завершена, он может снова вызвать функцию вывода[654]. Так и вышло. Строка «обнулить баланс» до своей очереди не доходила, и запрос на вывод исполнялся снова и снова в пределах одной транзакции[655]. Бутерин в тот же день назвал это уязвимостью «рекурсивного вызова»[656], разработчики сегодня называют её повторным входом. Лекарство состоит в перестановке строк: сначала изменить записи, потом отправлять эфир[657].

Разберём это на круглых числах (они условные и с настоящими суммами The DAO не связаны). В кассе общего автомата 1000, и на его странице памяти записано, что доля одного адреса равна 10. За адресом стоит другой автомат, и у него одно правило — получив деньги, сразу снова попросить свою долю. Первый запрос. Общий автомат смотрит на страницу, видит 10 и отправляет 10. Получение будит второй автомат, и тот просит снова. Общий автомат снова смотрит на страницу, где по-прежнему записано 10, потому что до строки «обнулить» дело ещё не дошло, и снова отправляет 10. Так повторяется, пока не кончится газ или деньги в кассе, и сорока повторов хватает, чтобы доля в 10 превратилась в 400.

Если переставить две строки, всё останавливается на первом шаге. Автомат сначала запишет на странице 0, потом отправит 10, и на второй запрос у него найдётся ответ: доли больше нет. Код, который исполняет себя сам, не знает, что имели в виду его авторы, и порядок строк для него и есть смысл.

---

[652] Andreas M. Antonopoulos, Gavin Wood, «Mastering Ethereum», O'Reilly, 2018: приложение «Ethereum Fork History», https://cypherpunks-core.github.io/ethereumbook/appdx-forks-history.html; гл. «Smart Contract Security», https://cypherpunks-core.github.io/ethereumbook/09smart-contracts-security.html.

[653] Antonopoulos A. M., Wood G. Mastering Ethereum. O'Reilly, 2018, приложение «Ethereum Fork History»: «…a crucial function in the DAO had two lines of code in the wrong order, meaning that the attacker could have requests to withdraw ether acted upon repeatedly…» Статья в блоге фонда 10.06.2016 (Reitwiessner C. Smart Contract Security) описывала общий случай: «This means that while the send function is still in progress, the recipient can call back into withdrawRefund.» Общепринятое лекарство разработчики называют шаблоном «проверки — изменения — взаимодействия».

[654] Christian Reitwiessner, «Smart Contract Security», Ethereum Foundation Blog, 10.06.2016, https://blog.ethereum.org/2016/06/10/smart-contract-security.

[655] Andreas M. Antonopoulos, Gavin Wood, «Mastering Ethereum», O'Reilly, 2018: приложение «Ethereum Fork History», https://cypherpunks-core.github.io/ethereumbook/appdx-forks-history.html; гл. «Smart Contract Security», https://cypherpunks-core.github.io/ethereumbook/09smart-contracts-security.html.

[656] Vitalik Buterin, «CRITICAL UPDATE Re: DAO Vulnerability», Ethereum Foundation Blog, 17.06.2016, https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability.

[657] Christian Reitwiessner, «Smart Contract Security», Ethereum Foundation Blog, 10.06.2016, https://blog.ethereum.org/2016/06/10/smart-contract-security; Andreas M. Antonopoulos, Gavin Wood, «Mastering Ethereum», O'Reilly, 2018: приложение «Ethereum Fork History», https://cypherpunks-core.github.io/ethereumbook/appdx-forks-history.html; гл. «Smart Contract Security», https://cypherpunks-core.github.io/ethereumbook/09smart-contracts-security.html.

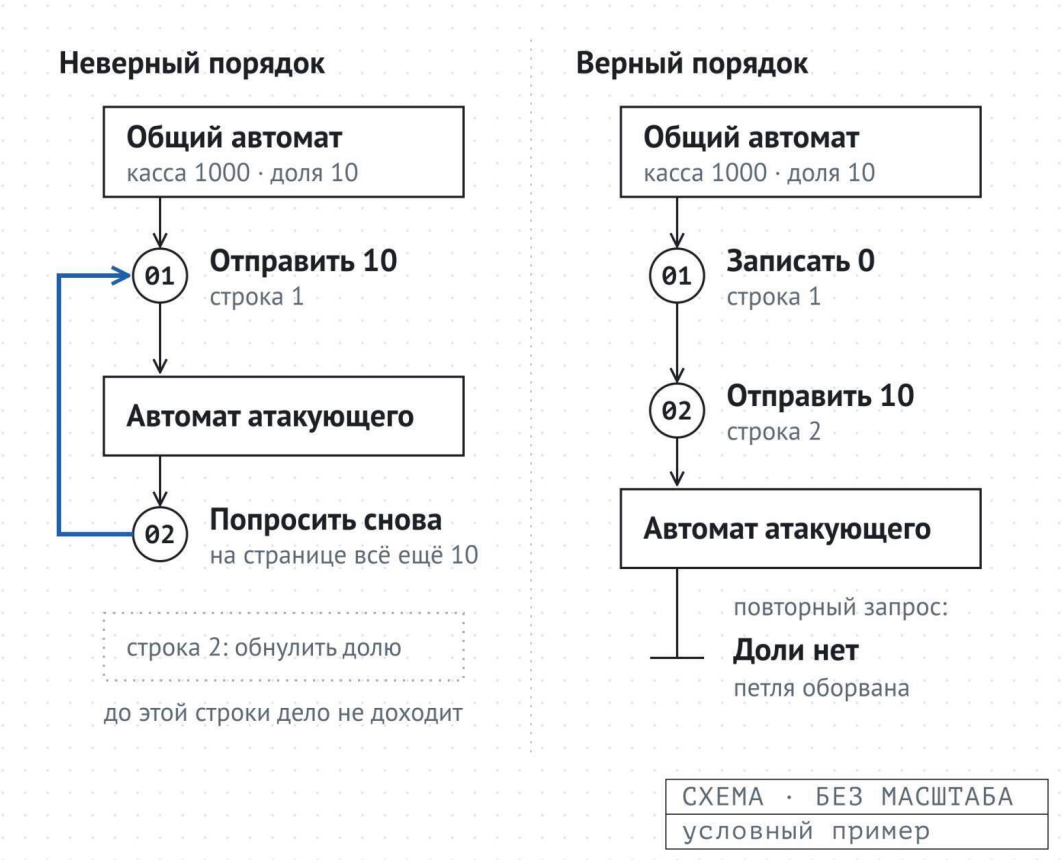


Рисунок 4.2. Повторный вход

Выведенный эфир ушёл в «дочернюю DAO», отдельный контракт, откуда код самой The DAO не давал его сразу забрать[658]. Тот же код, который позволил вывести эфир, запер его на время, и это время ушло у сообщества на спор.

Автомат Сабо защищала соразмерность (в кассе меньше, чем стоит взлом). У The DAO соотношение было обратным: касса больше сотни миллионов долларов, а для взлома хватало знать класс ошибок, который фонд Ethereum разобрал публично за неделю до атаки[659], и уметь обратиться к функции повторно. Аудит, пять дней анализа и публичные тревоги о безопасности The DAO атаку не предотвратили[660].

Была ли это кража?

Комиссия по ценным бумагам и биржам США (SEC), которая позже расследовала историю The DAO, во введении к отчёту пишет, что атакующий «украл» около трети активов, но в заголовке раздела ставит слово «атака» в кавычки[661].[662] 18 июня на сайте для публикации

---

[658] SEC, отчёт о The DAO, 2017, с. 9 (перенос , перепроверено); Vitalik Buterin, «CRITICAL UPDATE Re: DAO Vulnerability», Ethereum Foundation Blog, 17.06.2016, https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability.

[659] Christian Reitwiessner, «Smart Contract Security», Ethereum Foundation Blog, 10.06.2016, https://blog.ethereum.org/2016/06/10/smart-contract-security.

[660] SEC, отчёт о The DAO, 2017, с. 5, сноска 19 (ссылка на пост С. Туаля в блоге Slock.it от 05.04.2016); SEC, отчёт о The DAO, 2017, с. 7 (сноска 24: Dino Mark et al., «A Call for a Temporary Moratorium on The DAO», Hacking, Distributed, 27.05.2016) и с. 9 (сноски 28–29).

[661] SEC, отчёт о The DAO, 2017, с. 9 (перенос , перепроверено).

[662] SEC, отчёт о The DAO, с. 1: «…an attacker used a flaw in The DAO's code to steal approximately one-third of The DAO's assets»; с. 9, заголовок раздела: «Security Concerns, The „Attack" on The DAO, and The Hard Fork» (SEC, отчёт о The DAO, 2017, с. 9 (перенос , перепроверено)).

текстов появилось «открытое письмо» от имени атакующего. Автор утверждал, что законно получил 3 641 694 ETH через функцию, которую контракт сам предусматривал, называл это «намеренной возможностью» и писал, что его разочаровывают те, кто называет её использование кражей[663].[664] Любой софт- или хардфорк он называл изъятием своего законного эфира, полученного по условиям смарт-контракта[665].

Подлинность письма разработчики оспорили сразу. Цифровая подпись под ним, по их разбору, была устроена не так, как должна быть устроена действительная подпись, и Бутерин назвал её «сомнительной»[666].[667] Поэтому кто написал письмо, неизвестно. Но позиция в нём сформулирована чище, чем где-либо ещё: код разрешил, значит, всё законно. Хорош этот довод или плох, в ближайшие недели предстояло решить майнерам и держателям монет.

Тридцать три дня

Выбор у сообщества был из трёх вариантов: ничего не делать; принять новое правило, которое запретит трогать эфир атакующего; или переложить эфир обратно. Второй и третий путь меняют правила тетрадки, и отличаются они тем, как ведут себя старые программы.

Цена у каждого пути своя. Если ничего не делать, правило «взаимодействия необратимы» остаётся нетронутым, а вкладчики The DAO теряют треть собранного[668]. Если вернуть деньги, вкладчики остаются при своём, а у сети появляется прецедент, ведь однажды большинство уже поправило результат, который правила допустили. Первый путь дорог для тех, кто вложился, второй — для доверия к самим правилам. Положить эти две цены на одни весы нельзя, и поэтому я не думаю, что спор мог кончиться общим согласием.

Софтфорк, «мягкое» изменение, только ужесточает правила: то, что было запрещено, остаётся запрещённым, а к запретам добавляется новый (если посмотреть с этой стороны, так же исправили ошибку 2010 года из второй главы)[669]. Страницы, написанные по новым правилам, старые программы тоже признают, и, если новое правило поддерживает большинство тех, кто пишет страницы, сеть не делится. Хардфорк вводит правило, которое старые программы сочтут нарушением. Если на новую версию переходят все, ничего не происходит, а если не все, тетрадка раскалывается на две, и у каждой своя история. В 2016 году Ethereum ещё работал на доказательстве работы, как биткоин (на залог он перешёл в 2022 году[670]), и голос в этом споре был у майнеров.

Первым предложили софтфорк. 17 июня Бутерин написал, что начиная с блока 1 760 000 новое правило сделает вывод этих средств невозможным[671]. 24 июня фонд Ethereum выпустил

---

[663] «An Open Letter», Pastebin, 18.06.2016, https://pastebin.com/CcGUBgDG.

[664] «An Open Letter», Pastebin, 18.06.2016, подпись «The Attacker»: «I am disappointed by those who are characterizing the use of this intentional feature as „theft“»; «A soft or hard fork would amount to seizure of my legitimate and rightful ether, claimed legally through the terms of a smart contract.» Авторство не установлено.

[665] «An Open Letter», Pastebin, 18.06.2016, https://pastebin.com/CcGUBgDG.

[666] Coinfox, «Open letter from The DAO attacker – fake?», 20.06.2016, https://www.coinfox.info/news/5743-otkrytoe-pismo-ot-pokhititelya-tokenov-the-dao-poddelka-2/.

[667] Разработчик Ethereum Ник Джонсон указал, что действительная подпись этого типа длиной 65 байт должна заканчиваться на 0x00 или 0x01, а подпись под письмом заканчивалась на 0x32. Бутерин: «Signature looks shady at first glance; the first byte is 0x5f, which is not a standard v value by any encoding.» Обе реплики — в пересказе Coinfox, 20.06.2016; первоисточник на Reddit не сверялся.

[668] SEC, отчёт о The DAO, 2017, с. 9 (перенос , перепроверено).

[669] Bitcoin Wiki, «Value overflow incident», https://en.bitcoin.it/wiki/Value_overflow_incident; Накамото, архив bitcointalk, посты 16.08.2010 01:00:45 и 12:59:38 UTC.

[670] ethereum.org, «The Merge», https://ethereum.org/en/roadmap/merge/; «Ethereum energy consumption», https://ethereum.org/en/energy-consumption/ (перенесено из https://ethereum.org/en/roadmap/merge//https://ethereum.org/energy-consumption/, перепроверено 26.09.2026).

[671] Vitalik Buterin, «CRITICAL UPDATE Re: DAO Vulnerability», Ethereum Foundation Blog, 17.06.2016, https://

версию программы узла Geth 1.4.8, где софтфорк можно было включить, и оставил решение майнерам[672].[673] Голосовали самим способом сборки страниц. Сторонники включали флажок и понемногу снижали предел газа в своих блоках, и если бы к блоку 1 800 000 этот предел опустился ниже 4 млн, софтфорк вступил бы в силу[674].

28 июня от софтфорка отказались. В его коде нашли уязвимость. Код, который приводил софтфорк в действие, позволял выполнять вычисления вплоть до предела газа в блоке и ничего за них не платить[675].[676] Так открывался путь для атаки типа «отказ в обслуживании», когда сеть заваливают бесплатной работой[677]. Софтфорк, который должен был исправить ошибку одного контракта, сам нарушил тринадцатое правило, то самое, которое делает бесконечную работу дорогой. Фонд рекомендовал голосовать против, пока не найдётся лучшее решение[678].

Выбор сузился до двух вариантов: ничего не делать или хардфорк.

15 июля фонд объявил параметры хардфорка[679].[680] По плану на блоке 1 920 000 эфир из The DAO и её дочерних контрактов переходил на контракт возврата, где держатели токенов могли обменять их по курсу 100 токенов DAO за 1 ETH. Будет ли хардфорк включён в программе узла по умолчанию, должно было решить голосование в инструменте carbonvote с подсчётом на блоке 1 894 000. В том же сообщении фонд подчеркнул, что такое решение не может принять ни он сам, ни кто-либо другой в одиночку[681].

Допустим, вы купили на продаже 10 000 токенов по нижней цене, 1 ETH за 100 токенов, то есть заплатили 100 ETH[682]. Контракт возврата меняет 100 токенов на 1 ETH, и после форка вы получаете свои 100 ETH обратно, как если бы атаки не было[683]. Для этого вам не нужно было ни голосовать, ни даже знать о голосовании. Вернуло ваши деньги решение, которое приняли другие.

Carbonvote — голосование монетами. Вес голоса равен количеству эфира на адресе[684]. Проголосовало около 5,5% всех монет, и подавляющее большинство проголосовавших высказалось за форк[685].[686] Критики, среди них сооснователь конкурирующего проекта, упрекали про-

---

blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability.

[672] Péter Szilágyi, «DAO Wars: Your voice on the soft-fork dilemma», Ethereum Foundation Blog, 24.06.2016, https://blog.ethereum.org/2016/06/24/dao-wars-youre-voice-soft-fork-dilemma.

[673] Szilágyi P. DAO Wars: Your voice on the soft-fork dilemma. Ethereum Foundation Blog, 24.06.2016: «…we've decided to give the power to the people running Ethereum to decide whether they support this decision or not.»

[674] Péter Szilágyi, «DAO Wars: Your voice on the soft-fork dilemma», Ethereum Foundation Blog, 24.06.2016, https://blog.ethereum.org/2016/06/24/dao-wars-youre-voice-soft-fork-dilemma.

[675] Felix Lange, «Security Alert – DoS Vulnerability in the Soft Fork», Ethereum Foundation Blog, 28.06.2016, https://blog.ethereum.org/2016/06/28/security-alert-dos-vulnerability-in-the-soft-fork.

[676] Lange F. Security Alert – DoS Vulnerability in the Soft Fork. Ethereum Foundation Blog, 28.06.2016: «The fork enactment code in geth (and other clients) allows execution of EVM code up to the block gas limit without paying for gas.»

[677] Felix Lange, «Security Alert – DoS Vulnerability in the Soft Fork», Ethereum Foundation Blog, 28.06.2016, https://blog.ethereum.org/2016/06/28/security-alert-dos-vulnerability-in-the-soft-fork.

[678] Felix Lange, «Security Alert – DoS Vulnerability in the Soft Fork», Ethereum Foundation Blog, 28.06.2016, https://blog.ethereum.org/2016/06/28/security-alert-dos-vulnerability-in-the-soft-fork.

[679] Jeffrey Wilcke, «To fork or not to fork», Ethereum Foundation Blog, 15.07.2016, https://blog.ethereum.org/2016/07/15/to-fork-or-not-to-fork.

[680] Wilcke J. To fork or not to fork. Ethereum Foundation Blog, 15.07.2016: «…this is not a decision that can be made by the foundation or any other single entity.»

[681] Jeffrey Wilcke, «To fork or not to fork», Ethereum Foundation Blog, 15.07.2016, https://blog.ethereum.org/2016/07/15/to-fork-or-not-to-fork.

[682] SEC, отчёт о The DAO, 2017, с. 6.

[683] Jeffrey Wilcke, «To fork or not to fork», Ethereum Foundation Blog, 15.07.2016, https://blog.ethereum.org/2016/07/15/to-fork-or-not-to-fork; SEC, отчёт о The DAO, 2017, с. 9–10 и сноска 32 (перенос , перепроверено).

[684] Jeffrey Wilcke, «To fork or not to fork», Ethereum Foundation Blog, 15.07.2016, https://blog.ethereum.org/2016/07/15/to-fork-or-not-to-fork.

[685] Antonopoulos, Wood, «Mastering Ethereum», 2018, приложение «Ethereum Fork History», https://cypherpunks-core.github.io/ethereumbook/appdx-forks-history.html; Wikipedia, «Ethereum Classic» (со ссылкой на «Ethereum timeline» в

цедуру в том, что голосование длилось меньше суток, объявили о нём только в блоге фонда, в Twitter и на Reddit, а участвовала малая доля держателей[687].[688]

20 июля 2016 года в 13:20:40 по всемирному времени сеть дошла до блока 1 920 000[689]. По сообщению Бутерина, этот блок содержал «нерегулярное изменение состояния», которое перевело около 12 млн ETH из контрактов под названиями «Dark DAO» и «Whitehat DAO» на контракт возврата[690].[691] Форк прошёл гладко, на новой цепочке работали около 85% майнеров, а держателям токенов к моменту сообщения уже вернули около 4,5 млн ETH[692].

Историю при этом задним числом не переписывали. Старые блоки остались на месте, а балансы переложили в новом блоке одним изменением. Описание форка в документации Ethereum отдельно подчёркивает, что протокол не менялся, и команды виртуальной машины, формат транзакций и устройство блоков остались прежними[693].[694] Поэтому слово «откатили», которое часто встречается в пересказах, неточно. Точнее сказать, что большинство задним числом отменило правило «взаимодействия с контрактом необратимы» ради одного контракта.

Несогласные, по отчёту SEC, считали, что переход противоречит самой идее неизменяемого блокчейна, и продолжили пользоваться прежней версией[695].[696] Официальная хронология Ethereum объясняет это короче. По её словам, часть майнеров отказалась от форка, потому что инцидент с The DAO не был дефектом протокола, и они образовали Ethereum Classic[697]. Старую цепочку, по оценке справочника «Mastering Ethereum», поддержали примерно 10% сообщества по стоимости и по мощности майнинга[698].[699] Это та самая сеть, которую через четыре года трижды атаковали, как мы видели в прошлой главе[700].

Mastering Ethereum), https://en.wikipedia.org/wiki/Ethereum_Classic.

[686] Точные цифры голосования расходятся по источникам, и первичная страница результатов больше не существует. Наиболее подробная версия (Wikipedia со ссылкой на «Mastering Ethereum»): из 82 054 716 ETH проголосовали 4 542 416, за форк — 87%, против — 13%, причём четверть голосов «за» пришла с одного адреса; в тексте самой книги — «около 80% голосов», в других пересказах — 85/15 (Antonopoulos, Wood, «Mastering Ethereum», 2018, приложение «Ethereum Fork History», https://cypherpunks-core.github.io/ethereumbook/appdx-forks-history.html; Wikipedia, «Ethereum Classic» (со ссылкой на «Ethereum timeline» в Mastering Ethereum), https://en.wikipedia.org/wiki/Ethereum_Classic). Подсчёт — 16.07.2016. Устройство голосования подтверждено по открытому коду: голос подаётся транзакцией без суммы на один из двух контрактов, «за» или «против».

[687] Kathleen Breitman, «Op Ed: Why Ethereum's Hard Fork Will Cause Problems In The Coming Year», Bitcoin Magazine, 03.02.2017, https://bitcoinmagazine.com/business/op-ed-why-ethereums-hard-fork-will-cause-problems-coming-year.

[688] Breitman K. Why Ethereum's Hard Fork Will Cause Problems In The Coming Year. Bitcoin Magazine, 03.02.2017. Автор колонки — сооснователь конкурирующего проекта Tezos, то есть заинтересованная сторона.

[689] ethereum.org, «Ethereum Fork Timeline», https://ethereum.org/ethereum-forks/ (перенос https://ethereum.org/en/ethereum-forks/, перепроверено).

[690] Vitalik Buterin, «Hard Fork Completed», Ethereum Foundation Blog, 20.07.2016, https://blog.ethereum.org/2016/07/20/hard-fork-completed.

[691] Buterin V. Hard Fork Completed. Ethereum Foundation Blog, 20.07.2016: «Block 1920000 contained the execution of an irregular state change which transferred ~12 million ETH from the „Dark DAO" and „Whitehat DAO" contracts into the WithdrawDAO recovery contract.»

[692] Vitalik Buterin, «Hard Fork Completed», Ethereum Foundation Blog, 20.07.2016, https://blog.ethereum.org/2016/07/20/hard-fork-completed.

[693] EIP-779, «Hardfork Meta: DAO Fork», https://eips.ethereum.org/EIPS/eip-779.

[694] EIP-779, Hardfork Meta: DAO Fork (Casey Detrio, 26.11.2017): «The DAO Fork did not change the protocol; all EVM opcodes, transaction format, block structure, and so on remained the same.» В документе перечислены 114 адресов The DAO и её дочерних контрактов, с которых эфир переведён на контракт возврата.

[695] SEC, отчёт о The DAO, 2017, с. 9–10 и сноска 32 (перенос , перепроверено).

[696] SEC, отчёт о The DAO, с. 9–10: «A minority group, however, elected not to adopt the new Ethereum Blockchain created by the Hard Fork because to do so would run counter to the concept that a blockchain is immutable.» Хронология ethereum.org: «Some miners refused to fork because the DAO incident wasn't a defect in the protocol. They went on to form Ethereum Classic.»

[697] ethereum.org, «Ethereum Fork Timeline», https://ethereum.org/ethereum-forks/ (перенос https://ethereum.org/en/ethereum-forks/).

[698] Antonopoulos, Wood, «Mastering Ethereum», 2018, приложение «Ethereum Fork History», https://cypherpunks-core.github.io/ethereumbook/appdx-forks-history.html.

Безопасность открытой сети, как мы помним, покупается мощностью, которую на неё тратят. Раскол делит не только людей, но и эту охрану. Цепочка, за которой осталась примерно десятая часть мощности[701], охраняется слабее, и переписать её дешевле. Утверждать, что атаки 2020 года прямо вытекают из раскола 2016-го, я не стану, между ними четыре года и много других перемен. Механизм, однако, тот же, и чем меньше мощности держит сеть, тем дешевле её атаковать[702].

Полезно сравнить эту историю с ночью 15 августа 2010 года из второй главы. Тогда сломались правила самой тетрадки: ошибка в проверке позволила создать из ничего монеты, которых правила не допускали[703]. В 2016 году правила тетрадки сработали в точности как записано, и контракт тоже исполнил свой код. Ошиблись люди, которые этот код написали, и вопрос стоял иначе: вправе ли большинство поправить результат, который правила допустили? Для одних это был ремонт после аварии, для других — нарушение правил ради тех, кто вложился в неудачный контракт, и из этой разницы вырос раскол.

---

[699] Antonopoulos, Wood. Mastering Ethereum, приложение «Ethereum Fork History»: «…roughly 10% by value and mining power». Метод и дата оценки не указаны.

[700] CoinDesk (Zack Voell), «Ethereum Classic Hit by Third 51% Attack in a Month», 29.08.2020, https://www.coindesk.com/markets/2020/08/29/ethereum-classic-hit-by-third-51-attack-in-a-month (по отчётам майнинговой компании Bitfly).

[701] Antonopoulos, Wood, «Mastering Ethereum», 2018, приложение «Ethereum Fork History», https://cypherpunks-core.github.io/ethereumbook/appdx-forks-history.html.

[702] CoinDesk (Zack Voell), «Ethereum Classic Hit by Third 51% Attack in a Month», 29.08.2020, https://www.coindesk.com/markets/2020/08/29/ethereum-classic-hit-by-third-51-attack-in-a-month (по отчётам майнинговой компании Bitfly).

[703] Bitcoin Wiki, «Value overflow incident» (CVE-2010-5139), https://en.bitcoin.it/wiki/Value_overflow_incident.

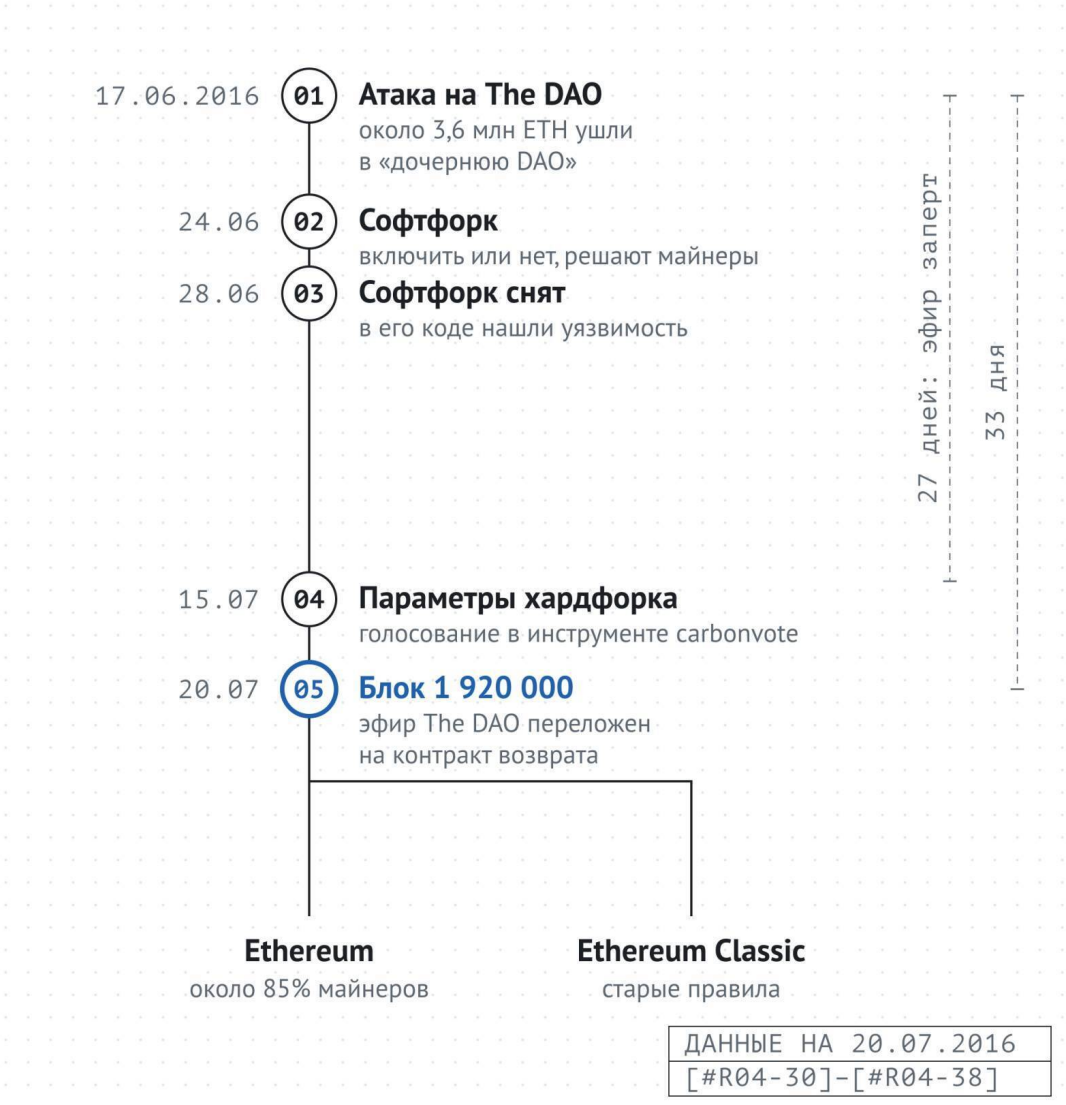


Рисунок 4.3. Тридцать три дня

Кто же принимал решение? Фонд написал код форка и назвал дату, но решать в одиночку отказался[704]. Держатели монет голосовали монетами, и голос у каждого был пропорционален его эфиру[705]. Майнеры голосовали мощностью, выбирая, какую программу запустить[706]. У пользователя без монет на адресе и без машин для майнинга голоса не было вовсе. Для посёлка это сход, где один голос у того, у кого больше строчек, другой у того, кто пишет страницы, а у остальных никакого, и где несогласные уносят свою копию тетрадки и продолжают вести её отдельно. Это и есть «социальный слой» из прошлой главы, та договорённость людей,

[704] Jeffrey Wilcke, «To fork or not to fork», Ethereum Foundation Blog, 15.07.2016, https://blog.ethereum.org/2016/07/15/to-fork-or-not-to-fork.

[705] Jeffrey Wilcke, «To fork or not to fork», Ethereum Foundation Blog, 15.07.2016, https://blog.ethereum.org/2016/07/15/to-fork-or-not-to-fork; Antonopoulos, Wood, «Mastering Ethereum», 2018, приложение «Ethereum Fork History», https://cypherpunks-core.github.io/ethereumbook/appdx-forks-history.html; Wikipedia, «Ethereum Classic» (со ссылкой на «Ethereum timeline» в Mastering Ethereum), https://en.wikipedia.org/wiki/Ethereum_Classic.

[706] Vitalik Buterin, «Hard Fork Completed», Ethereum Foundation Blog, 20.07.2016, https://blog.ethereum.org/2016/07/20/hard-fork-completed.

которую сайт Ethereum называет последней защитой сети[707]. Здесь он сработал на деле, за шесть лет до того, как Ethereum перешёл на залог.

Три прочтения одной фразы

Спор о The DAO шёл под лозунгом «код — это закон». У этой фразы есть автор, и думал он о другом. Так называется первая глава книги юриста Лоуренса Лессига «Код и другие законы киберпространства», вышедшей в 1999 году[708]. Лессиг писал, что в киберпространстве людей регулирует код, то есть программы и железо, из которых это пространство сделано, и в этом смысле код и есть его закон[709].[710]

Для Лессига это было предупреждение. Код может защищать ценности, а может их уничтожать, и его всегда пишут люди, которые выбирают, какие ценности в него заложить[711]. По его формуле, код никогда не находят, его только делают, и делаем его мы[712].[713] Отсюда, на мой взгляд, следует вывод, противоположный тому, что из фразы сделали позже. Раз код пишут люди, спрашивать надо о людях: кто пишет, в чьих интересах и кто может поменять. В журнальной статье 2000 года Лессиг назвал код архитектурой, которая задаёт условия жизни в сети, например насколько легко в ней защитить частную жизнь или запретить чьи-то высказывания[714]. Для смарт-контракта такая архитектура — это, среди прочего, ответ на вопрос, есть ли у него хозяин, способный его остановить.

Второе прочтение принадлежит Ethereum Classic. На сайте сообщества «код — это закон» объявлен принципом: код смарт-контракта — окончательный судья того, чем кончилось взаимодействие в сети, и никакая сила извне не вправе его отменить[715].[716] По версии сообщества, той же философии держался и Ethereum, пока не случилась The DAO[717]. Лессиг предупреждал, что код решает за людей, а сообщество Ethereum Classic этого требует.

Третье прочтение дало государство. 25 июля 2017 года SEC опубликовала отчёт о расследовании, где признала токены The DAO ценными бумагами по законам США, но дела против их выпускающих возбуждать не стала[718]. В том же отчёте сказано, что автоматизация с помощью «смарт-контрактов» или кода не выводит поведение участников из-под действия законов

---

[707] ethereum.org, «Proof-of-stake attack and defense», https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/attack-and-defense/.

[708] Lawrence Lessig, «Code and Other Laws of Cyberspace», Basic Books, 1999, гл. 1 «Code Is Law», с. 6 (PDF с сайта автора: https://lessig.org/images/resources/1999-Code.pdf).

[709] Lawrence Lessig, «Code and Other Laws of Cyberspace», Basic Books, 1999, гл. 1 «Code Is Law», с. 6 (PDF с сайта автора: https://lessig.org/images/resources/1999-Code.pdf).

[710] Lessig L. Code and Other Laws of Cyberspace. Basic Books, 1999, ch. 1 «Code Is Law», p. 6: «In cyberspace we must understand how code regulates—how the software and hardware that make cyberspace what it is regulate cyberspace as it is. As William Mitchell puts it, this code is cyberspace's „law." Code is law.»

[711] Lessig, «Code and Other Laws of Cyberspace», 1999, с. 6.

[712] Lessig, «Code and Other Laws of Cyberspace», 1999, с. 6.

[713] Там же: «Code is never found; it is only ever made, and only ever made by us.» Ту же мысль Лессиг изложил в Harvard Magazine (январь — февраль 2000 года): «This code, or architecture, sets the terms on which life in cyberspace is experienced.»

[714] Lawrence Lessig, статья в Harvard Magazine, январь–февраль 2000 (URL-слаг «code-is-law»), https://www.harvardmagazine.com/2000/01/code-is-law-html.

[715] ethereumclassic.org, «Code is Law», https://ethereumclassic.org/why-classic/code-is-law.

[716] ethereumclassic.org, Code is Law: «It means that the code of a Smart Contract is the ultimate arbiter of the outcome of an on-chain interaction, as opposed to some overriding force from outside the network.»

[717] ethereumclassic.org, «Code is Law», https://ethereumclassic.org/why-classic/code-is-law.

[718] SEC, Report of Investigation… The DAO, Release No. 81207, 25.07.2017, с. 1, https://www.sec.gov/files/litigation/investreport/34-81207.pdf; пресс-релиз 2017-131, https://www.sec.gov/newsroom/press-releases/2017-131 (перенос https://www.sec.gov/newsroom/press-releases/2017-131, отчёт перепроверен).

о ценных бумагах[719].[720] Иными словами, автомат может исполнять себя сам, но те, кто через него продаёт ценные бумаги, остаются под тем же законом, что и без автомата.

Суды тоже вынуждены подгонять старые понятия под автоматы. В ноябре 2024 года апелляционный суд в США решил, что неизменяемые контракты сервиса Tornado Cash нельзя считать чьей-то собственностью в смысле закона о санкциях, а значит, их нельзя было включать в санкционный список, и в марте 2025 года Минфин США их из списка исключил[721].[722] Суд увидел в контракте без хозяина скорее инструмент, чем чьё-то имущество (к этому делу и к тому, как государства отвечают на крипту, мы вернёмся в главе 11).

Какое из прочтений верно? Я думаю, что история The DAO подтвердила первое. На каждом её шаге за кодом стояли люди: авторы контракта, кураторы, аудиторы, исследователи, которые предупреждали, разработчики фонда, держатели монет, майнеры, регулятор. Код исполнил себя в точности, а всё, что произошло потом, решали они.

Если вы встретите эту фразу в описании какого-нибудь проекта, полезно спросить, в каком из трёх смыслов её употребляют. Если в смысле Ethereum Classic, проект обещает, что при ошибке никто не вмешается, а значит, и помочь вам тогда будет некому. Если же при первой серьёзной ошибке люди всё-таки вмешаются, фраза была рекламой, и лучше заранее знать, кто эти люди и чем они будут руководствоваться.

Автомат не видит улицы

Вернёмся к колодцу. Автомат знает, какие взносы пришли и какое сегодня число по тетрадке, но выкопан ли колодец, он не знает. Всё, что происходит за пределами тетрадки, для контракта не существует, пока кто-то не внесёт это в тетрадку.

Почему контракт не может сам посмотреть, скажем, курс валюты на каком-нибудь сайте? Потому что все узлы обязаны получить одинаковый результат. Если бы каждый узел ходил за данными в интернет сам, узлы получали бы разные ответы (сайт обновился, ответил с задержкой, был недоступен), и договориться о новом состоянии тетрадки они бы не смогли[723].[724] Поэтому внешние данные в контракт приносят оракулы, отдельные приложения, которые доставляют в блокчейн сведения извне, например цены или результаты выборов[725]. Документация Ethereum приводит два примера: рынку ставок нужен итог президентских выборов, а кредитному сервису — текущая цена залога[726]. В обоих случаях автомат платит деньги по сведениям, которые не может проверить сам. Если итог выборов в контракт вносит один оракул, то победителей ставки на деле определяет тот, кто этим оракулом управляет.

У такого решения есть цена, и документация называет её сама. Контракт исполнится правильно, только если данные оракула верны, а необходимость доверять тому, кто ведёт оракул,

---

[719] SEC, отчёт о The DAO, 2017, с. 2.

[720] SEC, отчёт о The DAO, с. 1: «…the Commission has determined that DAO Tokens are securities under the Securities Act of 1933…»; с. 2: «The automation of certain functions through this technology, „smart contracts," or computer code, does not remove conduct from the purview of the U.S. federal securities laws.»

[721] Van Loon v. Department of the Treasury, No. 23-50669 (5th Cir., 26.11.2024), https://law.justia.com/cases/federal/appellate-courts/ca5/23-50669/23-50669-2024-11-26.html; U.S. Treasury, «Tornado Cash Delisting», 2025, https://home.treasury.gov/news/press-releases/sb0057 (перенос из 00-landscape-stories.md, не перепроверялся).

[722] Van Loon v. Department of the Treasury, No. 23-50669 (5th Cir., 26.11.2024): неизменяемые смарт-контракты Tornado Cash нельзя считать «собственностью» по закону IEEPA; исключение из санкционного списка — сообщение Минфина США, март 2025 года.

[723] ethereum.org, «Oracles», https://ethereum.org/developers/docs/oracles/.

[724] ethereum.org, Oracles: «…if blockchains received information from external sources (i.e., from the real world), determinism would be impossible to achieve, preventing nodes from agreeing on the validity of changes to the blockchain's state.»

[725] ethereum.org, «Oracles», https://ethereum.org/developers/docs/oracles/.

[726] ethereum.org, «Oracles», https://ethereum.org/developers/docs/oracles/.

подрывает главное обещание смарт-контрактов, работу без доверия[727].[728] Хранитель, которого изгнали из тетрадки, возвращается через вход для данных. Контракт может быть написан без единой ошибки и всё равно исполнить неправильное решение, если ему сообщили неправильную цену. Поэтому надёжность сервиса, который выдаёт займы под залог, зависит от оракула не меньше, чем от кода, и о таком сервисе прежде всего стоит знать, откуда он берёт цены и что будет, если их подделают.

Посмотрим, как это выглядит в посёлке (пример условный). Автомат выдаёт муку в долг под залог строчек, которые пекарь выпустил на свои будущие караваи, и цену этих строчек ему каждое утро приносит гонец, который смотрит, почём их продают на трёх лотках рынка. Кто-то с утра скупает эти строчки на всех трёх лотках, цена за полчаса вырастает в десять раз, и гонец честно приносит автомату новую цену. Автомат видит, что залог у этого двора подорожал вдесятеро, и по своим правилам выдаёт ему вдесятеро больше муки. Гонец и автомат сделали ровно то, что должны, а неверной оказалась цена, которую оба приняли на веру.

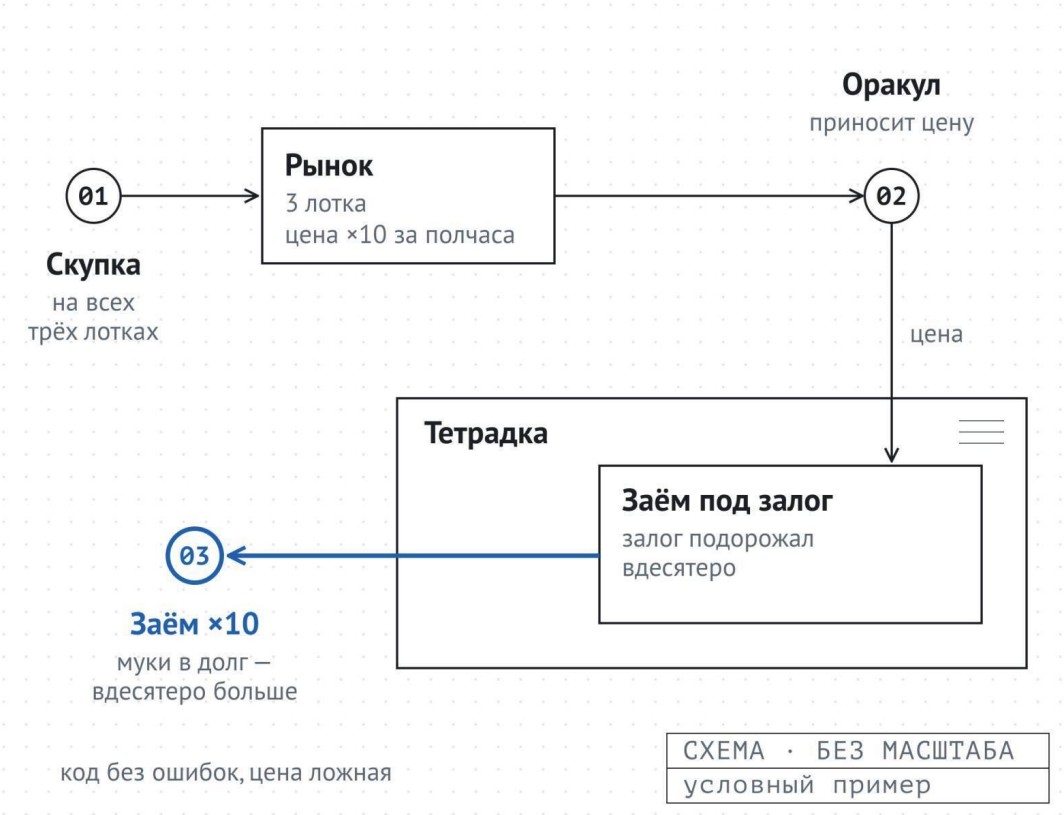


Рисунок 4.4. Оракул

Похожая история, по версии Комиссии по торговле товарными фьючерсами США (CFTC), случилась 11 октября 2022 года на бирже Mango Markets. Трейдер, которому CFTC предъявила обвинение, скупил крупные объёмы токена MNGO на трёх биржах, с которых оракул Mango брал цену. По данным оракула, цена MNGO выросла больше чем в 13 раз за 30 минут, после чего он занял у биржи под раздутую стоимость своей позиции и вывел больше

[727] ethereum.org, «Oracles», https://ethereum.org/developers/docs/oracles/.

[728] Там же: «Data from an oracle must be correct for a smart contract to execute correctly. Further, having to „trust“ oracle operators to provide accurate information undermines the „trustless“ aspect of smart contracts.»

110 млн долларов[729].[730] По данным CFTC, позже он вернул около 67 млн долларов, а остальное оставил себе[731].

Код Mango при этом, насколько известно, сработал без ошибок. Он поверил цене, которую ему сообщили, и выдал заём по своим правилам. Судьба дела показывает, насколько трудно решить, кто здесь нарушил закон. В апреле 2024 года присяжные в Нью-Йорке признали трейдера виновным в мошенничестве и манипулировании рынком[732]. В мае 2025 года судья отменил все три вердикта, но по разным причинам[733]. Два обвинения по товарному законодательству он снял из-за подсудности: сделки совершались из Пуэрто-Рико, и обвинение не доказало, что дело относится к нью-йоркскому суду. При этом в решении сказано, что доказательств манипулирования ценой в деле в избытке. По третьему обвинению, в мошенничестве с использованием электронных средств связи, судья вынес оправдательное решение. У Mango Markets не было никаких правил, инструкций или запретов о займах, и обвинение не доказало, что трейдер обманул платформу ложным заявлением[734].[735]

Это похоже на «код — это закон» в устах суда, но относится только к обвинению в мошенничестве: судья решал, был ли обман, а манипулирование ценой в том же решении описано как подтверждённое материалами дела[736]. Прокуратура обжаловала и отмену обвинений по

---

[729] CFTC, «CFTC Charges Avraham Eisenberg with Manipulative and Deceptive Scheme to Misappropriate Over $110 million from Mango Markets, a Digital Asset Exchange», пресс-релиз 8647-23, 09.01.2023, https://www.cftc.gov/PressRoom/PressReleases/8647-23.

[730] CFTC, пресс-релиз 8647-23, 09.01.2023: «…the price of MNGO as reported by the oracle, jumped over 13-fold during a 30-minute span…» Это изложение позиции обвинения в гражданском деле; его исход в этой книге не проверялся. По данным CFTC, трейдер вернул около 67 млн долларов и оставил себе около 47 млн (CFTC, пресс-релиз 8647-23, 09.01.2023).

[731] CFTC, пресс-релиз 8647-23, 09.01.2023.

[732] Venable LLP, «Venue Fatal in Crypto Fraud Case…», 06.2025, https://www.venable.com/insights/publications/2025/06/venue-fatal-in-crypto-fraud-case-an-important; TRM Labs, «Federal Judge Overturns All Criminal Convictions in Mango Markets Case…», 05.2025, https://www.trmlabs.com/resources/blog/breaking-federal-judge-overturns-all-criminal-convictions-in-mango-markets-case-against-avraham-eisenberg; дата вердикта — Bloomberg и Axios, 18.04.2024 (заголовки в выдаче, не открыты).

[733] Opinion and Order, дело 23-cr-10 (AS), Окружной суд США по Южному округу Нью-Йорка, 23.05.2025, https://nysd.uscourts.gov/sites/default/files/2025-05/23cr10%20Opinion%20and%20Order.pdf (с. 1–3, 24–27, 32–35 прочитаны фактчекером 27.09.2026); Venable LLP, 06.2025; CoinDesk, «Judge Overturns Convictions in Mango Markets Exploiter's Crypto Fraud Case», 24.05.2025, https://www.coindesk.com/business/2025/05/24/judge-overturns-convictions-in-mango-markets-exploiters-crypto-fraud-case; DL News, 07.01.2026 (разделяет два решения: «vacate… commodities fraud conviction and acquit him of wire fraud»).

[734] Opinion and Order, дело 23-cr-10 (AS), Окружной суд США по Южному округу Нью-Йорка, 23.05.2025, https://nysd.uscourts.gov/sites/default/files/2025-05/23cr10%20Opinion%20and%20Order.pdf (с. 1–3, 24–27, 32–35 прочитаны фактчекером 27.09.2026); Venable LLP, 06.2025; CoinDesk, «Judge Overturns Convictions in Mango Markets Exploiter's Crypto Fraud Case», 24.05.2025, https://www.coindesk.com/business/2025/05/24/judge-overturns-convictions-in-mango-markets-exploiters-crypto-fraud-case; DL News, 07.01.2026 (разделяет два решения: «vacate… commodities fraud conviction and acquit him of wire fraud»).

[735] Opinion and Order, дело 23-cr-10 (AS), Окружной суд США по Южному округу Нью-Йорка, 23.05.2025 (правило 29 федеральных правил уголовного процесса), с. 1: «The Court vacates counts one and two and will enter a judgment of acquittal on count three»; с. 32: «On a platform with no rules, instructions, or prohibitions about borrowing, the government needed more to show that [the defendant] made an implicit misrepresentation»; с. 24: доказательств того, что подсудимый «intended to and did manipulate» цену, в деле «в избытке» («the trial record was replete with evidence»). Вердикт присяжных — 18.04.2024: мошенничество с товарами, манипулирование товарным рынком, мошенничество с использованием электронных средств связи (Venable LLP, «Venue Fatal in Crypto Fraud Case…», 06.2025, https://www.venable.com/insights/publications/2025/06/venue-fatal-in-crypto-fraud-case-an-important; TRM Labs, «Federal Judge Overturns All Criminal Convictions in Mango Markets Case…», 05.2025, https://www.trmlabs.com/resources/blog/breaking-federal-judge-overturns-all-criminal-convictions-in-mango-markets-case-against-avraham-eisenberg; дата вердикта — Bloomberg и Axios, 18.04.2024 (заголовки в выдаче, не открыты)).

[736] Opinion and Order, дело 23-cr-10 (AS), Окружной суд США по Южному округу Нью-Йорка, 23.05.2025, https://nysd.uscourts.gov/sites/default/files/2025-05/23cr10%20Opinion%20and%20Order.pdf (с. 1–3, 24–27, 32–35 прочитаны фактчекером 27.09.2026); Venable LLP, 06.2025; CoinDesk, «Judge Overturns Convictions in Mango Markets Exploiter's Crypto Fraud Case», 24.05.2025, https://www.coindesk.com/business/2025/05/24/judge-overturns-convictions-in-mango-markets-exploiters-crypto-fraud-case; DL News, 07.01.2026 (разделяет два решения: «vacate… commodities fraud conviction and acquit him of wire fraud»).

товарному законодательству, и оправдание, настаивая, что само слово «занять» подразумевает намерение вернуть. На момент работы над книгой апелляция, по доступным данным, не рассмотрена[737].[738] Спор открыт, и где он окажется, когда вы будете читать эти строки, смотрите в приложении Б.

Кто решает, когда правила меняются

После 2016 года вопрос вставал ещё не раз: в аварию, где форка так и не случилось, во взломах, где деньги вернул сам взломщик, и планово, в биткоине.

Аварию устроили кошельки Parity. Среди кошельков-контрактов Ethereum были кошельки Parity с несколькими подписями, то есть такие, которые отдают деньги, только когда перевод подписали несколько владельцев. В июле 2017 года из трёх крупных кошельков этого типа, где лежали деньги с прошлых продаж токенов, украли около 150 тыс. ETH[739].[740] Функция, которая назначает кошельку владельцев, оказалась доступна любому, и атакующий просто назначил владельцем себя[741].

Вторая история вышла страннее. Кошельки Parity опирались на общую библиотеку, то есть на отдельный контракт с кодом, к которому все они обращались[742]. 6 ноября 2017 года пользователь GitHub открыл в хранилище кода Parity запись с заголовком «любой может убить ваш контракт» и текстом «Я случайно убил его»[743].[744] Он сделал себя владельцем библиотеки и вызвал её самоуничтожение[745]. Была ли это случайность, не установлено, и я могу сказать только, что так утверждал он сам[746].

Чтобы не переписывать в каждый автомат одни и те же длинные инструкции, их можно держать в одной общей книге, и каждый автомат, когда к нему обращаются, будет открывать книгу и делать, что там написано. Книга тоже записана в тетрадку и тоже автомат. У Parity в ней была инструкция «уничтожить себя», исполнить которую мог хозяин книги, а назначить

---

[737] DL News, «Prosecutors appeal acquittal of Mango Markets exploiter Avraham Eisenberg», 07.01.2026, https://www.dlnews.com/articles/defi/prosecutors-appeal-acquittal-of-mango-markets-exploiter/.

[738] Доводы прокуратуры поданы 22.12.2025; цитата по DL News, 07.01.2026: «The plain meaning of the word „borrow“ itself conveys an intent to repay, typically with interest». По DL News, прокуратура обжалует и отмену обвинений по товарному законодательству, и оправдание по обвинению в мошенничестве с использованием электронных средств связи. Статус апелляции на дату сдачи рукописи — см. приложение Б.

[739] Santiago Palladino (OpenZeppelin), «On the Parity Wallet Multisig Hack», 19.07.2017, https://www.openzeppelin.com/news/on-the-parity-wallet-multisig-hack-405a8c12e8f7; сумма в долларах — Mastering Ethereum, гл. «Smart Contract Security», https://cypherpunks-core.github.io/ethereumbook/09smart-contracts-security.html.

[740] Palladino S. (OpenZeppelin). On the Parity Wallet Multisig Hack, 19.07.2017: 153 037 ETH, около 31 млн долларов по тогдашнему курсу (сумма в долларах — по «Mastering Ethereum»). Уязвимой была функция инициализации кошелька initWallet (Santiago Palladino (OpenZeppelin), «On the Parity Wallet Multisig Hack», 19.07.2017, https://www.openzeppelin.com/news/on-the-parity-wallet-multisig-hack-405a8c12e8f7; сумма в долларах — Mastering Ethereum, гл. «Smart Contract Security», https://cypherpunks-core.github.io/ethereumbook/09smart-contracts-security.html).

[741] Santiago Palladino (OpenZeppelin), «On the Parity Wallet Multisig Hack», 19.07.2017, https://www.openzeppelin.com/news/on-the-parity-wallet-multisig-hack-405a8c12e8f7; сумма в долларах — Mastering Ethereum, гл. «Smart Contract Security», https://cypherpunks-core.github.io/ethereumbook/09smart-contracts-security.html.

[742] Santiago Palladino (OpenZeppelin), «The Parity Wallet Hack Reloaded», 07.11.2017, https://www.openzeppelin.com/news/parity-wallet-hack-reloaded.

[743] GitHub, openethereum/parity-ethereum, issue #6995, 06.11.2017, https://github.com/openethereum/parity-ethereum/issues/6995; механизм — Mastering Ethereum, гл. «Smart Contract Security».

[744] GitHub, openethereum/parity-ethereum, issue #6995, 06.11.2017: заголовок «anyone can kill your contract», текст «I accidentally killed it.» Аккаунт автора позже удалён.

[745] GitHub, openethereum/parity-ethereum, issue #6995, 06.11.2017, https://github.com/openethereum/parity-ethereum/issues/6995; механизм — Mastering Ethereum, гл. «Smart Contract Security».

[746] GitHub, openethereum/parity-ethereum, issue #6995, 06.11.2017, https://github.com/openethereum/parity-ethereum/issues/6995; механизм — Mastering Ethereum, гл. «Smart Contract Security».

себя хозяином, как выяснилось, мог любой[747]. Однажды кто-то сделал и то и другое. Автоматы продолжали открывать книгу, но открывать стало нечего.

Все кошельки, которые зависели от библиотеки, мгновенно замёрзли. Они продолжали отправлять вызовы на адрес, где больше не было кода[748]. По оценке компании OpenZeppelin на следующий день, заморожено могло быть больше 500 000 ETH, и крупнейшая доля принадлежала команде Web3 Foundation[749].[750] Parity в своём разборе признала, что без функции самоуничтожения в коде библиотеки захват владения ничего бы не дал[751].[752] Одна сломанная деталь остановила все механизмы, в которые её встроили. Особые права владельца работают в обе стороны: владелец может спасти деньги при ошибке, а может их заморозить или забрать, и оба раза у Parity беда пришла через права, которые код отдал не тому.

Отсюда ответ на второй и третий из пяти вопросов первой главы, если задать их контрактам. Дописать строчку в контракт может любой, кого код к этому допускает, и порой это не тот, кого имели в виду авторы. Стереть или заморозить чужую строчку по своему желанию одиночка не может, если код не даёт ему особых прав, но ошибка в чужом коде может заморозить её навсегда, а большинство по общему согласию может её переложить, как в 2016 году.

Для Parity такое согласие попробовали собрать. В апреле 2018 года разработчик Parity внёс предложение EIP-999 (EIP — так в Ethereum нумеруют предложения по улучшению)[753]. Он предлагал одним изменением состояния заново записать по адресу уничтоженной библиотеки её исправленный код, уже без функции самоуничтожения, и отдельно подчёркивал, что никакой эфир при этом никуда не переходит[754].[755] По сравнению с 2016 годом, когда эфир The DAO переложили на контракт возврата[756], вмешательство было мягче.

---

[747] GitHub, openethereum/parity-ethereum, issue #6995, 06.11.2017, https://github.com/openethereum/parity-ethereum/issues/6995; механизм — Mastering Ethereum, гл. «Smart Contract Security»; Coin Bureau, «Parity issues a Post Mortem on the Kill that Froze Millions», 11.2017, https://coinbureau.com/news/parity-issues-post-mortem-kill-froze-millions/ (пересказ поста Parity).

[748] Santiago Palladino (OpenZeppelin), «The Parity Wallet Hack Reloaded», 07.11.2017, https://www.openzeppelin.com/news/parity-wallet-hack-reloaded.

[749] Santiago Palladino (OpenZeppelin), «The Parity Wallet Hack Reloaded», 07.11.2017, https://www.openzeppelin.com/news/parity-wallet-hack-reloaded.

[750] Palladino S. (OpenZeppelin). The Parity Wallet Hack Reloaded, 07.11.2017: «Estimated losses may total over 500,000 ETH ($150 million USD), including over 300,000 ETH from the Web3 Foundation team.» В разборе самой Parity, по пересказу, называлась сумма около 514 тыс. ETH (Coin Bureau, «Parity issues a Post Mortem on the Kill that Froze Millions», 11.2017, https://coinbureau.com/news/parity-issues-post-mortem-kill-froze-millions/ (пересказ поста Parity)).

[751] Coin Bureau, «Parity issues a Post Mortem on the Kill that Froze Millions», 11.2017, https://coinbureau.com/news/parity-issues-post-mortem-kill-froze-millions/ (пересказ поста Parity).

[752] Разбор Parity, ноябрь 2017 года, по пересказу Coin Bureau (сам пост удалён): «If the contract code had not included the functionality to suicide or kill, even if someone had taken ownership, they would not have been able to do anything.»

[753] EIP-999, «Restore Contract Code at 0x863DF6BFa4469f3ead0bE8f9F2AAE51c91A907b4», автор Afri Schoedon, создан 04.04.2018, статус Withdrawn, https://eips.ethereum.org/EIPS/eip-999.

[754] Afri Schoedon, EIP-999 «Restore Contract Code at 0x863DF6BFa4469f3ead0bE8f9F2AAE51c91A907b4», создан 04.04.2018, https://eips.ethereum.org/EIPS/eip-999; исходник — https://github.com/ethereum/EIPs/blob/master/EIPS/eip-999.md.

[755] EIP-999, «Restore Contract Code at 0x863DF6BFa4469f3ead0bE8f9F2AAE51c91A907b4», создан 04.04.2018, статус Withdrawn: «This proposal is necessary because the Ethereum protocol does not allow the restoration of self-destructed contracts and there is no other simple way to enable the affected users and companies regaining access to their tokens and Ether.» Оговорка редактора EIP при приёме черновика (16.04.2018): «Merging as a draft does not imply approval» (GitHub, ethereum/EIPs, Pull Request #999, https://github.com/ethereum/EIPs/pull/999; история файла — https://github.com/ethereum/EIPs/commits/master/EIPS/eip-999.md (коммит e30becf, 16.04.2018)). Голосование монетами на обозревателе блоков Etherchain, 17–24.04.2018: по Cointelegraph, 55% «против», 39,4% «за»; в других изданиях — 52,6% «против» (промежуточный срез) и 330 голосов против 300 (по числу адресов) (Cointelegraph, «#EIP-999: Why A Vote To Release Parity Locked Funds Evoked So Much Controversy», 03.05.2018, https://cointelegraph.com/news/eip-999-why-a-vote-to-release-parity-locked-funds-evoked-so-much-controversy; платформа Etherchain и взвешивание по балансу — Brave New Coin (Kieran Smith), 27.04.2018, https://bravenewcoin.com/insights/parity-tech-has-no-intention-of-splitting-ethereum-over-513000-stranded-eth; CCN, «$330 Million: EIP-999 Stokes Debate Over ETH Frozen by Parity's Contract Bug», 23.04.2018, зеркало Yahoo Finance https://finance.yahoo.com/news/330-million-eip-999-stokes-194329494.html; Colin Harper, «The Evolving Debate Over EIP-999: Can (or Should) Trapped Ether Be Freed?», Bitcoin Magazine, 02.05.2018, https://bitcoinmagazine.com/business/evolving-debate-over-eip-999-can-or-should-trapped-ether-be-freed (зеркало Yahoo: https://finance.yahoo.com/news/evolving-debate-over-eip-999-164500215.html); Cointelegraph, 03.05.2018).

Его так и не приняли. Черновик внесли в общий список предложений с оговоркой редактора, что это не означает ни одобрения, ни включения в хардфорк[757]. В апреле прошло неофициальное голосование монетами, и против оказалось небольшое большинство (подсчёты разных изданий расходятся, но во всех «против» впереди)[758]. Процедуру упрекали в том же, в чём carbonvote, и ещё в одном: владельцы замороженных кошельков могли голосовать эфиром, лежавшим в этих самых кошельках[759]. Бутерин сказал, что принимать это решение или даже сильно на него влиять — не его дело[760]. В 2020 году автор отозвал предложение, объяснив, что больше в нём не заинтересован[761], и средства так и остались замороженными[762].[763]

Почему The DAO вернули, а Parity нет, если технически второе было проще? Одной причины источники не называют, но картина из них складывается. В 2016 году форк продвигал фонд Ethereum, чьи разработчики написали код, назначили блок и выпустили программу, в которой держатели и майнеры могли его включить[764]. В 2018 году продвигать форк было некому. Предложение исходило от Parity, компании, которая сама выпускала одну из программ узла Ethereum, а среди пострадавших был проект основателя самой Parity[765]. Форк вернул бы деньги в том числе её собственному кругу, и после голосования компания публично заявила,

---

Parity, по Brave New Coin: «we have no intention to split the Ethereum chain» (Parity Technologies, блог «Our Commitment to Ethereum and a Decentralised Future», апрель 2018 — цитата по Brave New Coin, 27.04.2018, https://bravenewcoin.com/insights/parity-tech-has-no-intention-of-splitting-ethereum-over-513000-stranded-eth; то же по Bitcoin Magazine, 02.05.2018). Бутерин, по CoinDesk (19.07.2018): «I do not think it is my place to make that decision or even heavily influence it» (Rachel-Rose O'Leary, «Ethereum's Most Heated Tech Debate Is Proving It's Far From Over», CoinDesk, 19.07.2018, https://www.coindesk.com/markets/2018/07/19/ethereums-most-heated-tech-debate-is-proving-its-far-from-over). Попытка перевести предложение в статус «принято» в июле 2018 года закрыта по просьбе автора (GitHub, ethereum/EIPs, Pull Request #1221 «Update EIP-999 status», 15.07.2018, https://github.com/ethereum/EIPs/pull/1221; контекст — CoinDesk, 19.07.2018); формальный отзыв — 27.01.2020: «I'm no longer interested in restoring the contract code…» (GitHub, ethereum/EIPs, Pull Request #2441 «Withdraw EIP-999», https://github.com/ethereum/EIPs/pull/2441; коммит 75e354b, 27.01.2020, https://github.com/ethereum/EIPs/commits/master/EIPS/eip-999.md).

[756] Vitalik Buterin, «Hard Fork Completed», Ethereum Foundation Blog, 20.07.2016, https://blog.ethereum.org/2016/07/20/hard-fork-completed.

[757] GitHub, ethereum/EIPs, Pull Request #999, https://github.com/ethereum/EIPs/pull/999; история файла — https://github.com/ethereum/EIPs/commits/master/EIPS/eip-999.md (коммит e30becf, 16.04.2018).

[758] Cointelegraph, «#EIP-999: Why A Vote To Release Parity Locked Funds Evoked So Much Controversy», 03.05.2018, https://cointelegraph.com/news/eip-999-why-a-vote-to-release-parity-locked-funds-evoked-so-much-controversy; платформа Etherchain и взвешивание по балансу — Brave New Coin (Kieran Smith), 27.04.2018, https://bravenewcoin.com/insights/parity-tech-has-no-intention-of-splitting-ethereum-over-513000-stranded-eth; CCN, «$330 Million: EIP-999 Stokes Debate Over ETH Frozen by Parity's Contract Bug», 23.04.2018, зеркало Yahoo Finance https://finance.yahoo.com/news/330-million-eip-999-stokes-194329494.html; Colin Harper, «The Evolving Debate Over EIP-999: Can (or Should) Trapped Ether Be Freed?», Bitcoin Magazine, 02.05.2018, https://bitcoinmagazine.com/business/evolving-debate-over-eip-999-can-or-should-trapped-ether-be-freed (зеркало Yahoo: https://finance.yahoo.com/news/evolving-debate-over-eip-999-164500215.html); Cointelegraph, 03.05.2018.

[759] CCN, 23.04.2018; Brave New Coin, 27.04.2018; Cointelegraph, 03.05.2018.

[760] Rachel-Rose O'Leary, «Ethereum's Most Heated Tech Debate Is Proving It's Far From Over», CoinDesk, 19.07.2018, https://www.coindesk.com/markets/2018/07/19/ethereums-most-heated-tech-debate-is-proving-its-far-from-over.

[761] GitHub, ethereum/EIPs, Pull Request #2441 «Withdraw EIP-999», https://github.com/ethereum/EIPs/pull/2441; коммит 75e354b, 27.01.2020, https://github.com/ethereum/EIPs/commits/master/EIPS/eip-999.md.

[762] The Daily Hodl, «$3,430,000,000 in Ethereum (ETH) 'Lost Forever'…», 28.07.2025, https://dailyhodl.com/2025/07/28/3430000000-in-ethereum-eth-lost-forever-due-to-this-reason-according-to-coinbase-director/ (пересказ поста Грогана в X).

[763] Подсчёт Конора Грогана (Coinbase), июль 2025 года, в пересказе The Daily Hodl, 28.07.2025: всего не меньше 913 111 ETH, около 0,76% всего эфира, заблокированы навсегда из-за ошибок пользователей и контрактов, и крупнейшая позиция — кошелёк Parity фонда Web3 Foundation. Сам Гроган оговаривает, что это заниженная оценка. Состояние кошелька на дату сдачи — см. приложение Б.

[764] Jeffrey Wilcke, «To fork or not to fork», Ethereum Foundation Blog, 15.07.2016, https://blog.ethereum.org/2016/07/15/to-fork-or-not-to-fork.

[765] CCN, 23.04.2018; Brave New Coin, 27.04.2018; Cointelegraph, 03.05.2018; Parity Technologies, блог «Our Commitment to Ethereum and a Decentralised Future», апрель 2018 — цитата по Brave New Coin, 27.04.2018, https://bravenewcoin.com/insights/parity-tech-has-no-intention-of-splitting-ethereum-over-513000-stranded-eth; то же по Bitcoin Magazine, 02.05.2018.

что не намерена раскалывать цепочку Ethereum[766]. Некоторые разработчики Ethereum к тому же предупреждали, что такой форк почти наверняка снова расколет сеть[767]. На мой взгляд, решило то, что за предложением не нашлось никого, кто мог бы провести его без раскола, а мягкость самого вмешательства значила меньше.

Единого правила, когда тетрадку можно поправить, эти два случая не дают. Каждый раз решали по случаю, и решали люди.

Два более поздних взлома подошли к тому же с другой стороны. В 2021 году из Poly Network, сервиса для переводов между разными блокчейнами, вывели больше 610 млн долларов, после того как взломщик записал свой ключ вместо доверенных ключей, которые подтверждали переводы[768]. В 2023 году из кредитного сервиса Euler Finance ушло около 197 млн долларов, хотя его код, по словам сооснователя, проверяли больше, чем принято в отрасли[769]. Правил сети никто не менял, и код вернуть деньги не мог. Почти всё вернули сами взломщики: первый — за полмесяца, после того как Poly Network назвала его «мистером белым хакером» и предложила вознаграждение, второй — после переговоров[770].[771][772] Исход снова решали люди, только на этот раз главным из них был тот, кто взял деньги.

В биткоине правила меняют иначе, но решают и там люди.

---

[766] Parity Technologies, блог «Our Commitment to Ethereum and a Decentralised Future», апрель 2018 — цитата по Brave New Coin, 27.04.2018, https://bravenewcoin.com/insights/parity-tech-has-no-intention-of-splitting-ethereum-over-513000-stranded-eth; то же по Bitcoin Magazine, 02.05.2018.

[767] Colin Harper, Bitcoin Magazine, 02.05.2018.

[768] Wikipedia, «Poly Network exploit» (со ссылками на Reuters, BBC, CNBC, Chainalysis), https://en.wikipedia.org/wiki/Poly_Network_exploit; CNBC, «Poly Network hacker returns remaining cryptocurrency», 23.08.2021, https://www.cnbc.com/2021/08/23/poly-network-hacker-returns-remaining-cryptocurrency.html; Kudelski Security Research, «The Poly Network Hack Explained», 12.08.2021, https://kudelskisecurity.com/research/the-poly-network-hack-explained.

[769] Euler Finance, «War & Peace: Behind the Scenes of Euler's $240M Exploit Recovery», январь 2024, https://www.euler.finance/blog/war-peace-behind-the-scenes-of-eulers-240m-exploit-recovery; Chainalysis, «Euler Finance Flash Loan Attack Explained», 15.03.2023, https://www.chainalysis.com/blog/euler-finance-flash-loan-attack/; Euler Finance, «War & Peace…», январь 2024.

[770] Wikipedia, «Poly Network exploit» (со ссылками на Reuters, BBC, CNBC, Chainalysis), https://en.wikipedia.org/wiki/Poly_Network_exploit; CNBC, «Poly Network hacker returns remaining cryptocurrency», 23.08.2021, https://www.cnbc.com/2021/08/23/poly-network-hacker-returns-remaining-cryptocurrency.html; Decrypt, «Euler Finance Exploiter Returns All 'Recoverable Funds' From $200M Hack», 03.2023, https://decrypt.co/125373/euler-finance-exploiter-returns-recoverable-funds-200m-hack (по выдаче, не открыт); Euler Finance, «War & Peace…», январь 2024.

[771] Хронология — по статье Wikipedia «Poly Network exploit» со ссылками на Reuters, BBC и CNBC; первичные заявления компании не сверялись. Средства возвращены за 15 дней; ещё около 33 млн долларов в токене USDT сразу после взлома заморозил его эмитент, Tether, так что их атакующий не возвращал (Wikipedia, «Poly Network exploit» (со ссылками на Reuters, BBC, CNBC, Chainalysis), https://en.wikipedia.org/wiki/Poly_Network_exploit; CNBC, «Poly Network hacker returns remaining cryptocurrency», 23.08.2021, https://www.cnbc.com/2021/08/23/poly-network-hacker-returns-remaining-cryptocurrency.html). Poly Network предлагала ему и должность главного советника по безопасности; специалисты по безопасности ярлык «белого хакера» критиковали (Wikipedia, «Poly Network exploit» (со ссылками на Reuters, BBC, CNBC, Chainalysis), https://en.wikipedia.org/wiki/Poly_Network_exploit; CNBC, «Poly Network hacker returns remaining cryptocurrency», 23.08.2021, https://www.cnbc.com/2021/08/23/poly-network-hacker-returns-remaining-cryptocurrency.html). По разбору Kudelski Security (12.08.2021), атакующий подобрал имя функции так, чтобы её короткий идентификатор совпал с идентификатором служебной функции смены доверенных ключей (keepers); контракт-менеджер, который был владельцем контракта с данными, выполнил вызов, и атакующий записал вместо доверенных ключей свой (Kudelski Security Research, «The Poly Network Hack Explained», 12.08.2021, https://kudelskisecurity.com/research/the-poly-network-hack-explained). Предложенное вознаграждение — 500 000 долларов (Wikipedia, «Poly Network exploit» (со ссылками на Reuters, BBC, CNBC, Chainalysis), https://en.wikipedia.org/wiki/Poly_Network_exploit; CNBC, «Poly Network hacker returns remaining cryptocurrency», 23.08.2021, https://www.cnbc.com/2021/08/23/poly-network-hacker-returns-remaining-cryptocurrency.html).

[772] Euler Finance. War & Peace: Behind the Scenes of Euler's $240M Exploit Recovery, январь 2024; Chainalysis, 15.03.2023. Уязвимой была функция donateToReserves (Euler Finance, «War & Peace: Behind the Scenes of Euler's $240M Exploit Recovery», январь 2024, https://www.euler.finance/blog/war-peace-behind-the-scenes-of-eulers-240m-exploit-recovery; Chainalysis, «Euler Finance Flash Loan Attack Explained», 15.03.2023, https://www.chainalysis.com/blog/euler-finance-flash-loan-attack/). По подсчёту самого Euler, к 3 апреля 2023 года вернулось всё похищенное — около 240 млн долларов с учётом подорожания эфира; по данным Decrypt на конец марта — больше 177 млн долларов (Decrypt, «Euler Finance Exploiter Returns All 'Recoverable Funds' From $200M Hack», 03.2023, https://decrypt.co/125373/euler-finance-exploiter-returns-recoverable-funds-200m-hack (по выдаче, не открыт); Euler Finance, «War & Peace…», январь 2024).

Возьмём Taproot, изменение правил согласия в биткоине 2021 года. Согласие на него собирали заранее[773]. В версии программы Bitcoin Core 0.21.1 новое правило включалось, только если за один период пересчёта сложности (2016 блоков) не меньше 90% блоков будут помечены знаком поддержки[774]. Майнеры начали ставить эти пометки после 24 апреля 2021 года, порог набрали в июне, а в силу Taproot вступил на блоке 709 632, в ноябре 2021 года[775].[776] Разработчики написали правило, майнеры собирали голоса блоками, и только потом правило заработало. Для посёлка это уговор, заключённый заранее, что новое правило вступит в силу, если из ближайших двух тысяч страниц девять десятых выйдут с пометкой «за», а до тех пор все пишут по-старому.

Разница между двумя историями — в том, когда люди договариваются. Taproot был плановой переменой, где сначала собрали согласие, а потом ввели правило. The DAO была аварией, где сначала случилось непоправимое, а потом решали, считать ли его непоправимым. В аварию согласие собирают наспех, за дни или недели, под давлением денег, которые можно вернуть или потерять, и, как показал 2016 год, несогласные могут уйти со своей копией тетрадки.

Прошлая глава оставила открытым вопрос, кто решает, когда правила нужно изменить. В одиночку никто, и фонд Ethereum сам сказал это в 2016 году[777]. Решают те, у кого есть рычаг: разработчики, которые пишут новую версию; майнеры или валидаторы, которые пишут страницы; держатели монет, если их спросили; владельцы узлов, которые выбирают, какую программу запустить. Снаружи к ним добавляются регуляторы и суды. В спокойное время их решение похоже на процедуру, в кризис — на сход, где каждый голосует тем, что у него есть, а исход зависит ещё и от того, найдётся ли тот, кто возьмётся перемену продвигать.

The DAO работала как инвестиционный фонд, Mango Markets — как биржа с займами, Euler — как кредитный сервис. Автоматы, записанные в тетрадку без хранителя, взяли на себя работу банков: принимать вклады, выдавать займы под залог, обещать доходность. Вместе с этой работой к ним перешёл старый вопрос первой главы, кто выдаёт строчки в долг и что

---

[773] Bitcoin Core 0.21.1 release notes, https://github.com/bitcoin/bitcoin/blob/master/doc/release-notes/release-notes-0.21.1.md (механизм, порог, высота 709 632); время блока — Blockstream Explorer API, https://blockstream.info/api/block-height/709632 и https://blockstream.info/api/block/000000000000000000000687bca986194dc2c1f949318629b44bb54ec0a94d8244 (метка 1636866927); блок фиксации — CoinDesk, «Locked In: Bitcoin's Taproot Upgrade Gets Its 90% Mandate», 12.06.2021, https://www.coindesk.com/tech/2021/06/12/locked-in-bitcoins-taproot-upgrade-gets-its-90-mandate (по выдаче).

[774] Bitcoin Core 0.21.1 release notes, https://github.com/bitcoin/bitcoin/blob/master/doc/release-notes/release-notes-0.21.1.md (механизм, порог, высота 709 632); время блока — Blockstream Explorer API, https://blockstream.info/api/block-height/709632 и https://blockstream.info/api/block/000000000000000000000687bca986194dc2c1f949318629b44bb54ec0a94d8244 (метка 1636866927); блок фиксации — CoinDesk, «Locked In: Bitcoin's Taproot Upgrade Gets Its 90% Mandate», 12.06.2021, https://www.coindesk.com/tech/2021/06/12/locked-in-bitcoins-taproot-upgrade-gets-its-90-mandate (по выдаче).

[775] Bitcoin Core 0.21.1 release notes, https://github.com/bitcoin/bitcoin/blob/master/doc/release-notes/release-notes-0.21.1.md (механизм, порог, высота 709 632); время блока — Blockstream Explorer API, https://blockstream.info/api/block-height/709632 и https://blockstream.info/api/block/000000000000000000000687bca986194dc2c1f949318629b44bb54ec0a94d8244 (метка 1636866927); блок фиксации — CoinDesk, «Locked In: Bitcoin's Taproot Upgrade Gets Its 90% Mandate», 12.06.2021, https://www.coindesk.com/tech/2021/06/12/locked-in-bitcoins-taproot-upgrade-gets-its-90-mandate (по выдаче).

[776] Bitcoin Core 0.21.1, release notes: «taproot will then be active as of block 709632 (expected in early or mid November)». Способ активации назывался Speedy Trial. Порог, по сообщениям прессы, набран на блоке 687 284 (12.06.2021); блок 709 632 найден 14.11.2021 около 05:15 по всемирному времени. В составе Taproot — подписи Шнорра (BIP-340) (Bitcoin Core 0.21.1 release notes, https://github.com/bitcoin/bitcoin/blob/master/doc/release-notes/release-notes-0.21.1.md (механизм, порог, высота 709 632); время блока — Blockstream Explorer API, https://blockstream.info/api/block-height/709632 и https://blockstream.info/api/block/000000000000000000000687bca986194dc2c1f949318629b44bb54ec0a94d8244 (метка 1636866927); блок фиксации — CoinDesk, «Locked In: Bitcoin's Taproot Upgrade Gets Its 90% Mandate», 12.06.2021, https://www.coindesk.com/tech/2021/06/12/locked-in-bitcoins-taproot-upgrade-gets-its-90-mandate (по выдаче)). SegWit активирован 24.08.2017 на блоке 481 824 (BIP-141 «Segregated Witness (Consensus layer)», Lombrozo E., Lau J., Wuille P., created 21.12.2015, https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki; дата и блок активации — Trezor Blog, «SegWit and its legacy: Taproot, UASFs and Lightning», https://trezor.io/blog/insights/segwit-and-its-legacy-taproot-uasfs-and-lightning).

[777] Jeffrey Wilcke, «To fork or not to fork», Ethereum Foundation Blog, 15.07.2016, https://blog.ethereum.org/2016/07/15/to-fork-or-not-to-fork.

будет, когда их начнут вычёркивать. А рядом с ним встал вопрос этой главы, на который сам автомат не ответит: кто соберётся решать, когда он ошибётся, и хватит ли у этих людей рычага, чтобы вмешаться?

Глава 5. Новые посредники: стейблкоины, DeFi и кредит поверх блокчейна

Тетрадка без хранителя недолго оставалась тетрадкой без должников. В первой главе я показал место, где посёлок перестаёт объяснять биткоин: за строчкой биткоина нет должника, и никто не обещает отдать за неё хлеб, крышу или доллары. Через семнадцать лет после первого блока в открытых тетрадках ходят строчки примерно на триста миллиардов долларов, и почти за каждой стоит обещание, чаще всего частной компании, выкупить её за настоящий доллар[778]. Такие строчки называют стейблкоинами, то есть «стабильными монетами». Под них автоматы из прошлой главы и начали выдавать займы.

Крипта ушла от банков и построила их заново. В ней снова есть вклады, которые тут же выдаются в долг, залог, требование довнести залог и принудительная продажа, а в худшие дни и спаситель, который закрывает дыру своими деньгами. Работает всё это большей частью без банковских правил и без страховки вкладов. У кредита же, как мы видели в посёлке, есть привычка то расширяться, то сжиматься волнами, и поэтому самые большие риски крипты, по-моему, сидят не в технологии, а в кредите, который на ней построен.

Строчка, за которой снова стоит должник

Вернёмся в посёлок. Пусть в соседнем городе ходят обычные деньги, городские доллары, и жителям они нужны, потому что соль и гвозди продают только в городе. Строчки общей тетрадки для этого неудобны: сколько они стоят в городских долларах, меняется изо дня в день. Тогда на краю посёлка открывается лавка. Лавочник принимает городские доллары, кладёт их в сундук и пишет в общую тетрадку строчку «лавочник должен предъявителю один городской доллар», а по первому требованию выкупает её обратно.

Так появляется четырнадцатое правило посёлка: в тетрадку без хранителя можно записать строчку, за которой стоит должник вне тетрадки. Такая строчка ходит как любая другая. Её можно передать соседу, положить в автомат или заплатить ею за хлеб, и переводы по-прежнему никто в одиночку не проверяет. Но стоит она ровно столько, сколько стоит слово лавочника и сколько лежит в его сундуке. Тетрадка осталась без хозяина, а доверие к одному человеку, которое из неё убрали, вернулось вместе с лавкой.

Стейблкоин устроен так же. Компания-эмитент (так называют того, кто выпускает монету) принимает доллары, выпускает на блокчейне столько же токенов и обещает выкупать их по номиналу, один токен за один доллар. Напрямую у эмитента обычно выкупают крупные проверенные клиенты. Остальные продают токен на бирже, и держится он у доллара как раз потому, что крупные клиенты могут в любой день сдать его эмитенту[779].[780] Токен, напомню, — строчка на странице памяти контракта. Крупнейшие стейблкоины — USDT компании Tether и USDC компании Circle, и в середине 2026 года на USDT приходилось около 60% всех выпущенных стейблкоинов[781].[782]

---

[778] CoinGecko, «2026 Q2 Crypto Industry Report», https://www.coingecko.com/research/publications/2026-q2-crypto-report.

[779] Tether, «Fees», https://tether.to/en/fees/ (открыто фактчекером 27.09.2026).

[780] Tether, страница комиссий (tether.to/en/fees): минимальная сумма прямого выкупа — 100 000 долларов, комиссия — большая из двух величин, 1000 долларов или 0,1% (Tether, «Fees», https://tether.to/en/fees/ (открыто фактчекером 27.09.2026)). Европейский регламент, о котором речь ниже, требует от эмитента выкупа по номиналу без комиссии (MiCA, Art. 49(4), 49(6), 51(4)(b), OJ L 150, pp. 108–109).

[781] CoinGecko, «2026 Q2 Crypto Industry Report», https://www.coingecko.com/research/publications/2026-q2-crypto-report.

[782] По отчёту CoinGecko, к концу II квартала 2026 года капитализация стейблкоинов составила 305,1 млрд долларов, из них USDT — 184,4 млрд, USDC — 73,5 млрд (CoinGecko, «2026 Q2 Crypto Industry Report», https://

Что лавочник делает с городскими долларами, пока его строчки ходят по посёлку? Держать их в сундуке без дела невыгодно. Он может отнести их в городской банк или купить короткие долговые бумаги городской управы, по которым платят проценты, и проценты достанутся ему, а держателю строчки не достанется ничего. Настоящие эмитенты поступают так же. Tether, по собственному сообщению компании, заработал за 2025 год больше 10 млрд долларов чистой прибыли[783]. Основную часть резервов он держит в казначейских векселях США (коротких долговых бумагах американского правительства) и в сделках под их залог, и проценты по ним — его главный постоянный доход. Ещё часть прибыли принёс рост цен на золото и биткоин, которые тоже лежат в его сундуке[784].[785]

Лавок стало так много, что их покупки заметны на рынке государственного долга. Экономист Банка международных расчётов (его называют клубом центральных банков) и его соавтор в работе, которую Банк выпустил в своей серии исследований, подсчитали, что приток денег в стейблкоины снижает доходность трёхмесячных векселей США, а в неспокойные дни сильнее[786].[787] Эффект измеряется сотыми долями процента, и интереснее в нём направление. Деньги, которые люди держат в открытой тетрадке как «доллары», на деле работают кредитом правительству США, как работали бы деньги в фонде, покупающем короткие государственные долги.

Закон тоже смотрит на стейблкоин как на беспроцентный долг эмитента. Американский закон о стейблкоинах, подписанный в июле 2025 года (его называют GENIUS Act), запрещает эмитенту платить держателям проценты или доходность в любой форме за одно лишь владение токеном[788].[789] Похожий запрет есть в европейском регламенте о криптоактивах MiCA, причём процентом там считается любая выгода, которая зависит от того, как долго вы держите токен[790].

---

www.coingecko.com/research/publications/2026-q2-crypto-report). По записке сотрудников ФРС, на 6 апреля 2026 года — 317 млрд, больше чем на 50% выше, чем в начале 2025 года (Federal Reserve, FEDS Notes, «Stablecoins in 2025: Developments and Financial Stability Implications», 08.04.2026, https://www.federalreserve.gov/econres/notes/feds-notes/stablecoins-in-2025-developments-and-financial-stability-implications-20260408.html). Разные агрегаторы расходятся на 5–15 млрд долларов, поэтому источник нужно указывать всегда. Свежие цифры — в приложении Б.

[783] Tether, «Tether Delivers $10B+ Profits in 2025, $6.3B in Excess Reserves, and Record $141 billion Exposure in U.S. Treasury Holdings», 30.01.2026, https://tether.io/news/tether-delivers-10b-profits-in-2025-6-3b-in-excess-reserves-and-record-141-billion-exposure-in-u-s-treasury-holdings/.

[784] Tether, «Tether Delivers $10B+ Profits in 2025, $6.3B in Excess Reserves, and Record $141 billion Exposure in U.S. Treasury Holdings», 30.01.2026, https://tether.io/news/tether-delivers-10b-profits-in-2025-6-3b-in-excess-reserves-and-record-141-billion-exposure-in-u-s-treasury-holdings/.

[785] Tether, пресс-релиз 30.01.2026 (итог 2025 года, без разбивки по источникам прибыли); на 31.12.2025 — около 141 млрд долларов в казначейских бумагах США с учётом сделок под них (Tether, «Tether Delivers $10B+ Profits in 2025, $6.3B in Excess Reserves, and Record $141 billion Exposure in U.S. Treasury Holdings», 30.01.2026, https://tether.io/news/tether-delivers-10b-profits-in-2025-6-3b-in-excess-reserves-and-record-141-billion-exposure-in-u-s-treasury-holdings/). За первое полугодие 2025 года компания разбивку давала: «$3.1 billion in recurrent profits, excluding mark-to-market contributions from gold and bitcoin, which added another $2.6 billion» (пресс-релиз 31.07.2025) (Tether, «Tether Delivers $10B+ Profits in 2025, $6.3B in Excess Reserves, and Record $141 billion Exposure in U.S. Treasury Holdings», 30.01.2026, https://tether.io/news/tether-delivers-10b-profits-in-2025-6-3b-in-excess-reserves-and-record-141-billion-exposure-in-u-s-treasury-holdings/).

[786] R. Ahmed, I. Aldasoro, «Stablecoins and safe asset prices», BIS Working Paper 1270, первая публикация 28.05.2025 (обновлённая версия с данными по март 2026), https://www.bis.org/publ/work1270.htm.

[787] Ahmed R. (Andersen Institute for Finance and Economics), Aldasoro I. (BIS). Stablecoins and safe asset prices. BIS Working Paper 1270, первая версия 28.05.2025, обновлённая — с данными по март 2026 года: «we find a $3.5 billion (2-standard deviation) inflow lowers 3-month Treasury bill yields by 0.71 basis points on impact, and up to 4 basis points within 10 days». Базисный пункт — сотая доля процента. В первой версии оценки были другими (2–2,5 базисного пункта). Работы этой серии выражают мнение авторов, позиция Банка может с ним не совпадать (R. Ahmed, I. Aldasoro, «Stablecoins and safe asset prices», BIS Working Paper 1270, первая публикация 28.05.2025 (обновлённая версия с данными по март 2026), https://www.bis.org/publ/work1270.htm).

[788] GENIUS Act, sec. 4(a)(11).

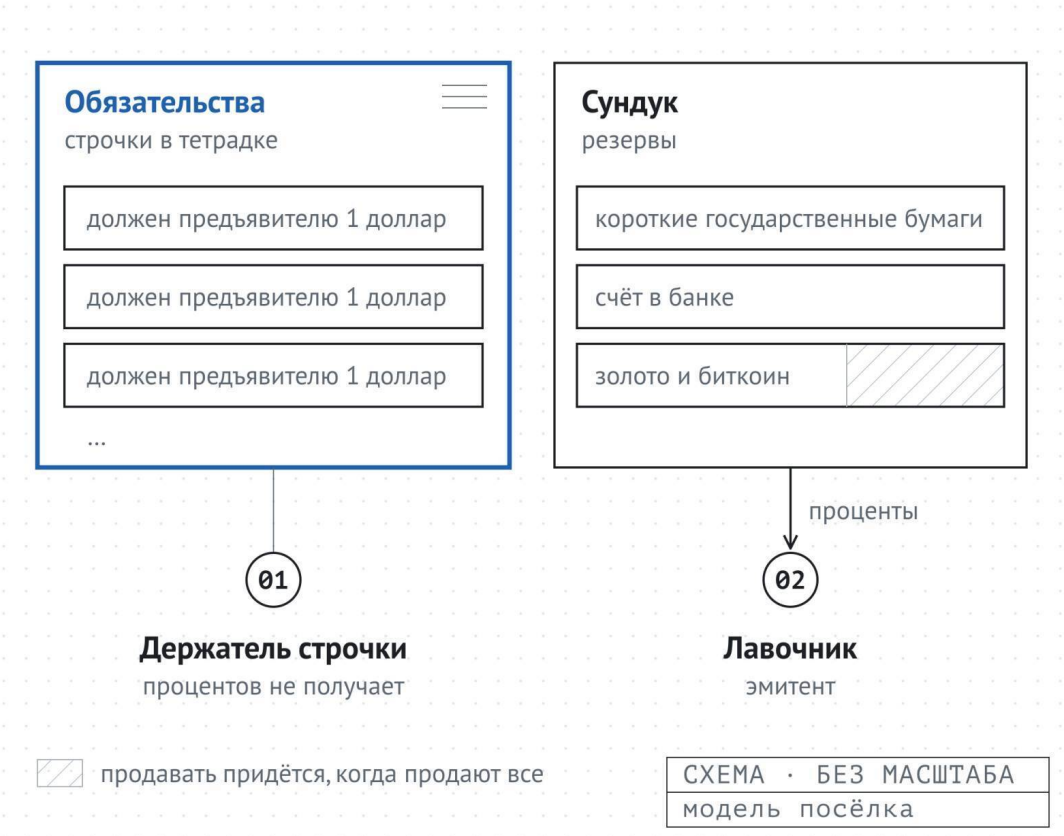
[789] GENIUS Act, sec. 4(a)(11): запрет касается выплат «solely in connection with the holding, use, or retention» стейблкоина. Вокруг этой оговорки идёт спор о доходных продуктах бирж и других посредников (GENIUS Act, sec. 4(a)(11)).

[790] MiCA, Art. 50(1)–(3), OJ L 150, p. 108.

Держатель отдаёт компании доллар и получает взамен её обещание без процентов, а компания вкладывает его доллар в государственный долг.

Это похоже на банковский вклад без процентов, только без банковского надзора и без страховки вкладов. Экономисты Гэри Гортон и Джеффри Чжан говорят прямо, что эмитенты стейблкоинов — это нерегулируемые банки[791].[792] Сами стейблкоины они сравнивают с частными банкнотами XIX века, которые принимали по номиналу не всегда, а выпускавшие их банки были беззащитны перед паникой, когда все разом приходили за деньгами[793]. К этим банкнотам мы вернёмся, когда будем разбирать пузыри прошлого.

Зачем строчка с должником понадобилась в тетрадке, которую строили ради того, чтобы обойтись без должников? Цена биткоина и эфира в долларах скачет, а считать долги, цены и залоги удобнее в чём-то неподвижном. Стейблкоин стал в открытых тетрадках тем же, чем в посёлке стал городской доллар из лавки, то есть общей мерой, в которой считают всё остальное. Дальше в этой главе почти каждый заём, каждая доходность и каждый залог будут выражены в стейблкоинах, так что на надёжности лавочника держится почти вся конструкция.



[791] G. B. Gorton, J. Y. Zhang, «Taming Wildcat Stablecoins», The University of Chicago Law Review, 90(3), 2023, https://lawreview.uchicago.edu/print-archive/taming-wildcat-stablecoins.

[792] Gorton G. B., Zhang J. Y. Taming Wildcat Stablecoins. The University of Chicago Law Review, 90(3), 2023: «stablecoin issuers are unregulated banks». Из трёх возможных ответов, которые обсуждают авторы (выпуск стейблкоинов только банками, «узкий банк» с резервами один к одному в безопасных активах и цифровые валюты центробанков), американский закон 2025 года, по-моему, ближе всего ко второму (G. B. Gorton, J. Y. Zhang, «Taming Wildcat Stablecoins», The University of Chicago Law Review, 90(3), 2023, https://lawreview.uchicago.edu/print-archive/taming-wildcat-stablecoins; GENIUS Act, enrolled bill text, sec. 4(a)(1)(A), https://www.govinfo.gov/content/pkg/BILLS-119s1582enr/html/BILLS-119s1582enr.htm; дата подписания — The White House, https://www.whitehouse.gov/briefings-statements/2025/07/the-president-signed-into-law-s-1582; Covington & Burling, 07.2025).

[793] G. B. Gorton, J. Y. Zhang, «Taming Wildcat Stablecoins», The University of Chicago Law Review, 90(3), 2023, https://lawreview.uchicago.edu/print-archive/taming-wildcat-stablecoins.

Рисунок 5.1. Лавка стейблкоина как баланс

Чем обеспечен цифровой доллар

Обещание стоит столько, сколько лежит в сундуке, и у Tether история сундука неровная. В феврале 2021 года генеральный прокурор штата Нью-Йорк объявила об урегулировании дела с Tether и связанной с ней биржей Bitfinex. Компании заплатили 18,5 млн долларов и обязались отчитываться о резервах каждый квартал, а расследование установило, что с середины 2017 года у Tether не было доступа к банкам и в отдельные периоды резервов в соотношении один к одному не было[794]. Заявления компании о том, что USDT всегда полностью обеспечен долларами, прокурор назвала ложью[795].[796]

Осенью того же года Tether оштрафовала и Комиссия по торговле товарными фьючерсами США. По её выводам, в 2016–2018 годах долларовых резервов на все USDT в обращении хватало лишь в 27,6% дней[797]. Часть резервов составляли необеспеченные долги третьих лиц и активы не в долларах, а хранились они вперемешку с рабочими деньгами Bitfinex[798]. Деньги лавки и деньги соседней биржи той же группы лежали в одном сундуке, а Bitfinex тем временем, по данным прокуратуры, потеряла у платёжного посредника крупную сумму и скрывала это[799].[800]

Всё это история 2016–2019 годов, и переносить её на сегодня нельзя ни в одну сторону. Сотрудники ФРС в записке, вышедшей в апреле 2026 года, по заверенным отчётам эмитентов оценили, что резервы USDT покрывали выпуск примерно в 1,04 раза, а высококачественными ликвидными активами (казначейскими бумагами, сделками под них и банковскими вкладами) — примерно в 0,74 раза. У USDC то же соотношение было равно единице[801].[802] Разницу объяс-

---

[794] New York State Attorney General, «Attorney General James Ends Virtual Currency Trading Platform Bitfinex's Illegal Activities in New York», 23.02.2021, https://ag.ny.gov/press-release/2021/attorney-general-james-ends-virtual-currency-trading-platform-bitfinexs-illegal.

[795] New York State Attorney General, «Attorney General James Ends Virtual Currency Trading Platform Bitfinex's Illegal Activities in New York», 23.02.2021, https://ag.ny.gov/press-release/2021/attorney-general-james-ends-virtual-currency-trading-platform-bitfinexs-illegal.

[796] New York State Attorney General, пресс-релиз 23.02.2021: «Tether's claims that its virtual currency was fully backed by U.S. dollars at all times was a lie.» По тому же релизу, уже на следующий день после опубликованной 1 ноября 2018 года «проверки» полного обеспечения со счетов Tether начали выводить сотни миллионов (New York State Attorney General, «Attorney General James Ends Virtual Currency Trading Platform Bitfinex's Illegal Activities in New York», 23.02.2021, https://ag.ny.gov/press-release/2021/attorney-general-james-ends-virtual-currency-trading-platform-bitfinexs-illegal).

[797] CFTC, Press Release 8450-21, «CFTC Orders Tether and Bitfinex to Pay Fines Totaling $42.5 Million», 15.10.2021, https://www.cftc.gov/PressRoom/PressReleases/8450-21.

[798] CFTC, 15.10.2021.

[799] NYAG, 23.02.2021.

[800] CFTC, пресс-релиз 15.10.2021: штраф Tether — 41 млн долларов; проверенный период — 26 месяцев 2016–2018 годов; резервы хранились в том числе через нерегулируемые структуры (CFTC, Press Release 8450-21, «CFTC Orders Tether and Bitfinex to Pay Fines Totaling $42.5 Million», 15.10.2021, https://www.cftc.gov/PressRoom/PressReleases/8450-21; CFTC, 15.10.2021). Потеря Bitfinex у платёжного посредника — около 850 млн долларов, по данным генерального прокурора штата Нью-Йорк (NYAG, 23.02.2021).

[801] Federal Reserve, FEDS Notes, 08.04.2026.

[802] Federal Reserve, FEDS Notes, «Stablecoins in 2025: Developments and Financial Stability Implications», 08.04.2026. Оценки сделаны «according to their attested disclosures», то есть по последним заверенным отчётам на момент записки; точной даты отчёта записка не указывает. Записки этой серии выражают мнение авторов, официальной позицией ФРС они не считаются (Federal Reserve, FEDS Notes, «Stablecoins in 2025: Developments and Financial Stability Implications», 08.04.2026, https://www.federalreserve.gov/econres/notes/feds-notes/stablecoins-in-2025-developments-and-financial-stability-implications-20260408.html; Federal Reserve, FEDS Notes, 08.04.2026).

няет остальное содержимое сундука Tether, где кроме векселей и сделок под них лежат физическое золото и биткоин[803].[804]

Из этих цифр я не стал бы выводить ни «Tether не обеспечен», ни «Tether полностью обеспечен долларами», потому что обе формулы неверны. Обещание Tether покрыто активами с небольшим запасом, но больше четверти этих активов относится к тем, которые в панику трудно продать быстро и по полной цене[805]. Сколько удастся выручить за них в такой день, заранее не знает никто, и я тоже.

На лавке это видно лучше. Допустим, лавочник выписал 100 строчек по доллару, а в сундуке у него на 104 доллара добра. Из них 74 лежат в городских бумагах, которые продаются в любой день по полной цене, а 30 — в золоте и в строчках самой тетрадки, которые в спокойное время тоже стоят своих денег (числа условные, хотя и близки к оценке ФРС для USDT[806]). В обычный день приходят двое-трое, и лавочник расплачивается из надёжной части. Теперь пусть по посёлку прошёл слух. Первые 74 пришедших получат свой доллар без труда. Остальным придётся ждать, пока лавочник продаст золото, а продавать его придётся в тот же день, когда продают все.

Каждый житель это понимает, и поэтому в плохой день выгоднее прийти первым. Так и выглядит паника вкладчиков, и для неё не нужны ни мошенничество, ни недостача. Достаточно, чтобы часть сундука нельзя было быстро продать по полной цене, а люди об этом знали. Гортон и Чжан пишут об уязвимости эмитентов к такой панике[807], аналитики Банка международных расчётов — о том же[808].

У такого сундука есть свойство, знакомое по любому банку. Tether держит активов больше, чем выпустил токенов, и этот запас работает как капитал банка, который растёт, пока золото и биткоин дорожают, и тает, когда они дешевеют. За второй квартал 2026 года запас сократился примерно вдвое, хотя квартал компания закончила с операционной прибылью[809]. Обязательства держателям при этом по-прежнему покрывались, но запас прочности лавки заметно зависел от цены золота и биткоина. По разбору отраслевой прессы, на их удешевление пришлось больше двух пятых потери.[810]

---

[803] Tether, 01.05.2026.

[804] По данным компании на 31 марта 2026 года — около 141 млрд долларов в казначейских векселях и сделках под них, около 20 млрд в физическом золоте и около 7 млрд в биткоине (Tether, 01.05.2026). По отчёту Tether, на векселя и сделки под них приходится 141 из 191,8 млрд активов, остальное — около 26%; по цифрам ФРС (1,04 и 0,74) — около 29% (Federal Reserve, FEDS Notes, 08.04.2026; Tether, 01.05.2026).

[805] Federal Reserve, FEDS Notes, 08.04.2026.

[806] Federal Reserve, FEDS Notes, 08.04.2026.

[807] G. B. Gorton, J. Y. Zhang, «Taming Wildcat Stablecoins», The University of Chicago Law Review, 90(3), 2023, https://lawreview.uchicago.edu/print-archive/taming-wildcat-stablecoins.

[808] BIS Quarterly Review, 06.12.2021.

[809] Tether, «Tether Posts $1.04B Q1 2026 Profit Despite Highly Volatile Global Markets, Reaches All-Time-Highs $8.23B Reserve Buffer…», 01.05.2026, https://tether.io/news/tether-posts-1-04b-q1-2026-profit-despite-highly-volatile-global-markets-reaches-all-time-highs-8-23b-reserve-buffer-and-maintains-u-s-treasury-heavy-backing/; Tether, «Tether Posts Strong Q2 Performance, Generates $1.5B Net Operating Profit, Maintains $4.11B Reserve Buffer, and Expands Gold Holdings to More Than 146 Tons», 31.07.2026, https://tether.io/news/tether-posts-strong-q2-performance-generates-1-5b-net-operating-profit-maintains-4-11b-reserve-buffer-and-expands-gold-holdings-to-more-than-146-tons/.

[810] Tether, пресс-релизы 01.05.2026 и 31.07.2026, со ссылкой на заверения аудиторской фирмы BDO: запас 8,23 млрд долларов на 31 марта и 4,11 млрд на 30 июня 2026 года, операционная прибыль за квартал — около 1,5 млрд (Tether, «Tether Posts $1.04B Q1 2026 Profit Despite Highly Volatile Global Markets, Reaches All-Time-Highs $8.23B Reserve Buffer…», 01.05.2026, https://tether.io/news/tether-posts-1-04b-q1-2026-profit-despite-highly-volatile-global-markets-reaches-all-time-highs-8-23b-reserve-buffer-and-maintains-u-s-treasury-heavy-backing/; Tether, «Tether Posts Strong Q2 Performance, Generates $1.5B Net Operating Profit, Maintains $4.11B Reserve Buffer, and Expands Gold Holdings to More Than 146 Tons», 31.07.2026, https://tether.io/news/tether-posts-strong-q2-performance-generates-1-5b-net-operating-profit-maintains-4-11b-reserve-buffer-and-expands-gold-holdings-to-more-than-146-tons/). Сама компания сокращение запаса не объясняет и пишет, что USDT «остался полностью обеспечен». По разбору crypto.news, на нереализованные убытки по золоту и биткоину пришлось около 1,8 млрд долларов из выпавших примерно 4,1 млрд, остальное — покупки активов, расходы и прочие движения

USDC устроен строже. Основную часть его резервов Circle держит в государственном фонде денежного рынка под управлением BlackRock (так называют фонд, вкладывающий в самые короткие и надёжные долги), остальное — наличными на счетах в крупных банках, а раз в месяц состояние резервов заверяет аудиторская фирма[811]. Заверение подтверждает остаток резервов на определённую дату, но всю работу компании, как полный аудит, не проверяет[812].

Самый чистый из крупных стейблкоинов подвёл в марте 2023 года, и подвёл его обычный банк. Когда рухнул калифорнийский Silicon Valley Bank, Circle не могла добраться до резервов, лежавших там на счетах, а это около 8% всего сундука. За выходные USDC подешевел до 86–87 центов и вернулся к доллару после того, как власти США гарантировали все вклады этого банка[813].[814] Держатель USDC верил Circle, Circle доверила часть денег банку, а банк в тот раз спасло государство. Доверие, которое в первой главе было двухэтажным, здесь стало трёхэтажным, и нижний этаж держался на гарантии, которую никто держателям стейблкоина не обещал.

Законы последних лет требуют от лавочника одного и того же: держать в сундуке только самое надёжное. GENIUS Act требует резервов не меньше чем один к одному и перечисляет, из чего они могут состоять. Это наличные доллары и средства в ФРС, банковские вклады до востребования, казначейские бумаги со сроком до погашения не больше 93 дней, короткие сделки под них и фонды денежного рынка из тех же активов[815]. Когда закон заработает, состав резервов придётся публиковать каждый месяц, каждый месяц их будет проверять зарегистрированная аудиторская фирма, а генеральный и финансовый директора будут подписываться под отчётом[816]. MiCA требует держать не меньше 30% полученных денег на отдельных счетах в банках, а остальное вкладывать в безопасные ликвидные бумаги в той же валюте[817].[818]

баланса; Blockonomi связывает сокращение с колебаниями цен без разбивки (Tether, «Tether Posts Strong Q2 Performance, Generates $1.5B Net Operating Profit, Maintains $4.11B Reserve Buffer, and Expands Gold Holdings to More Than 146 Tons», 31.07.2026, https://tether.io/news/tether-posts-strong-q2-performance-generates-1-5b-net-operating-profit-maintains-4-11b-reserve-buffer-and-expands-gold-holdings-to-more-than-146-tons/). Свежие цифры — в приложении Б.

[811] Circle, «USDC Transparency», https://www.circle.com/transparency (обращение 26.09.2026).

[812] Circle, «USDC Transparency», https://www.circle.com/transparency (обращение 26.09.2026).

[813] Du C., Sonawane R., Watsky C., «In the Shadow of Bank Run…», FEDS Notes, 17.12.2025, https://www.federalreserve.gov/econres/notes/feds-notes/in-the-shadow-of-bank-run-lessons-from-the-silicon-valley-bank-failure-and-its-impact-on-stablecoins-20251217.html; CNBC, 11.03.2023, https://www.cnbc.com/2023/03/11/stablecoin-usdc-breaks-dollar-peg-after-firm-reveals-it-has-3point3-billion-in-svb-exposure.html.

[814] В Silicon Valley Bank лежали 3,3 млрд долларов резервов USDC. Минимум цены — 86 или 87 центов в зависимости от площадки и момента замера (по часовым данным — около 90 центов) (Du C., Sonawane R., Watsky C., «In the Shadow of Bank Run…», FEDS Notes, 17.12.2025, https://www.federalreserve.gov/econres/notes/feds-notes/in-the-shadow-of-bank-run-lessons-from-the-silicon-valley-bank-failure-and-its-impact-on-stablecoins-20251217.html; CNBC, 11.03.2023, https://www.cnbc.com/2023/03/11/stablecoin-usdc-breaks-dollar-peg-after-firm-reveals-it-has-3point3-billion-in-svb-exposure.html). Du C., Sonawane R., Watsky C. In the Shadow of Bank Run… FEDS Notes, 17.12.2025.

[815] GENIUS Act, enrolled bill text, sec. 4(a)(1)(A), https://www.govinfo.gov/content/pkg/BILLS-119s1582enr/html/BILLS-119s1582enr.htm; дата подписания — The White House, https://www.whitehouse.gov/briefings-statements/2025/07/the-president-signed-into-law-s-1582; Covington & Burling, 07.2025.

[816] GENIUS Act, sec. 4(a)(1)(C), 4(a)(3)(A)–(B).

[817] Regulation (EU) 2023/1114 (MiCA), Art. 54, OJ L 150, 09.06.2023, p. 111, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1114.

[818] GENIUS Act, S. 1582, подписан 18.07.2025, sec. 4(a)(1)(A): «Treasury bills, notes, or bonds … with a remaining maturity of 93 days or less» (GENIUS Act, enrolled bill text, sec. 4(a)(1)(A), https://www.govinfo.gov/content/pkg/BILLS-119s1582enr/html/BILLS-119s1582enr.htm; дата подписания — The White House, https://www.whitehouse.gov/briefings-statements/2025/07/the-president-signed-into-law-s-1582; Covington & Burling, 07.2025). Закон вступает в силу в более раннюю из двух дат — 18 января 2027 года или через 120 дней после окончательных правил регуляторов; на сентябрь 2026 года правила ещё не приняты (Covington & Burling, «The GENIUS Act Becomes Law: Key Provisions…», 07.2025, https://www.cov.com/news-and-insights/insights/2025/07/the-genius-act-becomes-law-key-provisions-from-the-federal-stablecoin-regulatory-framework). Regulation (EU) 2023/1114 (MiCA), Art. 54: «at least 30 % of the funds received is always deposited in separate accounts in credit institutions» (Regulation (EU) 2023/1114 (MiCA), Art. 54, OJ L 150, 09.06.2023, p. 111, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1114). Сроки и состояние подзаконных правил — в главе 11 и приложении Б.

В первой главе доверие к немецким деньгам в 1923 году вернуло правило, которое связало хранителю руки: столько строчек и не больше. Здесь ход похожий. Лавочнику не ограничивают число строчек, зато ограничивают то, что он может держать в сундуке против каждой из них, и заставляют показывать сундук каждый месяц. Насколько это поможет в настоящую панику, покажет только первая большая паника после того, как эти правила заработают в полную силу.

В европейском регламенте есть деталь, которую стоит знать каждому, кто считает стейблкоин долларом на счёте. Держатель вправе в любой момент вернуть токен эмитенту по номиналу и без комиссии, но в документе о токене эмитент обязан предупредить, что системы страхования вкладов на токен не распространяются[819]. Закон заставляет лавочника написать на вывеске, что он не банк, хотя делает он почти то же, что банк.

Из историй Tether и USDC складывается короткая проверка для любого стейблкоина, в котором вы собираетесь держать заметную часть денег. Смотреть стоит на долю самого надёжного в сундуке (коротких государственных бумаг и денег в центральном банке), на то, кто и как часто сундук проверяет, и на банки, где лежит остальное, потому что на них держится нижний этаж. Долю надёжного и результаты проверок американский закон обяжет эмитентов раскрывать каждый месяц[820]. Про банки придётся думать самим.

Чей это доллар

Центральные банки смотрят на стейблкоины настороженно, и их довод легче понять на посёлке. Пусть лавок стало две, на восточном краю и на западном. В тетрадке ходят строчки «восточный лавочник должен один доллар» и «западный лавочник должен один доллар». Пока про обоих ничего дурного не слышно, их берут одинаково. Но однажды проходит слух, что у западного лавочника в сундуке недостача, и его строчку начинают брать за 90 центов. Теперь пекарь, прежде чем продать хлеб за «доллар», должен спросить, чей это доллар.

Сам Банк международных расчётов в отчёте 2025 года заключил, что стейблкоины не проходят три проверки, которые он считает обязательными для здоровых денег. Первая — единство, то есть приём по номиналу. Вторая — эластичность, то есть способность денежной системы вовремя расплатиться по обязательствам и не застрять в заторе. Третья — целостность, защита от финансовых преступлений[821].[822] Провал первой проверки объяснён ровно нашим примером с двумя лавками. Стейблкоин, пишет Банк, помечен именем эмитента, как частные банкноты эпохи свободного банкинга XIX века, и любое отклонение от номинала разрушает главное свойство денег, их приём без лишних вопросов[823].[824]

Со второй проверкой связан вопрос о запасе. У банковской системы в трудный день есть центральный банк, который может дать банкам столько денег, сколько нужно, чтобы расчёты не встали, а у лавочника есть только сундук. В отчёте 2026 года Банк добавил, что широкое

---

[819] MiCA, Art. 49(4), 49(6), 51(4)(b), OJ L 150, pp. 108–109.

[820] GENIUS Act, sec. 4(a)(1)(C), 4(a)(3)(A)–(B).

[821] BIS, пресс-релиз 24.06.2025, https://www.bis.org/press/p250624.htm; глава III, https://www.bis.org/publ/arpdf/ar2025e3.htm.

[822] BIS, Annual Economic Report 2025, ch. III; пресс-релиз 24.06.2025: «they do not deliver singleness of money (acceptance for payment at par), elasticity (timely discharge of obligations, preventing gridlock) and integrity (safeguarding against financial crime).» Сам пример с долларами разных эмитентов в отчёте тоже есть; в тексте я переложил его на посёлок (BIS, Annual Economic Report 2025, ch. III, https://www.bis.org/publ/arpdf/ar2025e3.htm (открыто 26.09.2026)).

[823] BIS, Annual Economic Report 2025, ch. III, https://www.bis.org/publ/arpdf/ar2025e3.htm (открыто 26.09.2026).

[824] Там же: «Stablecoin holdings are tagged with the name of the issuer, much like private banknotes circulating in the 19th century Free Banking era».

распространение стейблкоинов может заметно изменить то, как банки привлекают деньги и выдают кредиты, и угрожать денежной независимости более слабых экономик[825].[826]

Этот довод стоит взвешивать с поправкой на того, кто его приводит. Центральные банки — сторона спора, ведь стейблкоины отнимают у них часть той самой работы, которую они считают своей. Последнее предупреждение Банка к тому же можно прочитать с другой стороны. «Угроза денежной независимости» для жителя страны с обесценивающейся валютой выглядит как способ держать сбережения в долларах, до которых иначе не дотянуться.

Спрос на такие доллары виден и в цифрах. По оценке аналитической компании Chainalysis, в Аргентине с июля 2023 по июнь 2024 года на стейблкоины пришлось почти 62% всего объёма криптовалютных операций[827]. В Турции покупки стейблкоинов за год до марта 2024 года составили около 4% ВВП, больше, чем в любой другой стране[828]. В Нигерии после резкого падения найры выросли поступления стейблкоинов суммами до миллиона долларов, а перевод 200 долларов из стран Африки южнее Сахары в стейблкоине, по расчёту той же компании, обходится в среднем примерно на 60% дешевле обычного[829].[830] Сама компания объясняет этот спрос инфляцией, скачками курса и ограничениями на вывоз капитала[831].

По-моему, правы обе стороны. Для человека, чьё песо дешевеет каждый месяц, частный доллар с чужим именем надёжнее собственных денег, и он охотно доверится лавочнику, которого никогда не видел. Центральный банк, в свою очередь, видит, как часть денег страны переезжает в сундук частной компании за границей. Кто выиграет в этом споре, решат не технологии, и к нему мы вернёмся, когда будем говорить о том, как отвечают государства.

Три замены сундука

Лавка с сундуком — самый простой способ привязать строчку к доллару, и два крупнейших стейблкоина устроены именно так. Обойтись без лавочника можно тремя способами, и все три опробованы. Монету можно выдавать в долг под залог из других криптовалют (так устроен DAI). Можно обещать обменять её на другой токен той же системы без всякого внешнего залога (так был устроен UST). А можно держать криптовалюту вместе с противоположной

---

[825] BIS, пресс-релиз 23.06.2026, «The path to the next-generation monetary and financial system lies in safeguarding trust in money», https://www.bis.org/press/p260623.htm.

[826] BIS, пресс-релиз 23.06.2026: «wider stablecoin adoption could usher in significant changes in bank funding and credit provision and potentially pose financial stability challenges». Там же — о том, что спрос на долларовые стейблкоины может сделать потоки капитала беспокойнее и угрожать денежному суверенитету (BIS, пресс-релиз 23.06.2026, «The path to the next-generation monetary and financial system lies in safeguarding trust in money», https://www.bis.org/press/p260623.htm).

[827] Chainalysis, «2024 LATAM Crypto Adoption: The Rise of Stablecoins», 09.10.2024, https://www.chainalysis.com/blog/2024-latin-america-crypto-adoption/.

[828] Cointelegraph, «Turkey tops the world in stablecoin buying share vs. GDP», 04.2024, https://cointelegraph.com/news/stablecoin-buys-turkey-4-percent-gdp (пересказ отчёта Chainalysis и слов директора по исследованиям Ким Грауэр).

[829] Chainalysis, «Sub-Saharan Africa: Nigeria Takes #2…», 02.10.2024, https://www.chainalysis.com/blog/subsaharan-africa-crypto-adoption-2024/.

[830] Chainalysis, отчёты о Латинской Америке (09.10.2024) и об Африке южнее Сахары (02.10.2024); данные по Турции — из отчёта Crypto Spring Report (25.04.2024) в пересказе Cointelegraph. «Мелкие и средние» поступления у Chainalysis — суммы до 1 млн долларов; 60% — средняя цифра по региону, не по одной Нигерии. В расчёт стоимости перевода в стейблкоине компания включает биржевые комиссии и курсовую разницу на региональных биржах; в остальном методика закрыта. Доля Турции посчитана к ВВП 2022 года, что может её завышать (Chainalysis, «2024 LATAM Crypto Adoption: The Rise of Stablecoins», 09.10.2024, https://www.chainalysis.com/blog/2024-latin-america-crypto-adoption/; Chainalysis, «Sub-Saharan Africa: Nigeria Takes #2…», 02.10.2024, https://www.chainalysis.com/blog/subsaharan-africa-crypto-adoption-2024/; Cointelegraph, «Turkey tops the world in stablecoin buying share vs. GDP», 04.2024, https://cointelegraph.com/news/stablecoin-buys-turkey-4-percent-gdp (пересказ отчёта Chainalysis и слов директора по исследованиям Ким Грауэр)). В Венесуэле, по той же компании, чем ниже падает боливар, тем больше криптовалюты получают жители; это связь, причинность ею не доказана (Chainalysis, 2024 LATAM).

[831] Chainalysis, «Latin America Crypto Adoption 2025», 02.10.2025, https://www.chainalysis.com/blog/latin-america-crypto-adoption-2025/.

ставкой на её цену, и тогда получится так называемый «синтетический доллар» (USDe)[832]. За строчкой по-прежнему стоит обещание, у обещания есть исполнитель, и меняется только то, что лежит на месте сундука и кто за ним следит.

У DAI лавочника с сундуком долларов нет, его выдаёт автомат. Пользователь вносит залог в «хранилище» автомата и берёт под него DAI в долг. Долг нужно вернуть вместе с годовой платой, а если залог дешевеет ниже заданного порога, автомат продаёт его на аукционе за DAI и берёт штраф[833]. Для эфира залог в 2020–2021 годах должен был стоить не меньше 150% долга[834]. Если после продажи залога долг покрыт не полностью, система выпускает новые токены MKR и продаёт их за DAI, чтобы закрыть дыру[835].

В посёлке мы такое уже видели. Это второе правило из первой главы, по которому хранитель пишет строчку в долг, а сарай плотника записан за ним до погашения. Здесь строчку в долг пишет автомат, сарай заменяет эфир, а DAI появляются в момент займа, как появлялись деньги в посёлке, когда хранитель выдавал кредит. Держатели MKR, токена, которым голосуют за параметры системы, играют роль последнего запаса прочности. Когда залога не хватает, их доля размывается новым выпуском, как размывается доля акционеров банка, которому нужен новый капитал.

12 марта 2020 года этот механизм проверили на прочность. За сутки эфир подешевел на 43%[836], множество хранилищ одновременно ушло под продажу залога, а сеть Ethereum оказалась перегружена, и плата за место на странице резко выросла[837]. Программы-ликвидаторы, которые обычно соревнуются на аукционах за залог, остановились, и два-три часа аукционы выигрывал один участник, предлагая за эфир ноль DAI[838].[839] Авторы исследования ликвидаций в DeFi потом отметили, что при перегрузке блокчейна не справились даже профессиональные программы-ликвидаторы[840].

У этого дня две цифры, и путать их нельзя. Заёмщики, чей залог ушёл за ноль, потеряли, по оценке CoinDesk, эфира примерно на 8,33 млн долларов[841]. Система потеряла другое. Залог

---

[832] MakerDAO / Sky, «The Maker Protocol White Paper», https://makerdao.com/en/whitepaper/ (открыто 26.09.2026; текст обновлён под бренд Sky); SEC, Press Release 2023-32, «SEC Charges Terraform and CEO Do Kwon with Defrauding Investors in Crypto Schemes», 16.02.2023, https://www.sec.gov/news/press-release/2023-32; Ethena, «Ethena Overview», https://docs.ethena.fi/overview/ethena-overview.md (открыто 26.09.2026).

[833] MakerDAO / Sky, «The Maker Protocol White Paper», https://makerdao.com/en/whitepaper/ (открыто 26.09.2026; текст обновлён под бренд Sky).

[834] K. Qin, L. Zhou, P. Gamito, P. Jovanovic, A. Gervais, «An Empirical Study of DeFi Liquidations: Incentives, Risks, and Instabilities», ACM IMC '21, 2021, https://arxiv.org/abs/2106.06389 (DOI 10.1145/3487552.3487811).

[835] MakerDAO / Sky, «The Maker Protocol White Paper», https://makerdao.com/en/whitepaper/ (открыто 26.09.2026; текст обновлён под бренд Sky).

[836] Qin et al., IMC '21, разд. 4.3.1 и рис. 5.

[837] MakerDAO Forum, «Black Thursday Response Thread», 12.03.2020 (с последующими сводками созвонов), https://forum.skyeco.com/t/black-thursday-response-thread/1433 (бывш. forum.makerdao.com).

[838] MakerDAO Forum, «Black Thursday Response Thread», 12.03.2020 (с последующими сводками созвонов), https://forum.skyeco.com/t/black-thursday-response-thread/1433 (бывш. forum.makerdao.com).

[839] MakerDAO Forum, «Black Thursday Response Thread», 12.03.2020: «only one keeper continued triggering liquidations, and bidding 0$ for the ETH, with no competition. This situation lasted around 2/3hours.» Это оперативные записи участников; итоговый отчёт MakerDAO о тех днях недоступен. По всемирному времени падение пришлось на 12–13 марта (MakerDAO Forum, «Black Thursday Response Thread», 12.03.2020 (с последующими сводками созвонов), https://forum.skyeco.com/t/black-thursday-response-thread/1433 (бывш. forum.makerdao.com); Qin et al., IMC '21, разд. 4.3.1 и рис. 5). Аукцион MKR: 20 980 токенов за 5,3 млн DAI, 19–28 марта 2020 года (The Block, «In a first, MakerDAO protocol to auction MKR tokens to cover $4M bad debt», 03.2020, https://www.theblock.co/post/58606/in-a-first-makerdao-protocol-to-auction-mkr-tokens-to-cover-4m-bad-debt; Blockonomi, «MakerDAO Emergency Auctions Conclude with 5.3 Million Dai Raised», 02.04.2020, https://blockonomi.com/makerdao-emergency-5-million-dai-raised/).

[840] Qin et al., IMC '21, разд. 1, 4.2, табл. 1.

[841] CoinDesk, «MakerDAO Users Hosed by March Flash Crash Won't Get MKR Payouts, Say MKR Whales», 23.09.2020 (обновлено 12.2022), https://www.coindesk.com/tech/2020/09/23/makerdao-users-hosed-by-march-flash-crash-wont-get-mkr-payouts-say-mkr-whales.

продали, а выданные под него DAI остались в обращении без обеспечения, и резерв системы ушёл в минус примерно на 4 млн долларов (по более поздним пересказам — до 5,7 млн)[842]. Дыру закрыли первым в истории протокола долговым аукционом. С 19 по 28 марта система выпустила и продала почти 21 000 новых MKR за 5,3 млн DAI[843].

Дальше решали люди. В сентябре 2020 года держатели MKR проголосовали по вопросу компенсации тем, кто потерял залог. 65% голосов было подано за то, чтобы не платить ничего, а голосовали всего 38 адресов[844]. CoinDesk обратил внимание на конфликт интересов: компенсацию пришлось бы оплатить новым выпуском MKR, то есть из кармана тех же голосующих[845]. Решение о потерях клиентов в системе, которую называют децентрализованной, приняли несколько десятков крупных держателей одного токена.

Урок чёрного четверга касается любой автоматической продажи залога. Она защищает кредитора, только если в панике находятся покупатели и сеть успевает записывать их заявки. Те же два условия нужны и на обычной бирже, когда брокер требует довнести залог и продаёт позицию клиента. В чёрный четверг не выполнилось ни одно из двух.

UST обходился и без залога. Компания Terraform Labs, по иску Комиссии по ценным бумагам и биржам США, продвигала его как монету, привязку которой к доллару держит возможность обменять её на другой токен той же системы, LUNA, и рекламировала доходность до 20% годовых через протокол Anchor[846]. Лавочника здесь нет, сундука тоже, а строчку «один доллар» обещают обменять на строчку другого сорта, которая стоит столько, сколько за неё готовы дать.

В мае 2021 года привязка сорвалась. В 2025 году глава компании До Квон признал, что скрыл от инвесторов роль торговой фирмы в её восстановлении; по версии обвинения, фирма по тайной договорённости с ним скупала UST[847]. Через год привязка сорвалась снова, и механизм рухнул целиком. Инвесторы, по данным прокуратуры, потеряли около 40 млрд долларов, а в декабре 2025 года Квона приговорили к 15 годам заключения[848]. Как шло это обрушение, мы разберём во второй части.

«Синтетический доллар» USDe компании Ethena, по описанию самой компании, обеспечен криптовалютой и соответствующими ставками на её падение[849]. Если компания держит эфир на 100 долларов и одновременно ставку на то, что эфир подешевеет, на те же 100, рост и падение цены гасят друг друга. Доход держателям идёт в первую очередь из платы, которую платят участники, играющие на рост в долг, тем, кто держит обратную позицию[850].[851] Пока желающих играть в долг много, доход высок; когда их становится мало, он падает.

---

[842] MakerDAO Forum, «Black Thursday Response Thread», 12.03.2020 (с последующими сводками созвонов), https://forum.skyeco.com/t/black-thursday-response-thread/1433 (бывш. forum.makerdao.com); The Block, «In a first, MakerDAO protocol to auction MKR tokens to cover $4M bad debt», 03.2020, https://www.theblock.co/post/58606/in-a-first-makerdao-protocol-to-auction-mkr-tokens-to-cover-4m-bad-debt; Blockonomi, «MakerDAO Emergency Auctions Conclude with 5.3 Million Dai Raised», 02.04.2020, https://blockonomi.com/makerdao-emergency-5-million-dai-raised/.

[843] The Block, «In a first, MakerDAO protocol to auction MKR tokens to cover $4M bad debt», 03.2020, https://www.theblock.co/post/58606/in-a-first-makerdao-protocol-to-auction-mkr-tokens-to-cover-4m-bad-debt; Blockonomi, «MakerDAO Emergency Auctions Conclude with 5.3 Million Dai Raised», 02.04.2020, https://blockonomi.com/makerdao-emergency-5-million-dai-raised/.

[844] CoinDesk, 23.09.2020.

[845] CoinDesk, 23.09.2020.

[846] SEC, Press Release 2023-32, «SEC Charges Terraform and CEO Do Kwon with Defrauding Investors in Crypto Schemes», 16.02.2023, https://www.sec.gov/news/press-release/2023-32.

[847] U.S. DOJ, SDNY, «Do Kwon Pleads Guilty To Fraud», 08.2025, https://www.justice.gov/usao-sdny/pr/do-kwon-pleads-guilty-fraud.

[848] U.S. DOJ, SDNY, «Crypto-Enabled Fraudster Sentenced For Orchestrating $40 Billion Fraud», 12.2025, https://www.justice.gov/usao-sdny/pr/crypto-enabled-fraudster-sentenced-orchestrating-40-billion-fraud.

[849] Ethena, «Ethena Overview», https://docs.ethena.fi/overview/ethena-overview.md (открыто 26.09.2026).

[850] Ethena, «Ethena Overview», https://docs.ethena.fi/overview/ethena-overview.md (открыто 26.09.2026).

[851] Речь о так называемых бессрочных фьючерсах, где ставка финансирования (фандинг) периодически переводит пла-

10–11 октября 2025 года, когда за сутки было принудительно закрыто позиций, взятых в долг, больше чем на 19 млрд долларов по публичным данным, USDe на бирже Binance на время подешевел до 65 центов, и аналитики CoinDesk считают, что это стало дополнительным толчком к принудительным продажам[852].[853] Монету, которую на этой бирже принимали в залог как доллар, внезапно стали оценивать в две трети доллара, и залог, который должен был страховать кредиторов, сам начал подгонять распродажу.

Кредитный котёл

Займы под залог в DeFi, то есть в «децентрализованных финансах» (так называют финансовые сервисы, собранные из смарт-контрактов), устроены проще, чем DAI. В кредитных сервисах вроде Aave и Compound кредиторы вносят монеты в общий котёл, которым управляет контракт, и получают проценты. Заёмщики берут из котла в долг под залог, который стоит больше долга. Сверхобеспечение здесь необходимость, потому что личность заёмщика никто не проверяет и взыскать долг иначе, чем продав залог, контракт не может[854].

В таком котле есть деталь, которая роднит его с банком больше, чем кажется. Залог заёмщика не лежит без дела. Контракт выдаёт в долг и его, так что каждый заёмщик автоматически становится ещё и кредитором[855], а одна и та же монета служит залогом по одному займу и вкладом, из которого выдают другой. С банком первой главы есть и различие. Банк выдавал кредит, создавая новую строчку, а котёл может выдать только то, что в него положили. Новые строчки в долг в DeFi пишут автоматы вроде того, что выдаёт DAI.

Процентную ставку назначает сам контракт, глядя на то, сколько денег в котле, и чем больше из него заняли, тем дороже новый заём[856]. У этого решения интересное следствие. Цену денег в котле определяет загрузка котла, центрального банка над ним нет, и цена мгновенно реагирует на спрос. Когда все хотят занимать, ставка взлетает; когда желающих нет, она падает почти до нуля.

Переведём это в пятнадцатое правило посёлка. Дворы складывают свои строчки в общий котёл автомата и получают за это плату. Другие дворы берут из котла в долг, оставляя в автомате залог дороже долга. Если залог дешевеет ниже порога, любой житель может погасить часть чужого долга и забрать соответствующую часть залога со скидкой. Хранителя, который знает заёмщика в лицо и может подождать до осени, в этом правиле нет. Есть порог, скидка и первый, кто успел.

Состояние займа описывает одно число, «коэффициент здоровья», то есть отношение того, сколько можно занять под залог, к тому, сколько занято. Пока оно не ниже единицы, заём в порядке. Когда опускается ниже, заём открыт для ликвидации, и любой желающий может погасить часть долга и забрать залог со скидкой[857]. На момент исследования 2021 года Aave

---

тёж от одной стороны к другой: когда цена бессрочного фьючерса выше биржевой, платят покупатели с плечом, когда ниже — продавцы. Ethena называет среди источников дохода также кредитование и короткие государственные бумаги в токенизированном виде, так что при падении спроса на плечо доход скорее снижается, чем исчезает (Ethena, «Ethena Overview», https://docs.ethena.fi/overview/ethena-overview.md (открыто 26.09.2026)). Ethena, «Ethena Overview»: «USDe is a synthetic dollar, backed with crypto assets and corresponding short futures positions.»

[852] CoinDesk Research, «Market Spotlight: Inside Crypto's $19 Billion Liquidation Event», https://www.coindesk.com/research/market-spotlight-the-19-billion-liquidation-that-shook-crypto.

[853] CoinDesk Research: «On Binance, stablecoin USDe fell to $0.65, acting as a secondary trigger that forced liquidations». Падение было локальным: на других площадках отклонение было меньше, и «USDe стоил 65 центов» везде сказать нельзя (CoinDesk Research, «Market Spotlight: Inside Crypto's $19 Billion Liquidation Event», https://www.coindesk.com/research/market-spotlight-the-19-billion-liquidation-that-shook-crypto).

[854] Qin et al., IMC '21, разд. 1, 3.1.

[855] Qin et al., IMC '21, разд. 1, 3.1.

[856] Qin et al., IMC '21, разд. 3.3.

[857] Qin et al., IMC '21, разд. 2.3, 3.2; Aave, «Liquidations» (Aave v4 docs), https://aave.com/docs/concepts/liquidations.

позволял за одну операцию погасить не больше половины долга и получить залог со скидкой от 5 до 15% в зависимости от монеты[858].

Допустим, вы вносите в котёл эфир на 1500 долларов и берёте под него 1000 долларов в стейблкоинах. Пусть правила котла разрешают занять под эфир до 80% его цены (числа условные, у настоящих сервисов свои). Коэффициент здоровья равен 1500 × 0,8 / 1000, то есть 1,2. Если эфир подешевеет чуть больше чем на шестую часть, залог будет стоить меньше 1250 долларов, коэффициент опустится ниже единицы, и ваш заём откроется для ликвидации. Кто-то погасит за вас 500 долларов долга и заберёт эфира примерно на 550 (500 и ещё 10% скидки). Долг уменьшится на 500, а залог на 550, и эти 50 долларов разницы — плата за то, что вы не успели.

Тот же пример показывает, чем заёмщик, который переживает спад, отличается от того, кто его не переживает. Возьмите под тот же эфир 500 долларов вместо 1000, и коэффициент здоровья будет 2,4. Тогда до ликвидации эфиру придётся подешеветь больше чем вдвое, тогда как заём на 1000 выдерживал падение лишь на шестую часть. Сколько брать, решаете вы, но цена решения видна заранее: чем ближе коэффициент к единице, тем меньшее движение цены отнимает залог.

Теперь добавим к примеру то, ради чего такие займы чаще всего и берут. Если вы уверены, что эфир подорожает, вы берёте 1000 долларов в стейблкоинах, покупаете на них ещё эфира, вносите его в котёл как залог, под него снова занимаете и снова покупаете. Через несколько кругов эфира у вас намного больше, чем вы могли бы купить на свои деньги, и разница взята в долг. Это и есть кредитное плечо. Исследователи прямо называют кредитование в DeFi популярным способом получить плечо[859].[860]

[858] Qin et al., IMC ’21, разд. 3.3.

[859] Qin et al., IMC ’21, разд. 2.2.

[860] Qin K. et al. An Empirical Study of DeFi Liquidations: Incentives, Risks, and Instabilities. ACM IMC ’21, 2021: «Lending and borrowing is a popular way to realize a leverage use case in DeFi.» Пример авторов обратный моему: трейдер вносит в залог 5000 USDT, занимает 1 ETH и продаёт его, рассчитывая выкупить дешевле (Qin et al., IMC ’21, разд. 2.2).

Рисунок 5.2. Петля плеча в кредитном котле

Если так поступают многие, из отдельных займов складывается та самая петля, которую мы собрали в первой главе. Эфир дорожает, залог растёт, под него занимают больше, на заёмные деньги покупают ещё эфира, и цена растёт дальше. На спаде петля крутится обратно. Эфир дешевеет, займы по очереди проходят порог, ликвидаторы продают залог, продажи давят на цену, и порог проходят следующие займы. С апреля 2019 по апрель 2021 года на четырёх крупнейших кредитных сервисах Ethereum прошло 28 138 ликвидаций, по которым было продано залога на 807 млн долларов[861].[862]

У каждой ликвидации есть получатель скидки. Ликвидаторов за те два года было около двух тысяч адресов, среди них программы, которые следят за займами и первыми гасят те, что прошли порог[863]. Исследователи показали, что фиксированная скидка выгодна ликвидаторам за счёт заёмщиков[864]. В марте 2020 года прибыль ликвидаторов MakerDAO за месяц составила 13,13 млн долларов, и авторы объясняют этот всплеск тем же чёрным четвергом, когда залог

[861] Qin et al., IMC ’21, разд. 1, 4.2, табл. 1.

[862] Там же. Aave, Compound, dYdX и MakerDAO вместе занимали больше 85% кредитного рынка Ethereum; ликвидаторов было 2011 разных адресов (Qin et al., IMC ’21, разд. 1, 4.2, табл. 1).

[863] Qin et al., IMC ’21, разд. 1, 4.2, табл. 1.

[864] K. Qin, L. Zhou, P. Gamito, P. Jovanovic, A. Gervais, «An Empirical Study of DeFi Liquidations: Incentives, Risks, and Instabilities», ACM IMC ’21, 2021, https://arxiv.org/abs/2106.06389 (DOI 10.1145/3487552.3487811).

уходил почти даром[865]. Чем глубже и быстрее обвал, тем больше заработок тех, кто продаёт чужой залог.

На этом месте модель посёлка ломается, и, по-моему, разрыв здесь объясняет больше, чем сходство. Хранитель в посёлке мог подождать до осени, договориться с должником или попросить помощи у главного хранителя.

Автомату не у кого просить.

Аналитики Банка международных расчётов в 2021 году объясняли, почему у DeFi нет амортизаторов. В обычных финансах банк в трудный день может выдавать кредиты и покупать проблемные активы, потому что у него есть доступ к центральному банку, а стейблкоины при плохом управлении рисками подвержены панике изъятий[866]. Уязвимости DeFi они назвали серьёзными из-за высокого плеча, несовпадения сроков (вкладчик вправе забрать деньги в любую минуту, а выданные из котла займы разом не вернуть), взаимной связанности сервисов и отсутствия способности поглощать удары[867].[868]

Чья-то плата под названием «доходность»

Любая доходность в DeFi — это чьи-то деньги, и полезно каждый раз спрашивать, чьи. Источников немного. Проценты кредиторам платят заёмщики, и ставка растёт, когда занимать хотят многие[869]. Держателям USDe платят участники, играющие на рост в долг[870]. Третий источник — комиссии трейдеров на автоматических обменниках, и его стоит разобрать чуть подробнее.

Автоматический обменник вроде Uniswap устроен как котёл с двумя монетами. Контракт следит, чтобы произведение их количеств не уменьшалось, и из этого правила сама собой получается цена, равная отношению запасов двух монет в котле[871]. Если цена в котле отстаёт от рыночной, её выравнивают арбитражёры (торговцы, которые покупают там, где дешевле, и продают там, где дороже)[872]. В первых версиях Uniswap с каждой сделки трейдер платил 0,30%, и эти деньги шли тем, кто положил монеты в котёл[873].

Бесплатной эта плата не бывает. Когда цены двух монет расходятся, тот, кто положил монеты в котёл (его называют поставщиком ликвидности), оказывается не с тем набором монет, который внёс, и может получить меньше, чем если бы просто держал их у себя. Авторы Uniswap называют это «непостоянными потерями»[874]. Они же предупреждали, что цену из котла первой версии легко подделать, поэтому другим контрактам нельзя полагаться на неё как на источник данных[875]. Это та самая проблема оракула, с которой мы встретились в прошлой главе на истории Mango Markets (схема 4.4).

---

[865] Qin et al., IMC ’21, разд. 4.3.1 и рис. 5.

[866] BIS Quarterly Review, 06.12.2021.

[867] S. Aramonte, W. Huang, A. Schrimpf, «DeFi risks and the decentralisation illusion», BIS Quarterly Review, 06.12.2021, https://www.bis.org/publ/qtrpdf/r_qt2112b.htm.

[868] Aramonte S., Huang W., Schrimpf A. DeFi risks and the decentralisation illusion. BIS Quarterly Review, 06.12.2021: «DeFi’s vulnerabilities are severe because of high leverage, liquidity mismatches, built-in interconnectedness and the lack of shock-absorbing capacity.» Там же: «full decentralisation in DeFi is illusory» (S. Aramonte, W. Huang, A. Schrimpf, «DeFi risks and the decentralisation illusion», BIS Quarterly Review, 06.12.2021, https://www.bis.org/publ/qtrpdf/r_qt2112b.htm).

[869] Qin et al., IMC ’21, разд. 3.3.

[870] Ethena, «Ethena Overview», https://docs.ethena.fi/overview/ethena-overview.md (открыто 26.09.2026).

[871] H. Adams, N. Zinsmeister, D. Robinson, «Uniswap v2 Core», март 2020, https://app.uniswap.org/whitepaper.pdf (с. 1); «Uniswap v2 Core», разд. 2.2.

[872] «Uniswap v2 Core», разд. 2.2.

[873] H. Adams, N. Zinsmeister, D. Robinson, «Uniswap v2 Core», март 2020, https://app.uniswap.org/whitepaper.pdf (с. 1).

[874] «Uniswap v2 Core», разд. 2.1.

[875] «Uniswap v2 Core», разд. 2.2.

Остаётся четвёртый источник, самый опасный: доходность, за которой не стоит ничей платёж, кроме денег новых вкладчиков или чужой беды. 20% годовых, которые Anchor обещал держателям UST, по версии обвинения, были частью мошеннической схемы[876]. Свежий пример — Stream Finance. Её токен xUSD, тоже «синтетический доллар» с доходностью, широко принимали как залог в других кредитных сервисах, и, по оценке независимого аналитика, займы под залог, связанный со Stream, вероятно, превышали 280 млн долларов[877]. 4 ноября 2025 года платформа сообщила, что внешний управляющий её средствами раскрыл убыток около 93 млн долларов, и приостановила вклады и выводы[878]. xUSD быстро упал ниже половины номинала[879].

Версия самой компании ведёт к тому же октябрьскому дню. В декабре 2025 года Stream подала иск, в котором утверждает, что 10 октября управляющий получил требование довнести залог по личному займу, денег не нашёл, его позицию закрыли, и тогда он покрыл свой убыток активами протокола[880]. Это утверждения истца, суд их не установил. Если они подтвердятся, получится цепочка из трёх звеньев: личное плечо одного человека, «доллар» протокола, который принимали как залог чужие протоколы, и займы третьих лиц под этот залог.

Централизованные посредники устроены иначе, но в главном похожи. Celsius предлагал клиентам процентные счета, а в январе 2023 года суд по делу о его банкротстве решил, что монеты на этих счетах по условиям договора перешли в собственность компании и вошли в конкурсную массу[881]. Клиент, думавший, что держит вклад, оказался кредитором компании без всякого обеспечения.

Кто в итоге платит всю эту доходность? Аналитики Банка международных расчётов в 2021 году писали, что DeFi пока служит главным образом спекуляции, вложениям и арбитражу в самих криптоактивах и почти не касается реальной экономики[882]. Если это так, то заёмщики платят проценты потому, что хотят играть в долг, трейдеры платят комиссии потому, что хотят торговать, а желание играть и торговать растёт вместе с ценами и пропадает вместе с ними. Поэтому доходности в DeFi высоки на подъёме и тают на спаде, как и сам кредит.

Отсюда простое упражнение для любой обещанной доходности. Назовите, кто её платит: заёмщик, трейдер, игрок с плечом или никто. Если платит заёмщик или трейдер, прикиньте, захочет ли он платить столько же, когда рынок упадёт на треть. Если платит игрок с плечом, вы зарабатываете на чужом долге и разделите его судьбу, как те, кто держал USDe залогом на Binance в октябре 2025 года. Если же плательщика назвать не удаётся, я не стал бы класть туда деньги, какой бы высокой ни была цифра, потому что у доходности без плательщика остаётся один источник, деньги тех, кто придёт после вас.

Размер всего этого хозяйства обычно меряют одним числом, TVL (от английского total value locked, «сколько всего заблокировано» в контрактах). Это оценка, и бухгалтерской точности от неё ждать не стоит. Агрегаторы считают его по методикам, которые пишут сами участники сообщества, и единого стандарта нет. Исследователи, среди которых были сотрудники Банка международных расчётов, построили проверяемую версию метрики без двойного счёта,

---

[876] SEC, Press Release 2023-32, «SEC Charges Terraform and CEO Do Kwon with Defrauding Investors in Crypto Schemes», 16.02.2023, https://www.sec.gov/news/press-release/2023-32.

[877] CoinDesk, 04.11.2025.

[878] CoinDesk, «Stream Finance Faces $93 Million Loss, Launches Legal Investigation», 04.11.2025, https://www.coindesk.com/markets/2025/11/04/stream-finance-faces-usd93-million-loss-launches-legal-investigation.

[879] CoinDesk, 04.11.2025.

[880] DL News, «Stream Finance founders sue business partner, allege $93m used to cover personal losses», 11.12.2025, https://www.dlnews.com/articles/defi/stream-finance-founders-sue-partner-over-alleged-93m-loss/.

[881] Morrison Foerster, 2023, https://www.mofo.com/resources/insights/230109-celsius-bankruptcy-court-customer-deposits-earn-accounts.

[882] S. Aramonte, W. Huang, A. Schrimpf, «DeFi risks and the decentralisation illusion», BIS Quarterly Review, 06.12.2021, https://www.bis.org/publ/qtrpdf/r_qt2112b.htm.

и её значения совпали с публикуемыми цифрами меньше чем у половины из 400 проверенных сервисов[883].[884]

Двойной счёт возникает просто. Вы вносите эфир в сервис А, получаете расписку, вносите расписку в сервис Б, и агрегатор видит две суммы там, где эфир один. А если эфир подешевеет вдвое, TVL упадёт вдвое, хотя из сервисов никто не ушёл. Я пользуюсь этим числом как грубым ориентиром размера и никогда не читаю его рост как приток новых денег, пока не посмотрю, что за это время было с ценами.

Сундук на меже: мосты

У посёлка есть сосед со своей тетрадкой, и жителям хочется, чтобы их строчки ходили и там. Прямо переписать строчку из одной тетрадки в другую нельзя, потому что тетрадки ничего друг о друге не знают. Тогда на меже ставят сундук. Житель запирает свою строчку в сундук на стороне посёлка, а в соседней тетрадке ему пишут расписку «в сундуке заперто столько-то», и расписка ходит у соседей. Это шестнадцатое правило: строчка в одной тетрадке может означать монету, запертую в сундуке в другой.

Нужда в сундуках выросла вместе с числом тетрадок. Блокчейнов стало много, над ними появились сети второго уровня, о которых шла речь в третьей главе, и деньги в каждой из них хотят переводить в другие. Биткоин, например, нельзя положить в котёл на Ethereum, пока кто-то не запрёт его в сундук и не выпишет на Ethereum расписку. Каждая такая расписка — обещание того, кто сторожит сундук.

Мосты между блокчейнами устроены так же, и слабое место у них то же. Аналитики Chainalysis объясняют, почему мосты так часто грабят. У моста обычно есть одно хранилище монет, которые обеспечивают «перенесённые» монеты в другой сети, в контракте или у тех, кто держит от него ключи, а как построить надёжный мост, никто пока толком не знает[885]. По подсчёту компании на 2 августа 2022 года, в 13 взломах мостов было украдено около 2 млрд долларов, большая часть в том же году, и на мосты пришлось 69% всего украденного в 2022 году к тому дню[886]. Украли содержимое сундука, и расписки на него обесценились.

Сундук можно ограбить тремя способами, и каждый был опробован. Можно завладеть ключами сторожей (взломщик Poly Network из прошлой главы, например, записал вместо них свой). Можно обмануть сторожа, чтобы он признал несуществующий вклад. И можно сломать замок так, что сундук откроется любому.

Мост сети Ronin, созданной для игры Axie Infinity, открывался подписями пяти из девяти сторожей-валидаторов. 23 марта 2022 года из него вывели 173 600 ETH и 25,5 млн USDC, около 540 млн долларов по тогдашнему курсу[887]. Четыре ключа атакующий получил у компании Sky Mavis, разработчика игры, а пятую подпись — через старое разрешение. В ноябре

---

[883] P. Saggese, M. Fröwis, S. Kitzler, B. Haslhofer, R. Auer, «Towards verifiability of total value locked (TVL) in decentralized finance», BIS Working Paper 1268, 14.05.2025, https://www.bis.org/publ/work1268.htm.

[884] Saggese P., Fröwis M., Kitzler S., Haslhofer B., Auer R. Towards verifiability of total value locked (TVL) in decentralized finance. BIS Working Paper 1268, 14.05.2025: «A case study on 400 protocols shows that our estimations align with published figures for 46.5% of protocols». Порог совпадения в работе численно не задан. Из 939 изученных протоколов на Ethereum 10,5% зависят от внешних серверов (P. Saggese, M. Fröwis, S. Kitzler, B. Haslhofer, R. Auer, «Towards verifiability of total value locked (TVL) in decentralized finance», BIS Working Paper 1268, 14.05.2025, https://www.bis.org/publ/work1268.htm).

[885] Chainalysis, 02.08.2022.

[886] Chainalysis, «Vulnerabilities in Cross-chain Bridge Protocols Emerge as Top Security Risk», 02.08.2022, https://www.chainalysis.com/blog/cross-chain-bridge-hacks-2022/.

[887] Elliptic, «$540 Million Stolen from the Ronin DeFi Bridge», 2022, https://www.elliptic.co/blog/540-million-stolen-from-the-ronin-defi-bridge; CoinDesk, 14.04.2022, https://www.coindesk.com/policy/2022/04/14/us-officials-tie-north-korean-hacker-group-to-axies-ronin-exploit.

2021 года ещё один сторож разрешил Sky Mavis подписывать от своего имени, в декабре эту практику прекратили, но разрешение так и не отозвали[888].

Начался взлом, по сообщениям прессы, с фальшивого предложения работы. Старшему инженеру прислали «оффер» в PDF, и файл заразил его компьютер[889]. Кражу заметили только через шесть дней, когда у пользователя не прошёл вывод 5000 ETH[890].[891] Всё это время транзакции вывода лежали в открытой тетрадке на виду у каждого, кто держит её копию. Прозрачность, о которой шла речь во второй главе, ничего не стоит, если в тетрадку никто не смотрит.

Мост Wormhole между Solana и Ethereum в феврале 2022 года обманули. Из-за ошибки в проверке подписей он признал 120 000 ETH внесёнными на стороне Ethereum, которых там не было, и позволил выпустить на Solana столько же расписок без обеспечения, примерно на 326 млн долларов[892].

Мост Nomad в августе 2022 года открылся всем. При плановом обновлении контракта ошибочная настройка заставила его считать любое сообщение подлинным, и за два с половиной часа мост опустел примерно на 190 млн долларов[893]. Первая успешная транзакция вывела 100 WBTC (биткоинов, «обёрнутых» для сети Ethereum) без всяких хитрых приёмов, и за ней последовало больше 300 адресов, которые просто копировали её, подставляя свой адрес[894]. Около 80% добычи унёс 41 адрес[895].

Сундук на меже доверили нескольким ключам или одной строке настроек, и тетрадка без хозяина тут ничем не помогла, потому что сундук стоит снаружи неё. Интереснее всего, чем кончились эти истории. Недостачу Wormhole уже 3 февраля восполнила Jump Trading, владелец компании-разработчика, вернув в сундук 120 000 ETH[896].[897] Sky Mavis пообещала вернуть

---

[888] Sky Mavis / Ronin, «Community Alert: Ronin Validators Compromised», 29.03.2022, — цитаты по сводке tayvano, «lazarus-bluenoroff-research: ronin_bridge.md», https://github.com/tayvano/lazarus-bluenoroff-research/blob/main/hacks-and-thefts/ronin_bridge.md; постмортем «Back to Building: Ronin Security Breach Postmortem», 27.04.2022 — только сводка на lazarus.day, https://lazarus.day/reports/back-to-building-ronin-security-breach-postmortem-bbMOK/.

[889] The Hacker News, «Hackers Used Fake Job Offer to Hack and Steal $540 Million from Axie Infinity», 07.2022, https://thehackernews.com/2022/07/hackers-used-fake-job-offer-to-hack-and.html (со ссылкой на расследование The Block).

[890] Elliptic, «$540 Million Stolen from the Ronin DeFi Bridge», 2022, https://www.elliptic.co/blog/540-million-stolen-from-the-ronin-defi-bridge; CoinDesk, 14.04.2022, https://www.coindesk.com/policy/2022/04/14/us-officials-tie-north-korean-hacker-group-to-axies-ronin-exploit.

[891] ФБР и Минфин США 14.04.2022 связали кражу с группой Lazarus, которую связывают с КНДР (Elliptic, «$540 Million Stolen from the Ronin DeFi Bridge», 2022, https://www.elliptic.co/blog/540-million-stolen-from-the-ronin-defi-bridge; CoinDesk, 14.04.2022, https://www.coindesk.com/policy/2022/04/14/us-officials-tie-north-korean-hacker-group-to-axies-ronin-exploit). Оценки в долларах разнятся (540, 615, 625 млн) из-за курса эфира на дату. Сообщение Sky Mavis 29.03.2022 и её разбор взлома доступны только в цитатах исследовательских архивов; история с «оффером» — по публикации The Hacker News со ссылкой на расследование The Block (Sky Mavis / Ronin, «Community Alert: Ronin Validators Compromised», 29.03.2022, — цитаты по сводке tayvano, «lazarus-bluenoroff-research: ronin_bridge.md», https://github.com/tayvano/lazarus-bluenoroff-research/blob/main/hacks-and-thefts/ronin_bridge.md; постмортем «Back to Building: Ronin Security Breach Postmortem», 27.04.2022 — только сводка на lazarus.day, https://lazarus.day/reports/back-to-building-ronin-security-breach-postmortem-bbMOK/; The Hacker News, «Hackers Used Fake Job Offer to Hack and Steal $540 Million from Axie Infinity», 07.2022, https://thehackernews.com/2022/07/hackers-used-fake-job-offer-to-hack-and.html (со ссылкой на расследование The Block)). По оценке Chainalysis, связанные с КНДР хакеры с начала 2022 года до августа украли около 1 млрд долларов, целиком из мостов и других сервисов DeFi (Chainalysis, «Vulnerabilities in Cross-chain Bridge Protocols Emerge as Top Security Risk», 02.08.2022, https://www.chainalysis.com/blog/cross-chain-bridge-hacks-2022/).

[892] rekt.news, «Wormhole — REKT», 2022, https://rekt.news/wormhole-rekt/.

[893] rekt.news, «Nomad Bridge — REKT», 2022, https://rekt.news/nomad-rekt/; Chainalysis, 02.08.2022 (дата).

[894] The Block, «Nomad's $190 million bridge exploit drew hacking feeding frenzy of 300 addresses», 08.2022, https://www.theblock.co/post/160851/nomads-190-million-bridge-exploit-drew-hacking-feeding-frenzy-of-300-addresses.

[895] The Block, «Nomad's $190 million bridge exploit drew hacking feeding frenzy of 300 addresses», 08.2022, https://www.theblock.co/post/160851/nomads-190-million-bridge-exploit-drew-hacking-feeding-frenzy-of-300-addresses.

[896] CoinDesk, «Jump Trading Backstops Wormhole's $320M Exploit Loss», 03.02.2022, https://www.coindesk.com/business/2022/02/03/jump-trading-backstops-wormholes-320m-exploit-loss-sources; твит Jump Crypto, https://x.com/jump_/status/1489301013408497666.

[897] CoinDesk, 03.02.2022. Jump Crypto: «That's why we replaced 120k ETH to make community members whole and support Wormhole now as it continues to develop.» Компанию-разработчика Certus One Jump купила в августе 2021 года (CoinDesk,

деньги всем пострадавшим от взлома Ronin, собрала для этого раунд инвестиций, а в итоге заплатила пользователям в основном из собственных средств[898]. В обоих случаях систему, которая обходилась без доверия, спас частный владелец с деньгами. В обычных финансах эту роль называют кредитором последней инстанции, и играет её центральный банк.

Образ автомата, которому не у кого просить, после этих историй стоит уточнить. Держатели MKR в чёрный четверг закрыли дыру потому, что так было записано в правилах самой системы, и заплатили размыванием своей доли, как акционеры банка. Jump и Sky Mavis пришли сами, потому что им было что терять и было чем платить. Обязанности спасать не было ни у кого из них, и следующий сундук вполне может остаться без спасителя. Центральный банк держит эту роль для всей системы, а частный спаситель решает сам и спасает то, что считает своим.

Весной 2026 года мост и кредитный котёл сошлись в одной истории. 19–20 апреля из моста KelpDAO похитили около 292 млн долларов в токенах rsETH (это расписки на эфир, который KelpDAO держит в залоге за своих клиентов), а затем использовали украденные токены как залог и взяли под них займы в кредитных сервисах, прежде всего в Aave[899]. Сам Aave никто не взламывал, но вкладчики не стали ждать, чем кончится дело: за двое суток они вывели из него 8,45 млрд долларов, а общий TVL DeFi упал с 99,5 до 86,3 млрд[900].

Кто-то принёс в автомат расписки на опустевший соседский сундук и занял под них настоящие строчки, а дворы, узнав об этом, бросились забирать свои строчки из котла, пока там ещё что-то есть. Это та же паника вкладчиков, что у лавки с неполным сундуком, только в котле без банкира.

Кредит, который дышит вместе с ценой

Теперь можно сложить части. Объём кредитов под криптовалютный залог считает Galaxy Research, аналитическое подразделение компании, которая сама работает на этом рынке кредитором. В её подсчёт входят централизованные кредиторы, займы в DeFi и стейблкоины, выпущенные под залог, как DAI. Galaxy пересматривает свои ряды задним числом, поэтому цифры разных выпусков отчёта складывать нельзя[901].[902] Весь ряд ниже я беру из выпуска августа 2026 года, по нему же построен рис. 5.3.

«Jump Trading Backstops Wormhole's $320M Exploit Loss», 03.02.2022, https://www.coindesk.com/business/2022/02/03/jump-trading-backstops-wormholes-320m-exploit-loss-sources; твит Jump Crypto, https://x.com/jump_/status/1489301013408497666).

[898] Axie Infinity (Sky Mavis), «Sky Mavis Raises $150M Led By Binance, Funds to be Restored on the Ronin Bridge», 06.04.2022, https://blog.axieinfinity.com/p/funding.

[899] CoinDesk, 20.04.2026, https://www.coindesk.com/markets/2026/04/20/defi-tvl-drops-more-than-usd13-billion-in-two-days-following-kelp-dao-hack (данные DefiLlama).

[900] CoinDesk, 20.04.2026, https://www.coindesk.com/markets/2026/04/20/defi-tvl-drops-more-than-usd13-billion-in-two-days-following-kelp-dao-hack (данные DefiLlama).

[901] Galaxy Research, «The State of Crypto Lending», 14.04.2025, https://www.galaxy.com/insights/research/the-state-of-crypto-lending/.

[902] Galaxy Research — участник рынка кредитования, методика раскрыта в отчётах. Ряд в тексте и на рис. 5.3 — из выпуска «The State of Crypto Leverage – Q2 2026» (17.08.2026): пик IV квартала 2021 года — около 73,8 млрд долларов, дно 2022–2023 годов — около 19 млрд, пик III квартала 2025 года — 78,69 млрд, II квартал 2026 года — 56,16 млрд. Таблицей Galaxy ряд не публикует; значения 2021–2023 годов сняты с графика отчёта с точностью около ±0,5 млрд, точные цифры — только те, что названы в тексте отчёта (Galaxy Research, «The State of Crypto Leverage – Q2 2026: An Orderly, Measured Decline», 17.08.2026, https://www.galaxy.com/insights/research/crypto-leverage-report-q2-2026-defi-lending-decline-futures-open-interest). Тот же пик 2021 года в прежних выпусках: 64,4 млрд (апрель 2025 года; там же минимум III квартала 2023 года — 14,2 млрд, спад на 78%) и 69,37 млрд (ноябрь 2025 года) (Galaxy Research, «The State of Crypto Lending», 14.04.2025, https://www.galaxy.com/insights/research/the-state-of-crypto-lending/; Galaxy Research, «The State of Crypto Leverage – Q3 2025», 19.11.2025, https://www.galaxy.com/insights/research/crypto-leverage-q3-2025-defi-cefi-lending-digital-asset-treasury-debt-futures-perpetuals). Пик 2025 года тоже пересматривали: сначала 73,59 млрд, потом 78,67–78,69 млрд (Galaxy Research, «The State of Crypto Leverage – Q3 2025», 19.11.2025, https://www.galaxy.com/insights/research/crypto-leverage-q3-2025-defi-cefi-lending-digital-asset-treasury-debt-futures-perpetuals; Galaxy Research, Q1 2026; Galaxy Research, «The

В этом выпуске объём таких кредитов достиг первого пика в последнем квартале 2021 года, около 74 млрд долларов, а к 2023 году сжался примерно на три четверти[903]. Весь рынок криптовалют за тот спад подешевел примерно на столько же[904], так что кредит опускался вместе с ним и почти так же глубоко. Новый рекорд, выше пика 2021 года, пришёлся на третий квартал 2025 года, а к концу второго квартала 2026 года объём три квартала подряд снижался и стоял больше чем на четверть ниже вершины[905].[906] Вершины этого ряда совпадают с вершинами рынка 2021 и 2025 годов с точностью до квартала[907].

На этот раз спад идёт мягче, чем падает цена. Биткоин к концу того же квартала стоил больше чем вдвое дешевле своего пика[908], а кредит сократился только на четверть с небольшим. Сама Galaxy описала это снижение как спуск «по лестнице, а не на лифте»[909].[910]

State of Crypto Leverage – Q2 2026: An Orderly, Measured Decline», 17.08.2026, https://www.galaxy.com/insights/research/crypto-leverage-report-q2-2026-defi-lending-decline-futures-open-interest). Ошибки ни в одном из выпусков нет, данные просто пересчитали, поэтому цифры разных выпусков в книге не смешиваются.

[903] Galaxy Research, «The State of Crypto Leverage – Q2 2026: An Orderly, Measured Decline», 17.08.2026, https://www.galaxy.com/insights/research/crypto-leverage-report-q2-2026-defi-lending-decline-futures-open-interest.

[904] CoinDesk, «FTX Collapse Leaves Total Crypto Market Cap Under $800B…», 17.11.2022, https://www.coindesk.com/markets/2022/11/17/ftx-collapse-leaves-total-crypto-market-cap-under-800b-close-to-2022-low.

[905] Galaxy Research, «The State of Crypto Leverage – Q2 2026: An Orderly, Measured Decline», 17.08.2026, https://www.galaxy.com/insights/research/crypto-leverage-report-q2-2026-defi-lending-decline-futures-open-interest.

[906] Galaxy Research, «The State of Crypto Leverage – Q2 2026», 17.08.2026: 56,16 млрд долларов на конец II квартала 2026 года против пика 78,69 млрд; снижения по кварталам — примерно −10%, −5% и −17%. Galaxy пишет, что рынок «на 40,13% ниже» пика, но это ошибка в направлении счёта: (78,69 − 56,16) / 78,69 ≈ 28,6%, а 40% — это насколько пик выше нынешнего уровня. Ту же «сороковку» повторяют и другие издания (Galaxy Research, «The State of Crypto Leverage – Q2 2026: An Orderly, Measured Decline», 17.08.2026, https://www.galaxy.com/insights/research/crypto-leverage-report-q2-2026-defi-lending-decline-futures-open-interest). Свежие цифры — в приложении Б.

[907] CoinDesk, «FTX Collapse Leaves Total Crypto Market Cap Under $800B…», 17.11.2022, https://www.coindesk.com/markets/2022/11/17/ftx-collapse-leaves-total-crypto-market-cap-under-800b-close-to-2022-low; Forbes, 05.10.2025, https://www.forbes.com/sites/digital-assets/2025/10/05/bitcoin-breaks-125000-the-convergence-of-confidence-capital-code/; CoinDesk (многократные упоминания «record high of $126,000 reached last October», напр. 05.02.2026).

[908] Forbes, 05.10.2025, https://www.forbes.com/sites/digital-assets/2025/10/05/bitcoin-breaks-125000-the-convergence-of-confidence-capital-code/; CoinDesk (многократные упоминания «record high of $126,000 reached last October», напр. 05.02.2026); CoinDesk, 25.06.2026, https://www.coindesk.com/markets/2026/06/25/bitcoin-plunges-to-new-multi-year-low-of-usd58-000-but-a-short-squeeze-setup-emerges; CoinDesk, 01.07.2026, https://www.coindesk.com/markets/2026/07/01/bitcoin-s-20-june-crash-looks-even-deadlier-on-the-charts-here-s-why; CoinGecko, «2026 Q2 Crypto Industry Report», https://www.coingecko.com/research/publications/2026-q2-crypto-report.

[909] Galaxy Research, «The State of Crypto Leverage – Q2 2026: An Orderly, Measured Decline», 17.08.2026, https://www.galaxy.com/insights/research/crypto-leverage-report-q2-2026-defi-lending-decline-futures-open-interest.

[910] «taking the stairs down, not the elevator» (Galaxy Research, «The State of Crypto Leverage – Q2 2026: An Orderly, Measured Decline», 17.08.2026, https://www.galaxy.com/insights/research/crypto-leverage-report-q2-2026-defi-lending-decline-futures-open-interest).

Рисунок 5.3. Кредит под криптозалог по кварталам, 2021–2026 (Galaxy Research, выпуск 17.08.2026)

Кредит следует за ценой так послушно из-за устройства самого котла. Пусть правила по-прежнему разрешают занять 80% цены залога. Когда эфир дорожает, каждый лишний доллар в цене залога даёт право занять ещё 80 центов, и новый вкладчик для этого не нужен. Займы растут сами, вместе с ценой, а заёмные деньги уходят на покупку того же эфира и подталкивают цену дальше. На спаде связь работает несимметрично. Долг записан в стейблкоинах и сам не дешевеет, дешевеет только залог, и уменьшить долг можно лишь двумя способами: погасить его самому или дождаться, пока его погасит ликвидатор, продав ваш залог. Вверх кредит растёт по желанию заёмщиков и постепенно. Вниз его часто сжимают принудительно и у всех сразу, в те самые часы, когда покупателей меньше всего.

Плечо умножает эту волну для каждого, кто им пользуется. Возьмём условного заёмщика, который прошёл петлю из прошлого раздела три раза подряд. Он внёс эфира на 1000 долларов, занял 800, купил на них эфира и внёс его в котёл, занял под него ещё 640, снова купил и внёс. Эфира у него теперь на 2440 долларов, долга 1440, а своих денег по-прежнему 1000. Если эфир подорожает на десятую часть, его собственные деньги вырастут почти на четверть. Если подешевеет на четверть, от его тысячи останется меньше четырёхсот долларов, а коэффициент здоровья подойдёт к единице вплотную. Когда таких заёмщиков тысячи, их общий долг и складывается в ту кривую, которую рисует Galaxy.

Котлы при этом — меньшая часть криптовалютного плеча. Плечо дают и биржи, которые выдают клиентам займы на покупку и принимают ставки на рост или падение цены в долг, и

почти вся такая торговля идёт на централизованных биржах[911]. По оценке той же Galaxy, летом 2025 года открытые позиции на фьючерсах стоили около 133 млрд долларов, примерно в два с половиной раза больше всех кредитов под криптозалог[912].[913] На этом биржевом плече держатся и самые громкие истории второй части.

Состав кредиторов тоже показателен. В конце 2024 года на займы в DeFi вместе со стейблкоинами под залог приходилось 69% рынка против 34% в цикле 2020–2021 годов[914]. Среди централизованных кредиторов, которых отслеживает Galaxy, на конец марта 2026 года больше 60% займов приходилось на одну компанию, Tether[915]. Эмитент самого крупного цифрового доллара оказался и самым крупным частным кредитором под криптовалютный залог, так что вклады и кредиты снова собрались в одних руках, как в любом банке.

В 2022 году сжатие сопровождалось крахом крупных кредиторов, среди них Celsius[916]. В 2026-м, по оценке той же Galaxy, оно пока идёт спокойнее. Во втором квартале займы в DeFi сжимались почти втрое быстрее, чем у компаний-кредиторов, и у централизованных кредиторов впервые с 2023 года оказалось больше займов, чем в DeFi[917]. Механизм один, а насколько глубоким окажется спад, решают плечо и то, кто стоит на другом конце чужих долгов.

Где в этой конструкции самое слабое место? Я бы искал его в связях между автоматами. Код отдельных сервисов ломают, и мосты это показали, но самые неприятные истории этой главы начинались там, где «доллар» одного сервиса служил залогом в другом. Украденные расписки KelpDAO обернулись бегством вкладчиков из Aave[918], «синтетический доллар» Stream держал займы в чужих котлах[919], а просевший USDe сам подтолкнул принудительные продажи[920]. Аналитики Банка международных расчётов ещё в 2021 году назвали эту встроенную связанность одной из главных уязвимостей DeFi[921].

Из всего банковского хозяйства поверх тетрадки не выросли две вещи, страховка вкладов и центральный банк. В обычных деньгах они дают системе время. Вкладчику незачем бежать первым, а банку в трудный день есть у кого занять. У автомата с порогом ликвидации такого времени нет, и в крипте место этих двух опор занимают автоматическая продажа залога, которая волну ускоряет, и частные спасители, которые приходят, только если сами так решат.

---

[911] CoinGecko, «2025 Annual Crypto Industry Report» и «2026 Q2 Crypto Industry Report», https://www.coingecko.com/research/publications/2025-annual-crypto-report; https://www.coingecko.com/research/publications/2026-q2-crypto-report.

[912] Z. Pokorny, «The State of Crypto Leverage – Q2 2025», Galaxy Research, 14.08.2025, https://www.galaxy.com/insights/research/the-state-of-crypto-leverage-q2-2025.

[913] Galaxy Research, «The State of Crypto Leverage – Q2 2025», 14.08.2025: открытые позиции на фьючерсах — 132,6 млрд долларов (82% — бессрочные фьючерсы), кредиты под криптозалог — 53,1 млрд (Z. Pokorny, «The State of Crypto Leverage – Q2 2025», Galaxy Research, 14.08.2025, https://www.galaxy.com/insights/research/the-state-of-crypto-leverage-q2-2025). Меры разные: открытая позиция показывает размер ставок, а заёмных денег в ней меньше, так что сравнение говорит о масштабе, а не о точной доле долга. По CoinGecko, в 2025 году объём торгов бессрочными фьючерсами на централизованных биржах составил 86,2 трлн долларов, на децентрализованных — 6,7 трлн (CoinGecko, «2025 Annual Crypto Industry Report» и «2026 Q2 Crypto Industry Report», https://www.coingecko.com/research/publications/2025-annual-crypto-report; https://www.coingecko.com/research/publications/2026-q2-crypto-report). Свежие цифры — в приложении Б.

[914] Galaxy Research, 14.04.2025.

[915] Galaxy Research, «The State of Crypto Leverage – Q1 2026: DeFi Exploits, Price Declines, and Capital Flight», 21.05.2026, https://www.galaxy.com/insights/research/crypto-lending-leverage-q1-2026.

[916] Morrison Foerster, 2023, https://www.mofo.com/resources/insights/230109-celsius-bankruptcy-court-customer-deposits-earn-accounts.

[917] Galaxy Research, «The State of Crypto Leverage – Q2 2026: An Orderly, Measured Decline», 17.08.2026, https://www.galaxy.com/insights/research/crypto-leverage-report-q2-2026-defi-lending-decline-futures-open-interest.

[918] CoinDesk, 20.04.2026, https://www.coindesk.com/markets/2026/04/20/defi-tvl-drops-more-than-usd13-billion-in-two-days-following-kelp-dao-hack (данные DefiLlama).

[919] CoinDesk, 04.11.2025.

[920] CoinDesk Research, «Market Spotlight: Inside Crypto's $19 Billion Liquidation Event», https://www.coindesk.com/research/market-spotlight-the-19-billion-liquidation-that-shook-crypto.

[921] S. Aramonte, W. Huang, A. Schrimpf, «DeFi risks and the decentralisation illusion», BIS Quarterly Review, 06.12.2021, https://www.bis.org/publ/qtrpdf/r_qt2112b.htm.

Законы о стейблкоинах огораживают один сундук лавочника, и в котлах волну кредита пока тормозить почти нечему, кроме осторожности самих заёмщиков.

Прежде чем следить за такими волнами от цикла к циклу, отойдём от денег. Тетрадку без хранителя пробовали и в делах, где денег нет вовсе, и прижилась она там далеко не везде.

Глава 6. Блокчейн вне денег: что прижилось, что нет и почему

Австралийская биржа ASX несколько лет строила на распределённом реестре замену своей расчётной системы CHESS, а в ноябре 2022 года остановила работы и объявила, что пересматривает проект целиком[922]. Решение приняли после независимого обзора, который по заказу биржи провела консалтинговая компания Accenture. По словам биржи, обзор выявил «значительные трудности с дизайном решения», приложение было готово на 63%, а назвать срок окончания было нельзя. Капитализированные затраты на программу, 245–255 млн австралийских долларов, биржа решила списать[923].[924]

Главную фразу этой истории написали авторы отчёта. ASX, по их словам, — «центральный источник истины и окончательный арбитр результатов», и это сводит на нет многие преимущества распределённой архитектуры[925].[926] Через год биржа выбрала для замены CHESS готовый продукт другого поставщика, и распределённого реестра в его основе нет[927].

Зачем бирже понадобилась общая запись без хозяина, если эту запись и так вела она одна?

Распределённым реестром называют блокчейны и похожие на них системы, в которых копии общей записи ведут несколько участников. Такая запись полезна там, где нескольким сторонам, которые не доверяют друг другу, нужна общая тетрадка, а быть её хозяином никто из них не хочет или не может. Там, где хозяин есть и устраивает всех, ту же работу быстрее и дешевле делает обычная база данных. Вне денег хозяин находится почти в каждой задаче,

---

[922] ASX, «ASX will reassess all aspects of the CHESS replacement project and derecognise capitalised software of $245-255 million pre-tax in 1H23», 17.11.2022, https://www.asx.com.au/content/dam/asx/about/media-releases/2022/60-17-november-2022-CHESS-Replacement-ASX-reassessing-financial-derecognition_.pdf.

[923] ASX, «ASX will reassess all aspects of the CHESS replacement project and derecognise capitalised software of $245-255 million pre-tax in 1H23», 17.11.2022, https://www.asx.com.au/content/dam/asx/about/media-releases/2022/60-17-november-2022-CHESS-Replacement-ASX-reassessing-financial-derecognition_.pdf.

[924] Сообщение ASX рынку 17.11.2022 о выводах обзора: «The independent report identifies significant challenges with the solution design and its ability to meet ASX's requirements.» Списывается капитализированное ПО: «The CHESS replacement capitalised software will be derecognised… resulting in a charge of $245–255 million pre-tax»; после налогов — 172–179 млн, сумма названа оценкой (ASX, «ASX will reassess all aspects of the CHESS replacement project and derecognise capitalised software of $245-255 million pre-tax in 1H23», 17.11.2022, https://www.asx.com.au/content/dam/asx/about/media-releases/2022/60-17-november-2022-CHESS-Replacement-ASX-reassessing-financial-derecognition_.pdf). Председатель ASX Дэмиан Роуч: «…we have concluded that the path we were on will not meet ASX's and the market's high standards.» (ASX, «ASX will reassess all aspects of the CHESS replacement project and derecognise capitalised software of $245-255 million pre-tax in 1H23», 17.11.2022, https://www.asx.com.au/content/dam/asx/about/media-releases/2022/60-17-november-2022-CHESS-Replacement-ASX-reassessing-financial-derecognition_.pdf) Проект объявлен в 2016–2017 годах (дата начала в источниках расходится, вероятно, из-за разницы между выбором технологии и запуском проекта); технологический партнёр — Digital Asset (Ledger Insights, «ASX pauses DLT settlement project», 17.11.2022. https://www.ledgerinsights.com/asx-pauses-dlt-settlement-chess/; The Register, «Australian Securities Exchange pauses blockchain project…», 17.11.2022. https://www.theregister.com/2022/11/17/asx_blockchain_reading_project_paused/).

[925] Accenture, «ASX CHESS Replacement Application Delivery Review», November 2022, с. 18 и с. 6 (PDF, копия: https://www.euromoney.com/pdf/asx-chess-replacement-application-delivery-review-2022-pdf/; ASX в сообщении https://www.asx.com.au/content/dam/asx/about/media-releases/2022/60-17-november-2022-CHESS-Replacement-ASX-reassessing-financial-derecognition_.pdf даёт ссылку на тот же отчёт).

[926] Accenture. ASX CHESS Replacement Application Delivery Review, ноябрь 2022, с. 18: «ASX is the central source of truth and final arbiter of outcomes, minimising many of the benefits of a DLT architecture.» (Accenture, «ASX CHESS Replacement Application Delivery Review», November 2022, с. 18 и с. 6 (PDF, копия: https://www.euromoney.com/pdf/asx-chess-replacement-application-delivery-review-2022-pdf/; ASX в сообщении https://www.asx.com.au/content/dam/asx/about/media-releases/2022/60-17-november-2022-CHESS-Replacement-ASX-reassessing-financial-derecognition_.pdf даёт ссылку на тот же отчёт))

[927] ASX, «ASX announces product based solution for CHESS replacement – industry consultation on next phase to commence in 2024», 20.11.2023, https://www.asx.com.au/content/dam/asx/about/media-releases/2023/70-20-november-2023-chess-replacement-solution-announced-and-2024-consultation.pdf.

и поэтому большая часть громких проектов, о которых пойдёт речь, закрылась с многомиллионными потерями, а выжившие устроены иначе, чем обещали в 2017 году.

Кто может писать в тетрадку

Под словом «блокчейн» живут системы, у которых общего меньше, чем кажется, и различаются они прежде всего одним признаком. Национальный институт стандартов и технологий США (NIST) в обзоре 2018 года, написанном для читателей без специальной подготовки, делит блокчейны по тому, кто может добавлять новые страницы[928]. Если любой, блокчейн называют открытым, или блокчейном «без разрешений». Если только определённые участники, его называют разрешённым[929]. Там же дано сравнение. Разрешённая сеть похожа на внутреннюю сеть компании, которую кто-то контролирует, а открытая похожа на интернет, куда может прийти каждый[930].[931]

Биткоин и Ethereum относятся к первому типу, и всё, что разбиралось в третьей главе, было платой за открытость. Раз войти в сеть может кто угодно, в том числе злоумышленник, право написать страницу приходится покупать работой или залогом, а честность поощрять встроенной монетой[932]. В разрешённой сети пишущие известны заранее, разрешение у них можно отозвать за плохое поведение, и договариваться им быстрее и дешевле[933]. Такие сети обычно строят для группы организаций, консорциума[934].

Добавим семнадцатое правило посёлка: страницы в тетрадку пишут только дворы из списка, а список ведёт совет из нескольких старших дворов. Согласие сразу дешевеет. Перебор отпечатков и жребий с залогом больше не нужны, достаточно обмена подписями между дворами из списка, как в клубе с закрытым списком членов из третьей главы, который выдерживает жульничество меньше чем трети участников[935]. Но вопрос первой главы возвращается в новом виде: кто ведёт список и почему ему верят?

В обзоре NIST на этот вопрос отвечают без обиняков. Если одна организация решает, кто может публиковать блоки, пользователям блокчейна придётся доверять этой организации[936].[937] Разрешённый блокчейн переносит доверие на того, кто выдаёт разрешения, и хранитель из первой главы никуда не девается, он только пересаживается от тетрадки к списку. Если список ведёт одна компания, перед вами её база данных, у которой копии лежат у нескольких партнёров.

---

[928] Yaga D., Mell P., Roby N., Scarfone K. «Blockchain Technology Overview». NISTIR 8202, National Institute of Standards and Technology, October 2018, section 2, p. 5. https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf; DOI https://doi.org/10.6028/NIST.IR.8202.

[929] Yaga D., Mell P., Roby N., Scarfone K. «Blockchain Technology Overview». NISTIR 8202, National Institute of Standards and Technology, October 2018, section 2, p. 5. https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf; DOI https://doi.org/10.6028/NIST.IR.8202.

[930] NISTIR 8202, 2018, section 2, p. 5.

[931] NISTIR 8202 (Yaga D. и др., Blockchain Technology Overview, 2018), разд. 2: «In simple terms, a permissioned blockchain network is like a corporate intranet that is controlled, while a permissionless blockchain network is like the public internet, where anyone can participate.» (NISTIR 8202, 2018, section 2, p. 5)

[932] NISTIR 8202, 2018, section 2.1, p. 5.

[933] NISTIR 8202, 2018, section 2.2, pp. 5–6.

[934] NISTIR 8202, 2018, section 2, p. 5.

[935] M. Castro, B. Liskov, «Practical Byzantine Fault Tolerance», Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, February 1999; PDF (зеркало курса MIT 6.824): https://css.csail.mit.edu/6.824/2014/papers/castro-practicalbft.pdf.

[936] NISTIR 8202, 2018, section 2.2, pp. 5–6.

[937] NISTIR 8202, разд. 2.2: «However, if a single entity controls who can publish blocks, the users of the blockchain will need to have trust in that entity.» (NISTIR 8202, 2018, section 2.2, pp. 5–6)

Возьмём список из двадцати дворов, в котором совет из трёх старших решает, кого вписать и кого вычеркнуть. Пока совет честен, всё работает быстро и дёшево. Но если совет вычеркнет двор, который ему мешает, этот двор теряет право писать, и никакая работа и никакой залог ему не помогут. В открытой тетрадке так сделать нельзя, потому что вход в неё не выдают, а покупают.

У такого переноса есть и достоинство, которое в том же обзоре названо отдельно. Участники разрешённой сети известны, поэтому при нарушении понятно, где зарегистрирована организация, какие у пострадавшего есть средства защиты и в какой суд с ними идти[938]. В открытой сети обманщика ищут по следам в тетрадке, как во второй главе, а в разрешённой его знают по имени и с ним судятся.

Между двумя типами есть промежуточный. Исследователи Вюст и Жерве в статье 2018 года выделяют публичный разрешённый блокчейн (писать в него могут немногие, а читать и проверять запись — все)[939]. В той же статье есть сравнительная таблица, и по пропускной способности и скорости обычная централизованная база данных в ней обходит оба типа блокчейнов[940]. Медленнее базы оказывается любой из них, открытый и разрешённый различаются только тем, насколько.

Модное слово «гибридный» строгого определения не имеет, и каждый раз приходится отдельно выяснять, что в такой системе централизовано, а что нет[941]. Вывеска здесь говорит мало. Когда вам рассказывают о блокчейне компании или консорциума, первым делом стоит узнать, кто вносит дворы в список, кто их вычёркивает и может ли это сделать кто-то один.

Рисунок 6.1. Кто может писать в тетрадку

[938] NISTIR 8202, 2018, section 2.2, p. 6.

[939] Wüst K., Gervais A. «Do you Need a Blockchain?» 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), IEEE, pp. 45–54. DOI 10.1109/CVCBT.2018.00011; открытая версия: https://eprint.iacr.org/2017/375.pdf.

[940] Wüst K., Gervais A. «Do you Need a Blockchain?» 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), IEEE, pp. 45–54. DOI 10.1109/CVCBT.2018.00011; открытая версия: https://eprint.iacr.org/2017/375.pdf.

[941] Wikipedia, «Blockchain», раздел о типах блокчейнов (обращение 26.09.2026). https://en.wikipedia.org/wiki/Blockchain.

Биржа, которая и так была хозяином

Проверить, нужен ли в задаче блокчейн, можно по шагам, и такие проверки уже составлены. Вюст и Жерве свели свой ответ к одной фразе: блокчейн, открытый или разрешённый, имеет смысл, только когда несколько не доверяющих друг другу сторон хотят вместе менять общую запись и не готовы договориться о доверенной третьей стороне, которая всегда на связи[942].[943] К фразе они приложили схему из шести вопросов, и большинство ответов в ней уводит от блокчейна. Если хранить нечего, база не нужна вовсе, если пишущий один, обычная база быстрее, а если все пишущие доверяют друг другу, хватит базы с общим доступом на запись[944].

Похожую схему, тоже из шести вопросов, составил научно-технический директорат Министерства внутренней безопасности США, и NIST воспроизвёл её в своём обзоре. Вывод «возможно, у вас полезный сценарий для блокчейна» она даёт только тому, кто на все шесть ответил «да», а при «нет» на самый первый вопрос советует электронную почту и таблицы[945].[946] Авторы NIST проверили и интерактивную версию схемы Вюста и Жерве, сделанную сторонними разработчиками, увидели, что почти все пути в ней ведут к ответу «нет», и назвали такой строгий взгляд правильным для организаций[947]. Там же описана типичная ошибка. Организации, боясь упустить технологию, начинают с вопроса «мы хотим где-нибудь применить блокчейн, где бы это сделать?», и кончается это разочарованием, потому что технология подходит не для всего[948].[949]

Двенадцать вопросов держать в голове трудно, и в этой главе я буду проверять каждую историю тремя, которые свёл из обеих схем. Обобщение моё, в таком виде у авторов схем его нет. Первый вопрос — пишут ли в запись несколько независимых сторон. Второй — есть ли хозяин, которому все пишущие готовы доверить запись. Третий — можно ли проверить записанное, не доверяя тому, кто его вносит. Блокчейн окупается, когда на первый вопрос ответ «да», на второй «нет», а на третий снова «да».

Прогоним через них условный пример с пятью мельницами из соседних посёлков, которые хотят вести общий учёт того, сколько зерна им сдали и сколько муки они выдали. Пишущих пять, и они независимы, так что первый вопрос пройден. Ответ на второй зависит от того, как мельники относятся друг к другу. Если все пять согласны, чтобы учёт вёл один из них или писарь в городе, дальше идти незачем, хватит его базы. Если не согласны, потому что кон-

---

[942] Wüst & Gervais, 2018, section III.

[943] Wüst K., Gervais A. Do you Need a Blockchain? 2018 Crypto Valley Conference on Blockchain Technology, разд. III: «In general, using an open or permissioned blockchain only makes sense when multiple mutually mistrusting entities want to interact and change the state of a system, and are not willing to agree on an online trusted third party.» В сравнительной таблице той же статьи централизованная база данных превосходит оба типа блокчейна по пропускной способности и скорости (Wüst & Gervais, 2018, section III; Wüst K., Gervais A. «Do you Need a Blockchain?» 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), IEEE, pp. 45–54. DOI 10.1109/CVCBT.2018.00011; открытая версия: https://eprint.iacr.org/2017/375.pdf).

[944] Wüst & Gervais, 2018, Fig. 1.

[945] NISTIR 8202, 2018, Figure 6 «DHS Science & Technology Directorate Flowchart», p. 42.

[946] Схема научно-технического директората Министерства внутренней безопасности США (NISTIR 8202, рис. 6). Пятый вопрос схемы — трудно ли пишущим решить, кто должен управлять хранилищем данных; исход при «нет»: «If there are no trust or control issues over who runs the data store, traditional database solutions should suffice» (NISTIR 8202, 2018, Figure 6 «DHS Science & Technology Directorate Flowchart», p. 42). На втором вопросе у схемы есть обход для задач аудита: даже при одном источнике данных она ведёт дальше.

[947] NISTIR 8202, 2018, section 8, p. 43.

[948] NISTIR 8202, 2018, section 8, p. 41.

[949] NISTIR 8202, разд. 8: «…most organizations approach the problem as „we want to use blockchain somewhere, where can we do that?“ which leads to frustrations with the technology as it cannot be applied universally.» О схеме Вюста и Жерве, реализованной на сайте сторонними разработчиками: «most paths lead to „no“ with only a few leading to „maybe.“» (NISTIR 8202, 2018, section 8, p. 41; NISTIR 8202, 2018, section 8, p. 43)

курируют и подозревают друг друга, встаёт третий вопрос: как проверить, что мельник записал о мешках правду? Никак, и общая тетрадка сохранит неправду каждого из пяти так же надёжно, как правду. Ответ «можно» на третий вопрос бывает, когда строчка и есть сама вещь, как монета биткоина, а о мешке на складе тетрадка знает лишь то, что ей сообщили.

Теперь вернёмся к бирже. Когда на бирже заключена сделка, акции и деньги ещё нужно передать, а в записи о владельцах отметить, у кого теперь бумаги. Эта работа называется расчётами, и ведёт её расчётная система. У ASX такой системой была CHESS, и в ней же велась часть реестра владельцев акций (её называют субреестром)[950]. Новую CHESS биржа строила вместе с технологическим партнёром, компанией Digital Asset[951].

На первый вопрос CHESS отвечает «да», пишущих в расчётной системе много (брокеры, банки, сама биржа). На втором вопросе история заканчивается. Хозяин у записи есть, это ASX, и спора о нём нет[952]. Accenture записала то же своими словами: раз биржа — центральный оператор рынка, надо заново продумать, зачем этой системе вообще согласие узлов[953].[954] Распределённую запись в проекте использовали в основном ради отказоустойчивости, и авторы отчёта сочли, что это добавляет «излишнюю сложность» (согласие узлов само увеличивало время ответа системы)[955]. До третьего вопроса дело не дошло, хотя его CHESS прошла бы легко: запись о том, чьи теперь акции, в субреестре и есть учёт права на них.

Сложность проявилась в испытаниях. Путь каждой транзакции через узел клиента, общую запись и обратно добавлял задержку, параллельные транзакции к одним и тем же данным конфликтовали, а при нагрузке свыше 100 тысяч транзакций расчёты заканчивались сбоем[956].[957] Снаружи трудности были видны и до отчёта. В августе 2022 года биржа и Digital Asset сообщали о проблемах с масштабируемостью и устойчивостью в части проекта[958], а регу-

---

[950] ASX, «ASX announces product based solution for CHESS replacement – industry consultation on next phase to commence in 2024», 20.11.2023, https://www.asx.com.au/content/dam/asx/about/media-releases/2023/70-20-november-2023-chess-replacement-solution-announced-and-2024-consultation.pdf.

[951] Ledger Insights, «ASX pauses DLT settlement project», 17.11.2022. https://www.ledgerinsights.com/asx-pauses-dlt-settlement-chess/; The Register, «Australian Securities Exchange pauses blockchain project…», 17.11.2022. https://www.theregister.com/2022/11/17/asx_blockchain_reading_project_paused/.

[952] Accenture, «ASX CHESS Replacement Application Delivery Review», November 2022, с. 18 и с. 6 (PDF, копия: https://www.euromoney.com/pdf/asx-chess-replacement-application-delivery-review-2022-pdf/; ASX в сообщении https://www.asx.com.au/content/dam/asx/about/media-releases/2022/60-17-november-2022-CHESS-Replacement-ASX-reassessing-financial-derecognition_.pdf даёт ссылку на тот же отчёт).

[953] Accenture, «ASX CHESS Replacement Application Delivery Review», November 2022, с. 18 и с. 6 (PDF, копия: https://www.euromoney.com/pdf/asx-chess-replacement-application-delivery-review-2022-pdf/; ASX в сообщении https://www.asx.com.au/content/dam/asx/about/media-releases/2022/60-17-november-2022-CHESS-Replacement-ASX-reassessing-financial-derecognition_.pdf даёт ссылку на тот же отчёт).

[954] Accenture, ноябрь 2022, с. 6: «Greater consideration is required regarding the purpose of the consensus layer given ASX's position as the central market operator for the CHESS use case.» С. 19: «CHESS use case primarily uses the ledger for resiliency which adds undue complexity to the solution e.g., the consensus contributes to the round-trip latency.» (Accenture, «ASX CHESS Replacement Application Delivery Review», November 2022, с. 18 и с. 6 (PDF, копия: https://www.euromoney.com/pdf/asx-chess-replacement-application-delivery-review-2022-pdf/; ASX в сообщении https://www.asx.com.au/content/dam/asx/about/media-releases/2022/60-17-november-2022-CHESS-Replacement-ASX-reassessing-financial-derecognition_.pdf даёт ссылку на тот же отчёт); Accenture, ноябрь 2022, с. 5, 18–19)

[955] Accenture, ноябрь 2022, с. 5, 18–19.

[956] Accenture, ноябрь 2022, с. 5, 18–19.

[957] Accenture, ноябрь 2022, с. 19: «…settlement under load with 100K+ transactions fail because of data or running out of time.» Об ограничениях пакетной обработки отчёт говорит осторожнее, чем пересказы в СМИ: ограничение «могло бы» возникнуть и в интерфейсе реестра Daml, и в реестре VMware (с. 5) (Accenture, ноябрь 2022, с. 5, 18–19; The Register, 17.11.2022 (цитаты из отчёта Accenture),). Всего в отчёте 45 рекомендаций в 12 направлениях; в нумерации отчёта рекомендации по дизайну идут последними: пересмотр стратегии распределённого реестра — первый подпункт группы R40, оценка «ценности против сложности» слоёв (реестр, язык смарт-контрактов) — группа R41 (с. 33–34) (Accenture, ноябрь 2022, с. 5 и 34).

[958] Ledger Insights, «ASX pauses DLT settlement project», 17.11.2022. https://www.ledgerinsights.com/asx-pauses-dlt-settlement-chess/; The Register, «Australian Securities Exchange pauses blockchain project…», 17.11.2022. https://www.theregister.com/2022/11/17/asx_blockchain_reading_project_paused/.

ляторы публично выражали недовольство очередными задержками[959].[960] Среди 45 рекомендаций в части о дизайне Accenture первым делом советовала пересмотреть стратегию распределённого реестра, а следом — оценить, стоят ли сама распределённая запись и язык смарт-контрактов той сложности, которую они добавляют[961].

Пусть за день на бирже прошло сто тысяч сделок. Если запись ведёт сама биржа, каждая сделка проходит один путь, от брокера к бирже и обратно. Если запись распределена, каждой сделке нужно ещё и согласие узлов, на каждом лишнем круге теряется время, а две сделки с одной и той же бумагой могут столкнуться. Все эти лишние круги окупаются в одном случае — когда сторонам нужно защищаться друг от друга без судьи, а у ASX судья был, и это была она сама.

Отсюда легко сделать неверный вывод, будто проект погубили плохие программисты или неработающая технология. Тот же отчёт высоко оценил сам код. Проверка нашла качественную реализацию, заметно более эффективную, чем старая CHESS, и к ключевым проблемам код отношения не имел[962].[963] Зато раздельным было управление. Биржа и Digital Asset работали и отчитывались каждая сама по себе, поэтому по-разному видели ход работ, риски и проблемы[964]. Главных причин неудачи, по-моему, две: архитектура, выбранная для задачи с одним хозяином, и раздельное управление. Остальное, от несогласованных требований до слабого тестирования, выросло из них[965].

Сама Digital Asset от распределённых реестров не отказалась. Летом 2025 года она привлекла 135 млн долларов на развитие сети Canton, которую называет «единственным публичным блокчейном без разрешений» с настраиваемой приватностью и соответствием требованиям финансовых институтов[966].[967] В Австралии, как я это понимаю, провалился выбор задачи, а компания и её технология нашли себе другое применение.

---

[959] ASIC, 22-204MR «Delay to the ASX CHESS Replacement Project and Independent Review», 2022. https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2022-releases/22-204mr-delay-to-the-asx-chess-replacement-project-and-independent-review/.

[960] ASIC, 22-204MR, совместное заявление ASIC и Резервного банка Австралии от 03.08.2022 (до решения ASX о паузе). Председатель ASIC Джозеф Лонго: «It is very disappointing that there is a further delay to the CHESS Replacement Project.» Регуляторы требовали, чтобы новая система отвечала нынешним требованиям к надёжности и производительности, и приветствовали назначение Accenture для независимого обзора (ASIC, 22-204MR «Delay to the ASX CHESS Replacement Project and Independent Review», 2022. https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2022-releases/22-204mr-delay-to-the-asx-chess-replacement-project-and-independent-review/). О проблемах августа 2022 года — по Ledger Insights (Ledger Insights, «ASX pauses DLT settlement project», 17.11.2022. https://www.ledgerinsights.com/asx-pauses-dlt-settlement-chess/; The Register, «Australian Securities Exchange pauses blockchain project…», 17.11.2022. https://www.theregister.com/2022/11/17/asx_blockchain_reading_project_paused/).

[961] Accenture, ноябрь 2022, с. 5 и 34.

[962] Accenture, ноябрь 2022, с. 6.

[963] Accenture, ноябрь 2022, с. 6: «The code review highlighted the existence of a high quality Daml implementation providing considerable efficiencies relative to the current CHESS and is not contributing to the Core Issues…» Риски, по отчёту, — в долгосрочной поддержке из-за нехватки специалистов и связности контрактов. Кроме архитектуры и управления, отчёт называет несогласованные функциональные и нефункциональные требования, слабое тестирование и «высокорисковый» план поставки Digital Asset (с. 7–8); что эти причины выросли из двух главных — оценка автора (Accenture, ноябрь 2022, с. 6).

[964] ASX, «ASX will reassess all aspects of the CHESS replacement project and derecognise capitalised software of $245-255 million pre-tax in 1H23», 17.11.2022, https://www.asx.com.au/content/dam/asx/about/media-releases/2022/60-17-november-2022-CHESS-Replacement-ASX-reassessing-financial-derecognition_.pdf.

[965] Accenture, ноябрь 2022, с. 6.

[966] Digital Asset, «Digital Asset raises $135 million to accelerate adoption of Canton Network», 24.06.2025. https://blog.digitalasset.com/press-release/digital-asset-raises-135-million-to-accelerate-adoption-of-canton-network; Canton Network. https://canton.network/.

[967] Digital Asset, пресс-релиз 24.06.2025: «the only public, permissionless Layer-1 blockchain that offers configurable privacy and institutional-grade compliance at scale». Раунд в 135 млн долларов возглавили DRW и Tradeweb; среди инвесторов также BNP Paribas, Citadel Securities, центральный депозитарий американских ценных бумаг DTCC и Goldman Sachs. Число участников сети (почти 400) — по данным самой компании (Digital Asset, «Digital Asset raises $135 million to accelerate adoption of Canton Network», 24.06.2025. https://blog.digitalasset.com/press-release/digital-asset-raises-135-million-to-accelerate-adoption-of-

Суд, которым история продолжилась, разбирал слова биржи, а технологию не оценивал. В июне 2026 года ASX признала, что в феврале 2022-го ввела рынок в заблуждение, назвав проект идущим хорошо, хотя её внутренняя оценка проекта с декабря 2021 года была «красной», а в июле Федеральный суд обязал её заплатить 20,5 млн австралийских долларов штрафа[968].[969] Первый этап новой системы, уже без распределённого реестра в основе, был намечен на 2026 год[970].

Холодильник в кузове

Самая частая мечта о блокчейне вне денег связана с вещами, будь то груз, продукты, лекарства или земля. Хочется, чтобы путь товара от поля до прилавка лежал в записи, которую никто не может подделать. Здесь тетрадка упирается в третий вопрос.

Вюст и Жерве показывают это на мысленном примере. Датчик температуры пишет в блокчейн, что груз всю дорогу ехал в холоде. Недобросовестный поставщик ставит в кузов маленький охлаждаемый отсек, кладёт туда датчик, а товар везёт без охлаждения[971]. Запись останется неизменной навсегда, и она будет ложной. В обзоре NIST та же беда названа подделкой входных данных[972].

Вывод авторов статьи жёсткий. Если людям на стыке вещей и записей не доверяют, цепочка поставок скомпрометирована, потому что любые данные может ввести злонамеренный участник, а если им доверяют, хватит обычной базы данных[973]. По словам авторов, стартап Skuchain, который сам строил блокчейн для цепочек поставок, признал в переписке с ними, что для большинства таких задач достаточно единого источника истины[974].

Щель между записью и миром встречалась в этой книге и раньше. В четвёртой главе автомату понадобился гонец с рынка, чтобы узнать цену, в пятой строчка стейблкоина лежала

---

canton-network; Canton Network. https://canton.network/).

[968] ASIC, 24-177MR «ASIC sues ASX for alleged misleading statements», 13.08.2024, https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2024-releases/24-177mr-asic-sues-asx-for-alleged-misleading-statements/; ASIC, 26-119MR «ASX admits misleading conduct relating to CHESS replacement project», 2026, https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2026-releases/26-119mr-asx-admits-misleading-conduct-relating-to-chess-replacement-project; ASIC, 26-143MR «ASX ordered to pay $20.5 million penalty…», 2026, https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2026-releases/26-143mr-asx-ordered-to-pay-205-million-penalty-for-misleading-conduct-relating-to-chess-replacement-project.

[969] Иск ASIC подан в Федеральный суд 13.08.2024: 10.02.2022 ASX сообщила, что проект «progressing well» и идёт к запуску в срок, хотя внутренняя оценка проекта с 21.12.2021 была «красной»; через шесть недель, 28.03.2022, ASX объявила о вероятной задержке запуска (ASIC, 24-177MR «ASIC sues ASX for alleged misleading statements», 13.08.2024, https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2024-releases/24-177mr-asic-sues-asx-for-alleged-misleading-statements/). Признание — 15.06.2026; решение суда — июль 2026 года (ASIC, 26-143MR); кроме штрафа, ASX возмещает 3 млн австралийских долларов судебных расходов ASIC. Судья Маркович: «ASX is a gatekeeper for preserving the integrity of, and confidence in, Australia's financial system and should have been setting a benchmark for accuracy and transparency in its own market disclosures.» (ASIC, 26-119MR «ASX admits misleading conduct relating to CHESS replacement project», 2026, https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2026-releases/26-119mr-asx-admits-misleading-conduct-relating-to-chess-replacement-project; ASIC, 26-143MR «ASX ordered to pay $20.5 million penalty…», 2026, https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2026-releases/26-143mr-asx-ordered-to-pay-205-million-penalty-for-misleading-conduct-relating-to-chess-replacement-project) Новая система — продукт TCS BaNCS компании Tata Consultancy Services; распределённый реестр в ней остался лишь как возможность подключения к «альтернативным технологиям»; запустился ли первый этап — см. приложение Б (ASX, «ASX announces product based solution for CHESS replacement – industry consultation on next phase to commence in 2024», 20.11.2023, https://www.asx.com.au/content/dam/asx/about/media-releases/2023/70-20-november-2023-chess-replacement-solution-announced-and-2024-consultation.pdf).

[970] ASX, «ASX announces product based solution for CHESS replacement – industry consultation on next phase to commence in 2024», 20.11.2023, https://www.asx.com.au/content/dam/asx/about/media-releases/2023/70-20-november-2023-chess-replacement-solution-announced-and-2024-consultation.pdf.

[971] Wüst & Gervais, 2018, section IV.A и Fig. 3.

[972] Wüst & Gervais, 2018, section IV.A и Fig. 3.

[973] Wüst & Gervais, 2018, section IV.A и Fig. 3.

[974] Wüst & Gervais, 2018, section IV.A.

в тетрадке, а сундук с долларами стоял снаружи. Там щель была одной деталью механизма. В цепочке поставок она становится всей задачей. Проверить, есть ли у пекаря 10 монет биткоина, значит прочитать тетрадку, и больше проверять нечего. Запись о грузе описывает вещь снаружи, и между вещью и записью всегда стоит человек или датчик, которому приходится верить. Правила посёлка, собранные в первых главах, отвечают за то, что записано, и ни одно из них не говорит, правдиво ли записанное о мешке муки или о поле за околицей.

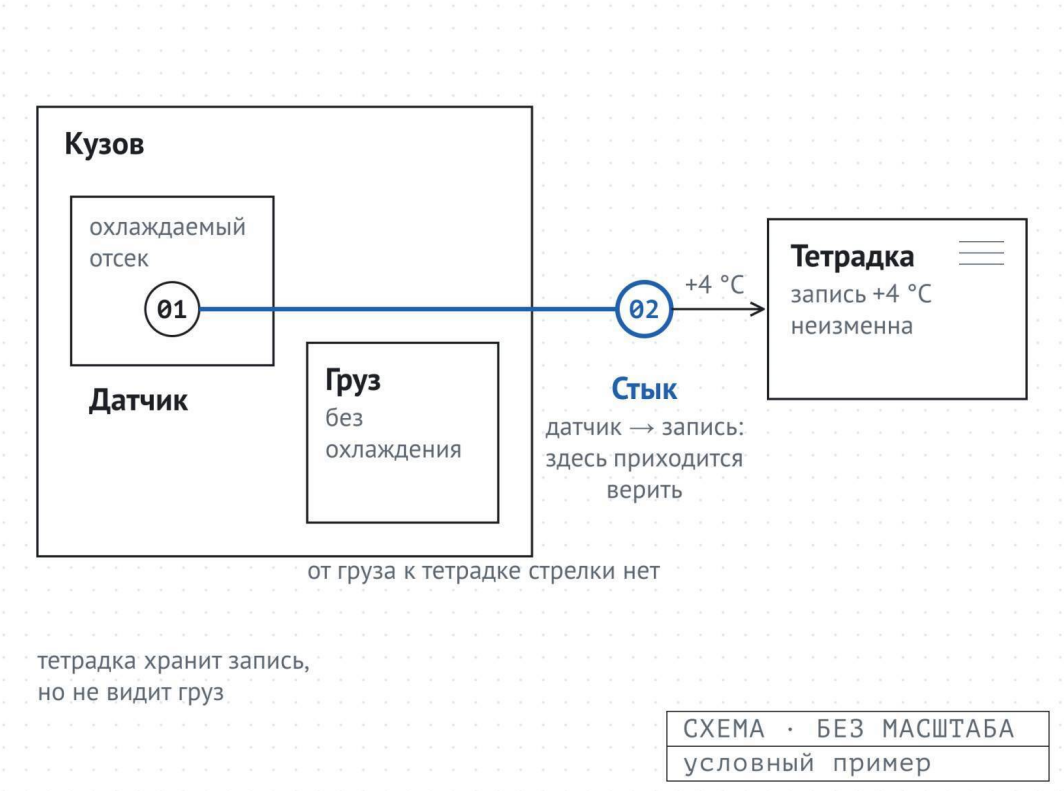


Рисунок 6.2. Холодильник в кузове

Самый известный успех в этой области начинался как пилот. В октябре 2016 года Walmart и IBM объявили, что отслеживают на блокчейне манго в США и свинину в Китае. Строили систему на Hyperledger Fabric, программе из открытого проекта для корпоративных блокчейнов[975].[976] Время, за которое удавалось установить, откуда пришла партия манго, сократилось с семи дней до 2,2 секунды[977]. Эту пару чисел с тех пор пересказывают как доказательство пользы блокчейна, хотя сравнивали в ней другое.

---

[975] LF Decentralized Trust (Hyperledger), «How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric». https://www.lfdecentralizedtrust.org/case-studies/walmart-case-study; Wikipedia, «Hyperledger» (обращение 26.09.2026). https://en.wikipedia.org/wiki/Hyperledger; LF Decentralized Trust, «About». https://www.lfdecentralizedtrust.org/about.

[976] Hyperledger — открытый проект Linux Foundation для корпоративных блокчейнов (объявлен в 2015 году; Fabric создан на основе кода IBM и Digital Asset). Иногда пишут, что его закрыли; это неточно: в 2024 году он вошёл в более широкий фонд LF Decentralized Trust, часть его проектов прекращена (Wikipedia, «Hyperledger» (обращение 26.09.2026). https://en.wikipedia.org/wiki/Hyperledger; LF Decentralized Trust, «About». https://www.lfdecentralizedtrust.org/about). Позже Walmart отслеживал так больше 25 продуктов от пяти поставщиков (LF Decentralized Trust (Hyperledger), «How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric». https://www.lfdecentralizedtrust.org/case-studies/walmart-case-study).

[977] LF Decentralized Trust (Hyperledger), «How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric». https://www.lfdecentralizedtrust.org/case-studies/walmart-case-study.

Сам Walmart в пресс-релизе 2018 года описал, с чем сравнивали. Обычно отрасль прослеживает товар на шаг вперёд и на шаг назад, и делает это чаще всего по бумажным записям[978].[979] Семь дней, по-видимому, уходили на обычный для отрасли путь по бумагам и звонкам, а 2,2 секунды — на поиск по цифровой записи. Отделить по этим цифрам вклад именно блокчейна от выигрыша оцифровки нельзя[980]. Для этого понадобилось бы сравнение с обычной базой данных, а его в кейсе нет.

Важнее, как систему распространили. После вспышки кишечной палочки в салате романо Walmart объявил, что к сентябрю 2019 года потребует от поставщиков листовой зелени прослеживать товар до фермы в этой системе[981]. Распространял систему, получается, крупнейший покупатель, который может обязать остальных, и на второй вопрос здесь есть ответ. Хозяин у данных — сам Walmart. Что стало с платформой потом, я не знаю. IBM прекратила поддержку своего продукта для блокчейнов 30 апреля 2023 года[982], а официального сообщения о судьбе сервиса для продуктов, выросшего из этого пилота, в моих источниках нет.[983]

С лекарствами опыт вышел поучительнее, потому что выводы из него делал регулятор. В 2019–2020 годах Управление по санитарному надзору за качеством пищевых продуктов и медикаментов США (FDA) провело пилотную программу по закону о безопасности цепочки поставок лекарств, и из двадцати отраслевых проектов блокчейн использовали шесть[984]. Рабочая группа одного из них, MediLedger, где было 24 компании, среди них Pfizer и Walgreens, заявила в итоговом отчёте, что хорошо спроектированная отраслевая блокчейн-платформа способна выполнить требования закона[985].[986] FDA в своём итоговом отчёте мая 2023 года

---

[978] Walmart, «Walmart and Sam's Club to Require Real-Time, End-to-End Food Traceability with Blockchain», 24.09.2018, https://corporate.walmart.com/content/dam/corporate/documents/press-center/in-wake-of-romaine-e-coli-scare-walmart-deploys-blockchain-to-track-leafy-greens/press-release-leafy-greens-on-blockchain.pdf.

[979] Walmart, пресс-релиз 24.09.2018: «Today, the most frequently used process to address issues in the industry is referred to as one-step-up and one-step-back traceability, which is often based on paper records…» По тому же релизу, сеть строили больше года вместе с IBM и 11 другими пищевыми компаниями (Walmart, «Walmart and Sam's Club to Require Real-Time, End-to-End Food Traceability with Blockchain», 24.09.2018, https://corporate.walmart.com/content/dam/corporate/documents/press-center/in-wake-of-romaine-e-coli-scare-walmart-deploys-blockchain-to-track-leafy-greens/press-release-leafy-greens-on-blockchain.pdf). Цифры 7 дней и 2,2 секунды — из кейса и релиза заинтересованных сторон, независимой оценки нет; на что именно уходили семь дней, в релизе не сказано (LF Decentralized Trust (Hyperledger), «How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric». https://www.lfdecentralizedtrust.org/case-studies/walmart-case-study).

[980] LF Decentralized Trust (Hyperledger), «How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric». https://www.lfdecentralizedtrust.org/case-studies/walmart-case-study.

[981] Walmart, «Walmart and Sam's Club to Require Real-Time, End-to-End Food Traceability with Blockchain», 24.09.2018, https://corporate.walmart.com/content/dam/corporate/documents/press-center/in-wake-of-romaine-e-coli-scare-walmart-deploys-blockchain-to-track-leafy-greens/press-release-leafy-greens-on-blockchain.pdf; LF Decentralized Trust, кейс Walmart.

[982] IBM Support, «IBM Blockchain Platform software reaches end of support on April 30, 2023», https://www.ibm.com/support/pages/ibm-blockchain-platform-software-reaches-end-support-april-30-2023.

[983] В феврале 2021 года CoinDesk со ссылкой на анонимные источники писал, что блокчейн-подразделение IBM почти расформировано; IBM это отрицала (CoinDesk, «IBM Blockchain Is a Shell of Its Former Self After Revenue Misses, Job Cuts: Sources», 01.02.2021, https://www.coindesk.com/business/2021/02/01/ibm-blockchain-is-a-shell-of-its-former-self-after-revenue-misses-job-cuts-sources). Прекращение поддержки IBM Blockchain Platform — 30.04.2023, клиентам предложили перейти на поддержку открытого Hyperledger Fabric (IBM Support, «IBM Blockchain Platform software reaches end of support on April 30, 2023», https://www.ibm.com/support/pages/ibm-blockchain-platform-software-reaches-end-support-april-30-2023).

[984] FDA, «Drug Supply Chain Security Act Pilot Project Program: Final Program Report», May 2023, pp. 2, 11 (Table 5), 17–18, https://www.fda.gov/media/168307/download.

[985] PR Newswire, «Leaders from 24 companies in the US Pharmaceutical Supply Chain collaborate to submit the MediLedger DSCSA Pilot Project Final Report to the FDA…», 21.02.2020, https://www.prnewswire.com/news-releases/leaders-from-24-companies-in-the-us-pharmaceutical-supply-chain-collaborate-to-submit-the-mediledger-dscsa-pilot-project-final-report-to-the-fda-proposing-blockchain-for-an-interoperable-track-and-trace-system-for-us-prescription-301008871.html.

[986] PR Newswire, 21.02.2020: «A well-designed, industry-led, decentralized blockchain platform can successfully meet the 2023 DSCSA requirements». Это позиция участников пилота, а не вывод FDA (PR Newswire, «Leaders from 24 companies in the US Pharmaceutical Supply Chain collaborate to submit the MediLedger DSCSA Pilot Project Final Report to the FDA…»,

упомянуло блокчейн одной строкой, среди «других носителей и способов передачи данных», рядом с радиометками, и отдельно оговорило, что отчёт нельзя считать одобрением какой-либо технологии[987].[988] Участники пилота говорили, что блокчейн может справиться, регулятор ответил, что это один из возможных способов передать данные.

Земельные реестры кажутся самым очевидным применением (кто чем владеет, записано навсегда, и чиновник ничего не перепишет тайком). Истории здесь короче своих пересказов. В мае 2015 года компания Factom объявила о проекте блокчейн-реестра земли в Гондурасе, подписав необязывающее письмо о намерениях, а к концу того же года её глава сам сказал, что проект застопорился[989]. Шведский земельный кадастр в 2016–2017 годах испытывал регистрацию сделок на блокчейне вместе с банками и технологическими компаниями, а сведений о переходе в рабочую систему в открытых данных нет[990]. Самый известный земельный случай, грузинский, устроен иначе, и к нему я вернусь в разделе о том, что прижилось.

Слово в названии компании

Пока одни компании годами строили реестры, другим хватало слова. 21 декабря 2017 года производитель напитков Long Island Iced Tea Corp. объявил, что переименуется в Long Blockchain Corp., и его акции в моменте выросли больше чем на 380%[991]. Блокчейн-компанией он так и не стал. Весной 2018 года от планов купить оборудование для майнинга отказались, биржа Nasdaq исключила акции из торгов, а в феврале 2021 года Комиссия по ценным бумагам и биржам США (SEC) отозвала их регистрацию, потому что отчётности компания не подавала с осени 2018 года[992]. Позже та же комиссия обвинила троих человек в торговле на инсайдерской информации перед объявлением о переименовании[993].[994] На первом же вопросе теста такая компания отсеивается, потому что общей записи у неё нет и писать в неё некому.

21.02.2020, https://www.prnewswire.com/news-releases/leaders-from-24-companies-in-the-us-pharmaceutical-supply-chain-collaborate-to-submit-the-mediledger-dscsa-pilot-project-final-report-to-the-fda-proposing-blockchain-for-an-interoperable-track-and-trace-system-for-us-prescription-301008871.html).

[987] FDA, «Drug Supply Chain Security Act Pilot Project Program: Final Program Report», May 2023, pp. 2, 11 (Table 5), 17–18, https://www.fda.gov/media/168307/download.

[988] FDA. Drug Supply Chain Security Act Pilot Project Program: Final Program Report, май 2023, с. 17: «Other data carriers and methods to transfer data exist and could be leveraged for supply chain security and other uses (e.g., radio frequency identification [RFID] tags, blockchain).» С. 18: «…this program report should not be viewed as FDA's endorsement of a particular technology, system, or approach used in the pilot projects.» Подсчёт «шесть из двадцати» — по таблице 5 отчёта (FDA, «Drug Supply Chain Security Act Pilot Project Program: Final Program Report», May 2023, pp. 2, 11 (Table 5), 17–18, https://www.fda.gov/media/168307/download).

[989] CoinDesk, «Blockchain Land Title Project 'Stalls' in Honduras», 26.12.2015, https://www.coindesk.com/markets/2015/12/26/blockchain-land-title-project-stalls-in-honduras.

[990] EU Blockchain Observatory and Forum, «The Land Registry in the blockchain – testbed (2017)», 31.05.2018, https://blockchain-observatory.ec.europa.eu/news/land-registry-blockchain-testbed-2017-2018-05-31_en?prefLang=fr.

[991] U.S. SEC, press release 2021-121 «SEC Charges Three Individuals with Insider Trading», 09.07.2021. https://www.sec.gov/newsroom/press-releases/2021-121; пресс-релиз компании о переименовании (21.12.2017): https://www.nasdaq.com/press-release/long-island-iced-tea-corp-to-rebrand-as-long-blockchain-corp-20171221-00468 (ссылка по Википедии, не открыта).

[992] Wikipedia, «Long Blockchain Corp.» (обращение 26.09.2026), со ссылками на MarketWatch, 11.04.2018 (https://www.marketwatch.com/story/nasdaq-to-delist-long-blockchain-corp-underlining-fading-bitcoin-fervor-2018-04-11) и Bloomberg, 22.02.2021 (https://www.bloomberg.com/news/articles/2021-02-22/long-blockchain-delisted-by-sec-after-riding-2017-s-crypto-craze). https://en.wikipedia.org/wiki/Long_Blockchain_Corp.

[993] U.S. SEC, press release 2021-121 «SEC Charges Three Individuals with Insider Trading», 09.07.2021. https://www.sec.gov/newsroom/press-releases/2021-121; пресс-релиз компании о переименовании (21.12.2017): https://www.nasdaq.com/press-release/long-island-iced-tea-corp-to-rebrand-as-long-blockchain-corp-20171221-00468 (ссылка по Википедии, не открыта).

[994] SEC, пресс-релиз 2021-121, 09.07.2021. По версии обвинения, один из троих купил 35 000 акций в течение нескольких часов после того, как узнал о предстоящем переименовании, и продал их в течение двух часов после объявления с прибылью больше 160 тыс. долларов. Обвинение — не приговор; имена не приводим, исход дел в наших источниках не указан (U.S. SEC, press release 2021-121 «SEC Charges Three Individuals with Insider Trading», 09.07.2021. https://www.sec.gov/newsroom/press-releases/2021-121; пресс-релиз компании о переименовании (21.12.2017):

Председатель SEC Джей Клейтон ещё в январе 2018 года описал такой сценарий как гипотетический: компания без опыта в блокчейне начинает им «баловаться», меняет название на что-нибудь вроде «Blockchain-R-Us» и сразу выпускает ценные бумаги. Он предупредил, что комиссия пристально следит за раскрытием информации компаниями, которые меняют бизнес ради обещаний распределённого реестра[995].[996]

Long Blockchain была заметным, но не единственным случаем. Исследователи, изучившие отчёты американских публичных компаний о существенных событиях (формы 8-K), нашли резкий всплеск первых упоминаний блокчейна в последнем квартале 2017 года, особенно у фирм с расплывчатыми планами. Инвесторы отвечали на такие объявления ростом цены в первые семь дней, а за следующие 30 дней реакция в основном сходила на нет[997].[998] Слово «блокчейн» в объявлениях работало как ставка на цену биткоина: чем сильнее рос биткоин, тем сильнее отвечали инвесторы. Смеяться над покупателями таких акций я бы не спешил. По этому исследованию, так в среднем реагировали инвесторы на подобные отчёты[999], а переоценка всего, что связано с модной историей, — одна из примет пузыря, к которым мы вернёмся во второй части.

Обратный путь тоже был. В октябре 2017 года компания Bioptix, занимавшаяся ветеринарной и медицинской диагностикой, сменила название на Riot Blockchain и в ноябре купила 1200 машин для майнинга[1000]. В отличие от Long Blockchain, она действительно стала майнером, хотя и получила весной 2018 года повестку SEC с запросом информации[1001]. А 3 января 2023 года она переименовалась в Riot Platforms и убрала слово «блокчейн» из названия, объяснив это тем, что бизнес вырос за пределы майнинга[1002]. В 2017 году слово добавляли в название, в 2023-м его убирали.

---

https://www.nasdaq.com/press-release/long-island-iced-tea-corp-to-rebrand-as-long-blockchain-corp-20171221-00468 (ссылка по Википедии, не открыта)). Даты по Long Blockchain (исключение из Nasdaq 10.04.2018, отзыв регистрации 19.02.2021) — по пересказу MarketWatch и Bloomberg (Wikipedia, «Long Blockchain Corp.» (обращение 26.09.2026), со ссылками на MarketWatch, 11.04.2018 (https://www.marketwatch.com/story/nasdaq-to-delist-long-blockchain-corp-underlining-fading-bitcoin-fervor-2018-04-11) и Bloomberg, 22.02.2021 (https://www.bloomberg.com/news/articles/2021-02-22/long-blockchain-delisted-by-sec-after-riding-2017-s-crypto-craze). https://en.wikipedia.org/wiki/Long_Blockchain_Corp).

[995] Jay Clayton, «Opening Remarks at the Securities Regulation Institute», SEC, 22.01.2018. https://www.sec.gov/news/speech/speech-clayton-012218.

[996] Джей Клейтон, выступление 22.01.2018: «The SEC is looking closely at the disclosures of public companies that shift their business models to capitalize on the perceived promise of distributed ledger technology and whether the disclosures comply with the securities laws, particularly in the case of an offering.» Гипотетический пример: «(1) start to dabble in blockchain activities, (2) change its name to something like „Blockchain-R-Us," and (3) immediately offer securities» (Jay Clayton, «Opening Remarks at the Securities Regulation Institute», SEC, 22.01.2018. https://www.sec.gov/news/speech/speech-clayton-012218).

[997] Cheng S. F., De Franco G., Jiang H., Lin P. «Riding the Blockchain Mania: Public Firms' Speculative 8-K Disclosures». Management Science 65(12), 2019, pp. 5901–5913. DOI 10.1287/mnsc.2019.3357 (аннотация по Crossref: https://api.crossref.org/works/10.1287/mnsc.2019.3357).

[998] Cheng S. F., De Franco G., Jiang H., Lin P. Riding the Blockchain Mania: Public Firms' Speculative 8-K Disclosures. Management Science, 2019: «…investors overreact to a firm's first 8-K disclosure of a potential foray into Blockchain technology and that overreaction is a function of the Bitcoin price bubble.» Исследование касается первых упоминаний блокчейна в отчётах 8-K у «спекулятивных» фирм, а не смены названий (Cheng S. F., De Franco G., Jiang H., Lin P. «Riding the Blockchain Mania: Public Firms' Speculative 8-K Disclosures». Management Science 65(12), 2019, pp. 5901–5913. DOI 10.1287/mnsc.2019.3357 (аннотация по Crossref: https://api.crossref.org/works/10.1287/mnsc.2019.3357)).

[999] Cheng S. F., De Franco G., Jiang H., Lin P. «Riding the Blockchain Mania: Public Firms' Speculative 8-K Disclosures». Management Science 65(12), 2019, pp. 5901–5913. DOI 10.1287/mnsc.2019.3357 (аннотация по Crossref: https://api.crossref.org/works/10.1287/mnsc.2019.3357).

[1000] Riot Blockchain, Form 8-K, 04.10.2017, https://www.sec.gov/Archives/edgar/data/0001167419/000107997317000569/bioptix_8k.htm; Riot Blockchain, Form 10-K за 2017 год, https://www.sec.gov/Archives/edgar/data/1167419/000107997318000264/riot_10k-123117.htm.

[1001] Riot Blockchain, Form 10-K за 2017 год.

[1002] Riot Blockchain, «Riot Blockchain, Inc. Announces Corporate Rebranding to Riot Platforms, Inc.», GlobeNewswire, 03.01.2023, https://www.globenewswire.com/news-release/2023/01/03/2582242/0/en/Riot-Blockchain-Inc-Announces-Corporate-Rebranding-to-Riot-Platforms-Inc.html.

Большие компании в это время в основном присматривались. По опросу ИТ-директоров, результаты которого консалтинговая компания Gartner опубликовала в мае 2018 года, о каком-либо внедрении блокчейна сообщил 1%, а 77% ответили, что технология их организации не интересна или изучать её там не планируют[1003]. Через полтора года в «цикле хайпа» Gartner (это собственная модель компании, измерением её считать нельзя) блокчейн сполз во «впадину разочарования», и аналитик Gartner сказала, что большинство корпоративных проектов застряло в экспериментах[1004].[1005]

Общая тетрадка без общего кошелька

В ту же волну родились консорциумы, которые делали всё по учебнику. Они брали задачу, где пишущих действительно много, строили разрешённую сеть и приглашали в неё целую отрасль, то есть проходили первый вопрос с запасом. Сеть торгового финансирования Marco Polo запустили в сентябре 2017 года, к ней присоединились больше 30 банков, а заработала она после двух сорванных сроков, только в конце 2020 года и с ограниченным использованием[1006]. Прототип платформы аккредитивов (так называют обязательство банка заплатить продавцу, как только тот представит документы об отгрузке), позже названной Contour, появился тогда же[1007]. Проект we.trade европейских банков тоже вырос в эти годы[1008]. Третий вопрос у торгового финансирования тоже непрост. Аккредитив платят по документам об отгрузке, а документ описывает груз, который лежит в трюме, за пределами тетрадки.

Все три закрылись в течение восемнадцати месяцев, и официальная причина у всех одна: деньги. В мае 2022 года we.trade, где было двенадцать банков-акционеров, сообщила, что не смогла договориться с акционерами о финансировании дальнейших вложений[1009]. В феврале 2023 года Marco Polo перешла под управление временных ликвидаторов, после того как Bank of America вышел из намеченного партнёрства на 12 млн долларов, а других инвесторов не

[1003] Computer Weekly, «Most CIOs not interested in 'massively hyped' blockchain, finds Gartner», 04.05.2018, https://www.computerweekly.com/news/252440559/Most-CIOs-not-interested-in-massively-hyped-blockchain-finds-Gartner; пресс-релиз Gartner 03.05.2018.

[1004] CIO Dive, «Most blockchain applications sunk in the 'trough of disillusionment,' Gartner says», 09.10.2019, https://www.ciodive.com/news/most-blockchain-applications-sunk-in-the-trough-of-disillusionment-gartn/564613/; The Next Web, «Gartner says blockchain is sliding into the 'trough of disillusionment'», 08.10.2019, https://thenextweb.com/news/gartner-says-blockchain-is-sliding-into-the-trough-of-disillusionment.

[1005] Результаты опроса ИТ-директоров (2018 CIO Survey) Gartner опубликовала 03.05.2018; когда проводился сам опрос, в пересказах не указано. Опираемся на синхронный пересказ Computer Weekly (04.05.2018) и перепечатку релиза; сам пресс-релиз Gartner недоступен. Ещё 8% сообщили о краткосрочных планах или активных экспериментах. Формулировка о 77%: «no interest in the technology and/or no action planned to investigate or develop it» (Computer Weekly, «Most CIOs not interested in 'massively hyped' blockchain, finds Gartner», 04.05.2018, https://www.computerweekly.com/news/252440559/Most-CIOs-not-interested-in-massively-hyped-blockchain-finds-Gartner; пресс-релиз Gartner 03.05.2018). Авива Литан, Gartner, 2019: «Blockchain technologies have not yet lived up to the hype and most enterprise blockchain projects are stuck in experimentation mode.» Полной масштабируемости Gartner тогда ждал не раньше 2028 года (CIO Dive, «Most blockchain applications sunk in the 'trough of disillusionment,' Gartner says», 09.10.2019, https://www.ciodive.com/news/most-blockchain-applications-sunk-in-the-trough-of-disillusionment-gartn/564613/; The Next Web, «Gartner says blockchain is sliding into the 'trough of disillusionment'», 08.10.2019, https://thenextweb.com/news/gartner-says-blockchain-is-sliding-into-the-trough-of-disillusionment).

[1006] Global Trade Review, «Marco Polo brings in liquidators as funds run dry», 23.02.2023. https://www.gtreview.com/news/top-stories/marco-polo-brings-in-liquidators-as-funds-run-dry/; Irish Times, 22.02.2023. https://www.irishtimes.com/business/2023/02/22/provisional-liquidators-appointed-to-software-company-with-52m-debts/.

[1007] Global Trade Review, «Exclusive: Contour to shut down as bank shareholders pull funding», 27.10.2023. https://www.gtreview.com/news/top-stories/exclusive-contour-to-shut-down-as-bank-shareholders-pull-funding/.

[1008] Global Trade Review, «we.trade calls it quits after running out of cash», 06.06.2022. https://www.gtreview.com/news/top-stories/we-trade-calls-it-quits-after-running-out-of-cash/.

[1009] Global Trade Review, «we.trade calls it quits after running out of cash», 06.06.2022. https://www.gtreview.com/news/top-stories/we-trade-calls-it-quits-after-running-out-of-cash/.

нашлось[1010]. Contour закрылась в ноябре 2023 года, когда девять банков-владельцев прекратили её финансировать[1011].[1012]

Объяснение главы Contour, которое пересказало отраслевое издание Global Trade Review, стоит прочитать внимательно. Среди многих банков-акционеров не было ведущего инвестора, и громоздкая совместная собственность отпугивала венчурный капитал[1013]. По-моему, это объяснение весит больше, чем ссылка самой компании на трудный инвестиционный климат. Общую тетрадку, у которой нет одного хозяина, некому оказалось оплачивать. Каждый банк был готов пользоваться сетью, но нести её расходы в одиночку не хотел никто, и решить за остальных никто не мог.

Пусть десять банков вместе строят сеть, и она обходится в 10 млн долларов в год, по миллиону с каждого. Пока сделок мало, каждый банк получает от сети меньше миллиона и спрашивает себя, зачем платить. Если один банк выйдет, оставшимся девяти придётся платить больше, а сеть станет полезна меньшему числу клиентов, и следующему банку выйти будет уже проще. Сеть с одним хозяином так тоже может закрыться, но там решение принимает один, а здесь каждый из десяти может решить уйти в любой квартал, и договориться об общем кошельке им труднее, чем о формате записи.

Морская торговля попробовала другой путь. Платформу TradeLens основали в 2018 году Maersk и IBM, её задумывали как открытую и нейтральную площадку для всей отрасли, но принадлежала она крупнейшему игроку этой отрасли[1014]. В ноябре 2022 года компании объявили о её закрытии. Официальная причина: не удалось добиться полноценного сотрудничества всей отрасли, и платформа не стала коммерчески жизнеспособной как самостоятельный бизнес[1015].[1016] Распространённое объяснение состоит в том, что конкуренты Maersk не хотели работать на платформе конкурента, но в пресс-релизе этого нет, и это толкование со стороны[1017].

[1010] Global Trade Review, «Marco Polo brings in liquidators as funds run dry», 23.02.2023. https://www.gtreview.com/news/top-stories/marco-polo-brings-in-liquidators-as-funds-run-dry/; Irish Times, 22.02.2023. https://www.irishtimes.com/business/2023/02/22/provisional-liquidators-appointed-to-software-company-with-52m-debts/.

[1011] Global Trade Review, «Exclusive: Contour to shut down as bank shareholders pull funding», 27.10.2023. https://www.gtreview.com/news/top-stories/exclusive-contour-to-shut-down-as-bank-shareholders-pull-funding/.

[1012] we.trade: 12 банков-акционеров и IBM, лицензия у 16 банков в 15 странах; меморандум о прекращении работы — 26.05.2022 (Global Trade Review, «we.trade calls it quits after running out of cash», 06.06.2022. https://www.gtreview.com/news/top-stories/we-trade-calls-it-quits-after-running-out-of-cash/). Marco Polo: платформа TradeIX на R3 Corda; рабочей сеть должна была стать в начале 2019 года, потом во II квартале 2020-го; временных ликвидаторов назначил Высокий суд Ирландии, долги — 5,2 млн евро (Global Trade Review, «Marco Polo brings in liquidators as funds run dry», 23.02.2023. https://www.gtreview.com/news/top-stories/marco-polo-brings-in-liquidators-as-funds-run-dry/; Irish Times, 22.02.2023. https://www.irishtimes.com/business/2023/02/22/provisional-liquidators-appointed-to-software-company-with-52m-debts/). Contour: запуск в октябре 2020 года на R3 Corda; компания заявляла о сокращении обработки аккредитива примерно с 10 дней до суток — это её собственные данные. Цитата компании по GTR: «The investment climate has been incredibly challenging in the past year, and like many companies, it has affected our ability to raise funds and sustain our operations.» (Global Trade Review, «Exclusive: Contour to shut down as bank shareholders pull funding», 27.10.2023. https://www.gtreview.com/news/top-stories/exclusive-contour-to-shut-down-as-bank-shareholders-pull-funding/)

[1013] Global Trade Review, «Exclusive: Contour to shut down as bank shareholders pull funding», 27.10.2023. https://www.gtreview.com/news/top-stories/exclusive-contour-to-shut-down-as-bank-shareholders-pull-funding/.

[1014] A.P. Moller – Maersk, «A.P. Moller – Maersk and IBM to discontinue TradeLens, a blockchain-enabled global trade platform», 29.11.2022. https://www.maersk.com/news/articles/2022/11/29/maersk-and-ibm-to-discontinue-tradelens.

[1015] A.P. Moller – Maersk, «A.P. Moller – Maersk and IBM to discontinue TradeLens, a blockchain-enabled global trade platform», 29.11.2022. https://www.maersk.com/news/articles/2022/11/29/maersk-and-ibm-to-discontinue-tradelens.

[1016] Maersk, 29.11.2022. Ротем Хершко, Maersk: «Unfortunately, while we successfully developed a viable platform, the need for full global industry collaboration has not been achieved. As a result, TradeLens has not reached the level of commercial viability necessary to continue work and meet the financial expectations as an independent business.» Отключение — к концу I квартала 2023 года (A.P. Moller – Maersk, «A.P. Moller – Maersk and IBM to discontinue TradeLens, a blockchain-enabled global trade platform», 29.11.2022. https://www.maersk.com/news/articles/2022/11/29/maersk-and-ibm-to-discontinue-tradelens).

[1017] A.P. Moller – Maersk, «A.P. Moller – Maersk and IBM to discontinue TradeLens, a blockchain-enabled global trade platform», 29.11.2022. https://www.maersk.com/news/articles/2022/11/29/maersk-and-ibm-to-discontinue-tradelens.

У разрешённых сетей была и техническая трудность, и её хорошо видно на опыте SWIFT, международной системы обмена платёжными сообщениями между банками. В 2018 году SWIFT испытал распределённый реестр на сверке счетов с 34 банками. Технология справилась с задачей, но чтобы данные каждого счёта видели только его стороны, реестр пришлось разделить на 528 отдельных каналов, а для рабочей системы их понадобилось бы больше 100 000[1018].[1019] Общую тетрадку пришлось порезать на тысячи двусторонних тетрадок, то есть заново построить ту сеть двусторонних отношений, которую она должна была заменить.

Две линии неудач складываются в парадокс, и сидит он между первым и вторым вопросами. Блокчейн нужен там, где много сторон, не доверяющих друг другу, но именно таких участников труднее всего собрать на одной платформе. Если у платформы есть хозяин, как у TradeLens, остальные не хотят отдавать ему свои данные. Если хозяина нет, как у банковских консорциумов, некому платить и некому решать. Выход нашли те, кто перестал искать тетрадку без хозяина. Выжили проекты, которые тянул один оператор. Ему и так доверяли, а общая запись служила ему языком для разговора с другими.

Что прижилось

Прижилось меньше, чем обещали в 2017 году, и в двух местах. Первое место — деньги и ценные бумаги, которые ведёт известный оператор внутри существующей финансовой системы. Второе скромнее. Это реестры, которые по-прежнему ведут государство или компания, а в открытую тетрадку кладут только отпечатки своих записей.

Самые крупные цифры у сделок репо (так называют заём под залог ценных бумаг на короткий срок, часто на один день). Платформа компании Broadridge для таких сделок на распределённом реестре обработала в ноябре 2025 года в среднем 368 млрд долларов в день[1020].[1021] Это оборот, и сообщила о нём сама компания, без независимой проверки.

Почему общая запись прижилась именно здесь, проще всего понять на условном примере. Представим банк, у которого есть облигации на 100 млн долларов. Утром ему нужно занять под них деньги на несколько часов, а после обеда те же облигации понадобятся под другую сделку. Бумаги учитывает одна организация, деньги — другая, условия сделки записаны в системе третьей. Каждый раз, когда залог переходит из сделки в сделку, три записи должны сойтись, и пока они не сошлись, облигации заняты. Банк держит бумаги с запасом или платит за то, что они простаивают. Для сделки на одну ночь это терпимо, но чем короче сделки и чем их больше, тем дороже обходятся часы, когда залог застрял между тетрадками.

Теперь положим условия сделок и принадлежность залога в одну запись, которую видят все участники. Передать облигации из утренней сделки в послеобеденную можно, не дожидаясь, пока сверятся три чужие тетрадки, и тот же объём залога за день успевает поработать в

[1018] UNLOCK Blockchain, «SWIFT completes landmark DLT proof of concept», 12.03.2018 (пересказ пресс-релиза SWIFT), https://www.unlock-bc.com/news/2018-03-12/swift-completes-landmark-dlt-proof-of-concept; пресс-релиз SWIFT «Swift completes landmark DLT PoC», https://www.swift.com/news-events/press-releases/swift-completes-landmark-dlt-poc.

[1019] По пересказу пресс-релиза SWIFT (UNLOCK Blockchain, 12.03.2018): «To productise the solution, more than 100,000 channels would need to be established and maintained, covering all existing Nostro relationships» (UNLOCK Blockchain, «SWIFT completes landmark DLT proof of concept», 12.03.2018 (пересказ пресс-релиза SWIFT), https://www.unlock-bc.com/news/2018-03-12/swift-completes-landmark-dlt-proof-of-concept; пресс-релиз SWIFT «Swift completes landmark DLT PoC», https://www.swift.com/news-events/press-releases/swift-completes-landmark-dlt-poc).

[1020] Broadridge, пресс-релиз «Broadridge's Distributed Ledger Repo Platform Processes $368 Billion in Average Daily Trade Volumes in November», 04.12.2025. https://www.broadridge.com/press-release/2025/broadridge-distributed-ledger-repo-platform-november.

[1021] Broadridge, пресс-релиз 04.12.2025: всего 7,4 трлн долларов за месяц, на 466% больше, чем в ноябре 2024 года. Число участников и имена клиентов не раскрыты (Broadridge, пресс-релиз «Broadridge's Distributed Ledger Repo Platform Processes $368 Billion in Average Daily Trade Volumes in November», 04.12.2025. https://www.broadridge.com/press-release/2025/broadridge-distributed-ledger-repo-platform-november). Свежие цифры — в приложении Б.

большем числе сделок. Так мог бы переходить из рук в руки сарай плотника из первой главы, который утром записан за одним хранителем в залог, а к обеду уже за другим, и обе записи стоят на одной странице, где их видят оба.

Пример показывает только логику довода. Как именно устроен расчёт на платформе Broadridge, где там деньги, а где бумаги, я описывать не берусь. Но из него видно, что этот выигрыш требует общей записи для многих участников и не требует тетрадки без хозяина. Платформу ведёт одна компания, участники — банки и фонды, которых знают по имени, а запись касается самих денег и бумаг, у которых мало стыков с внешним миром. Второй вопрос такая система проходит плохо, хозяин у неё есть, а третий проходит хорошо.

Блокчейн-подразделение JPMorgan, которое в ноябре 2024 года переименовали из Onyx в Kinexys, по данным банка за 2025 год проводило в среднем больше 7 млрд долларов в день[1022].[1023] Методику подсчёта банк не раскрывает. В ноябре 2025 года JPMorgan сделал шаг, на котором граница между типами блокчейнов начала размываться. Банк выпустил для институциональных клиентов депозитный токен в долларах в публичной сети Base, сети второго уровня поверх Ethereum, а до того держал такие счета в собственной разрешённой сети[1024]. Депозитный токен устроен по четырнадцатому правилу посёлка: строчка в тетрадке, за которой стоит должник вне её. Только должник здесь — банк с лицензией, а в сундуке лежит вклад в этом банке.

Третья заметная линия — токенизированные фонды и облигации, то есть доли фондов и ценные бумаги, записанные строчками в блокчейне. Фонд денежного рынка BlackRock, запущенный в марте 2024 года, в конце сентября 2026 года управлял примерно 2,2 млрд долларов и имел всего 107 держателей[1025]. Всего токенизированных казначейских бумаг США на ту же дату было около 15 млрд долларов[1026].[1027] Сто семь держателей показывают, для кого этот инструмент. Им пользуются институты и криптокомпании, массовый инвестор до него пока не дошёл[1028].

У токенизированной облигации есть щель, знакомая по холодильнику, только узкая. Строчка в блокчейне означает бумагу, которую где-то хранит управляющий фондом, и держатель строчки верит, что бумага в сундуке есть, как держатель стейблкоина верит лавочнику. Закрывают эту щель тем же, чем в обычных финансах: лицензией управляющего, отчётностью, проверками и судом.

Центральные банки тоже строят общие реестры, и тоже с понятными хозяевами. В мае 2026 года Банк международных расчётов опубликовал отчёт о своём проекте Agorá, общей платформе для переводов между странами, а в июле 28 финансовых организаций и центробанков провели на ней настоящие переводы, пока на пробные суммы, около 800 тыс. швейцар-

---

[1022] J.P. Morgan, Kinexys (главная страница). https://www.jpmorgan.com/kinexys/index; J.P. Morgan, «Introducing Kinexys», 06.11.2024, https://www.jpmorgan.com/insights/payments/blockchain-digital-assets/introducing-kinexys.

[1023] Kinexys: «>$3 trillion in transaction volume across Kinexys since inception»; «>$7 billion in average daily transaction volume across Kinexys» (данные банка за 2025 год) (J.P. Morgan, Kinexys (главная страница). https://www.jpmorgan.com/kinexys/index). При переименовании 06.11.2024 банк сообщал о более чем 2 млрд долларов в день и более чем 1,5 трлн условного объёма с запуска (J.P. Morgan, «Introducing Kinexys», 06.11.2024, https://www.jpmorgan.com/insights/payments/blockchain-digital-assets/introducing-kinexys). Свежие цифры — в приложении Б.

[1024] J.P. Morgan Payments, «First bank issues USD deposit token on a public blockchain», 12.11.2025. https://www.jpmorgan.com/payments/newsroom/jpm-coin-usd-deposit-token-institutional-clients.

[1025] RWA.xyz, страница актива BUIDL (данные на 26.09.2026). https://app.rwa.xyz/assets/BUIDL.

[1026] RWA.xyz, «Tokenized Treasuries» (данные на 26.09.2026). https://app.rwa.xyz/treasuries.

[1027] RWA.xyz, данные на 26.09.2026: фонд BUIDL — 2,24 млрд долларов, 107 держателей, выпущен в десяти сетях (RWA.xyz, страница актива BUIDL (данные на 26.09.2026). https://app.rwa.xyz/assets/BUIDL); токенизированные казначейские бумаги США — 14,94 млрд долларов в 108 продуктах (RWA.xyz, «Tokenized Treasuries» (данные на 26.09.2026). https://app.rwa.xyz/treasuries). Свежие цифры — в приложении Б.

[1028] RWA.xyz, страница актива BUIDL (данные на 26.09.2026). https://app.rwa.xyz/assets/BUIDL.

ских франков на всех[1029]. Свои проекты есть у Денежно-кредитного управления Сингапура, которое вместе с банками пробует токенизацию активов, и у группы центробанков, строивших платформу для расчётов между странами в деньгах самих центробанков. В группу регуляторов сингапурского проекта входит и тот самый австралийский регулятор, что судился с ASX[1030].[1031] Все эти системы разрешённые: список короткий, и кто его ведёт, известно. Зачем центральным банкам собственные цифровые деньги и почему одни их строят, а другие запрещают, мы разберём, когда дойдём до того, как отвечает на крипту государство.

Путь SWIFT показательнее прочих, потому что это та самая сеть, что в 2018 году упёрлась в сто тысяч каналов. В 2023 году она испытала себя в роли посредника между тетрадками. Вместе с компанией Chainlink и больше чем десятком крупных финансовых институтов она показала, что через одну точку доступа к SWIFT можно передавать токенизированные активы между разными публичными и частными блокчейнами[1032]. Осенью 2025 года SWIFT объявил, что добавит в свою инфраструктуру общий реестр на блокчейне для круглосуточных платежей между странами[1033], а летом 2026 года, по пересказам его сообщений, запустил его в пилот с реальными переводами токенизированных вкладов, в котором участвуют 17 банков[1034].[1035] Оператором этого блокчейна остаётся сам SWIFT, а масштабы пилота пока не раскрыты.

У всех этих систем одинаковые черты. Оператор известен (банк, биржевая компания, центральный банк, SWIFT). Участники — закрытый круг профессионалов, которых можно

[1029] BIS Innovation Hub, «Project Agorá», https://www.bis.org/about/bisih/topics/fmis/agora.htm; BIS Innovation Hub, «Project Agorá». https://www.bis.org/about/bisih/topics/fmis/agora.htm.

[1030] MAS, media release «First industry pilot for digital asset and decentralised finance goes live», 02.11.2022. https://www.mas.gov.sg/news/media-releases/2022/first-industry-pilot-for-digital-asset-and-decentralised-finance-goes-live; MAS, «Project Guardian». https://www.mas.gov.sg/schemes-and-initiatives/project-guardian; MAS, «Project Guardian» (стр. опубликована 12.11.2025). https://www.mas.gov.sg/schemes-and-initiatives/project-guardian; BIS Innovation Hub, «Project mBridge». https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm.

[1031] Отчёт проекта Agorá — пресс-релиз BIS 27.05.2026 («Project Agorá shows how tokenisation can improve wholesale cross-border payments; work will advance to real-value testing»); тест на реальных деньгах — июль 2026 года, страница BIS «Real value testing»: «Twenty-eight private sector institutions and central banks completed transactions totalling approximately CHF 800,000»; расчёт занимал в среднем около 80 секунд (BIS Innovation Hub, «Project Agorá», https://www.bis.org/about/bisih/topics/fmis/agora.htm; BIS Innovation Hub, «Project Agorá». https://www.bis.org/about/bisih/topics/fmis/agora.htm). Проект Guardian Денежно-кредитного управления Сингапура запущен в 2022 году; в первом пилоте три финансовые компании, среди них DBS и JPMorgan, провели живую сделку с токенизированными вкладами в сингапурских долларах и японских иенах (MAS, media release «First industry pilot for digital asset and decentralised finance goes live», 02.11.2022. https://www.mas.gov.sg/news/media-releases/2022/first-industry-pilot-for-digital-asset-and-decentralised-finance-goes-live; MAS, «Project Guardian». https://www.mas.gov.sg/schemes-and-initiatives/project-guardian); австралийский регулятор (ASIC) входит в группу регуляторов проекта (MAS, «Project Guardian» (стр. опубликована 12.11.2025). https://www.mas.gov.sg/schemes-and-initiatives/project-guardian). mBridge — проект Банка международных расчётов с 2021 года, платформа для расчётов между странами в цифровых валютах центральных банков; в 2024 году передан самим участникам (BIS Innovation Hub, «Project mBridge». https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm).

[1032] CoinDesk, «Swift, Chainlink Tokenization Experiment Successfully Transfers Value Across Multiple Blockchains», 31.08.2023, https://www.coindesk.com/tech/2023/08/31/swift-chainlink-tokenization-experiment-successfully-transfers-value-across-multiple-blockchains; пресс-релиз SWIFT и копия на Business Wire не открыты.

[1033] Asset Servicing Times, «Swift adds blockchain-based ledger to technology infrastructure», 30.09.2025, https://www.assetservicingtimes.com/assetservicesnews/paymentsarticle.php?article_id=17219; пресс-релиз SWIFT.

[1034] Finadium, «Swift announces MVP go-live of open source blockchain-based ledger in 2026», 01.04.2026, https://finadium.com/swift-announces-mvp-go-live-of-open-source-blockchain-based-ledger-in-2026/; Finovate, «Swift Goes Live with New Blockchain-Based Ledger», 09.07.2026, https://finovate.com/swift-goes-live-with-new-blockchain-based-ledger/; первоисточник SWIFT «Swift's blockchain ledger ready for use as 17 banks set to pioneer tokenised cross-border payments…».

[1035] Asset Servicing Times, 30.09.2025 (прототип с Consensys, больше 30 финансовых институтов); Finovate, 09.07.2026 (пилот, 17 банков с шести континентов). Технологическая основа реестра в пересказах называется по-разному, до сверки с сообщением SWIFT мы её не указываем; масштабы пилота — в приложении Б (Asset Servicing Times, «Swift adds blockchain-based ledger to technology infrastructure», 30.09.2025, https://www.assetservicingtimes.com/assetservicesnews/paymentsarticle.php?article_id=17219; пресс-релиз SWIFT; Finadium, «Swift announces MVP go-live of open source blockchain-based ledger in 2026», 01.04.2026, https://finadium.com/swift-announces-mvp-go-live-of-open-source-blockchain-based-ledger-in-2026/; Finovate, «Swift Goes Live with New Blockchain-Based Ledger», 09.07.2026, https://finovate.com/swift-goes-live-with-new-blockchain-based-ledger/; первоисточник SWIFT «Swift's blockchain ledger ready for use as 17 banks set to pioneer tokenised cross-border payments…»).

назвать по именам и с которыми можно судиться. Запись касается денег и ценных бумаг, поэтому у неё меньше стыков с внешним миром, где правду нельзя проверить. Если не считать открытых сетей самой крипты, здесь блокчейн прижился прочнее всего.

Нужен ли в этих системах блокчейн вообще? По нашим трём вопросам многие из них прошли бы и на обычной базе у оператора. Их создатели отвечают, что выигрыш в другом: общий формат учёта между многими банками, расчёт без долгой сверки и программируемые активы. Сингапур прямо объясняет свой проект стремлением сделать рынки ликвиднее и эффективнее через токенизацию[1036]. Пример с облигациями показывает, откуда такой выигрыш мог бы браться. Я не возьмусь сказать, кто прав, потому что за вторую позицию говорят пока в основном пресс-релизы тех, кто эти системы продаёт. Обе стороны при этом согласны, что у каждой такой сети есть хозяин.

Есть и промежуточный ответ, он следует из первого раздела. Участники таких сетей — банки, которые сами ведут чужие деньги и не привыкли верить оператору на слово. Когда запись лежит только у оператора, каждый банк сверяет с ней свою тетрадку, а в спорном случае доказывает свою правоту письмами и выписками. Когда копия общей записи есть у каждого участника, сверять почти нечего, потому что все смотрят на одну страницу, и по замыслу таких сетей оператор не может тихо поправить строчку, не показав этого остальным. Хозяин остаётся, только пишет на виду. Окупает ли это распределённую запись по сравнению с общей базой, которую участники могут читать, решают издержки, а надёжных цифр о них у меня нет.

Вторая ниша скромнее, и лучше всего её видно на Грузии. С 2016 года Национальное агентство публичного реестра Грузии вместе с компанией Bitfury публикует в блокчейне биткоина отпечатки записей о собственности, а владелец получает цифровой сертификат с этим отпечатком[1037]. По одному из обзоров, так были отмечены 1,5 млн записей о земле[1038]. Сам реестр ведёт государственное агентство, и порядок регистрации от этого не изменился[1039].

Добавим восемнадцатое правило посёлка: хранитель ведёт свою тетрадку, как прежде, а в общую тетрадку без хозяина вписывает только отпечатки своих страниц. Это та самая метка времени из второй главы. Если хранитель позже тайком перепишет строчку, отпечаток перестанет совпадать с тем, что давно лежит в общей тетрадке, и подмену увидит любой. Но хранитель по-прежнему сам решает, что записать в свою тетрадку с самого начала, и общая тетрадка сохранит его ошибку или ложь так же надёжно, как правду[1040].

Эстония пошла тем же путём ещё раньше. Технология KSI, которой там защищают целостность государственных реестров и журналов, разработана в 2007 году, до биткоина, и официальный портал e-Estonia называет её «вдохновлённой блокчейном»[1041].[1042] Назначение у неё то же, что у восемнадцатого правила: доказать, что данные и системы не подменили[1043]. Иногда пишут, что Эстония хранит на блокчейне медицинские карты граждан. По описанию

[1036] MAS, media release «First industry pilot for digital asset and decentralised finance goes live», 02.11.2022. https://www.mas.gov.sg/news/media-releases/2022/first-industry-pilot-for-digital-asset-and-decentralised-finance-goes-live; MAS, «Project Guardian». https://www.mas.gov.sg/schemes-and-initiatives/project-guardian.

[1037] Exonum (Bitfury), «Improving the security of a government land registry», https://exonum.com/story-georgia.

[1038] New America, «Blockchain and Property Rights» (серия PropRightsTech Primers, без даты, ссылки 2018–2019), https://www.newamerica.org/insights/proprightstech-primers/blockchain-and-property-rights/.

[1039] Exonum (Bitfury), «Improving the security of a government land registry», https://exonum.com/story-georgia.

[1040] Per Aarvik, «Anti-corruption reforms have been successful in Georgia, but blockchain is stealing the limelight», U4 Anti-Corruption Resource Centre, 24.10.2022, https://www.u4.no/blog/anti-corruption-reforms-successful-in-georgia-blockchain-stealing-limelight.

[1041] e-Estonia, «KSI Blockchain». https://e-estonia.com/solutions/cyber-security/ksi-blockchain/.

[1042] e-Estonia: «KSI is a blockchain inspired technology designed in Estonia and used globally to ensure networks, systems, and data are free of compromise, all while retaining 100% data privacy.» (e-Estonia, «KSI Blockchain». https://e-estonia.com/solutions/cyber-security/ksi-blockchain/)

[1043] e-Estonia, «KSI Blockchain». https://e-estonia.com/solutions/cyber-security/ksi-blockchain/.

самого портала, KSI нужна для проверки целостности, а хранилищем данных её там не называют[1044].

О Грузии обычно спрашивают, помог ли блокчейн победить коррупцию в регистрации земли. Пер Орвик, независимый автор, пишущий о цифровых технологиях и борьбе с коррупцией, в блоге антикоррупционного центра U4 отвечает, что успех пришёл раньше. Его принесли реформы, начатые законом о реестре 2004 года: старые реестры распустили, создали новое агентство, записи оцифровали. Как быстро такие реформы меняли отношение людей, Орвик показывает на соседнем, гражданском реестре. В 2004 году 97% опрошенных называли его самым коррумпированным ведомством страны, а через два года 97% считали его свободным от коррупции[1045]. Отпечатки в биткоине появились больше чем через десять лет после начала реформ, когда доверие к реестру уже было.

Бесполезны ли они? Думаю, что нет. Отпечатки защищают от одной определённой беды, от того, что будущий чиновник тайком перепишет старую запись. Если однажды реформы откатятся и доверие к агентству пошатнётся, у владельца останется сертификат, который можно сверить с тетрадкой, где никто не хозяин. Стоит такая страховка немного. Хранитель может вписать в общую тетрадку один отпечаток сразу за много страниц, собрав их в дерево, как во второй главе, а принимать заявления, вести реестр и разбирать споры агентство продолжает по-старому. Источником доверия к реестру она не была и стать им не могла.

Три вопроса к слову «блокчейн»

Вопросы из второго раздела, которыми мы проверяли каждую историю главы, на схеме выглядят так[1046].

[1044] e-Estonia, «KSI Blockchain». https://e-estonia.com/solutions/cyber-security/ksi-blockchain/.

[1045] Per Aarvik, «Anti-corruption reforms have been successful in Georgia, but blockchain is stealing the limelight», U4 Anti-Corruption Resource Centre, 24.10.2022, https://www.u4.no/blog/anti-corruption-reforms-successful-in-georgia-blockchain-stealing-limelight.

[1046] Wüst & Gervais, 2018, section III; Wüst & Gervais, 2018, Fig. 1; NISTIR 8202, 2018, Figure 6 «DHS Science & Technology Directorate Flowchart», p. 42.

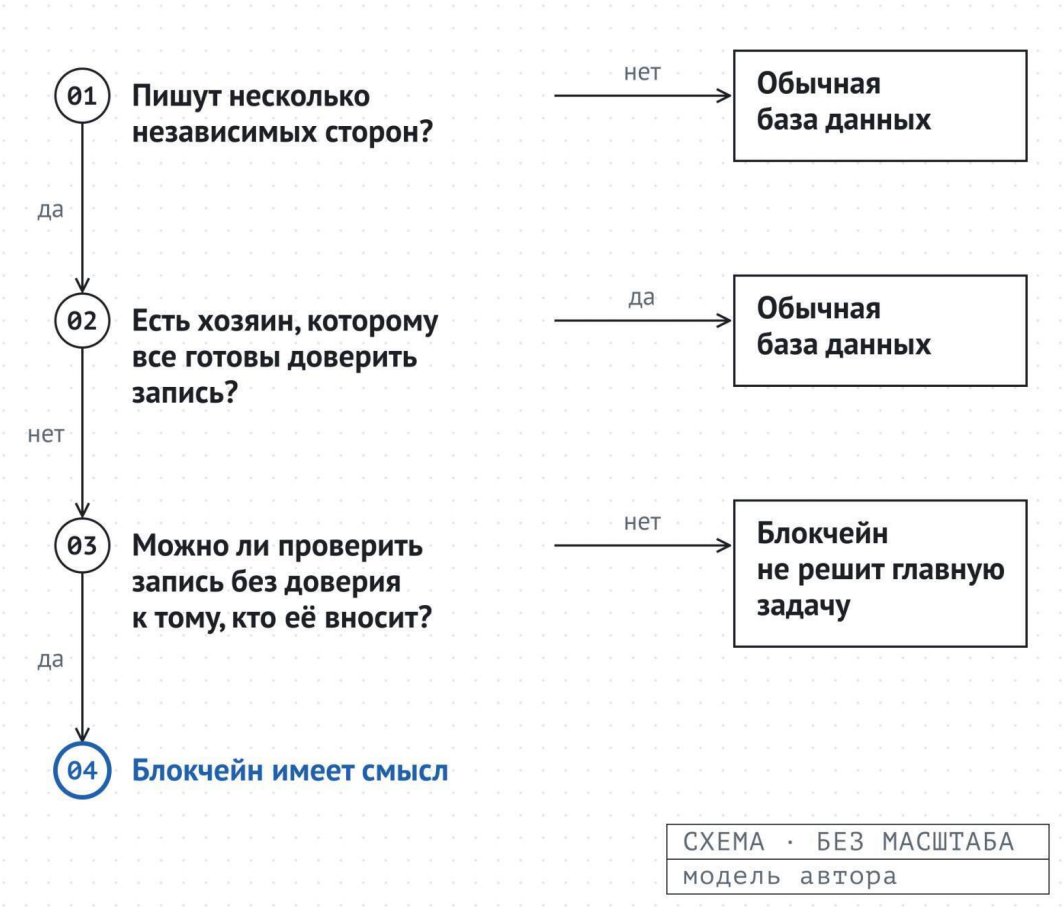


Рисунок 6.3. Три вопроса

Пишут ли в запись несколько независимых сторон? Если пишущий один, ему нужна база данных[1047]. Сюда же относятся проекты, где пишущих формально много, но все они вносят данные в систему одной компании, и компании, у которых блокчейн есть только в названии.

Есть ли тот, кому все пишущие готовы доверить запись? Если такой хозяин есть и спора о нём нет, база данных у этого хозяина быстрее и дешевле[1048]. Хозяином может оказаться и биржа, и регулятор, и крупнейший покупатель вроде Walmart, если остальные его слушаются.

Можно ли проверить записанное, не доверяя тому, кто его вносит? Если нельзя, блокчейн сохранит ложь так же надёжно, как правду, и главную задачу не решит[1049]. Чем ближе запись к деньгам и чем дальше от вещей, тем чаще ответ «можно».

Истории главы добавляют к трём вопросам две оговорки. Когда блокчейн разрешённый, ищите того, кто ведёт список, потому что вся честность записи теперь держится на нём, и проверять его стоит так же строго, как любого хранителя из первой главы[1050]. А цифры успеха взвешивайте строже, чем цифры провала. Обороты работающих платформ почти всегда сообщают сами компании, тогда как цифры закрытий чаще сверял кто-то посторонний (внешний

[1047] Wüst & Gervais, 2018, Fig. 1.

[1048] Accenture, «ASX CHESS Replacement Application Delivery Review», November 2022, с. 18 и с. 6 (PDF, копия: https://www.euromoney.com/pdf/asx-chess-replacement-application-delivery-review-2022-pdf/; ASX в сообщении https://www.asx.com.au/content/dam/asx/about/media-releases/2022/60-17-november-2022-CHESS-Replacement-ASX-reassessing-financial-derecognition_.pdf даёт ссылку на тот же отчёт).

[1049] Wüst & Gervais, 2018, section IV.A и Fig. 3.

[1050] NISTIR 8202, 2018, section 2.2, pp. 5–6.

обзор, ликвидаторы, суд)[1051]. Компании при этом не обязательно ошибаются, просто их цифры никто со стороны не проверял.

Если честно пройти все три вопроса, вы чаще всего придёте туда, откуда начиналась книга. Задача, в которой несколько сторон, не доверяющих друг другу, пишут в общую запись и никто не может и не хочет быть её хозяином, почти всегда оказывается задачей о деньгах. Вне денег тетрадка прижилась в двух видах, как общий формат у хозяина, которому выгодно вести свою тетрадку понятно для соседей, и как отпечатки чужих записей в открытой тетрадке, защищающие от тайной правки. Австралийская биржа могла бы остановиться на втором вопросе в самом начале проекта, а вместо этого через несколько лет его задал за неё внешний обзор[1052].

Слово «блокчейн» тем временем прошло свою волну. В 2017 году его вписывали в названия компаний, к 2023-му одни проекты под ним закрылись, а другие убрали его с вывески, и двигали эту волну ожидания и бюджеты[1053]. Восемнадцать правил посёлка описывали саму тетрадку. Во второй части речь пойдёт о людях, которые занимают под её строчки, и о волнах, которые движет долг, от цикла к циклу на самом крипторынке.

[1051] Broadridge, пресс-релиз «Broadridge's Distributed Ledger Repo Platform Processes $368 Billion in Average Daily Trade Volumes in November», 04.12.2025. https://www.broadridge.com/press-release/2025/broadridge-distributed-ledger-repo-platform-november; ASX, «ASX will reassess all aspects of the CHESS replacement project and derecognise capitalised software of $245-255 million pre-tax in 1H23», 17.11.2022, https://www.asx.com.au/content/dam/asx/about/media-releases/2022/60-17-november-2022-CHESS-Replacement-ASX-reassessing-financial-derecognition_.pdf; Global Trade Review, «Marco Polo brings in liquidators as funds run dry», 23.02.2023. https://www.gtreview.com/news/top-stories/marco-polo-brings-in-liquidators-as-funds-run-dry/; Irish Times, 22.02.2023. https://www.irishtimes.com/business/2023/02/22/provisional-liquidators-appointed-to-software-company-with-52m-debts/; ASIC, 26-119MR «ASX admits misleading conduct relating to CHESS replacement project», 2026, https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2026-releases/26-119mr-asx-admits-misleading-conduct-relating-to-chess-replacement-project; ASIC, 26-143MR «ASX ordered to pay $20.5 million penalty…», 2026, https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2026-releases/26-143mr-asx-ordered-to-pay-205-million-penalty-for-misleading-conduct-relating-to-chess-replacement-project.

[1052] ASX, «ASX will reassess all aspects of the CHESS replacement project and derecognise capitalised software of $245-255 million pre-tax in 1H23», 17.11.2022, https://www.asx.com.au/content/dam/asx/about/media-releases/2022/60-17-november-2022-CHESS-Replacement-ASX-reassessing-financial-derecognition_.pdf; Accenture, «ASX CHESS Replacement Application Delivery Review», November 2022, с. 18 и с. 6 (PDF, копия: https://www.euromoney.com/pdf/asx-chess-replacement-application-delivery-review-2022-pdf/; ASX в сообщении https://www.asx.com.au/content/dam/asx/about/media-releases/2022/60-17-november-2022-CHESS-Replacement-ASX-reassessing-financial-derecognition_.pdf даёт ссылку на тот же отчёт).

[1053] U.S. SEC, press release 2021-121 «SEC Charges Three Individuals with Insider Trading», 09.07.2021. https://www.sec.gov/newsroom/press-releases/2021-121; пресс-релиз компании о переименовании (21.12.2017): https://www.nasdaq.com/press-release/long-island-iced-tea-corp-to-rebrand-as-long-blockchain-corp-20171221-00468 (ссылка по Википедии, не открыта); Global Trade Review, «Exclusive: Contour to shut down as bank shareholders pull funding», 27.10.2023. https://www.gtreview.com/news/top-stories/exclusive-contour-to-shut-down-as-bank-shareholders-pull-funding/; Riot Blockchain, «Riot Blockchain, Inc. Announces Corporate Rebranding to Riot Platforms, Inc.», GlobeNewswire, 03.01.2023, https://www.globenewswire.com/news-release/2023/01/03/2582242/0/en/Riot-Blockchain-Inc-Announces-Corporate-Rebranding-to-Riot-Platforms-Inc.html.

Часть II. Как это уже работало: циклы криптоэпохи

Глава 7. Анатомия криптоцикла

Пока вы ищете причину каждого обвала крипторынка в новости того дня (в новых пошлинах, в решении американского центрального банка, в очередном запрете), рынок будет казаться вам погодой, которую нельзя понять и остаётся только переждать. Поводы у обвалов каждый раз новые, а сами обвалы похожи друг на друга куда больше, чем их поводы. С 2011 года биткоин прошёл пять больших циклов, и под разными декорациями в них повторялась одна последовательность: новая история, приток денег, заёмные деньги и плечо, пик, принудительные продажи, расчистка. Истории, биржи, монеты и люди меняются, механизм остаётся прежним. Кто его видит, тот может понять, на каком этапе рынок сейчас, и для этого ему не нужно угадывать цену.

Посёлок первой главы, где хранитель пишет строчки в долг, уже дышал такими волнами в игрушечном виде, и во второй части их пора проверить на настоящих ценах. Модель цикла я собираю из работ экономистов и историков, которые изучали мании и кризисы задолго до криптовалют, и каждое её звено опираю либо на них, либо на данные. Где мне приходится достраивать модель самому, я так и говорю.

Одно ограничение лучше назвать сразу. Модель говорит, что за чем следует и какие признаки видны на каждом шаге, но молчит о том, когда наступит следующий шаг и какой будет цена. Есть, правда, календарь циклов, привязанный к расписанию выпуска новых биткоинов, и три раза подряд он с ценой совпал. Почему он совпадал, пока никто не показал, и этот спор мы разберём ближе к концу главы.

Циклы биткоина в цифрах

Сначала посмотрим на то, что модель должна объяснить. Циклом я называю путь цены от одного глубокого дна до следующего, с пиком посередине, а падением цикла — расстояние от пика до ближайшего дна после него. Большим я называю цикл, на пике которого цена поставила новый рекорд. Цены всех циклов сняты заново по дневным данным Bitstamp, одной из старейших работающих криптобирж, чья история торгов начинается в 2011 году[1054].[1055] Индексы,

---

[1054] Bitstamp API, дневные свечи BTC/USD: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=12&start=1385337600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=15&start=1420416000; Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=4&start=1759622400; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782691200; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782172800; трёхдневные свечи за январь–март и июль–сентябрь 2026: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1767225600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1782864000.

[1055] Bitstamp, публичный API v2, дневные свечи BTC/USD по всемирному времени, данные сняты 26.09.2026. В таблице — внутридневные максимумы и минимумы; на закрытие дня цифры другие (например, 14.01.2015 день закрылся на 171,41 доллара) (Bitstamp API, дневные свечи BTC/USD: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=12&start=1385337600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=15&start=1420416000). Строка 2011 года собрана с двух бирж: пик — Mt. Gox (08.06.2011), дно — свечи Bitstamp, где в те дни проходили десятки–сотни биткоинов в сутки, а во многие дни ни одного, поэтому надёжность этой строки ниже остальных; повторный низ — 2,25 доллара 21.11.2011 (Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=61&start=1314835200 (сентябрь–октябрь 2011); https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=30&start=1320105600 (ноябрь 2011); https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=40&start=1322697600 (декабрь 2011 — начало января 2012); пик — Bitcoin Wiki). Строка 2019–2020 годов — по общему определению цикла: наибольший максимум между донными 15.12.2018 и 13.03.2020 — 13 880 долларов 26.06.2019 (Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?

которые собирают цену с разных площадок, дают немного другие числа, поэтому все цифры ниже стоит читать со словом «около». Первый пик 2011 года Bitstamp не застала, и для него взята цена биржи Mt. Gox[1056]. Рынок тогда был крошечным, и в день минимума 2011 года на Bitstamp сменили владельца всего 62 биткоина[1057].

Таблица 7.1. Циклы биткоина: пики и дна в долларах (внутридневные максимумы и минимумы)

Цикл	Пик	Дно	Падение	От пика до дна
2011	31,91 (08.06.2011, Mt. Gox)	2,22 (20.10.2011)	около 93%	около 4,5 месяца
2013–2015	1 163 (30.11.2013)	152,40 (14.01.2015)	87%	410 дней
2017–2018	19 666 (17.12.2017)	3 122 (15.12.2018)	84%	363 дня
2019–2020, малый	13 880 (26.06.2019)	3 850 (13.03.2020)	72%	261 день

step=86400&limit=6&start=1583798400; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=4&start=1581465600). Минимум открытого цикла на Bitstamp — 57 734,63 доллара 01.07.2026; прежние низы — 59 930 (начало февраля 2026 года) и 58 035 (25.06.2026) (Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=4&start=1759622400; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782691200; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782172800; трёхдневные свечи за январь–март и июль–сентябрь 2026: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1767225600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1782864000). Свежие цифры — в приложении Б.

[1056] Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=61&start=1314835200 (сентябрь–октябрь 2011); https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=30&start=1320105600 (ноябрь 2011); https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=40&start=1322697600 (декабрь 2011 — начало января 2012); пик — Bitcoin Wiki.

[1057] Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=61&start=1314835200 (сентябрь–октябрь 2011); https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=30&start=1320105600 (ноябрь 2011); https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=40&start=1322697600 (декабрь 2011 — начало января 2012); пик — Bitcoin Wiki.

2021–2022
69 000 (10.11.2021)
15 479 (21.11.2022)
78%
376 дней

2024–2026
126 272 (06.10.2025)
57 735 (01.07.2026), пока
54%, пока
268 дней, пока

Данные на 26.09.2026: Bitstamp, дневные свечи; пик 2011 года — Mt. Gox[1058].

Каждое большое падение было глубоким, и каждое следующее оказывалось мельче предыдущего, от 93% в 2011 году до 78% в 2021–2022 годах и пока 54% в открытом цикле[1059]. Малый цикл 2019–2020 годов в этот ряд не входит. Его пик, 13 880 долларов в июне 2019 года, до рекорда 2017-го не дотянул, а последний отрезок падения пришёлся на ковидный шок, когда с февральского максимума 2020 года цена меньше чем за месяц потеряла 63%[1060].[1061] Для модели этот цикл полезен своей непохожестью, и к его концу мы вернёмся ниже.

Все эти цифры относятся к биткоину. Модель я строю на нём, потому что у него самая длинная история цен и по нему есть первичные данные за все циклы. Остальной крипторынок проходит те же этапы, но размах у него бывает куда больше. В обвал 10–11 октября 2025 года токены из выборки CoinDesk подешевели в среднем примерно на 47%, а внутридневные просадки сотни крупнейших токенов доходили в среднем до 58%[1062]. Если биткоин в модели — средний случай, то мелкие монеты — случай с тем же механизмом и более тонким льдом.

[1058] Bitstamp API, дневные свечи BTC/USD: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=12&start=1385337600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=15&start=1420416000; Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=6&start=1513209600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=8&start=1544486400; Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=6&start=1583798400; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=4&start=1581465600; Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1636329600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1668816000; Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=4&start=1759622400; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782691200; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782172800; трёхдневные свечи за январь–март и июль–сентябрь 2026: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1767225600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1782864000; Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=61&start=1314835200 (сентябрь–октябрь 2011); https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=30&start=1320105600 (ноябрь 2011); https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=40&start=1322697600 (декабрь 2011 — начало января 2012); пик — Bitcoin Wiki.

[1059] расчёт автора по данным (Bitstamp); для 2011 — V. Ganne (Swissquote), TradingView, 17.11.2025, по данным Glassnode, https://www.tradingview.com/chart/BTC_ATHDRAWDOWN/9AUq2iAG-Bitcoin-What-Historical-Drawdown-in-a-Bear-Market/; CoinDesk, 24.09.2026.

[1060] Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=6&start=1583798400; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=4&start=1581465600.

[1061] Bitstamp: максимум перед шоком — 10 500,50 доллара 13.02.2020, минимум — 3 850 долларов 13.03.2020; падение около 63% за 29 дней (Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=6&start=1583798400; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=4&start=1581465600).

[1062] CoinDesk Research, «Market Spotlight: Inside Crypto's $19 Billion Liquidation Event», 17.10.2025 (обновлено 30.10.2025), https://www.coindesk.com/research/market-spotlight-the-19-billion-liquidation-that-shook-crypto.

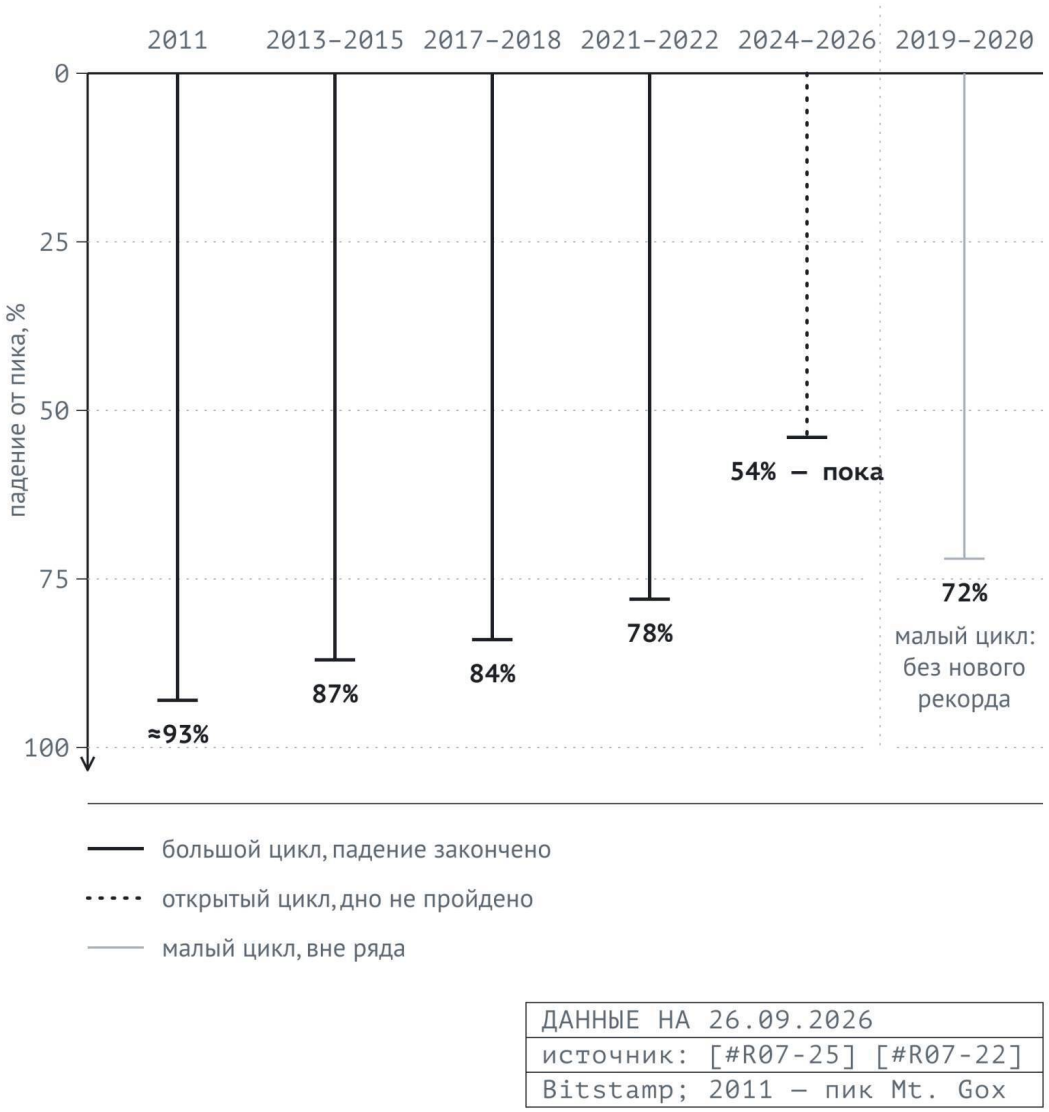


Рисунок 7.1. Глубина падений биткоина от пика до дна по циклам

Подъёмы от цикла к циклу тоже мельчали. От дна 2015 года до пика 2017-го цена выросла примерно в 129 раз, от дна 2018 года до пика 2021-го — примерно в 22 раза, от дна 2022 года до пика 2025-го — примерно в 8 раз[1063]. Размах цикла сжимается по мере того, как растёт сам рынок. Объяснения напрашиваются (рынок стал крупнее, в нём больше денег больших институтов, меньше доля новичков), но это гипотезы, и прямых доказательств ни одной из них у меня нет[1064].

Пять точек дают наблюдение, закона из них не выходит. Открытый цикл ещё может углубиться, и продолжить ряд словами «следующее падение будет таким-то» нельзя: ряд слишком короткий, а механизм не обязывает его продолжаться[1065]. Это хорошо видно на другом пра-

[1063] расчёт автора по данным (Bitstamp).

[1064] расчёт автора по данным (Bitstamp).

[1065] расчёт автора по данным (Bitstamp); для 2011 — V. Ganne (Swissquote), TradingView, 17.11.2025, по данным Glassnode, https://www.tradingview.com/chart/BTC_ATHDRAWDOWN/9AUq2iAG-Bitcoin-What-Historical-Drawdown-in-a-Bear-Market/; CoinDesk, 24.09.2026.

виле, которое любят повторять в годы подъёма, будто каждое дно выше прошлого пика. Для доньев 2015 и 2018 годов оно верно (152 доллара больше 32, а 3122 больше 1163), но мартовское дно 2020 года и дно 2022-го оказались ниже пика 2017-го, а минимум 2026 года — ниже пика 2021-го[1066].

Длительность спада держалась ровнее, чем глубина. В трёх полных больших циклах от пика до дна прошло примерно по году, а до нового рекорда цене после дна понадобилось ещё от года с небольшим до двух лет[1067].[1068] Тот, кто купил на самой вершине 2017 или 2021 года, возвращался к своей цене от двух с лишним до трёх лет. В открытом цикле нового рекорда пока нет.

Малый цикл кончился обвалом. В ковидный шок 12 и 13 марта 2020 года биткоин на Bitstamp подешевел примерно вдвое за двое суток, а объём торгов в эти дни был в семь раз выше обычного[1069]. Около 10:45 по всемирному времени 12 марта цена за 15 минут упала с 7200 до 5678 долларов, и только на одной бирже, BitMEX, это падение обернулось принудительным закрытием позиций на 702 млн долларов; больше 90% из них были ставками на рост, сделанными в долг[1070].

Следующий цикл начался резко: от мартовского дна до ноября 2021 года цена выросла примерно в 18 раз[1071], и почему так вышло, станет ясно, когда дойдём до денег центральных банков.

Что о пузырях знали до биткоина

Опор у модели четыре, и каждая смотрит на одно явление со своей стороны. Хайман Мински смотрел на то, что делает с подъёмом долг, Чарльз Киндлбергер — на порядок событий, Уильям Куинн и Джон Тёрнер — на условия, при которых загорается пузырь, Роберт Шиллер — на истории, которые люди рассказывают друг другу. Писали они о других временах, но в книгах троих из них крипта уже появилась (у Киндлбергера — в новом издании, которое готовили уже его продолжатели).

[1066] Bitstamp API, дневные свечи BTC/USD: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=12&start=1385337600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=15&start=1420416000; Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=6&start=1513209600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=8&start=1544486400; Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=6&start=1583798400; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=4&start=1581465600; Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1636329600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1668816000; Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=4&start=1759622400; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782691200; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782172800; трёхдневные свечи за январь–март и июль–сентябрь 2026: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1767225600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1782864000.

[1067] Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=6&start=1513209600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=8&start=1544486400; Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1636329600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1668816000.

[1068] Bitstamp: от дна 15.12.2018 до нового рекорда 30.11.2020 (19 864,15) — 716 дней; от дна 21.11.2022 до нового рекорда 05.03.2024 (69 210) — 470 дней (Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=6&start=1513209600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=8&start=1544486400; Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1636329600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1668816000).

[1069] Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=6&start=1583798400; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=4&start=1581465600.

[1070] O. Godbole, «Bitcoin's Crash Triggers Over $700M in Liquidations on BitMEX», CoinDesk, 12.03.2020 (по данным Skew), https://www.coindesk.com/markets/2020/03/12/bitcoins-crash-triggers-over-700m-in-liquidations-on-bitmex.

[1071] FRED, ряд M2SL (M2, сезонно скорректированный, млрд долл.): https://fred.stlouisfed.org/graph/fredgraph.csv?id=M2SL&cosd=2020-01-01&coed=2023-12-01.

Американский экономист Мински делил заёмщиков по тому, как их доход соотносится с долгом[1072]. У хедж-единиц, как он их называл, денежного потока хватает и на проценты, и на возврат самого долга. У спекулятивных доход покрывает проценты, а основной долг приходится раз за разом перезанимать. У единиц «понци» дохода не хватает ни на долг, ни на проценты, и расплачиваться можно, только продавая имущество или занимая снова[1073].[1074] В посёлке первой главы первым был бы плотник, который за лето отработает доски целиком, вторым — плотник, который отдаёт только плату за пользование и каждую осень просит продлить долг, третьим — тот, кто и эту плату берёт из нового займа. Название третьей группы напоминает о финансовых пирамидах, но у Мински «понци» — тип финансирования, и такой заёмщик может быть вполне честным человеком[1075].

Свою теорию Мински назвал гипотезой финансовой нестабильности, и держится она на том, что доли трёх групп со временем меняются. За долгие годы процветания, писал он, экономика переходит от финансовых отношений, при которых система устойчива, к таким, при которых она неустойчива[1076].[1077] Спокойные годы сами готовят неспокойные, потому что чем дольше всё идёт хорошо, тем больше в экономике заёмщиков второго и третьего типа.

Мински описал и то, что бывает дальше. Если в экономике с большой долей спекулятивных единиц начинается инфляция и власти поднимают ставки, спекулятивные единицы превращаются в единицы «понци», собственный капитал тех, кто уже был «понци», быстро тает, и всем, кому не хватает денежного потока, приходится продавать позиции. По его словам, это, скорее всего, ведёт к обвалу цен активов[1078].[1079] В нашей модели это этап принудительных продаж, и в 2022 году крипторынок прошёл его почти по Мински: ставка ФРС, американского центрального банка, за полтора года выросла с почти нулевой до 5,33%, а за ней пошли принудительные продажи и банкротства кредиторов[1080] (подробно — в главе 9).

Внешние шоки этой модели не нужны: циклы, по Мински, вырастают из внутренней динамики экономики и из системы вмешательств, которой экономику пытаются удержать в разумных границах[1081].[1082] Новость дня может поджечь накопленное, но накопила его не она, и масштаб пожара задаёт долг.

[1072] Hyman P. Minsky, «The Financial Instability Hypothesis», Levy Economics Institute, Working Paper No. 74, May 1992, pp. 6–7, https://www.levyinstitute.org/pubs/wp74.pdf.

[1073] Hyman P. Minsky, «The Financial Instability Hypothesis», Levy Economics Institute, Working Paper No. 74, May 1992, pp. 6–7, https://www.levyinstitute.org/pubs/wp74.pdf.

[1074] Minsky H. P. The Financial Instability Hypothesis. Levy Economics Institute, Working Paper No. 74, May 1992, pp. 6–7: «Hedge financing units are those which can fulfill all of their contractual payment obligations by their cash flows… For Ponzi units, the cash flows from operations are not sufficient to fulfill either the repayment of principle or the interest due on outstanding debts…» Написание principle — как в оригинале (Hyman P. Minsky, «The Financial Instability Hypothesis», Levy Economics Institute, Working Paper No. 74, May 1992, pp. 6–7, https://www.levyinstitute.org/pubs/wp74.pdf).

[1075] Hyman P. Minsky, «The Financial Instability Hypothesis», Levy Economics Institute, Working Paper No. 74, May 1992, pp. 6–7, https://www.levyinstitute.org/pubs/wp74.pdf.

[1076] Minsky, 1992, pp. 7–8.

[1077] Там же, pp. 7–8. Это вторая теорема гипотезы финансовой нестабильности: «The second theorem of the financial instability hypothesis is that over periods of prolonged prosperity, the economy transits from financial relations that make for a stable system to financial relations that make for an unstable system.» (Minsky, 1992, pp. 7–8)

[1078] Minsky, 1992, p. 8.

[1079] Там же, p. 8: «…speculative units will become Ponzi units and the net worth of previously Ponzi units will quickly evaporate. Consequently, units with cash flow shortfalls will be forced to try to make position by selling out position. This is likely to lead to a collapse of asset values.» (Minsky, 1992, p. 8)

[1080] FRED, Federal Reserve Bank of St. Louis, ряд FEDFUNDS (Effective Federal Funds Rate, в среднем за месяц): https://fred.stlouisfed.org/graph/fredgraph.csv?id=FEDFUNDS&cosd=2021-12-01&coed=2023-09-01; https://fred.stlouisfed.org/graph/fredgraph.csv?id=FEDFUNDS&cosd=2024-06-01&coed=2026-09-01; Galaxy Research, Q2 2026.

[1081] Minsky, 1992, p. 8.

[1082] Там же, p. 8: «The financial instability hypothesis is a model of a capitalist economy which does not rely upon exogenous shocks to generate business cycles of varying severity.» (Minsky, 1992, p. 8) Выражение «момент Мински», которое часто встречается в прессе, придумал экономист Пол Маккалли (PIMCO) в 1998 году; сам Мински так не говорил. Авторство

Чарльз Киндлбергер, историк финансовых кризисов, в 1978 году выпустил книгу «Мании, паники и крахи»[1083] и, отталкиваясь от ранней работы Мински, выстроил из идей экономистов-классиков последовательность событий[1084]. В восьмом издании (2023) она сведена к одной фразе: «смещение», то есть событие, открывающее новую возможность заработать, может повести к спекуляции, расширению кредита и эйфории; за ними следует финансовое напряжение, а затем кризис, который заканчивается паникой и крахом[1085].[1086] Завершается кризис в этой традиции «отвращением», когда цены обваливаются и участники спешат продать первыми[1087].[1088] У обмана в этой последовательности тоже было своё место. В первом издании между главами о денежном топливе и о «критической стадии» стоит отдельная глава «Появление жульничества»[1089],[1090] и в следующих двух главах, когда дойдём до ICO и FTX, это место пустовать не будет.

Куинн и Тёрнер, историки финансов, в книге «Бум и крах» (2020) описывают пузырь как огонь, для которого нужны три вещи, треугольник пузыря[1091]. Кислород — ликвидность рынка, то есть лёгкость, с которой актив можно купить, продать, разделить на части и передать

— по энциклопедической справке, сама речь Маккалли не открыта (Wikipedia, «Minsky moment», https://en.wikipedia.org/wiki/Minsky_moment (со ссылкой на P. McCulley, «Playing solitaire with a deck of 51…», PIMCO Global Central Bank Focus, April 2009, архив: https://web.archive.org/web/20090416003203/http://www.pimco.com/LeftNav/Featured+Market+Commentary/FF/2009/Global+Central+Bank+Focus+April+2009+Money+Marketeers+Solitaire+McCulley.htm)).

[1083] метаданные Crossref: https://api.crossref.org/works/10.1007/978-3-031-16008-0_2; https://api.crossref.org/works/10.1007/978-3-031-16008-0_14; книга: DOI 10.1007/978-3-031-16008-0 (ISBN 978-3-031-16007-3 печать, 978-3-031-16008-0 электронная); первое издание 1978 — DOI 10.1007/978-1-349-04338-5.

[1084] P. Mehrling, «Minsky and Kindleberger: Fellow Traveling Theorists of National and International Financial Instability», Boston University Global Development Policy Center, GEGI Working Paper 059, March 2023, pp. 3–4, https://www.bu.edu/gdp/files/2023/03/GEGI_WP_059_FIN.pdf (цитирует Kindleberger 1978, p. 15).

[1085] R. Z. Aliber, C. P. Kindleberger, R. N. McCauley, «The Anatomy of a Typical Crisis», в кн. «Manias, Panics, and Crashes», 8th ed., Palgrave Macmillan, Cham, 2023, pp. 17–35, DOI 10.1007/978-3-031-16008-0_2; аннотация: https://ideas.repec.org/h/spr/sprchp/978-3-031-16008-0_2.html.

[1086] Aliber R. Z., Kindleberger C. P., McCauley R. N. The Anatomy of a Typical Crisis // Manias, Panics, and Crashes. 8th ed. Palgrave Macmillan, 2023, pp. 17–35, аннотация главы: «A „displacement“ that flags a novel profit opportunity can lead to speculation, credit expansion, and euphoria; financial distress follows and then crisis that ends in a panic and crash.» Этапы даны по аннотации, внутренний текст главы не цитируется (R. Z. Aliber, C. P. Kindleberger, R. N. McCauley, «The Anatomy of a Typical Crisis», в кн. «Manias, Panics, and Crashes», 8th ed., Palgrave Macmillan, Cham, 2023, pp. 17–35, DOI 10.1007/978-3-031-16008-0_2; аннотация: https://ideas.repec.org/h/spr/sprchp/978-3-031-16008-0_2.html). «Моделью Мински» эту последовательность назвал сам Киндлбергер, хотя Мински предпочитал говорить о гипотезе финансовой нестабильности. Историк экономической мысли Перри Мерлинг замечает, что эта модель у Киндлбергера во многом его собственный вариант классической традиции (Милль, Маршалл, Викселль, Фишер), а от Мински в 1978 году он взял раннюю статью 1972 года: в первом издании «смещение» — внешний шок, а у самого Мински это слово ближе к «уколу», который обрушивает уже хрупкую систему в конце подъёма (P. Mehrling, «Minsky and Kindleberger: Fellow Traveling Theorists of National and International Financial Instability», Boston University Global Development Policy Center, GEGI Working Paper 059, March 2023, pp. 3–4, https://www.bu.edu/gdp/files/2023/03/GEGI_WP_059_FIN.pdf (цитирует Kindleberger 1978, p. 15)). Поэтому о «стадиях Мински» я не пишу: схема этапов принадлежит Киндлбергеру.

[1087] Wikipedia, «Economic bubble», раздел о стадиях, https://en.wikipedia.org/wiki/Economic_bubble — со ссылкой на Kindleberger C., «Manias, Panics and Crashes: A History of Financial Crises», 4th ed., Palgrave Macmillan, 2001, pp. 13–22.

[1088] Формулировка — по энциклопедическому пересказу схемы Киндлбергера (Wikipedia, «Economic bubble», со ссылкой на 4-е издание книги, 2001, pp. 13–22) (Wikipedia, «Economic bubble», раздел о стадиях, https://en.wikipedia.org/wiki/Economic_bubble — со ссылкой на Kindleberger C., «Manias, Panics and Crashes: A History of Financial Crises», 4th ed., Palgrave Macmillan, 2001, pp. 13–22). Модель, как сказано в аннотации к главе 2 восьмого издания, опирается на понятия классиков — «чрезмерную торговлю», за которой следуют «отвращение» и «дискредитация»: «musty terms used by earlier generations of economists including Adam Smith, John Stuart Mill, Knut Wicksell, and Irving Fisher» (R. Z. Aliber, C. P. Kindleberger, R. N. McCauley, «The Anatomy of a Typical Crisis», в кн. «Manias, Panics, and Crashes», 8th ed., Palgrave Macmillan, Cham, 2023, pp. 17–35, DOI 10.1007/978-3-031-16008-0_2; аннотация: https://ideas.repec.org/h/spr/sprchp/978-3-031-16008-0_2.html).

[1089] Mehrling, 2023, p. 5.

[1090] Главы первого издания по Мерлингу: «Speculative Manias», «Fueling the Flames: Monetary Expansion», «The Emergence of Swindles», «The Critical Stage», «International Propagation». В издании 2005 года Роберт Алибер переименовал четвёртую главу в «Fueling the Flames: The Expansion of Credit», сместив акцент с денег на кредит (Mehrling, 2023, p. 5).

[1091] Cambridge Core, аннотация главы 1 «The Bubble Triangle», с. 1–15, https://www.cambridge.org/core/product/identifier/9781108367677%23CN-bp-1/type/book_part; DOI книги 10.1017/9781108367677.

другому. Топливо — лёгкие деньги и кредит, без которых ценам активов, по словам авторов, не на чем расти[1092].[1093] Жар — спекуляция, покупка актива без оглядки на его качество, только в расчёте продать дороже[1094]. Поджигает треугольник искра, и ею бывает либо технологическое изменение, либо решение государства[1095].[1096]

Кислорода у крипты, по-моему, почти столько, сколько вообще может быть у рынка: торги идут круглые сутки, биткоин делится до стомиллионной доли, а купить его можно с телефона[1097]. Искры в её истории, если приложить к ней эту рамку, были обоих видов. Технологической стала сама тетрадка без хранителя, государственными — почти нулевые ставки 2020–2021 годов и разрешение в 2024 году биржевых фондов на биткоин (фондов, чьи акции продаются на обычной бирже, а за акциями лежат биткоины)[1098]. Последнюю главу своей книги авторы начинают с пузыря криптовалют 2017 года[1099], а сам Куинн, по его словам, на вопрос о крипте обычно отвечал, что она находится где-то между пузырём и мошенничеством[1100].

Шиллер, экономист из Йельского университета, в 2017 году предложил изучать экономику через истории, которые люди рассказывают друг другу, примерно так, как эпидемиологи изучают распространение болезней. Мозг, писал он, всегда был настроен на истории, которыми люди оправдывают даже самые обычные траты и вложения[1101].[1102] Сами пузыри, по его словам, лучше было бы назвать спекулятивными эпидемиями, ведь эпидемии мутируют и возвращаются[1103]. В его книге 2019 года биткоин — один из разобранных примеров[1104].

[1092] M. S. Rzepczynski, «Book Review: Boom and Bust», CFA Institute, Enterprising Investor, 22.11.2021, https://rpc.cfainstitute.org/blogs/enterprising-investor/2021/book-review-boom-and-bust.

[1093] «A bubble's fuel is easy money and credit. Without cheap and bountiful funds for investment, there is no opportunity for asset prices to be bid higher.» — цитата из книги по рецензии CFA Institute (M. S. Rzepczynski, «Book Review: Boom and Bust», CFA Institute, Enterprising Investor, 22.11.2021, https://rpc.cfainstitute.org/blogs/enterprising-investor/2021/book-review-boom-and-bust).

[1094] M. S. Rzepczynski, «Book Review: Boom and Bust», CFA Institute, Enterprising Investor, 22.11.2021, https://rpc.cfainstitute.org/blogs/enterprising-investor/2021/book-review-boom-and-bust.

[1095] Cambridge Core, аннотация главы 1 «The Bubble Triangle», с. 1–15, https://www.cambridge.org/core/product/identifier/9781108367677%23CN-bp-1/type/book_part; DOI книги 10.1017/9781108367677.

[1096] Quinn W., Turner J. D. Boom and Bust: A Global History of Financial Bubbles. Cambridge University Press, 2020, гл. 1 «The Bubble Triangle», аннотация: «…either technological change or a government policy decision.» Там же: «some bubbles may be useful» (Cambridge Core, аннотация главы 1 «The Bubble Triangle», с. 1–15, https://www.cambridge.org/core/product/identifier/9781108367677%23CN-bp-1/type/book_part; DOI книги 10.1017/9781108367677). Определения сторон треугольника — по рецензии М. Ржепчински (CFA Institute, 22.11.2021), где приведены цитаты из книги; СМИ авторы называют «ускорителем» (M. S. Rzepczynski, «Book Review: Boom and Bust», CFA Institute, Enterprising Investor, 22.11.2021, https://rpc.cfainstitute.org/blogs/enterprising-investor/2021/book-review-boom-and-bust). Приложение рамки искр к крипте — мой вывод.

[1097] M. S. Rzepczynski, «Book Review: Boom and Bust», CFA Institute, Enterprising Investor, 22.11.2021, https://rpc.cfainstitute.org/blogs/enterprising-investor/2021/book-review-boom-and-bust.

[1098] Cambridge Core, аннотация главы 1 «The Bubble Triangle», с. 1–15, https://www.cambridge.org/core/product/identifier/9781108367677%23CN-bp-1/type/book_part; DOI книги 10.1017/9781108367677.

[1099] Cambridge Core, аннотация главы 12, https://www.cambridge.org/core/product/identifier/9781108367677%23CN-bp-12/type/book_part; страницы — Crossref, DOI 10.1017/9781108367677.012.

[1100] W. Quinn, «Which historical bubble is most like the crypto bubble?», гостевой пост в блоге Дэвида Джерарда «Attack of the 50 Foot Blockchain», 05.01.2023, https://davidgerard.co.uk/blockchain/2023/01/05/which-historical-bubble-is-most-like-the-crypto-bubble-by-william-quinn/.

[1101] R. J. Shiller, «Narrative Economics», American Economic Review 107(4), April 2017, pp. 967–1004, DOI 10.1257/aer.107.4.967, https://www.aeaweb.org/articles?id=10.1257/aer.107.4.967.

[1102] Shiller R. J. Narrative Economics. American Economic Review 107(4), 2017, pp. 967–1004: «The human brain has always been highly tuned toward narratives, whether factual or not, to justify ongoing actions, even such basic actions as spending and investing.» (R. J. Shiller, «Narrative Economics», American Economic Review 107(4), April 2017, pp. 967–1004, DOI 10.1257/aer.107.4.967, https://www.aeaweb.org/articles?id=10.1257/aer.107.4.967)

[1103] Yale Insights, 19.10.2017.

[1104] Princeton University Press, страница книги, https://press.princeton.edu/books/hardcover/9780691182292/narrative-economics.

Четыре взгляда друг другу не противоречат, и шесть этапов этой главы собраны из их работ, но сборка моя, и в таком виде схемы нет ни у кого из четырёх. Новая история — это «смещение» Киндлбергера и искра Куинна и Тёрнера, рассказанная так, как это описывает Шиллер; приток денег и плечо — спекуляция и расширение кредита, топливо треугольника; пик — переход от эйфории к напряжению; принудительные продажи — продажа позиций у Мински и паника у Киндлбергера; расчистка начинается там, где у него наступает крах.

Старые пузыри в пересказе и в архивах

О криптовалютах часто говорят через исторические пузыри, но популярные пересказы этих пузырей сами бывают мифами[1105]. Прежде чем прикладывать модель к крипте, посмотрим, что остаётся от четырёх самых частых параллелей после проверки историками.

Голландская тюльпаномания 1630-х годов дошла до широкой публики в пересказе Чарльза Маккея 1841 года, опиравшегося на нравоучительные памфлеты[1106]. Историк Энн Голдгар изучила голландские архивы и не нашла ни одного человека, разорившегося из-за краха тюльпанного рынка. Участников, по её оценке, было немного, экономические последствия незначительны, а пострадали скорее доверие и честь в торговле[1107].[1108] Для книги о деньгах как о доверии это самый поучительный вариант истории.

Пузырь Компании Южных морей 1720 года обычно рассказывают вместе с фразой Исаака Ньютона о том, что он может вычислить движение небесных тел, но не безумие людей. В самой ранней известной записи этой истории о небесных телах нет ни слова[1109], зато потеря правдива: по подсчётам Эндрю Одлыжко, Ньютон почти наверняка потерял больше 10 000 фунтов[1110].[1111] Полезнее для нас другая деталь. Компания после краха не исчезла. В начале 1722 года она управляла больше чем 80% государственного долга Великобритании и была распущена только в 1850-х[1112]. Пузырь и настоящая финансовая инфраструктура оказались одной

[1105] Smithsonian; E. A. Thompson, «The tulipmania: Fact or artifact?», Public Choice 130, 2007, pp. 99–114, https://link.springer.com/article/10.1007/s11127-006-9074-4.

[1106] Smithsonian; E. A. Thompson, «The tulipmania: Fact or artifact?», Public Choice 130, 2007, pp. 99–114, https://link.springer.com/article/10.1007/s11127-006-9074-4.

[1107] L. Boissoneault, «There Never Was a Real Tulip Fever», Smithsonian Magazine, 18.09.2017, https://www.smithsonianmag.com/history/there-never-was-real-tulip-fever-180964915/; основа: A. Goldgar, «Tulipmania: Money, Honor, and Knowledge in the Dutch Golden Age», University of Chicago Press, 2007, https://press.uchicago.edu/ucp/books/book/chicago/T/bo5414939.html.

[1108] Smithsonian Magazine, 18.09.2017, интервью с Э. Голдгар, автором книги «Tulipmania: Money, Honor, and Knowledge in the Dutch Golden Age» (University of Chicago Press, 2007): «I couldn't find anybody that went bankrupt.» / «There weren't that many people involved and the economic repercussions were pretty minor.» (L. Boissoneault, «There Never Was a Real Tulip Fever», Smithsonian Magazine, 18.09.2017, https://www.smithsonianmag.com/history/there-never-was-real-tulip-fever-180964915/; основа: A. Goldgar, «Tulipmania: Money, Honor, and Knowledge in the Dutch Golden Age», University of Chicago Press, 2007, https://press.uchicago.edu/ucp/books/book/chicago/T/bo5414939.html)

[1109] A. Odlyzko, «Newton's financial misadventures in the South Sea Bubble», Notes and Records: the Royal Society Journal of the History of Science 73(1), 2019, pp. 29–59, https://royalsocietypublishing.org/doi/pdf/10.1098/rsnr.2018.0018; препринт: https://www-users.cse.umn.edu/~odlyzko/doc/mania13.pdf.

[1110] Odlyzko, 2019, с. 1–3 препринта.

[1111] Odlyzko A. Newton's financial misadventures in the South Sea Bubble. Notes and Records: the Royal Society Journal of the History of Science 73(1), 2019: «This is the earliest known version of the „madness of the people" story… It does not have the extra flourish about computing „the motions of the heavenly bodies" that is common.» Записи Джозефа Спенса — 1756 года, изданы в 1820-м; Спенс ссылается на лорда Раднора (A. Odlyzko, «Newton's financial misadventures in the South Sea Bubble», Notes and Records: the Royal Society Journal of the History of Science 73(1), 2019, pp. 29–59, https://royalsocietypublishing.org/doi/pdf/10.1098/rsnr.2018.0018; препринт: https://www-users.cse.umn.edu/~odlyzko/doc/mania13.pdf). О потерях: «His losses, even by conservative accounting, almost surely exceeded £10,000, and plausible methods easily produce values that exceed the £20,000 figure that family lore claimed…» Цифра 20 000 впервые появляется у Уильяма Сьюарда (1797); счета Ньютона, по-видимому, уничтожены в 1860-х (Odlyzko, 2019, с. 1–3 препринта).

[1112] Odlyzko, 2019, раздел 8 препринта, с. 20.

и той же компанией, а на крипторынке рядом с пузырём тоже вырастают биржи и эмитенты стейблкоинов.

Сам Куинн ближе всего к криптопузырю ставит пузырь Миссисипской компании во Франции 1718–1720 годов, а стейблкоины сравнивает с банкнотами Джона Ло[1113]. В январе 2023 года он писал, что полностью исключить системный кризис от краха крипты нельзя, механизмы заражения сложны, но почти невозможно представить, чтобы этот крах вызвал экономический или финансовый кризис, потому что крипта слабо связана с реальной экономикой[1114].[1115] Сказано это до биржевых фондов 2024 года и до того, как у банков появилось больше связей с криптой, и выдержала ли позиция время, покажут последние главы книги.

В пятой главе я обещал вернуться к частным банкнотам XIX века. В годы свободной банковской деятельности в США (1837–1863) частные банки ряда штатов выпускали собственные банкноты, и о «диких банках» того времени принято рассказывать как о сплошном мошенничестве[1116]. Экономисты Федерального резервного банка Миннеаполиса проверили четыре штата и показали, что потери держателей банкнот сильно преувеличены. На все четыре штата они составили около 1,6 млн долларов, многие банки не закрылись, а многие закрывшиеся выкупили свои банкноты по номиналу[1117].[1118] В Миннесоте в 1859 году ожидаемая стоимость банкноты падала ниже 50 центов за доллар, в Нью-Йорке не опускалась ниже 99[1119].

Бумажный доллар с именем банка похож на цифровой доллар с именем эмитента. Цена его зависела от того, что лежало в сундуке банка и кто это проверял, а котировки банкнот разных банков печатали особые справочники[1120]. Частные деньги не обязательно кончаются катастрофой, но их качество у разных эмитентов расходилось больше чем вдвое.

Ближе всех к крипте по цифрам пузырь доткомов. Индекс американских акций Nasdaq Composite, где много технологических компаний, с пика 10 марта 2000 года к октябрю 2002-го упал примерно на 78%, почти как биткоин в 2021–2022 годах[1121]. Выше прежнего пика он вернулся только через 15 лет[1122].[1123] Интернет был настоящей технологией и никуда не делся,

---

[1113] Quinn, 2023.

[1114] Quinn, 2023.

[1115] Quinn, 2023: «the market was deliberately created with the intention of causing a bubble»; «We can never completely rule it out — contagion mechanisms are complicated — but it's almost inconceivable that its bursting will cause an economic or financial crisis.» (Quinn, 2023)

[1116] A. J. Rolnick, W. E. Weber, «New Evidence on the Free Banking Era», American Economic Review 73(5), 1983, pp. 1080–1091, https://www.jstor.org/stable/1814673.

[1117] A. J. Rolnick, W. E. Weber, «New Evidence on the Free Banking Era», American Economic Review 73(5), 1983, pp. 1080–1091, https://www.jstor.org/stable/1814673.

[1118] Rolnick A. J., Weber W. E. New Evidence on the Free Banking Era. American Economic Review 73(5), 1983, pp. 1080–1091. Штаты — Нью-Йорк, Висконсин, Индиана, Миннесота; потери — около 1,6 млн долларов (диапазон 1,4–2,1 млн): «Our preliminary conclusion from this evidence is that it is misleading to characterize the overall free banking experience as a failure of laissez-faire banking.» Минимум по Миннесоте — 45,6 цента за доллар (январь 1859 года). Более критичный взгляд — у Дж. Двайера (FRB Atlanta Economic Review, 1996) (A. J. Rolnick, W. E. Weber, «New Evidence on the Free Banking Era», American Economic Review 73(5), 1983, pp. 1080–1091, https://www.jstor.org/stable/1814673).

[1119] A. J. Rolnick, W. E. Weber, «New Evidence on the Free Banking Era», American Economic Review 73(5), 1983, pp. 1080–1091, https://www.jstor.org/stable/1814673.

[1120] A. J. Rolnick, W. E. Weber, «New Evidence on the Free Banking Era», American Economic Review 73(5), 1983, pp. 1080–1091, https://www.jstor.org/stable/1814673.

[1121] FRED, ряд NASDAQCOM (NASDAQ Composite Index, закрытие дня): https://fred.stlouisfed.org/graph/fredgraph.csv?id=NASDAQCOM&cosd=2000-03-08&coed=2000-03-14; https://fred.stlouisfed.org/graph/fredgraph.csv?id=NASDAQCOM&cosd=2002-10-07&coed=2002-10-11; https://fred.stlouisfed.org/graph/fredgraph.csv?id=NASDAQCOM&cosd=2015-04-20&coed=2015-04-24; Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1636329600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1668816000.

[1122] FRED, ряд NASDAQCOM (NASDAQ Composite Index, закрытие дня): https://fred.stlouisfed.org/graph/fredgraph.csv?id=NASDAQCOM&cosd=2000-03-08&coed=2000-03-14; https://fred.stlouisfed.org/graph/fredgraph.csv?id=NASDAQCOM&cosd=2002-10-07&coed=2002-10-11; https://fred.stlouisfed.org/graph/fredgraph.csv?id=NASDAQCOM&cosd=2015-04-20&coed=2015-04-24.

пузырь вокруг него тоже был настоящим, и спор «технология это или пузырь» поэтому поставлен плохо.

Популярный пересказ каждой из этих историй преувеличивает разорение и мораль, а проверка сдвигает внимание на кредит и на посредников. О пузырях прошлого полезно спрашивать то же, что о тетрадке без хранителя: кто вёл запись, кто выдавал строчки в долг и кто остался стоять, когда пузырь сдулся.

Спор с залогом: девятнадцатое правило

В пятой главе плечо пришло в посёлок через кредитный котёл: берёшь в долг под залог, покупаешь ещё, снова закладываешь. На крипторынке у плеча есть второй путь, в котором никто не берёт денег в долг напрямую. Добавим его в посёлок девятнадцатым правилом.

Два двора могут заключить через автомат спор о цене строчек тетрадки без хранителя. Один выигрывает, если цена вырастет, другой — если упадёт. Каждый кладёт в автомат залог, а автомат всё время переносит выигрыш и проигрыш из залога одного спорщика в залог другого. Срока у спора нет, он длится, пока спорщик сам его не закроет. Если залог проигрывающего кончается, автомат закрывает его спор сам, по рыночной цене и не спрашивая владельца.

На бирже такой спор называют бессрочным фьючерсом. Обычный фьючерс — договор купить или продать актив в назначенный день по цене, о которой договорились заранее, а у бессрочного назначенного дня нет. Ставку на рост называют длинной позицией, ставку на падение — короткой, а принудительное закрытие позиции, у которой кончился залог, называют ликвидацией, как и в котле пятой главы. Сумму всех открытых споров называют открытым интересом, и это самая прямая мера того, сколько плеча на рынке сейчас.

Допустим, строчка стоит 100, а вы кладёте в автомат залог 10 и спорите на рост строчки на всю сумму 100. Вложили вы 10, а выигрываете и проигрываете так, будто держите строчку за 100, то есть плечо у вас десятикратное. Если цена поднимется до 110, ваш залог удвоится. Если опустится до 90, залог кончится, и автомат закроет ваш спор, даже если назавтра цена вернётся к 120 (числа условные, без платы и комиссий). У заёмщика из пятой главы, который занял две трети цены залога, порог лежал на падении в шестую часть, а здесь хватает падения на десятую.

По объёму этот путь сегодня крупнее котла. В пятой главе, летом 2025 года, споров на фьючерсах было примерно в два с половиной раза больше, чем кредитов под криптовалютный залог. К осени разрыв вырос. По оценке Galaxy Research, открытый интерес по криптофьючерсам доходил до 220 млрд долларов, а кредиты под криптовалютный залог в том же квартале не дотягивали до 80 млрд[1124].[1125] Величины разные (в первой считается весь размер спора, во второй только долг), и сравнивать их можно лишь грубо, но разница почти втрое.

[1123] FRED, NASDAQCOM, закрытие дня: 5048,62 пункта 10.03.2000; 1114,11 — 09.10.2002; 5056,06 — 23.04.2015 (FRED, ряд NASDAQCOM (NASDAQ Composite Index, закрытие дня): https://fred.stlouisfed.org/graph/fredgraph.csv?id=NASDAQCOM&cosd=2000-03-08&coed=2000-03-14; https://fred.stlouisfed.org/graph/fredgraph.csv?id=NASDAQCOM&cosd=2002-10-07&coed=2002-10-11; https://fred.stlouisfed.org/graph/fredgraph.csv?id=NASDAQCOM&cosd=2015-04-20&coed=2015-04-24).

[1124] Z. Pokorny, «The State of Crypto Leverage – Q3 2025», Galaxy Research, 19.11.2025, https://www.galaxy.com/insights/research/crypto-leverage-q3-2025-defi-cefi-lending-digital-asset-treasury-debt-futures-perpetuals; Z. Pokorny, «The State of Crypto Leverage Q2 2026: An Orderly, Measured Decline», 17.08.2026, https://www.galaxy.com/insights/research/crypto-leverage-report-q2-2026-defi-lending-decline-futures-open-interest; Galaxy Research, Q3 2025.

[1125] Galaxy Research: открытый интерес по криптофьючерсам — исторический максимум 220,37 млрд долларов 06.10.2025 (отчёт за III кв. 2025 года, 19.11.2025); кредит под криптовалютный залог в III кв. 2025 года — 73,59 млрд в том же отчёте и 78,69 млрд после пересмотра в отчёте за II кв. 2026 года (Z. Pokorny, «The State of Crypto Leverage – Q3 2025», Galaxy Research, 19.11.2025, https://www.galaxy.com/insights/research/crypto-leverage-q3-2025-defi-cefi-lending-digital-asset-treasury-debt-futures-perpetuals; Z. Pokorny, «The State of Crypto Leverage Q2 2026: An Orderly, Measured Decline», 17.08.2026, https://www.galaxy.com/insights/research/crypto-leverage-report-q2-2026-defi-lending-decline-futures-open-interest; Galaxy Research, Q3 2025). Летнее соотношение (около 133 млрд открытых позиций, в два с половиной раза больше

У спора на бирже есть собственная цена, и она может отходить от цены самой монеты. Чтобы она не уходила далеко, раз в несколько часов одна сторона доплачивает другой: если желающих держать спор на рост больше и контракт из-за этого стоит дороже монеты, платят те, кто ставит на рост, а если наоборот — те, кто ставит на падение[1126]. Эту плату называют ставкой финансирования, или фандингом. На бирже BitMEX, одной из старейших площадок таких контрактов, расчёт идёт каждые восемь часов, и обычная ставка равна 0,01% за восемь часов, около 11% годовых в простом пересчёте[1127].[1128] Когда желающих купить с плечом становится намного больше, чем готовых стоять на другой стороне, фандинг растёт, и по нему видно, сколько люди готовы платить за плечо.

Экономисты Банка международных расчётов вместе с соавтором измерили ту же цену плеча по-другому, через разницу между ценой фьючерса и ценой самой монеты. Эта разница (они называют её «крипто-керри») доходила до 60% годовых и сильно менялась во времени, а высокие её значения предсказывали последующие обвалы[1129].[1130] Дорогое плечо авторы объясняют двумя силами. Мелкие инвесторы гонятся за трендом и хотят плеча на подъёме, а капитала, готового стоять на другой стороне, мало, потому что его самого сдерживают скачки требований к залогу и ликвидации[1131].

Когда споров с тонким залогом много, падение цены закрывает самые тонкие из них, автомат продаёт, продажи толкают цену ниже, и порог проходят следующие. Это та же петля, что в котле пятой главы, только порог ближе, а автомат биржи закрывает позиции без промедления и без выходных.

Петля симметрична. Если на рынке накопилось много споров на падение и цена вдруг пошла вверх, автомат закрывает уже их, а закрыть спор на падение можно только покупкой, которая толкает цену ещё выше. Крупнейшие каскады, о которых пойдёт речь в этой главе, шли вниз и приходились в основном на ставки на рост[1132], но устроен механизм одинаково в обе стороны.

кредитов) — по отчёту Galaxy за II кв. 2025 года, см. главу 5 (Z. Pokorny, «The State of Crypto Leverage – Q2 2025», Galaxy Research, 14.08.2025, https://www.galaxy.com/insights/research/the-state-of-crypto-leverage-q2-2025). Galaxy — сама участник рынка кредитования; у разных агрегаторов цифры открытого интереса расходятся (у CoinDesk — 217 млрд на 10.10.2025) (CoinDesk Research, «Market Spotlight: Inside Crypto's $19 Billion Liquidation Event», 17.10.2025 (обновлено 30.10.2025), https://www.coindesk.com/research/market-spotlight-the-19-billion-liquidation-that-shook-crypto).

[1126] Ethena, «Ethena Overview», https://docs.ethena.fi/overview/ethena-overview.md (открыто 26.09.2026); BitMEX API, https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2017-12-05&endTime=2017-12-20&count=100&reverse=false.

[1127] BitMEX API, https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2017-12-05&endTime=2017-12-20&count=100&reverse=false.

[1128] BitMEX, публичный API, бессрочный контракт XBTUSD; расчёт в 04:00, 12:00 и 20:00 по всемирному времени; данные сняты 26.09.2026. Ставка складывается из премии контракта к цене монеты и процентной части (обычно 0,01% за восемь часов), так что знак и размер фандинга задаёт разница цены контракта и монеты; объём длинных и коротких позиций всегда одинаков. Годовые цифры здесь и дальше — простой пересчёт (ставка × 3 × 365), доходностью их считать нельзя. Доля BitMEX в торговле с 2020 года сильно упала, так что для 2021–2025 годов его ряд — срез одной биржи, и обо всём рынке по нему судить нельзя (BitMEX API, https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2017-12-05&endTime=2017-12-20&count=100&reverse=false; BitMEX API, https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2025-09-28&endTime=2025-10-14&count=100&reverse=false).

[1129] M. Schmeling, A. Schrimpf, K. Todorov, «Crypto carry», BIS Working Paper 1087, April 2023, https://www.bis.org/publ/work1087.htm.

[1130] Schmeling M., Schrimpf A., Todorov K. Crypto carry. BIS Working Paper 1087, April 2023: «can become very large (up to 60% p.a.) and varies strongly over time» (M. Schmeling, A. Schrimpf, K. Todorov, «Crypto carry», BIS Working Paper 1087, April 2023, https://www.bis.org/publ/work1087.htm). Маик Шмелинг — из Франкфуртского университета имени Гёте, работа вышла в серии Банка международных расчётов.

[1131] M. Schmeling, A. Schrimpf, K. Todorov, «Crypto carry», BIS Working Paper 1087, April 2023, https://www.bis.org/publ/work1087.htm.

[1132] O. Godbole, «Crypto Futures Saw Record $10B Worth of Liquidations on Sunday», CoinDesk, 19.04.2021 (по данным Bybt — прежнее название CoinGlass), https://www.coindesk.com/markets/2021/04/19/crypto-futures-saw-record-10b-worth-of-liquidations-on-sunday; O. Godbole, «Bitcoin's Crash Triggers Over $700M in Liquidations on BitMEX», CoinDesk, 12.03.2020 (по

Прогоним через новое правило условный цикл посёлка, чтобы увидеть этапы без шума настоящего рынка (посёлок, как и прежде, условный, и числа в нём круглые). Допустим, строчка тетрадки без хранителя стоит 10 городских долларов, и держат её десять дворов из ста. По посёлку идёт рассказ, будто скоро такими строчками станет расплачиваться весь уезд, и ещё десять дворов, среди них пекарь, покупают строчки на свои сбережения. Цена поднимается до 20. Опасного в этом пока ничего нет. Кто купил на свои, тот при падении потеряет, но продавать его никто не заставит.

Соседи видят, что пекарь, купивший строчки по 10, за сезон удвоил деньги, и на рынок приходят ещё тридцать дворов. Цена поднимается до 40. Желания у новичков больше, чем сбережений, поэтому часть из них заключает споры на рост по девятнадцатому правилу с залогом в десятую часть, а часть занимает в котле по пятнадцатому. Желающих спорить на рост становится намного больше, чем готовых спорить на падение, и доплата, которую первые отдают вторым, растёт. Плечо в посёлке дорожает, и спрос на него от этого не падает.

Лесоруб приходит последним, когда цена подбирается к 50. Сбережений у него нет, и он спорит на рост с залогом в десятую часть. К осени покупать больше некому: все, кто верил рассказу, уже купили, все, кто мог занять, заняли, и цена останавливается на 50. Для тех, кто спорит на рост с плечом, остановка уже плохая новость, потому что платить за плечо из стоящей на месте цены нечем. Несколько дворов закрывают споры сами, цена опускается до 45, то есть на десятую часть, и автомат закрывает все споры с тонким залогом, открытые у вершины, в том числе спор лесоруба.

Дальше посёлок проходит этап принудительных продаж за неделю. Продажи закрытых споров роняют цену до 40, и порог проходят займы из котла, взятые на последнем отрезке подъёма (им хватало падения на шестую часть). Автомат котла продаёт их залог, цена опускается до 35, и закрываются споры, открытые по 40. Путь, на который вверх ушло полгода, вниз цена проходит за несколько дней. Когда закрыты все тонкие споры и распроданы все залоги, продавать больше некого, и цена останавливается, скажем, на 20.

Из этого условного цикла видна разница между теми, кто переживает расчистку, и теми, кто её не переживает. Пекарь купил рано и на свои, и падение с 50 до 20 его задело, но с рынка не выбросило, ведь его строчки по-прежнему стоят вдвое дороже, чем он платил. Лесоруб купил на вершине и в долг, и его выбросило на первых десяти процентах падения, задолго до дна. Купи он на вершине на свои, он потерял бы на бумаге 60%, но решать, продавать ли и ждать ли следующего цикла, остался бы сам.

Долг здесь решает больше, чем момент покупки.

Криптоцикл резче обычной кредитной волны, и причина в том, чем строчка биткоина отличается от доски или буханки. Волна в посёлке первой главы начиналась с урожая. У плотника и пекаря был доход от работы, и из него, пусть не всегда, можно было вернуть долг. Мински тоже писал о фирмах, у которых есть денежный поток от производства[1133].

У строчки биткоина урожая нет: она не приносит ни процентов, ни дохода, и вернуть долг, взятый на её покупку, можно только продав её дороже или заняв снова. По-моему, это значит, что почти любая покупка такой строчки в долг — финансирование «понци» в терминах Мински. Вывод мой, у Мински его нет.

Продолжатели Киндлбергера исходят из того же и идут дальше. В главе «Биткоин: хуже, чем Понци», написанной для восьмого издания, они утверждают, что крипта не обещает денежного потока и почти не оказывает финансовых услуг; что прибыль ранних покупателей, как в схеме Понци, оплачивают поздние; что сама крипта в отличие от такой схемы не может

данным Skew), https://www.coindesk.com/markets/2020/03/12/bitcoins-crash-triggers-over-700m-in-liquidations-on-bitmex.

[1133] Hyman P. Minsky, «The Financial Instability Hypothesis», Levy Economics Institute, Working Paper No. 74, May 1992, pp. 6–7, https://www.levyinstitute.org/pubs/wp74.pdf.

рухнуть от паники вкладчиков, хотя биржи и кредиторы вокруг неё могут рушиться и рушились; и что добыча тратит электричество и машины, так что это игра с отрицательной суммой[1134]. Ближе всего биткоин, по их словам, к «децентрализованной схеме накачки и сброса с отрицательной суммой»[1135].[1136] Позиция полемическая, и уравновешивает её оговорка Куинна и Тёрнера о том, что некоторые пузыри могут быть полезны[1137]. Для модели цикла этот спор можно оставить открытым, потому что механизм работает одинаково, кто бы из них ни оказался прав.

Шесть этапов одного цикла

Теперь цикл можно пройти по этапам. Этапы сцеплены, каждый готовит следующий, но часов у них нет. Они наслаиваются друг на друга, а иногда рынок проскакивает какой-то из них, как в марте 2020 года, когда шок начался сразу с принудительных продаж.

[1134] R. Z. Aliber, C. P. Kindleberger, R. N. McCauley, «Bitcoin: Worse Than a Ponzi», в кн. «Manias, Panics, and Crashes», 8th ed., Palgrave Macmillan, 2023, pp. 349–371, DOI 10.1007/978-3-031-16008-0_14; аннотация: https://ideas.repec.org/h/spr/sprchp/978-3-031-16008-0_14.html.

[1135] R. Z. Aliber, C. P. Kindleberger, R. N. McCauley, «Bitcoin: Worse Than a Ponzi», в кн. «Manias, Panics, and Crashes», 8th ed., Palgrave Macmillan, 2023, pp. 349–371, DOI 10.1007/978-3-031-16008-0_14; аннотация: https://ideas.repec.org/h/spr/sprchp/978-3-031-16008-0_14.html.

[1136] «Bitcoin is more akin to a decentralized pump and dump scheme with a negative sum.» (R. Z. Aliber, C. P. Kindleberger, R. N. McCauley, «Bitcoin: Worse Than a Ponzi», в кн. «Manias, Panics, and Crashes», 8th ed., Palgrave Macmillan, 2023, pp. 349–371, DOI 10.1007/978-3-031-16008-0_14; аннотация: https://ideas.repec.org/h/spr/sprchp/978-3-031-16008-0_14.html)

[1137] Cambridge Core, аннотация главы 1 «The Bubble Triangle», с. 1–15, https://www.cambridge.org/core/product/identifier/9781108367677%23CN-bp-1/type/book_part; DOI книги 10.1017/9781108367677.

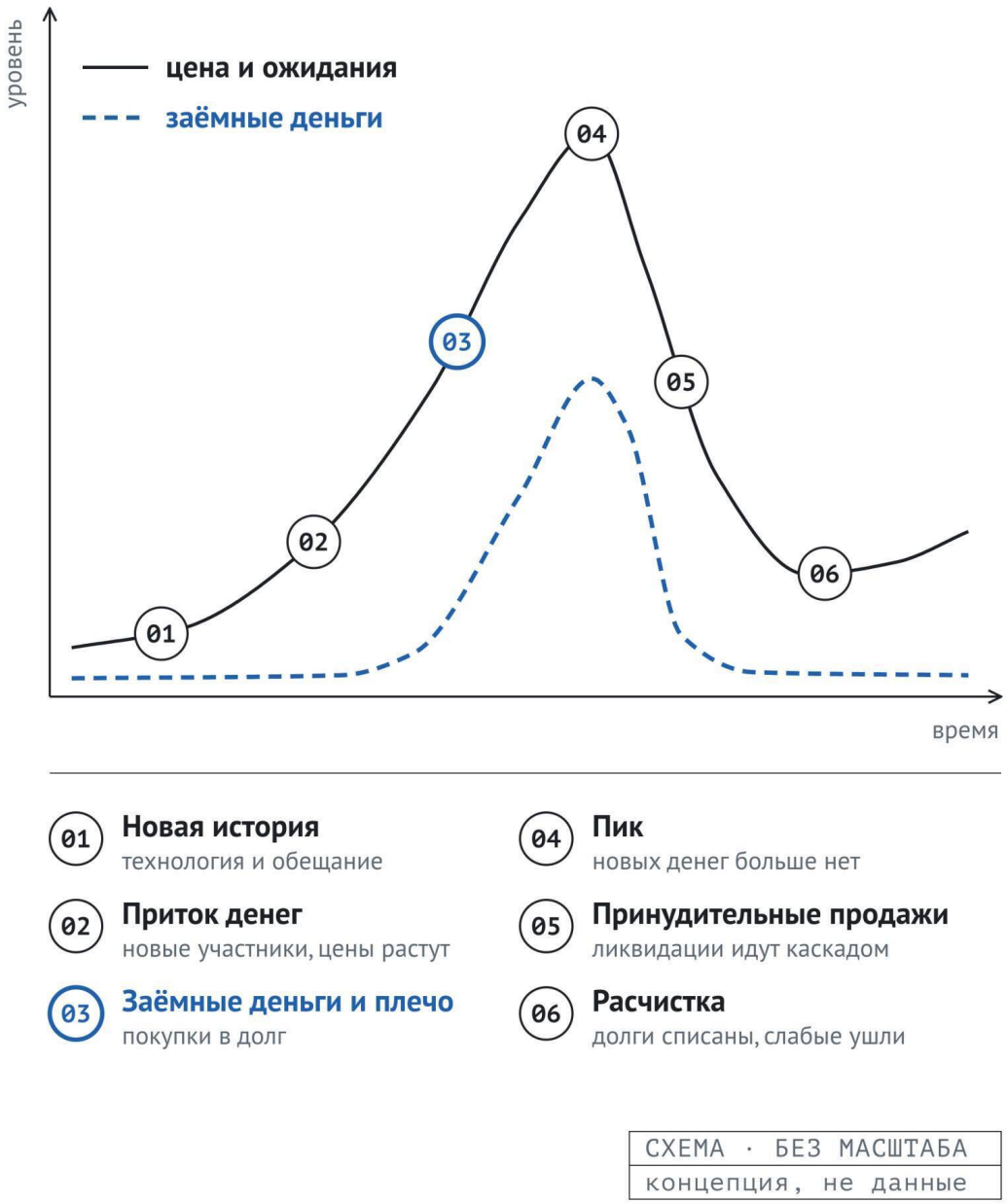


Рисунок 7.2. Анатомия криптоцикла

Первый этап — новая история. Всё начинается с события, которое открывает новую возможность заработать, и с рассказа, объясняющего, почему эта возможность огромна. В октябре 2017 года Шиллер перечислил истории, которые, на его взгляд, подняли биткоин в 2013 году: новая валюта, живущая в киберпространстве без вмешательства и контроля государств, криптография со шпионским обаянием в духе фильмов о Джеймсе Бонде, так и не найденный создатель Сатоши Накамото. Второй подъём, 2017 года, он связывал с ICO (первичными размещениями монет, о которых пойдёт речь в следующей главе), придавшими биткоину ещё и «лоск инвестиционного банкинга»[1138]. Там же он назвал биткоин лучшим на тот момент примером спекулятивного пузыря, по крайней мере в своём понимании этого слова[1139].[1140]

[1138] «Three Questions: Prof. Robert Shiller on Bitcoin», Yale Insights (Yale School of Management), 19.10.2017, https://

Со словом «пузырь» здесь легко ошибиться. Шиллер называл биткоин примером пузыря и в январе 2014 года, и в сентябре 2017-го, когда монета стоила около 4300 долларов[1141].[1142] После этого цена выросла больше чем вчетверо, упала на 84%, а к пику 2025 года поднялась почти в тридцать раз против той сентябрьской[1143]. Шиллер описывал механизм, которым истории разгоняют цену, и в следующих главах мы увидим этот механизм не раз. Срока в слове «пузырь» нет, и читать его как прогноз цены нельзя.

В данных первый этап почти не виден, история опережает цифры. Проверить её можно вопросами из первой части книги. Что именно новинка меняет в записи, кто эту запись ведёт и кто может выдавать строчки в долг? Если ответов в рассказе нет, перед вами пока только рассказ.

На втором этапе, притоке денег, рост цены сам становится рекламой. Экономисты Банка международных расчётов изучили ежедневное использование приложений криптобирж в 95 странах за 2015–2022 годы и увидели, что, когда биткоин дорожает, больше людей скачивают эти приложения и начинают ими пользоваться[1144].[1145] Около 40% новых пользователей оказались мужчинами младше 35 лет[1146]. Причинность авторы проверяли на двух внешних шоках, запрете майнинга в Китае в 2021 году и беспорядках в Казахстане в начале 2022-го[1147], так что речь идёт не только о совпадении во времени.

Петля здесь простая. Цена растёт, растущая цена приводит новых покупателей, новые покупатели поднимают цену. Киндлбергеру принадлежит фраза, которая описывает этот этап лучше графиков. Ничто так не расстраивает благополучие и здравый смысл, как зрелище разбогатевшего друга[1148].[1149] Сказана она задолго до биткоина и не о нём, но точнее описания второго этапа я не знаю.

---

insights.som.yale.edu/insights/three-questions-prof-robert-shiller-on-bitcoin.

[1139] «Three Questions: Prof. Robert Shiller on Bitcoin», Yale Insights (Yale School of Management), 19.10.2017, https://insights.som.yale.edu/insights/three-questions-prof-robert-shiller-on-bitcoin.

[1140] Three Questions: Prof. Robert Shiller on Bitcoin. Yale Insights, 19.10.2017: «The 2013 rise in value of Bitcoin was driven by some basic stories that have great resonance…»; «glamorous spy-vs-spy appeal, like a James Bond movie»; «In 2017, the second rise in Bitcoin appears to have something to do with the appearance of ICOs… which give Bitcoin an investment banking patina too»; «Bitcoin is the best example today of a speculative bubble, at least as I define a bubble.» («Three Questions: Prof. Robert Shiller on Bitcoin», Yale Insights (Yale School of Management), 19.10.2017, https://insights.som.yale.edu/insights/three-questions-prof-robert-shiller-on-bitcoin)

[1141] A. Oyedele, «ROBERT SHILLER: Bitcoin is the 'best example right now' of a bubble», Business Insider (перепечатка Yahoo Finance), 05.09.2017, https://finance.yahoo.com/news/robert-shiller-bitcoin-best-example-151300765.html.

[1142] Январь 2014 года (Всемирный экономический форум): «an amazing example of a bubble»; сентябрь 2017 года (интервью Quartz в пересказе Business Insider, 05.09.2017): «the best example right now»; цена биткоина на момент той публикации — 4337 долларов (A. Oyedele, «ROBERT SHILLER: Bitcoin is the 'best example right now' of a bubble», Business Insider (перепечатка Yahoo Finance), 05.09.2017, https://finance.yahoo.com/news/robert-shiller-bitcoin-best-example-151300765.html).

[1143] Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=6&start=1513209600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=8&start=1544486400; Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=4&start=1759622400; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782691200; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782172800; трёхдневные свечи за январь–март и июль–сентябрь 2026: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1767225600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1782864000.

[1144] R. Auer, G. Cornelli, S. Doerr, J. Frost, L. Gambacorta, «Crypto trading and Bitcoin prices: evidence from a new database of retail adoption», BIS Working Paper 1049, 14.11.2022, https://www.bis.org/publ/work1049.htm.

[1145] Auer R., Cornelli G., Doerr S., Frost J., Gambacorta L. Crypto trading and Bitcoin prices: evidence from a new database of retail adoption. BIS Working Paper 1049, 14.11.2022: «when the price of Bitcoin rises, more people download and actively use crypto exchange apps» (R. Auer, G. Cornelli, S. Doerr, J. Frost, L. Gambacorta, «Crypto trading and Bitcoin prices: evidence from a new database of retail adoption», BIS Working Paper 1049, 14.11.2022, https://www.bis.org/publ/work1049.htm).

[1146] R. Auer, G. Cornelli, S. Doerr, J. Frost, L. Gambacorta, «Crypto trading and Bitcoin prices: evidence from a new database of retail adoption», BIS Working Paper 1049, 14.11.2022, https://www.bis.org/publ/work1049.htm.

[1147] R. Auer, G. Cornelli, S. Doerr, J. Frost, L. Gambacorta, «Crypto trading and Bitcoin prices: evidence from a new database of retail adoption», BIS Working Paper 1049, 14.11.2022, https://www.bis.org/publ/work1049.htm.

[1148] B. Popik, «There is nothing so disturbing to one's well-being and judgment as to see

На третьем этапе, этапе заёмных денег и плеча, к деньгам новичков добавляются деньги, взятые в долг, и именно их Куинн и Тёрнер называют топливом. В 2023 году Куинн писал, что в 2021-м криптобиржи сами обеспечивали все три стороны треугольника: давали ликвидность, создавали через стейблкоины новое гибкое предложение денег, выдавали кредиты на покупку и принимали спекулятивную торговлю[1150].[1151] Площадка, которая одновременно служит рынком, кредитором и источником новых цифровых долларов, держит у себя и кислород, и топливо, и жар.

Плечо приходит на рынок не только займами и спорами. Посредник, у которого лежат чужие деньги (монеты клиентов на бирже, деньги, собранные под новый проект, доллары, которыми обеспечены стейблкоины), может пустить их в оборот: одолжить, вложить, купить на них монеты. Для рынка это то же топливо, только владельцы денег не знают, что стали кредиторами. Рядов фандинга и кредита для циклов до 2017 года найти не удалось, и третий этап там виден в основном через посредников. Здесь же копится и обман, которому Киндлбергер отвёл место между денежным топливом и «критической стадией»[1152]. Вскрывается он, по-моему, позже, на пятом и шестом этапах, когда деньги у посредника требуют назад все сразу.

Там, где данные есть, третий этап виден лучше остальных, потому что у плеча есть цена и объём. Цена плеча — это фандинг. На пике 2017 года, с вечера 8 по 19 декабря, ставка на BitMEX большую часть времени стояла на 0,375% за восемь часов[1153]. Покупатели с плечом платили больше 1% в день за то, чтобы удержать позицию, около 410% годовых в простом пересчёте[1154].[1155]

Объём плеча — это открытый интерес и кредит. Кредит под криптовалютный залог, как мы видели в пятой главе, дважды выходил на пик вместе с ценой[1156], а открытый интерес поставил рекорд 6 октября 2025 года, в тот же день, что и цена биткоина[1157].

---

a friend get rich», The Big Apple (barrypopik.com), https://barrypopik.com/index.php/new_york_city/entry/there_is_nothing_so_disturbing_to_ones_well_being_and_judgment_as_to_see_a.

[1149] «There is nothing so disturbing to one's well-being and judgment as to see a friend get rich.» Kindleberger C. P. Manias, Panics and Crashes, 1978, p. 15 — по разысканиям Барри Попика, более ранней атрибуции он не нашёл; с текстом книги это место не сверено (B. Popik, «There is nothing so disturbing to one's well-being and judgment as to see a friend get rich», The Big Apple (barrypopik.com), https://barrypopik.com/index.php/new_york_city/entry/there_is_nothing_so_disturbing_to_ones_well_being_and_judgment_as_to_see_a).

[1150] W. Quinn, «Which historical bubble is most like the crypto bubble?», гостевой пост в блоге Дэвида Джерарда «Attack of the 50 Foot Blockchain», 05.01.2023, https://davidgerard.co.uk/blockchain/2023/01/05/which-historical-bubble-is-most-like-the-crypto-bubble-by-william-quinn/.

[1151] Quinn W. Which historical bubble is most like the crypto bubble? Гостевой пост в блоге Д. Джерарда «Attack of the 50 Foot Blockchain», 05.01.2023: «During 2021, the crypto exchanges facilitated all of these: they provided liquidity, used stablecoins to create a new flexible money supply…» Там же Куинн пишет, что на вопрос о крипте обычно отвечал: «somewhere between a bubble and a fraud» (W. Quinn, «Which historical bubble is most like the crypto bubble?», гостевой пост в блоге Дэвида Джерарда «Attack of the 50 Foot Blockchain», 05.01.2023, https://davidgerard.co.uk/blockchain/2023/01/05/which-historical-bubble-is-most-like-the-crypto-bubble-by-william-quinn/).

[1152] Mehrling, 2023, p. 5.

[1153] BitMEX API, https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2017-12-05&endTime=2017-12-20&count=100&reverse=false.

[1154] BitMEX API, https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2017-12-05&endTime=2017-12-20&count=100&reverse=false.

[1155] BitMEX, XBTUSD, 26 расчётов из 34 с вечера 8 по 19 декабря 2017 года: 0,375% × 3 ≈ 1,1% в день, × 365 ≈ 410% годовых в простом пересчёте. Судя по повторяемости значения, 0,375% был верхним пределом ставки на бирже в то время (BitMEX API, https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2017-12-05&endTime=2017-12-20&count=100&reverse=false).

[1156] Galaxy Research, Q3 2025.

[1157] Z. Pokorny, «The State of Crypto Leverage – Q3 2025», Galaxy Research, 19.11.2025, https://www.galaxy.com/insights/research/crypto-leverage-q3-2025-defi-cefi-lending-digital-asset-treasury-debt-futures-perpetuals; Z. Pokorny, «The State of Crypto Leverage Q2 2026: An Orderly, Measured Decline», 17.08.2026, https://www.galaxy.com/insights/research/crypto-leverage-report-q2-2026-defi-lending-decline-futures-open-interest; Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=4&start=1759622400; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782691200;

Из шести этапов опаснее всего третий: первые два приводят на рынок деньги, третий делает рынок хрупким. Пока вы покупаете на свои, падение цены приносит вам убытки, но никто не заставляет вас продавать. Когда вы покупаете в долг, падение цены само превращается в продажи.

Четвёртый этап — пик. Почему рынок разворачивается, если ничего особенного не случилось? Пик наступает, когда новых денег больше нет: все, кого могла привести история, уже пришли, а все, кто мог занять, уже заняли. Шиллер говорил, что для разворота пузыря обычно не нужно ничего внешнего и пузырь просто выдыхается, как, по его словам, выдохся биткоин с 2014 года[1158].[1159] С Мински эти слова сходятся с другой стороны, ведь и у него цикл не нуждается во внешнем шоке[1160]. Киндлбергер называл это время финансовым напряжением[1161]. В энциклопедическом пересказе его схемы цены в такие месяцы перестают расти, а участники всё чаще думают, как продать, чтобы покрыть обязательства[1162].

Пик не обязательно бывает одной точкой. В цикле 2021 года рынок пережил два каскада ликвидаций, 18 апреля на 10 млрд долларов (тогдашний рекорд) и 19 мая на 8 млрд, за полгода и больше до ценового пика в ноябре[1163].[1164] Цена плеча в том же цикле достигла максимума задолго до цены. 10 апреля 2021 года, за неделю с небольшим до апрельского каскада, фандинг на BitMEX доходил до 0,30% за восемь часов, почти впятеро выше, чем в неделю ноябрьского рекорда[1165]. Перегрев плеча уже прошёл, а цена ещё росла, и тем, кто ждёт, что вершину отметит какой-то один сигнал, это стоит помнить.

Пятый этап, принудительные продажи, и описал Мински: тем, у кого не хватает денег, приходится продавать позиции, и это ведёт к обвалу цен[1166]. На крипторынке этап выглядит как каскад ликвидаций. 10–11 октября 2025 года, через четыре дня после пика, за сутки было

---

https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782172800; трёхдневные свечи за январь–март и июль–сентябрь 2026: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1767225600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1782864000.

[1158] Yale Insights, 19.10.2017.

[1159] Three Questions: Prof. Robert Shiller on Bitcoin. Yale Insights, 19.10.2017: «Usually nothing exogenous is needed to reverse a bubble. The bubble just wears off, as Bitcoin did starting in 2014.» (Yale Insights, 19.10.2017)

[1160] Minsky, 1992, p. 8.

[1161] R. Z. Aliber, C. P. Kindleberger, R. N. McCauley, «The Anatomy of a Typical Crisis», в кн. «Manias, Panics, and Crashes», 8th ed., Palgrave Macmillan, Cham, 2023, pp. 17–35, DOI 10.1007/978-3-031-16008-0_2; аннотация: https://ideas.repec.org/h/spr/sprchp/978-3-031-16008-0_2.html.

[1162] Wikipedia, «Economic bubble», раздел о стадиях, https://en.wikipedia.org/wiki/Economic_bubble — со ссылкой на Kindleberger C., «Manias, Panics and Crashes: A History of Financial Crises», 4th ed., Palgrave Macmillan, 2001, pp. 13–22.

[1163] O. Godbole, «Crypto Futures Saw Record $10B Worth of Liquidations on Sunday», CoinDesk, 19.04.2021 (по данным Bybt — прежнее название CoinGlass), https://www.coindesk.com/markets/2021/04/19/crypto-futures-saw-record-10b-worth-of-liquidations-on-sunday; O. Godbole, «Bitcoin Drops Below $31K Before Rebounding; $8B in Liquidations Triggered», CoinDesk, 19.05.2021 (по данным Bybt), https://www.coindesk.com/markets/2021/05/19/bitcoin-drops-below-31k-before-rebounding-8b-in-liquidations-triggered.

[1164] CoinDesk, 19.04.2021 и 19.05.2021, по данным агрегатора Bybt (ныне CoinGlass): 18 апреля — 10 млрд долларов при прежнем рекорде 5,77 млрд 23 февраля 2021 года, больше 90% — длинные позиции; 19 мая — 8 млрд. В статье от 19 мая апрельский рекорд датирован 17 апреля: обвал начался вечером субботы по времени США (O. Godbole, «Crypto Futures Saw Record $10B Worth of Liquidations on Sunday», CoinDesk, 19.04.2021 (по данным Bybt — прежнее название CoinGlass), https://www.coindesk.com/markets/2021/04/19/crypto-futures-saw-record-10b-worth-of-liquidations-on-sunday; O. Godbole, «Bitcoin Drops Below $31K Before Rebounding; $8B in Liquidations Triggered», CoinDesk, 19.05.2021 (по данным Bybt), https://www.coindesk.com/markets/2021/05/19/bitcoin-drops-below-31k-before-rebounding-8b-in-liquidations-triggered). Фандинг BitMEX: максимум 2021 года — 0,2997% за восемь часов 10.04.2021 в 20:00 по всемирному времени (≈328% годовых в простом пересчёте); 0,1954% 18.02.2021 (≈214%); во втором полугодии не выше 0,0719% (21.10.2021), в неделю ноябрьского пика не выше 0,0605% (≈66%) (BitMEX API: https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2021-02-01&endTime=2021-02-28&count=100&reverse=false; https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2021-10-25&endTime=2021-11-12&count=100&reverse=false).

[1165] BitMEX API: https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2021-02-01&endTime=2021-02-28&count=100&reverse=false; https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2021-10-25&endTime=2021-11-12&count=100&reverse=false.

[1166] Minsky, 1992, p. 8.

ликвидировано позиций больше чем на 19 млрд долларов по публичным данным, крупнейший такой случай в истории рынка[1167].

Поводом стало объявление о 100-процентных пошлинах на китайский импорт[1168]. Масштаб видно по другой цифре. Открытый интерес на крупных биржах за те же сутки сократился с 217 до 123 млрд долларов, на 43%[1169].[1170] Споры почти на сотню миллиардов копились месяцами, и пошлины застали их на рынке. Подробно об этих сутках пойдёт речь в главе 10.

Цифры ликвидаций стоит читать как нижнюю границу. По словам агрегатора CoinGlass, Binance публикует не больше одной ликвидации в секунду, и в пиковые минуты часть событий в публичные данные не попадает. Сооснователь конкурирующей биржи оценил, что занижение в такие минуты может быть стократным[1171].[1172] Настоящий масштаб тех суток, вероятно, больше. Масштаб крупнейших каскадов рос вместе с рынком: 702 млн долларов на одной бирже в марте 2020 года, 10 млрд по всему рынку в 2021-м, больше 19 млрд в 2025-м[1173].

К концу этапа перекос плеча может перевернуться. В панике вокруг краха FTX в ноябре 2022 года фандинг на BitMEX ушёл глубоко в минус, и платить начали уже те, кто ставил на падение, около 275% годовых в простом пересчёте[1174]. Через несколько дней ставка вернулась к обычной, и дно цены 21 ноября пришлось на спокойный фандинг[1175].

Последний, шестой этап — расчистка. После принудительных продаж долги списаны или погашены, слабые участники ушли, а посредники, державшие чужие деньги, проверены на прочность. Как мы видели в пятой главе, в 2022 году кредит под криптовалютный залог сжимался вместе с банкротствами кредиторов, а в открытом цикле он снижается постепенно и к концу второго квартала 2026 года стоял больше чем на четверть ниже пика, без каскада

[1167] CoinDesk Research, «Market Spotlight: Inside Crypto's $19 Billion Liquidation Event», 17.10.2025 (обновлено 30.10.2025), https://www.coindesk.com/research/market-spotlight-the-19-billion-liquidation-that-shook-crypto.

[1168] CoinDesk Research, «Market Spotlight: Inside Crypto's $19 Billion Liquidation Event», 17.10.2025 (обновлено 30.10.2025), https://www.coindesk.com/research/market-spotlight-the-19-billion-liquidation-that-shook-crypto.

[1169] CoinDesk Research, «Market Spotlight: Inside Crypto's $19 Billion Liquidation Event», 17.10.2025 (обновлено 30.10.2025), https://www.coindesk.com/research/market-spotlight-the-19-billion-liquidation-that-shook-crypto.

[1170] CoinDesk Research, «Market Spotlight: Inside Crypto's $19 Billion Liquidation Event», 17.10.2025: «Total perpetual futures open interest across major exchanges dropped 43%, falling from $217 billion on October 10 to $123 billion on October 11.» (CoinDesk Research, «Market Spotlight: Inside Crypto's $19 Billion Liquidation Event», 17.10.2025 (обновлено 30.10.2025), https://www.coindesk.com/research/market-spotlight-the-19-billion-liquidation-that-shook-crypto)

[1171] T. Shen, «Hyperliquid founder says certain CEXs may underreport liquidations», The Block, 13.10.2025, https://www.theblock.co/post/374311/hyperliquid-founder-says-certain-cexs-may-underreport-liquidations.

[1172] The Block, 13.10.2025. Ограничение одной публикуемой ликвидацией в секунду — со слов CoinGlass о Binance («Binance only reports one liquidation order per second»); оценка «до 100 раз» — слова сооснователя Hyperliquid Джеффа Яна, то есть конкурента Binance: «this could easily be 100x under-reporting under some conditions» (T. Shen, «Hyperliquid founder says certain CEXs may underreport liquidations», The Block, 13.10.2025, https://www.theblock.co/post/374311/hyperliquid-founder-says-certain-cexs-may-underreport-liquidations). Цифры 2020 и 2021 годов собраны при других правилах публикации, поэтому точное сравнение рекордов разных лет невозможно; 702 млн долларов на BitMEX в марте 2020 года — максимум этой биржи с ноября 2018-го, а не рекорд рынка (O. Godbole, «Bitcoin's Crash Triggers Over $700M in Liquidations on BitMEX», CoinDesk, 12.03.2020 (по данным Skew), https://www.coindesk.com/markets/2020/03/12/bitcoins-crash-triggers-over-700m-in-liquidations-on-bitmex).

[1173] O. Godbole, «Bitcoin's Crash Triggers Over $700M in Liquidations on BitMEX», CoinDesk, 12.03.2020 (по данным Skew), https://www.coindesk.com/markets/2020/03/12/bitcoins-crash-triggers-over-700m-in-liquidations-on-bitmex; O. Godbole, «Crypto Futures Saw Record $10B Worth of Liquidations on Sunday», CoinDesk, 19.04.2021 (по данным Bybt — прежнее название CoinGlass), https://www.coindesk.com/markets/2021/04/19/crypto-futures-saw-record-10b-worth-of-liquidations-on-sunday; CoinDesk Research, «Market Spotlight: Inside Crypto's $19 Billion Liquidation Event», 17.10.2025 (обновлено 30.10.2025), https://www.coindesk.com/research/market-spotlight-the-19-billion-liquidation-that-shook-crypto.

[1174] BitMEX API, https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2022-11-05&endTime=2022-11-25&count=100&reverse=false.

[1175] BitMEX API, https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2022-11-05&endTime=2022-11-25&count=100&reverse=false; Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1636329600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1668816000.

банкротств[1176].[1177] Разницу в скорости видно по одному кварталу 2022 года, когда этот кредит сжался на 55%[1178]. Расчистка бывает обвальной и бывает медленной, а какой она выйдет, решает то, сколько долга накопилось на третьем этапе и у кого он оказался.

У Мински рядом с рынком всегда стоит система вмешательств, которой экономику удерживают в разумных границах[1179]. У крипторынка такой опоры нет, и расчистка на нём, по-моему, идёт до тех пор, пока продавать не станет некому. Мягче она идёт только там, где долга к её началу накопилось меньше.

Продолжатели Киндлбергера предполагают, что в конце игры «отвращение» инвесторов может обратиться на злоупотребления централизованных учреждений, которые выросли вокруг торговли биткоином, то есть бирж и почти-денег, так называемых стейблкоинов[1180].[1181] Их резкий общий вывод о биткоине мы уже видели. Догадка о том, на кого обратится отвращение, для этой книги важнее, и следующие главы покажут, как часто на расчистке первыми падали именно посредники.

Расчистка — это ещё и время, когда убытки переходят из рук в руки. По оценке экономистов того же Банка, после краха Terra и FTX большинство пользователей криптоприложений почти во всех изученных странах оказались в убытке по своему биткоину, причём в 2022 году крупные держатели продавали, а мелкие розничные покупатели покупали[1182].[1183] В рабочей версии, вышедшей в ноябре 2022 года, экономисты Банка оценивали, что в минусе оказались около трёх четвертей пользователей[1184]. Оценки модельные и сделаны около дна, но смысл понятен и без точных долей. За расчистку в основном платят те, кто пришёл на втором этапе.

Почему же каждое большое падение мельче предыдущего? Прямого ответа в данных нет, но модель подсказывает, где его искать. Глубину падения задаёт третий этап, то есть то, сколько плеча накопилось и насколько дорогим оно было. Цена плеча на пиках от цикла к циклу снижалась. В декабре 2017 года покупатели на BitMEX платили за удержание позиции больше 1%

[1176] Galaxy Research, Q2 2026.

[1177] Galaxy Research, «The State of Crypto Leverage Q2 2026: An Orderly, Measured Decline», 17.08.2026: 56,16 млрд долларов на конец II кв. 2026 года против пика 78,69 млрд, снижения по кварталам примерно −10%, −5% и −17%; всего около −28,6%. «40%», которые приводит сам отчёт, — ошибка направления счёта (см. главу 5) (Galaxy Research, Q2 2026). Свежие цифры — в приложении Б.

[1178] Galaxy Research, Q2 2026.

[1179] Minsky, 1992, p. 8.

[1180] R. Z. Aliber, C. P. Kindleberger, R. N. McCauley, «Bitcoin: Worse Than a Ponzi», в кн. «Manias, Panics, and Crashes», 8th ed., Palgrave Macmillan, 2023, pp. 349–371, DOI 10.1007/978-3-031-16008-0_14; аннотация: https://ideas.repec.org/h/spr/sprchp/978-3-031-16008-0_14.html.

[1181] Aliber, Kindleberger, McCauley. Bitcoin: Worse Than a Ponzi // Manias, Panics, and Crashes. 8th ed., 2023, pp. 349–371, аннотация: «The end game for bitcoin and its ilk could see investor revulsion at the abuses of the centralized institutions that have sprung up to trade it, including exchanges and near monies, so-called stablecoins.» Киндлбергер умер в 2003 году; главу написали соавторы нового издания Роберт Алибер и Роберт Маккоули, и её аргументы здесь передаются только в объёме аннотации (R. Z. Aliber, C. P. Kindleberger, R. N. McCauley, «Bitcoin: Worse Than a Ponzi», в кн. «Manias, Panics, and Crashes», 8th ed., Palgrave Macmillan, 2023, pp. 349–371, DOI 10.1007/978-3-031-16008-0_14; аннотация: https://ideas.repec.org/h/spr/sprchp/978-3-031-16008-0_14.html).

[1182] BIS Working Paper 1049; развитие: G. Cornelli, S. Doerr, J. Frost, L. Gambacorta, «Crypto shocks and retail losses», BIS Bulletin No 69, 20.02.2023, https://www.bis.org/publ/bisbull69.htm.

[1183] Cornelli G., Doerr S., Frost J., Gambacorta L. Crypto shocks and retail losses. BIS Bulletin No 69, 20.02.2023: «a majority of crypto app users in nearly all economies made losses on their bitcoin holdings». В рабочей версии (BIS Working Paper 1049, 14.11.2022, пятеро авторов, среди них Р. Ауэр): «around three-quarters of users have lost money on their Bitcoin investments». Оценки модельные: их считали по дате входа в приложение и цене биткоина, реальные счета не проверялись (BIS Working Paper 1049; развитие: G. Cornelli, S. Doerr, J. Frost, L. Gambacorta, «Crypto shocks and retail losses», BIS Bulletin No 69, 20.02.2023, https://www.bis.org/publ/bisbull69.htm).

[1184] BIS Working Paper 1049; развитие: G. Cornelli, S. Doerr, J. Frost, L. Gambacorta, «Crypto shocks and retail losses», BIS Bulletin No 69, 20.02.2023, https://www.bis.org/publ/bisbull69.htm.

в день, в неделю пика 2021 года — по меньшей мере в шесть раз меньше, а в октябре 2025 года не больше обычной ставки[1185].

Нехватка капитала на другой стороне, которой экономисты Банка объясняли дорогое плечо[1186], со временем, вероятно, уменьшалась, и тогда перекос сглаживается, а петля на спаде раскручивается слабее. Это рифмуется со сжатием падений, но только рифмуется. У подешевевшего фандинга есть и другое возможное объяснение. Торговля ушла с BitMEX на другие биржи, и его ряд перестал показывать весь рынок[1187].

Спокойнее стала и расчистка. Мельче в процентах при этом не значит меньше в деньгах. Рекорды ликвидаций, как мы видели, росли, а открытый интерес осенью 2025 года был самым большим за всю историю рынка[1188]. Плечо в последнем цикле никуда не делось, оно подешевело и выросло в объёме. Почему его цена стояла на месте, я уверенно сказать не могу. Есть гипотеза, что её сдерживали крупные игроки, которые покупали биржевые фонды на биткоин и одновременно продавали фьючерсы, но доказательств в моих источниках нет, и к ней мы вернёмся в главе 10[1189]. Поэтому вывод у меня осторожный. Падения мельчали, пока плечо дешевело, а расчистка становилась спокойнее, и если в следующем цикле плечо снова станет дорогим, ничто не обязывает ряд продолжаться.

После расчистки у рынка остаются выжившие посредники, монеты у тех, кто не продал, и место для новой истории. С неё начнётся следующий цикл.

Календарь или цена денег

Знакомый с крипторынком читатель скажет, что цикл объясняется проще. Примерно раз в четыре года награда майнерам за блок уменьшается вдвое (это халвинг из третьей главы), новых монет становится меньше, и цена растёт по расписанию.

У этого взгляда есть сильный довод, и показать его нужно честно. Промежуток от халвинга до ценового пика в трёх последних больших циклах был на редкость ровным: 526 дней после халвинга 2016 года, 548 после халвинга 2020-го и 534 после халвинга 2024-го[1190].[1191] В апреле 2024 года аналитики Goldman Sachs предостерегали от того, чтобы переносить прошлые халвинг-циклы на будущее, потому что прежние халвинги приходились на быстрый рост

[1185] BitMEX API, https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2017-12-05&endTime=2017-12-20&count=100&reverse=false; BitMEX API: https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2021-02-01&endTime=2021-02-28&count=100&reverse=false; https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2021-10-25&endTime=2021-11-12&count=100&reverse=false; BitMEX API, https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2025-09-28&endTime=2025-10-14&count=100&reverse=false.

[1186] M. Schmeling, A. Schrimpf, K. Todorov, «Crypto carry», BIS Working Paper 1087, April 2023, https://www.bis.org/publ/work1087.htm.

[1187] BitMEX API: https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2021-02-01&endTime=2021-02-28&count=100&reverse=false; https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2021-10-25&endTime=2021-11-12&count=100&reverse=false.

[1188] CoinDesk Research, «Market Spotlight: Inside Crypto's $19 Billion Liquidation Event», 17.10.2025 (обновлено 30.10.2025), https://www.coindesk.com/research/market-spotlight-the-19-billion-liquidation-that-shook-crypto; Z. Pokorny, «The State of Crypto Leverage – Q3 2025», Galaxy Research, 19.11.2025, https://www.galaxy.com/insights/research/crypto-leverage-q3-2025-defi-cefi-lending-digital-asset-treasury-debt-futures-perpetuals; Z. Pokorny, «The State of Crypto Leverage Q2 2026: An Orderly, Measured Decline», 17.08.2026, https://www.galaxy.com/insights/research/crypto-leverage-report-q2-2026-defi-lending-decline-futures-open-interest.

[1189] BitMEX API, https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2025-09-28&endTime=2025-10-14&count=100&reverse=false.

[1190] расчёт: даты халвингов — (Bitcoin Wiki, mempool.space, The Block); даты пиков — (Bitstamp).

[1191] Даты халвингов и пиков: 09.07.2016 → 17.12.2017; 11.05.2020 → 10.11.2021; 20.04.2024 → 06.10.2025. В первом цикле, от халвинга 28.11.2012 до пика 30.11.2013, прошло 367 дней (расчёт: даты халвингов — (Bitcoin Wiki, mempool.space, The Block); даты пиков — (Bitstamp)).

денежной массы и почти нулевые ставки, а теперь ставки выше 5%[1192].[1193] Главным фактором цены они называли спрос на биржевые фонды[1194]. Пик после этого пришёл почти по расписанию.

Возражений у меня четыре: 1) три-четыре совпадения ещё не статистика; 2) халвинги 2012, 2016 и 2020 годов совпадали с мягкими деньгами, и по этим точкам не разделить, что подействовало[1195]; 3) доля новых монет в общем предложении с каждым халвингом всё меньше, так что сам «удар по предложению» слабеет[1196]; 4) ритм может держаться просто потому, что в него верят и покупают по календарю, и тогда это самосбывающаяся история в духе Шиллера[1197]. Надёжного исследования, которое разделило бы действие халвинга и действие денег, я не нашёл[1198].

Второй лагерь объясняет цикл ценой денег, и у него тоже есть сильный пример. Ставка ФРС, главный рычаг, которым центральный банк США двигает цену кредита, держалась около 0,08% до февраля 2022 года, а затем за полтора года выросла до 5,33%[1199]. Пик биткоина в ноябре 2021 года пришёлся на последние месяцы нулевой ставки, дно в ноябре 2022-го — на разгар её повышения[1200].

Денежная масса M2 в США (наличные и деньги на счетах, включая сберегательные) с февраля 2020 по март 2022 года выросла примерно на 41%, а биткоин от мартовского дна 2020 года до пика в ноябре 2021-го поднялся примерно в 18 раз[1201].[1202] Так закрывается вопрос о малом цикле из первого раздела. После мартовского шока внешние деньги стали дешёвыми и обильными, и цикл получил топливо.

[1192] O. Godbole, «Goldman Cautions Against Extrapolating Previous Bitcoin Halving Cycles for Price Predictions», CoinDesk, 17.04.2024 (по записке Goldman Sachs FICC and Equities от 12.04.2024), https://www.coindesk.com/markets/2024/04/17/goldman-cautions-against-extrapolating-previous-bitcoin-halving-cycles-for-price-predictions.

[1193] CoinDesk, 17.04.2024, по записке Goldman Sachs FICC and Equities от 12.04.2024: «Caution should be taken against extrapolating the past cycles and the impact of halving, given the respective prevailing macro conditions.» (O. Godbole, «Goldman Cautions Against Extrapolating Previous Bitcoin Halving Cycles for Price Predictions», CoinDesk, 17.04.2024 (по записке Goldman Sachs FICC and Equities от 12.04.2024), https://www.coindesk.com/markets/2024/04/17/goldman-cautions-against-extrapolating-previous-bitcoin-halving-cycles-for-price-predictions)

[1194] O. Godbole, «Goldman Cautions Against Extrapolating Previous Bitcoin Halving Cycles for Price Predictions», CoinDesk, 17.04.2024 (по записке Goldman Sachs FICC and Equities от 12.04.2024), https://www.coindesk.com/markets/2024/04/17/goldman-cautions-against-extrapolating-previous-bitcoin-halving-cycles-for-price-predictions.

[1195] O. Godbole, «Goldman Cautions Against Extrapolating Previous Bitcoin Halving Cycles for Price Predictions», CoinDesk, 17.04.2024 (по записке Goldman Sachs FICC and Equities от 12.04.2024), https://www.coindesk.com/markets/2024/04/17/goldman-cautions-against-extrapolating-previous-bitcoin-halving-cycles-for-price-predictions.

[1196] расчёт: даты халвингов — (Bitcoin Wiki, mempool.space, The Block); даты пиков — (Bitstamp).

[1197] R. J. Shiller, «Narrative Economics», American Economic Review 107(4), April 2017, pp. 967–1004, DOI 10.1257/aer.107.4.967, https://www.aeaweb.org/articles?id=10.1257/aer.107.4.967; расчёт: даты халвингов — (Bitcoin Wiki, mempool.space, The Block); даты пиков — (Bitstamp).

[1198] расчёт: даты халвингов — (Bitcoin Wiki, mempool.space, The Block); даты пиков — (Bitstamp).

[1199] FRED, Federal Reserve Bank of St. Louis, ряд FEDFUNDS (Effective Federal Funds Rate, в среднем за месяц): https://fred.stlouisfed.org/graph/fredgraph.csv?id=FEDFUNDS&cosd=2021-12-01&coed=2023-09-01; https://fred.stlouisfed.org/graph/fredgraph.csv?id=FEDFUNDS&cosd=2024-06-01&coed=2026-09-01.

[1200] FRED, Federal Reserve Bank of St. Louis, ряд FEDFUNDS (Effective Federal Funds Rate, в среднем за месяц): https://fred.stlouisfed.org/graph/fredgraph.csv?id=FEDFUNDS&cosd=2021-12-01&coed=2023-09-01; https://fred.stlouisfed.org/graph/fredgraph.csv?id=FEDFUNDS&cosd=2024-06-01&coed=2026-09-01.

[1201] FRED, ряд M2SL (M2, сезонно скорректированный, млрд долл.): https://fred.stlouisfed.org/graph/fredgraph.csv?id=M2SL&cosd=2020-01-01&coed=2023-12-01.

[1202] FRED: эффективная ставка по федеральным фондам (FEDFUNDS, среднее за месяц) — около 0,08% до февраля 2022 года, 5,33% в августе 2023-го, около 3,63–3,64% в 2026 году; M2 (M2SL, с сезонной поправкой) — 15,49 трлн долларов в феврале 2020 года, 21,79 трлн в марте 2022-го, 20,74 трлн в октябре 2023-го. Рост биткоина в 18 раз — от 3850 долларов (13.03.2020) до 69 000 (10.11.2021), Bitstamp (FRED, Federal Reserve Bank of St. Louis, ряд FEDFUNDS (Effective Federal Funds Rate, в среднем за месяц): https://fred.stlouisfed.org/graph/fredgraph.csv?id=FEDFUNDS&cosd=2021-12-01&coed=2023-09-01; https://fred.stlouisfed.org/graph/fredgraph.csv?id=FEDFUNDS&cosd=2024-06-01&coed=2026-09-01; FRED, ряд M2SL (M2, сезонно скорректированный, млрд долл.): https://fred.stlouisfed.org/graph/fredgraph.csv?id=M2SL&cosd=2020-01-01&coed=2023-12-01).

В те же годы биткоин стал двигаться вместе с акциями. Международный валютный фонд в январе 2022 года показал, что корреляция биткоина с индексом S&P 500 (индекс пятисот крупных американских компаний) выросла с 0,01 в 2017–2019 годах до 0,36 в 2020–2021-м[1203]. При корреляции около нуля две цены движутся независимо, при единице — в ногу, и 0,36 означает заметную, хотя и далеко не полную связь. По одному из объяснений, крипту стали держать те же инвесторы, что и акции, и продают они её в тех же ситуациях[1204]. Лин Олден, аналитик и сторонница биткоина, в сентябре 2024 года писала, что биткоин сильно коррелирует с глобальной ликвидностью, и ожидала, что так будет и дальше[1205].[1206]

Простая схема «ФРС поднимает ставку, биткоин падает» убедительно выглядит на 2020–2022 годах, но держится она слабее, чем кажется. Сёрен Карау из Бундесбанка изучил, как решения центральных банков влияют на цену биткоина, и получил неудобный для этой схемы результат. Ужесточение Европейского центрального банка в его данных снижало цену биткоина, а ужесточение ФРС её повышало, причём дополнительный спрос шёл в основном из развивающихся стран[1207].[1208] Сам автор объясняет это тем, что при ухудшении мировых условий биткоин востребован как глобальные цифровые наличные[1209]. Работа вышла в 2021 году, до резкого повышения ставок 2022-го, и одна работа ничего не решает, но утверждать, что наука доказала падение биткоина при ужесточении ФРС, нельзя.

Открытый цикл добавил второе неудобство. В 2025–2026 годах денежная масса M2 в США росла и ставила рекорды, ставку ФРС с сентября 2024 года снижали, а биткоин за это время упал больше чем вдвое от пика[1210].[1211] Пресса связывала падение 2026 года с ожиданием более жёсткой политики при новом председателе ФРС, хотя фактическая ставка до августа 2026 года не менялась[1212]. Сторонники тезиса о ликвидности отвечают, что имеют в виду миро-

---

[1203] T. Adrian, T. Iyer, M. Qureshi, «Crypto Prices Move More in Sync With Stocks, Posing New Risks», IMF Blog, 11.01.2022, https://www.imf.org/en/blogs/articles/2022/01/11/crypto-prices-move-more-in-sync-with-stocks-posing-new-risks.

[1204] T. Adrian, T. Iyer, M. Qureshi, «Crypto Prices Move More in Sync With Stocks, Posing New Risks», IMF Blog, 11.01.2022, https://www.imf.org/en/blogs/articles/2022/01/11/crypto-prices-move-more-in-sync-with-stocks-posing-new-risks.

[1205] L. Alden, September 2024 Newsletter, https://www.lynalden.com/september-2024-newsletter/.

[1206] Alden L. September 2024 Newsletter: «Bitcoin has been highly correlated with global liquidity, and I expect that to continue.» Популярную цифру о «83% совпадения» биткоина с мировой M2, которую приписывают Олден, подтвердить не удалось, и в книге она не используется (L. Alden, September 2024 Newsletter, https://www.lynalden.com/september-2024-newsletter/).

[1207] S. Karau, «Monetary policy and Bitcoin», Deutsche Bundesbank Discussion Paper No 41/2021, аннотация: https://ideas.repec.org/p/zbw/bubdps/412021.html; страница Бундесбанка: https://www.bundesbank.de/en/publications/research/discussion-papers/monetary-policy-and-bitcoin-880226; журнальная версия: Journal of International Money and Finance 137, 2023, 102880.

[1208] Karau S. Monetary policy and Bitcoin. Deutsche Bundesbank Discussion Paper No 41/2021; журнальная версия — Journal of International Money and Finance 137, 2023, 102880: «…a disinflationary monetary tightening by the ECB lowers valuations — consistent with the notion of Bitcoin as a digital gold —, whereas a Fed tightening increases Bitcoin prices.» Работа построена на недельных данных; период выборки в аннотации не указан (S. Karau, «Monetary policy and Bitcoin», Deutsche Bundesbank Discussion Paper No 41/2021, аннотация: https://ideas.repec.org/p/zbw/bubdps/412021.html; страница Бундесбанка: https://www.bundesbank.de/en/publications/research/discussion-papers/monetary-policy-and-bitcoin-880226; журнальная версия: Journal of International Money and Finance 137, 2023, 102880; метаданные Crossref и OpenAlex: https://api.crossref.org/works/10.1016/j.jimonfin.2023.102880; препринт SSRN 2021, DOI 10.2139/ssrn.3988527).

[1209] S. Karau, «Monetary policy and Bitcoin», Deutsche Bundesbank Discussion Paper No 41/2021, аннотация: https://ideas.repec.org/p/zbw/bubdps/412021.html; страница Бундесбанка: https://www.bundesbank.de/en/publications/research/discussion-papers/monetary-policy-and-bitcoin-880226; журнальная версия: Journal of International Money and Finance 137, 2023, 102880.

[1210] FRED, M2SL, https://fred.stlouisfed.org/graph/fredgraph.csv?id=M2SL&cosd=2024-01-01&coed=2026-09-01; FEDFUNDS; цены — https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=4&start=1759622400; FRED, Federal Reserve Bank of St. Louis, ряд FEDFUNDS (Effective Federal Funds Rate, в среднем за месяц): https://fred.stlouisfed.org/graph/fredgraph.csv?id=FEDFUNDS&cosd=2021-12-01&coed=2023-09-01; https://fred.stlouisfed.org/graph/fredgraph.csv?id=FEDFUNDS&cosd=2024-06-01&coed=2026-09-01.

[1211] FRED, M2SL: 22,41 трлн долларов в январе 2026 года, 23,34 трлн в августе 2026-го (FRED, M2SL, https://fred.stlouisfed.org/graph/fredgraph.csv?id=M2SL&cosd=2024-01-01&coed=2026-09-01; FEDFUNDS; цены — https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=4&start=1759622400).

[1212] FRED, M2SL, https://fred.stlouisfed.org/graph/fredgraph.csv?id=M2SL&cosd=2024-01-01&coed=2026-09-01;

вую ликвидность и ожидания ставок, а M2 одной страны и сегодняшняя ставка составляют только часть этой картины[1213]. Возражение законное, но чем шире определение ликвидности, тем труднее проверить, объясняет ли она хоть что-нибудь.

Что же тогда задаёт ритм, если ни календарь, ни ставка не объясняют всего?

Моя позиция в этом споре такая. Цикл складывается из трёх слоёв. Внешний слой — деньги центральных банков. Ставки и ликвидность задают прилив или отлив сразу для всех рискованных вложений, и в 2020–2022 годах этот слой был главным. Внутренний слой — плечо самого рынка, то есть споры с залогом, кредитные котлы и займы бирж. Он живёт отдельно от ФРС, и это показала осень 2025 года, когда рекорд открытого интереса и крупнейший каскад ликвидаций пришлись на время снижения ставки[1214]. Третий слой — история, и в неё входит вера в четырёхлетний календарь. Халвинг в этой модели скорее календарь, по которому рынок привык сверять часы, чем доказанная причина.

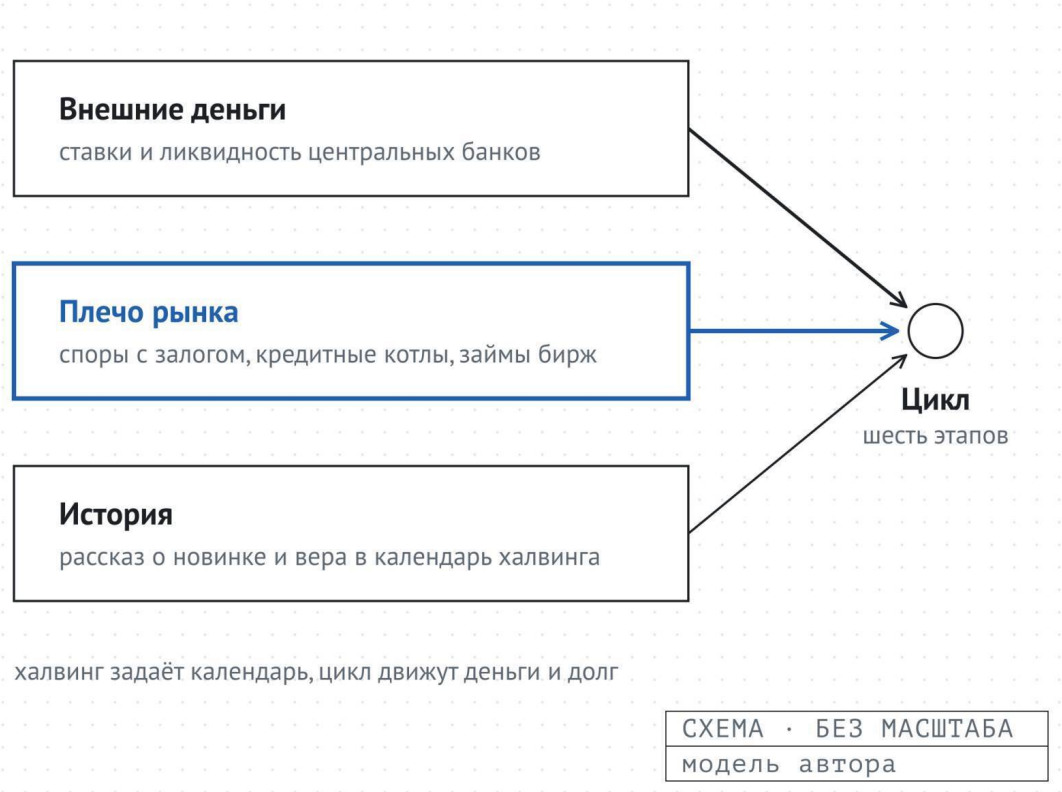


Рисунок 7.3. Три слоя цикла

FEDFUNDS; цены — https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=4&start=1759622400.

[1213] FRED, M2SL, https://fred.stlouisfed.org/graph/fredgraph.csv?id=M2SL&cosd=2024-01-01&coed=2026-09-01; FEDFUNDS; цены — https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=4&start=1759622400.

[1214] Z. Pokorny, «The State of Crypto Leverage – Q3 2025», Galaxy Research, 19.11.2025, https://www.galaxy.com/insights/research/crypto-leverage-q3-2025-defi-cefi-lending-digital-asset-treasury-debt-futures-perpetuals; Z. Pokorny, «The State of Crypto Leverage Q2 2026: An Orderly, Measured Decline», 17.08.2026, https://www.galaxy.com/insights/research/crypto-leverage-report-q2-2026-defi-lending-decline-futures-open-interest; CoinDesk Research, «Market Spotlight: Inside Crypto's $19 Billion Liquidation Event», 17.10.2025 (обновлено 30.10.2025), https://www.coindesk.com/research/market-spotlight-the-19-billion-liquidation-that-shook-crypto; FRED, Federal Reserve Bank of St. Louis, ряд FEDFUNDS (Effective Federal Funds Rate, в среднем за месяц): https://fred.stlouisfed.org/graph/fredgraph.csv?id=FEDFUNDS&cosd=2021-12-01&coed=2023-09-01; https://fred.stlouisfed.org/graph/fredgraph.csv?id=FEDFUNDS&cosd=2024-06-01&coed=2026-09-01.

Слои и шесть этапов описывают один цикл с двух сторон: слои говорят, откуда берётся топливо, этапы — в каком порядке оно горит. История запускает первый этап, внешние деньги и внутреннее плечо питают второй и третий, а от того, какой слой иссякнет первым, зависит, как придёт пик. В 2021 году перегрев плеча прошёл ещё до ценовой вершины, а внешний отлив начался уже после неё и углубил расчистку 2022-го. В 2025 году рынок развернулся при внешних деньгах, которые скорее помогали, и я считаю это доводом в пользу того, что внутренний слой способен развернуть рынок сам. Довод не решающий: падение 2026 года пресса связывала с ожиданием более жёсткой ФРС, и по одному циклу отделить одно от другого нельзя.

Спор проверит следующий цикл. Пик примерно через полтора года после халвинга, да ещё при дорогих деньгах, добавит доводов календарю; пик вслед за разворотом ставок или мировой ликвидности — второму лагерю; разворот при спокойных внешних деньгах, как в 2025 году, — внутреннему плечу.

Как узнать этап, не угадывая цену

У каждого этапа есть признаки, которые можно проверить, не зная будущей цены. Ни один из них не работает безотказно. Когда покупать и когда продавать, знание этапа тоже не подскажет, и такой подсказки в этой книге не будет. Зато оно подсказывает, какая ошибка на каком этапе обходится дороже всего.

К любому обвалу первый вопрос один: сколько на рынке было заёмных денег, когда пришёл повод. Смотреть при этом надо и на цену плеча, и на его объём. Открытый интерес публикуют агрегаторы вроде CoinGlass[1215], кредит под залог раз в квартал считает Galaxy[1216], а фандинг видно на самих биржах. Одного фандинга мало: в октябре 2025 года на BitMEX всю неделю пика и обвала он не поднимался выше обычных 0,01% за восемь часов, хотя открытый интерес был рекордным[1217]. Плечо копилось в объёме, а цена его оставалась обычной.

Таблица 7.2. Шесть этапов: как узнать и где ошибиться

Этап
Признак
Самая дорогая ошибка

1. Новая история
рассказ о том, почему на этот раз всё иначе, без ответа, кто ведёт запись и кто выдаёт строчки в долг; цифр почти нет
поверить рассказу без проверки

2. Приток денег
новых пользователей и скачиваний криптоприложений становится больше вслед за ценой; так бывает и на здоровом подъёме

[1215] T. Shen, «Hyperliquid founder says certain CEXs may underreport liquidations», The Block, 13.10.2025, https://www.theblock.co/post/374311/hyperliquid-founder-says-certain-cexs-may-underreport-liquidations.

[1216] Z. Pokorny, «The State of Crypto Leverage – Q3 2025», Galaxy Research, 19.11.2025, https://www.galaxy.com/insights/research/crypto-leverage-q3-2025-defi-cefi-lending-digital-asset-treasury-debt-futures-perpetuals; Z. Pokorny, «The State of Crypto Leverage Q2 2026: An Orderly, Measured Decline», 17.08.2026, https://www.galaxy.com/insights/research/crypto-leverage-report-q2-2026-defi-lending-decline-futures-open-interest.

[1217] BitMEX API, https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2025-09-28&endTime=2025-10-14&count=100&reverse=false; Z. Pokorny, «The State of Crypto Leverage – Q3 2025», Galaxy Research, 19.11.2025, https://www.galaxy.com/insights/research/crypto-leverage-q3-2025-defi-cefi-lending-digital-asset-treasury-debt-futures-perpetuals; Z. Pokorny, «The State of Crypto Leverage Q2 2026: An Orderly, Measured Decline», 17.08.2026, https://www.galaxy.com/insights/research/crypto-leverage-report-q2-2026-defi-lending-decline-futures-open-interest.

купить, потому что разбогател знакомый

3. Заёмные деньги и плечо

растут фандинг, открытый интерес и кредит под залог; плечо может копиться и при обычном фандинге

взять плечо самому: лесоруба выбросило с рынка на первых десяти процентах падения

4. Пик

приток и плечо перестают расти быстрее цены, перегрев фандинга проходит раньше вершины, на подъёме уже случаются каскады ликвидаций

ждать, что вершину отметит один сигнал

5. Принудительные продажи

каскады ликвидаций и резкое сокращение открытого интереса в тот же день; публичные цифры — нижняя граница

продажа, которую за человека сделал автомат

6. Расчистка

фандинг уходит в минус и возвращается к обычному, кредит под залог сжимается, посредники закрываются; дно может прийти после самой громкой паники

решить, что раз цена упала, хуже уже не будет: дно 2022 года пришло через десять дней после банкротства FTX

Источники:[1218].

Где рынок осенью 2026 года? Пик цикла пришёлся на 6 октября 2025 года, минимум после него, около 57 700 долларов, — на 1 июля 2026 года (Bitstamp), а в конце сентября цена держалась около 84 тыс. долларов[1219]. Открытый интерес к концу второго квартала 2026 года сократился до 103 млрд долларов, больше чем вдвое против рекорда[1220], кредит под залог

[1218] R. Auer, G. Cornelli, S. Doerr, J. Frost, L. Gambacorta, «Crypto trading and Bitcoin prices: evidence from a new database of retail adoption», BIS Working Paper 1049, 14.11.2022, https://www.bis.org/publ/work1049.htm; M. Schmeling, A. Schrimpf, K. Todorov, «Crypto carry», BIS Working Paper 1087, April 2023, https://www.bis.org/publ/work1087.htm; CoinDesk Research, «Market Spotlight: Inside Crypto's $19 Billion Liquidation Event», 17.10.2025 (обновлено 30.10.2025), https://www.coindesk.com/research/market-spotlight-the-19-billion-liquidation-that-shook-crypto; Z. Pokorny, «The State of Crypto Leverage – Q3 2025», Galaxy Research, 19.11.2025, https://www.galaxy.com/insights/research/crypto-leverage-q3-2025-defi-cefi-lending-digital-asset-treasury-debt-futures-perpetuals; Z. Pokorny, «The State of Crypto Leverage Q2 2026: An Orderly, Measured Decline», 17.08.2026, https://www.galaxy.com/insights/research/crypto-leverage-report-q2-2026-defi-lending-decline-futures-open-interest; Galaxy Research, Q3 2025; Galaxy Research, Q2 2026; Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1636329600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1668816000; O. Godbole, «Crypto Futures Saw Record $10B Worth of Liquidations on Sunday», CoinDesk, 19.04.2021 (по данным Bybt — прежнее название CoinGlass), https://www.coindesk.com/markets/2021/04/19/crypto-futures-saw-record-10b-worth-of-liquidations-on-sunday; T. Shen, «Hyperliquid founder says certain CEXs may underreport liquidations», The Block, 13.10.2025, https://www.theblock.co/post/374311/hyperliquid-founder-says-certain-cexs-may-underreport-liquidations; BitMEX API: https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2021-02-01&endTime=2021-02-28&count=100&reverse=false; https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2021-10-25&endTime=2021-11-12&count=100&reverse=false; BitMEX API, https://www.bitmex.com/api/v1/funding?symbol=XBTUSD&startTime=2022-11-05&endTime=2022-11-25&count=100&reverse=false.

[1219] Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=4&start=1759622400; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782691200; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782172800; трёхдневные свечи за январь–март и июль–сентябрь 2026: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1767225600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1782864000.

[1220] Z. Pokorny, «The State of Crypto Leverage – Q3 2025», Galaxy Research, 19.11.2025, https://www.galaxy.com/insights/research/crypto-leverage-q3-2025-defi-cefi-lending-digital-asset-treasury-debt-futures-perpetuals; Z. Pokorny, «The State of Crypto Leverage Q2 2026: An Orderly, Measured Decline», 17.08.2026, https://www.galaxy.com/insights/research/crypto-leverage-report-

сжимается уже три квартала[1221]. По признакам модели этап принудительных продаж рынок прошёл и находится в расчистке. Кончилась ли она, модель не говорит, и я судить не возьмусь. Минимум 1 июля остаётся минимумом «пока», и убрать это слово из таблицы 7.1 можно будет только задним числом[1222].

q2-2026-defi-lending-decline-futures-open-interest.

[1221] Galaxy Research, Q2 2026.

[1222] Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=4&start=1759622400; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782691200; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782172800; трёхдневные свечи за январь–март и июль–сентябрь 2026: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1767225600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1782864000.

Глава 8. Первые циклы: от пиццы до Mt. Gox и ICO (2010–2018)

Главная биржа первых лет биткоина почти три года торговала с дырой в кассе.

Дыра открылась в феврале 2014 года, через два с лишним месяца после вершины второго цикла, когда биржа остановила вывод монет[1223]. С 2010 по 2018 год рынок прошёл три больших цикла, и деньги в них терялись в похожих местах: в кассах бирж, на рынке, где за биткоины продавали наркотики, и в обещаниях проектов, собравших миллиарды долларов на продукт, которого ещё не было. Общую тетрадку биткоина за эти годы никто тайно не переписал. Дыры копились у посредников, которые держали чужие монеты или выпускали свои строчки, росли, пока их прятал подъём, и открывались после разворота цены. Первыми среди тех, кого накрывала расчистка, каждый раз оказывались посредники.

Масштаб за эти годы вырос до неузнаваемости. На пике 2011 года все биткоины вместе стоили около 206 млн долларов[1224], а за один 2018 год весь крипторынок потерял почти 700 млрд[1225], то есть потеря одного года оказалась в три с лишним тысячи раз больше, чем стоил весь рынок первого цикла. Механизм при этом оставался прежним.

Три первые цены биткоина

До цены у биткоина был расчёт. Первый известный курс опубликовал 5 октября 2009 года сервис New Liberty Standard. За доллар он давал 1309,03 BTC, то есть монета стоила около 0,08 цента[1226]. Рынка за этим числом не было. Владелец сервиса прикидывал, сколько монет его компьютер добывает на доллар, потраченный на электричество: брал месячный счёт за работу компьютера с полной загрузкой процессора и сравнивал его с числом монет, добытых за последние 30 дней[1227].[1228] Первой ценой биткоина стала себестоимость одного майнера, и даже её, судя по пометке в хронологии Bitcoin Wiki, один из участников форума считал завышенной[1229].

[1223] WizSec, «The missing MtGox bitcoins», 19.04.2015, https://blog.wizsec.jp/2015/04/the-missing-mtgox-bitcoins.html; Wikipedia, «Mt. Gox» (ссылки на Bloomberg, Reuters, Wired), https://en.wikipedia.org/wiki/Mt._Gox.

[1224] Bitcoin Wiki, «History», раздел 2011, https://en.bitcoin.it/wiki/History.

[1225] CoinDesk, «Down More than 70% in 2018, Bitcoin Closes Its Worst Year on Record», 02.01.2019, https://www.coindesk.com/markets/2019/01/02/down-more-than-70-in-2018-bitcoin-closes-its-worst-year-on-record.

[1226] Bitcoin Wiki, «History», раздел 2009, https://en.bitcoin.it/wiki/History.

[1227] R. Manly, «The Very Early Bitcoin Exchanges of 2009 to 2011», BullionStar, https://www.bullionstar.com/blogs/ronan-manly/dawn-of-bitcoin-price-discovery-2009-2011-the-very-early-bitcoin-exchanges/ (цитирует архив страницы NLS: web.archive.org/web/20091229132610/http://newlibertystandard.wetpaint.com/page/Exchange+Rate).

[1228] Manly R. The Very Early Bitcoin Exchanges of 2009 to 2011. BullionStar — цитата архивной страницы New Liberty Standard: «dividing $1.00 by the average amount of electricity required to run a computer with high CPU for a year, 1331.5 kWh, multiplied by the average residential cost of electricity in the United States for the previous year, $0.1136, divided by 12 months divided by the number of bitcoins generated by my computer over the past 30 days.» Пометка в Bitcoin Wiki (History): «theymos thought NLS was overcharging» (R. Manly, «The Very Early Bitcoin Exchanges of 2009 to 2011», BullionStar, https://www.bullionstar.com/blogs/ronan-manly/dawn-of-bitcoin-price-discovery-2009-2011-the-very-early-bitcoin-exchanges/ (цитирует архив страницы NLS: web.archive.org/web/20091229132610/http://newlibertystandard.wetpaint.com/page/Exchange+Rate); Bitcoin Wiki, «History», раздел 2009, https://en.bitcoin.it/wiki/History).

[1229] R. Manly, «The Very Early Bitcoin Exchanges of 2009 to 2011», BullionStar, https://www.bullionstar.com/blogs/ronan-manly/dawn-of-bitcoin-price-discovery-2009-2011-the-very-early-bitcoin-exchanges/ (цитирует архив страницы NLS: web.archive.org/web/20091229132610/http://newlibertystandard.wetpaint.com/page/Exchange+Rate).

Первая биржа появилась в 2010 году. Bitcoin Market, владельцем которой был пользователь форума с ником dwdollar, открылась 6 февраля, а торги на ней начались 17 марта[1230]. И всё же цену, которую помнят до сих пор, дала одна покупка вне биржи.

Программист Ласло Ханьеч, писавший на форуме bitcointalk под ником laszlo, 18 мая 2010 года предложил 10 000 BTC за пару больших пицц, «чтобы осталось на завтра», и указал свой город, Джексонвилл во Флориде[1231].[1232] Через четыре дня, 22 мая, он сообщил в той же ветке, что обмен состоялся, выложил ссылку на фотографии и поблагодарил пользователя jercos[1233].[1234] Кем jercos был за пределами форума, по первоисточнику проверить нельзя. Сам Ханьеч оценивал заказ примерно в 25 долларов, «может, в 30, если дать хорошие чаевые»[1235]. Если поделить одно на другое, выйдет четверть цента за монету.

Такую цену мог предложить только тот, у кого монет было больше, чем ему было нужно. Ханьеч одним из первых добывал биткоины на видеокартах и, по подсчёту CoinDesk, с апреля по ноябрь 2010 года потратил около 81 432 BTC[1236]. В июне он писал, что предложение остаётся в силе, а в августе признал, что больше не может его повторять, потому что уже не добывает тысячи монет в день[1237].

Эту покупку часто называют самой дорогой пиццей в истории. По цене конца сентября 2026 года, около 84 тыс. долларов за монету на Bitstamp[1238], 10 000 BTC стоили бы примерно 840 млн долларов. Сам Ханьеч в 2019 году смотрел на неё иначе. Сделка, говорил он, происходит, потому что обе стороны думают, что выгадали, а ему казалось, что он «обыгрывает интернет», получая бесплатную еду[1239].[1240] Монеты стоили ему электричества, пицца была настоящей, и в хозяйстве, где цен почти не было, такой обмен выглядел разумным.

[1230] Bitcoin Wiki, «History» (дата основания), https://en.bitcoin.it/wiki/History; Bitcoin Wiki, «Bitcoin Market» (начало торгов, PayPal), https://en.bitcoin.it/wiki/Bitcoin_Market.

[1231] laszlo, «Pizza for bitcoins?», bitcointalk.org, topic 137, пост от 18.05.2010, 12:35:20 AM, https://bitcointalk.org/index.php?topic=137.0.

[1232] laszlo. Pizza for bitcoins? bitcointalk.org, topic 137, 18.05.2010: «I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day.» Город — в посте того же дня: «Jacksonville, Florida zip code 32224 United States». Время постов форум показывает без часового пояса (laszlo, «Pizza for bitcoins?», bitcointalk.org, topic 137, пост от 18.05.2010, 12:35:20 AM, https://bitcointalk.org/index.php?topic=137.0).

[1233] laszlo, bitcointalk, topic 137, пост от 22.05.2010, 07:17:26 PM, https://bitcointalk.org/index.php?topic=137.0.

[1234] Там же, 22.05.2010: «I just want to report that I successfully traded 10,000 bitcoins for pizza. Pictures: … Thanks jercos!» Оценка заказа — пост от 12.06.2010: «the 2 pizzas are only about 25 dollars total, maybe 30 if you give the guy a nice tip.» Пост от 04.08.2010: «I can't really afford to keep doing it since I can't generate thousands of coins a day anymore» (laszlo, bitcointalk, topic 137, пост от 22.05.2010, 07:17:26 PM, https://bitcointalk.org/index.php?topic=137.0; laszlo, bitcointalk, topic 137, пост от 12.06.2010, 08:14:44 PM, https://bitcointalk.org/index.php?topic=137.0).

[1235] laszlo, bitcointalk, topic 137, пост от 12.06.2010, 08:14:44 PM, https://bitcointalk.org/index.php?topic=137.0.

[1236] CoinDesk, «What You Didn't Know About Laszlo Hanyecz, the Bitcoin Pizza Day Legend», 22.05.2025, https://www.coindesk.com/tech/2025/05/22/what-you-didnt-know-about-laszlo-hanyecz-the-bitcoin-pizza-day-legend.

[1237] laszlo, bitcointalk, topic 137, пост от 12.06.2010, 08:14:44 PM, https://bitcointalk.org/index.php?topic=137.0.

[1238] Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=4&start=1759622400; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782691200; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782172800; трёхдневные свечи за январь–март и июль–сентябрь 2026: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1767225600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1782864000.

[1239] CoinDesk, «What You Didn't Know About Laszlo Hanyecz, the Bitcoin Pizza Day Legend», 22.05.2025, https://www.coindesk.com/tech/2025/05/22/what-you-didnt-know-about-laszlo-hanyecz-the-bitcoin-pizza-day-legend.

[1240] CoinDesk, 22.05.2025, цитата Ханьеча 2019 года: «A trade happens because both parties think they're getting a good deal. I felt like I was beating the internet, getting free food.» Число 81 432 BTC — подсчёт журналиста по данным блокчейна, методика не раскрыта. Пересчёт 10 000 BTC — мой: 10 000 × около 84 000 долларов (Bitstamp, закрытие 26.09.2026 — 84 433 доллара) (CoinDesk, «What You Didn't Know About Laszlo Hanyecz, the Bitcoin Pizza Day Legend», 22.05.2025, https://www.coindesk.com/tech/2025/05/22/what-you-didnt-know-about-laszlo-hanyecz-the-bitcoin-pizza-day-legend; Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=4&start=1759622400; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782691200; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=5&start=1782172800; трёхдневные свечи за январь–март и июль–сентябрь 2026: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1767225600; https://

Цена одной сделки — это договорённость двух людей. Рынком она становится, когда сделок много и их видно всем, а для этого нужна площадка. В середине июля 2010 года программист Джед Маккалеб открыл биржу Mt. Gox, и название ей досталось от его прежнего проекта для обмена карточками игры Magic: The Gathering (Magic: The Gathering Online eXchange)[1241]. В те же дни рынок впервые показал, как на него действует новость. После заметки о биткоине на технологическом сайте Slashdot 11 июля курс, по хронологии Bitcoin Wiki, за пять дней вырос примерно в десять раз, с 0,008 до 0,08 доллара[1242].

К 6 ноября цена на Mt. Gox коснулась 50 центов, а «экономика биткоина», по той же хронологии, впервые превысила миллион долларов[1243]. За полгода после пиццы монета подорожала примерно в двести раз.

У появления биржи есть следствие, которое легко пропустить. С этого времени «цена биткоина» в хрониках означает цену на конкретной площадке, и почти все цены 2010–2011 годов в этой главе — цены Mt. Gox[1244]. Цена превращается в запись в базе данных биржи: там сходятся заявки её клиентов, и там же хранятся их деньги. С 2010 года у рынка появилась точка, где цена, деньги клиентов и доверие к ним собраны в одних руках, и первый же цикл показал, что бывает, когда эти руки подводят.

2011: первый пузырь и первая дыра

Где лежали деньги клиентов, когда летом 2011 года цена развернулась? В основном на одной бирже, и хроника первого цикла объясняет, как они там оказались.

9 февраля 2011 года биткоин на Mt. Gox впервые стоил доллар[1245], а 8 июня там же дошёл до 31,91 доллара[1246]. Рост в 32 раза за четыре месяца — приток денег в чистом виде. Новая история у этого подъёма была неудобной. 1 июня издание Gawker написало о Silk Road, запущенном в начале 2011 года рынке в даркнете (так называют сайты, на которые заходят через программы для анонимного доступа), где платили биткоинами, а 5 июня сенатор Чак Шумер потребовал от федеральных властей закрыть сайт[1247]. О биткоине заговорили далеко за пределами форумов, но прямой связи этой огласки с пиком 8 июня никто не показал.

Главная площадка к пику уже сменила хозяина. В марте 2011 года Маккалеб продал Mt. Gox французскому программисту Марку Карпелесу, который жил в Японии[1248]. Биржа, на которую в апреле 2013 года в отдельные дни будет приходиться около 90% торговли трёх крупнейших площадок[1249], перешла в другие руки через восемь месяцев после запуска.

От вершины цена отступила быстро, и уже 12 июня она ненадолго опускалась почти до 10 долларов[1250]. Цикл развернулся раньше, чем подвёл посредник. 19 июня кто-то воспользовался

---

www.bitstamp.net/api/v2/ohlc/btcusd/?step=259200&limit=30&start=1782864000). Свежая цена — в приложении Б.

[1241] Bitcoin Wiki, «History» («July 17: MtGox established»), https://en.bitcoin.it/wiki/History; Wikipedia, «Mt. Gox» (18 июля 2010), https://en.wikipedia.org/wiki/Mt._Gox.

[1242] Bitcoin Wiki, «History», раздел 2010, https://en.bitcoin.it/wiki/History.

[1243] Bitcoin Wiki, «History», https://en.bitcoin.it/wiki/History.

[1244] Bitcoin Wiki, «History», https://en.bitcoin.it/wiki/History; Bitcoin Wiki, «History», раздел 2011, https://en.bitcoin.it/wiki/History; Bitcoin Wiki, «History», раздел 2011, https://en.bitcoin.it/wiki/History.

[1245] Bitcoin Wiki, «History», раздел 2011, https://en.bitcoin.it/wiki/History.

[1246] Bitcoin Wiki, «History», раздел 2011, https://en.bitcoin.it/wiki/History.

[1247] Wikipedia, «Silk Road (marketplace)», https://en.wikipedia.org/wiki/Silk_Road_(marketplace); U.S. Attorney's Office SDNY, «Manhattan U.S. Attorney Announces Seizure Of Additional $28 Million Worth Of Bitcoins Belonging To Ross William Ulbricht…», 25.10.2013, https://www.justice.gov/archive/usao/nys/pressreleases/October13/SilkRoadSeizurePR.php.

[1248] Bitcoin Wiki, «History» («March 1: MagicalTux buys mtgox.com from its founder Jed McCaleb»), https://en.bitcoin.it/wiki/History; Wikipedia, «Mt. Gox», https://en.wikipedia.org/wiki/Mt._Gox.

[1249] G. Hileman, «2013 Bitcoin Trading Volume: The Winners and Losers», CoinDesk, 24.12.2013, https://www.coindesk.com/markets/2013/12/24/2013-bitcoin-trading-volume-the-winners-and-losers.

[1250] Bitcoin Wiki, «History», раздел 2011, https://en.bitcoin.it/wiki/History.

взломанной служебной учётной записью Mt. Gox (по большинству описаний — аудитора) и выставил на продажу сотни тысяч биткоинов, которых не существовало. Цена на бирже упала с 17,51 доллара до одного цента, а в те же дни в сеть утекла таблица пользователей, около 60 000 учётных записей[1251].[1252]

Отсюда популярная история о том, что в 2011 году биткоин стоил цент. Цент был записью в базе данных одной биржи (в общей тетрадке цен нет вовсе, она записывает только переводы), и общую тетрадку взлом не затронул, потому что проданных монет в ней просто не было.

В те же июньские дни подводили и другие посредники. 19 июня около 600 клиентов сервиса-кошелька MyBitcoin лишились балансов после кражи паролей, а 20 июня правозащитный фонд EFF перестал принимать пожертвования в биткоинах из-за правовой неопределённости[1253]. Ещё раньше, 4 июня, Bitcoin Market отказалась от платежей через PayPal из-за мошенничества[1254]. Ломались мосты между биткоином и обычными деньгами и кассы, где биткоины держали за других, а с самой тетрадкой ничего не случалось.

Во второй главе я говорил, что у клиента биржи остаётся только обещание выдать монеты по первому требованию. В общей тетрадке монеты числятся за ключами биржи, а кому из клиентов сколько причитается, биржа пишет в своей тетрадке, и эту вторую запись со стороны никто не сверяет. Клиент на деле дал бирже в долг, как вкладчик из первой главы, у которого в тетрадке банка написано «банк должен вам столько-то»[1255], только над такой биржей не стояло ни главного хранителя, ни правил для банков.

В седьмой главе чужие деньги у посредника отнесены к третьему этапу, к заёмным деньгам и плечу, и в первых циклах этот этап виден почти только через них: займов с плечом в данных 2011 года нет. Здесь полезно развести два случая. Пока посредник просто хранит чужие монеты, он определяет, кто заплатит на расчистке, но цену не разгоняет. Топливом эти деньги становятся, когда посредник пускает их в оборот: тратит, одалживает или продаёт клиентам строчки, за которыми ничего не лежит. В 2011 году виден только первый случай, второй появится в следующем цикле.

Расчистка заняла около четырёх с половиной месяцев. 20 октября 2011 года цена на Bitstamp опустилась до 2,22 доллара, примерно на 93% ниже июньской вершины Mt. Gox, а 21 ноября повторила этот низ[1256]. Токийская компания WizSec, позже расследовавшая пропажу монет Mt. Gox, датирует первые расхождения в них августом 2011 года[1257]. Пустеть биржа начала в первую же расчистку, а узнали об этом через два с половиной года.

У первого цикла был и посредник другого рода. На Silk Road покупатель платил биткоинами, а площадка держала его деньги на условном депонировании, то есть передавала их продавцу, только когда сделка закрыта, и брала за это комиссию[1258]. По уголовной жалобе 2013

[1251] Bitcoin Wiki, «History», https://en.bitcoin.it/wiki/History; Wikipedia, «Mt. Gox» (со ссылкой на Ars Technica, 15–19.06.2011), https://en.wikipedia.org/wiki/Mt._Gox.

[1252] Bitcoin Wiki, History: «June 19: Someone was able to access an admin account at MtGox and issue sell orders for hundreds of thousands of fake bitcoins, forcing the MtGox price down from $17.51 per bitcoin to $0.01.» Bitcoin Wiki (страница 2011) и Wikipedia говорят о взломанной учётной записи аудитора; дата утечки базы в источниках расходится («a few days later» у Wikipedia) (Bitcoin Wiki, «History», https://en.bitcoin.it/wiki/History; Wikipedia, «Mt. Gox» (со ссылкой на Ars Technica, 15–19.06.2011), https://en.wikipedia.org/wiki/Mt._Gox).

[1253] Bitcoin Wiki, «History», раздел 2011, https://en.bitcoin.it/wiki/History.

[1254] Bitcoin Wiki, «History» (дата основания), https://en.bitcoin.it/wiki/History; Bitcoin Wiki, «Bitcoin Market» (начало торгов, PayPal), https://en.bitcoin.it/wiki/Bitcoin_Market.

[1255] McLeay, Radia, Thomas, «Money creation in the modern economy», BoE QB 2014 Q1, стр. 16.

[1256] Bitstamp API: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=61&start=1314835200 (сентябрь–октябрь 2011); https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=30&start=1320105600 (ноябрь 2011); https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=40&start=1322697600 (декабрь 2011 — начало января 2012); пик — Bitcoin Wiki.

[1257] WizSec, «The missing MtGox bitcoins», 19.04.2015, https://blog.wizsec.jp/2015/04/the-missing-mtgox-bitcoins.html.

[1258] Wikipedia, «Silk Road (marketplace)» (пересказ жалобы ФБР, 2013), https://en.wikipedia.org/wiki/

года, продажи на ней составили больше 9,5 млн BTC, около 1,2 млрд долларов по курсам на момент сделок[1259].[1260] Биткоин обещал деньги, которым не нужен посредник, а одно из первых массовых применений нашёл там, где покупатель и продавец не знали друг друга и не могли пойти в суд. Доверие на таком рынке никуда не делось, его просто принимала на себя касса площадки. Тетрадка без хранителя обслуживала этот рынок исправно, а посредник с кассой всё равно понадобился, только вне закона.

Прятался этот рынок в открытой тетрадке. Исследователи из Калифорнийского университета в Сан-Диего, о которых шла речь во второй главе, для своей работы 2013 года пополняли счета в том числе на Silk Road и по этим следам помечали адреса площадки[1261]. Деньги сайта видел всякий, кто умел читать тетрадку, а кто стоит за адресами, тетрадка не говорила.

1 октября 2013 года ФБР арестовало основателя Silk Road Росса Ульбрихта в публичной библиотеке Сан-Франциско, и сайт закрыли[1262]. К концу месяца федеральные агенты изъяли около 174 000 BTC, и первую часть Служба маршалов США в июне 2014 года продала с аукциона[1263].[1264] Государство впервые стало крупным держателем биткоина, а затем и продавцом, и к этой роли государств книга ещё вернётся. Часть монет по дороге присвоили двое федеральных агентов, работавших по делу, и оба позже признали вину[1265].[1266] Ульбрихта в 2015 году приговорили к пожизненному заключению без права на досрочное освобождение, а 21 января 2025 года он получил полное и безусловное помилование[1267].[1268]

Silk_Road_(marketplace).

[1259] U.S. Attorney's Office SDNY, «Manhattan U.S. Attorney Announces Seizure Of Additional $28 Million Worth Of Bitcoins Belonging To Ross William Ulbricht…», 25.10.2013, https://www.justice.gov/archive/usao/nys/pressreleases/October13/SilkRoadSeizurePR.php.

[1260] U.S. Attorney's Office SDNY, 25.10.2013: «All told, the site generated sales revenue of more than 9.5 million Bitcoins and collected commissions from these sales totaling more than 600,000 Bitcoins», что «roughly equivalent to approximately $1.2 billion in sales and approximately $80 million in commissions». Там же начало работы сайта — январь 2011 года (по Wikipedia — февраль). Более точные числа (9 519 664 BTC, 1 229 465 сделок) есть только в пересказе Wikipedia. В приговорном сообщении 2015 года прокуратура приводит другую, более узкую оценку, больше 200 млн долларов нелегальных товаров, и смешивать две цифры нельзя (U.S. Attorney's Office SDNY, «Manhattan U.S. Attorney Announces Seizure Of Additional $28 Million Worth Of Bitcoins Belonging To Ross William Ulbricht…», 25.10.2013, https://www.justice.gov/archive/usao/nys/pressreleases/October13/SilkRoadSeizurePR.php; Wikipedia, «Silk Road (marketplace)» (пересказ жалобы ФБР, 2013), https://en.wikipedia.org/wiki/Silk_Road_(marketplace); SDNY/ICE, 29.05.2015).

[1261] Meiklejohn et al., 2013, разделы 3.1 и 4.5.

[1262] Wikipedia, «Ross Ulbricht», https://en.wikipedia.org/wiki/Ross_Ulbricht; Wikipedia, «Silk Road (marketplace)», https://en.wikipedia.org/wiki/Silk_Road_(marketplace).

[1263] SDNY, 25.10.2013; Wikipedia, «Silk Road (marketplace)», https://en.wikipedia.org/wiki/Silk_Road_(marketplace).

[1264] Аукцион прошёл 27.06.2014, монеты купил венчурный инвестор Тим Дрейпер (Wikipedia, «Silk Road (marketplace)», https://en.wikipedia.org/wiki/Silk_Road_(marketplace)). Изъятия по сообщению прокуратуры: «approximately 29,655 Bitcoins», затем около 144 336 BTC, всего около 173 991 BTC (SDNY, 25.10.2013). Бывшие администраторы запустили Silk Road 2.0 06.11.2013; ФБР вместе с Европолом и Евроюстом закрыло его 06.11.2014 (Wikipedia, «Silk Road (marketplace)», https://en.wikipedia.org/wiki/Silk_Road_(marketplace)).

[1265] Wikipedia, «Silk Road (marketplace)», https://en.wikipedia.org/wiki/Silk_Road_(marketplace).

[1266] Карл Форс (Управление по борьбе с наркотиками) и Шон Бриджес (Секретная служба), арестованы в марте 2015 года; оба признали вину по статьям об отмывании денег и воспрепятствовании правосудию (Форс — ещё и о вымогательстве) (Wikipedia, «Silk Road (marketplace)», https://en.wikipedia.org/wiki/Silk_Road_(marketplace)).

[1267] Wikipedia, «Ross Ulbricht», https://en.wikipedia.org/wiki/Ross_Ulbricht; SDNY, «Ross Ulbricht, A/K/A "Dread Pirate Roberts," Sentenced In Manhattan Federal Court To Life In Prison», 29.05.2015, https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison; тот же текст на сайте ICE: https://www.ice.gov/news/releases/ross-ulbricht-aka-dread-pirate-roberts-sentenced-life-federal-prison-creating; U.S. Department of Justice, Office of the Pardon Attorney, «Clemency Grants by President Donald J. Trump (2025–Present)», https://www.justice.gov/pardon/clemency-grants-president-donald-j-trump-2025-present.

[1268] Вердикт присяжных — 04.02.2015, по всем семи пунктам, среди них распространение наркотиков через интернет и руководство преступным предприятием (SDNY, «Ross Ulbricht, The Creator And Owner Of The "Silk Road" Website, Found Guilty In Manhattan Federal Court On All Counts», 05.02.2015, https://www.justice.gov/archive/usao/nys/pressreleases/February15/UlbrichtRossVerdictPR.php?print=1). Приговор в сообщении прокуратуры от 29.05.2015: «In addition to the life sentence prison term, Ulbricht was ordered to forfeit $183,961,921.» (SDNY, «Ross Ulbricht, A/K/A "Dread Pirate Roberts," Sentenced In Manhattan Federal Court To Life In Prison», 29.05.2015, https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-

2013–2015: биржа, которая торговала пустой

Откуда брался спрос на бирже, у которой к середине 2013 года почти не осталось монет? Его приводил сам рост цены, а часть спроса, по версии позднейшего расследования, биржа создавала сама.

Второй цикл разогнался весной 2013 года. 28 февраля цена на Mt. Gox превысила вершину 2011 года, 28 марта все биткоины вместе впервые стоили больше миллиарда долларов, а 1 апреля монета, по хронологии Bitcoin Wiki, впервые стоила больше 100 долларов[1269].

В те же недели на рынок всерьёз посмотрело государство. 18 марта FinCEN, подразделение Министерства финансов США по борьбе с финансовыми преступлениями, разъяснило, что обычных пользователей биткоина правила не касаются, а обменники подчиняются тем же требованиям, что и компании денежных переводов[1270]. Регулировать начали с точки обмена, то есть опять с посредника. (Первый халвинг прошёл 28 ноября 2012 года, за год и два дня до вершины этого цикла[1271], и почему одного совпадения мало для правила, мы разобрали в седьмой главе.)

Ту же весну часто объясняют кризисом на Кипре. 16 марта 2013 года Кипр объявил, что примет программу помощи с разовым налогом на банковские вклады, и вкладчики будто бы бросились в биткоин. Экономисты Лютер и Солтер проверили эту версию по загрузкам приложений для биткоина (цену они не изучали). После кипрских новостей загрузки выросли, но в странах, чьи банки тогда считались проблемными, рост не был особенно заметен[1272].[1273] Совпадение по времени есть, а доказательства, что рост вызвал именно Кипр, нет.

Первый обвал случился внутри того же подъёма. 10 апреля 2013 года биткоин на Mt. Gox начал день около 200 долларов, дошёл до рекордных 266, а за несколько часов упал до 105[1274]. Заявки клиентов исполнялись с опозданием больше чем на 70 минут. Сама биржа объяснила сбой наплывом: за первые дни апреля на ней открыли около 75 000 новых счетов, а паническая продажа, по её словам, «заморозила торговый движок»[1275].[1276] 11 апреля Mt. Gox

---

pirate-roberts-sentenced-manhattan-federal-court-life-prison; тот же текст на сайте ICE: https://www.ice.gov/news/releases/ross-ulbricht-aka-dread-pirate-roberts-sentenced-life-federal-prison-creating) Прокуратура утверждала также, что он заказывал убийства, и в том же сообщении оговаривала, что доказательств их совершения нет; в пункты вердикта эти обвинения не входили (SDNY/ICE, 29.05.2015). Апелляционный суд оставил приговор в силе в 2017 году, Верховный суд в 2018-м отказался его пересматривать (Wikipedia, «Ross Ulbricht», https://en.wikipedia.org/wiki/Ross_Ulbricht). В мае 2024 года Дональд Трамп обещал смягчить приговор (Wikipedia, «Ross Ulbricht» (ссылается на New York Times, 22.01.2025, и NBC News, 25.05.2024), https://en.wikipedia.org/wiki/Ross_Ulbricht). U.S. DOJ, Office of the Pardon Attorney. Clemency Grants by President Donald J. Trump (2025–Present): Ross William Ulbricht, 21.01.2025, «Full and unconditional pardon»; графа «Offense»: «Aiding and abetting distribution of drugs over internet; continuing criminal enterprise; computer hacking conspiracy; fraud with identification documents; money laundering conspiracy» (U.S. Department of Justice, Office of the Pardon Attorney, «Clemency Grants by President Donald J. Trump (2025–Present)», https://www.justice.gov/pardon/clemency-grants-president-donald-j-trump-2025-present).

[1269] Bitcoin Wiki, «History», раздел 2013, https://en.bitcoin.it/wiki/History.

[1270] Bitcoin Wiki, «History» («March 18: FinCEN declares Bitcoin users subject to regulation only at USD-BTC exchange point»), https://en.bitcoin.it/wiki/History; Wikipedia, «History of bitcoin», https://en.wikipedia.org/wiki/History_of_bitcoin.

[1271] расчёт: даты халвингов — (Bitcoin Wiki, mempool.space, The Block); даты пиков — (Bitstamp).

[1272] Luther W. J., Salter A. W. «Bitcoin and the Bailout». The Quarterly Review of Economics and Finance, vol. 66, 2017, pp. 50–56; аннотация: https://ideas.repec.org/a/eee/quaeco/v66y2017icp50-56.html.

[1273] Luther W. J., Salter A. W. Bitcoin and the Bailout. The Quarterly Review of Economics and Finance 66, 2017, pp. 50–56; аннотация: «…while downloads of bitcoin apps increased following the announcement, the observed effect was not especially pronounced in countries thought to have had troubled banking systems at the time.» Выводы касаются загрузок приложений, не цены (Luther W. J., Salter A. W. «Bitcoin and the Bailout». The Quarterly Review of Economics and Finance, vol. 66, 2017, pp. 50–56; аннотация: https://ideas.repec.org/a/eee/quaeco/v66y2017icp50-56.html).

[1274] P. Waldie, «Bitcoin exchange halted after panic “froze the trade engine!”», The Globe and Mail, 11.04.2013, https://www.theglobeandmail.com/report-on-business/international-business/bitcoin-exchange-halted-after-panic-froze-the-trade-engine/article11097521/; V. Buterin, «The Bitcoin Crash: An Examination», Bitcoin Magazine, 14.04.2013, https://bitcoinmagazine.com/markets/the-bitcoin-crash-an-examination-1365911041.

[1275] Buterin, Bitcoin Magazine, 14.04.2013 — задержка и 75 000 счетов; заявление Mt. Gox — The Globe and Mail,

остановила торги примерно на 12 часов, «чтобы дать рынку остыть», а после возобновления цена опустилась примерно до 55 долларов, на 80% ниже пика двухдневной давности, и лишь потом вернулась выше 100[1277].

Опоздание в час превращает биржу в усилитель паники. Клиент видит цену часовой давности, не знает, где рынок сейчас, и может продать вслепую, а его заявка встаёт в ту же очередь. В модели седьмой главы это маленький пик и маленькие принудительные продажи внутри одного большого цикла, и пятый этап здесь устроило узкое горло одной биржи, займов за ним не видно. Через несколько дней, 16 апреля 2013 года, по данным агрегатора bitcoincharts, на Mt. Gox пришлось около 90% объёма трёх крупнейших бирж[1278].[1279] Узкое горло было почти одно на весь рынок.

Трещины у главного посредника появились почти сразу. В мае–августе Министерство внутренней безопасности США по ордеру арестовало около 2,9 млн долларов на счёте дочерней компании Mt. Gox в платёжном сервисе Dwolla и около 2,1 млн в банке Wells Fargo, а 20 июня биржа приостановила вывод долларов[1280]. После возобновления в июле вывод шёл неделями и часто срывался[1281]. Забрать деньги было почти невозможно, а торговля продолжалась, и так шло до самого краха, ещё восемь месяцев.

К концу года картина изменилась. В декабре Bitstamp и китайская BTC China торговали сопоставимо с Mt. Gox, а 18 декабря Bitstamp проторговала даже больше неё[1282], и рост шёл уже через несколько площадок. Вершину цикла, 1163 доллара, Bitstamp отметила 30 ноября 2013 года[1283]. Через пять дней Народный банк Китая вместе с четырьмя другими ведомствами выпустил уведомление о рисках биткоина. Биткоин в нём назван «особым виртуальным товаром», который нельзя использовать как валюту, банкам и платёжным организациям запрещено

11.04.2013.

[1276] Заявление Mt. Gox в пересказе The Globe and Mail, 11.04.2013: «As expected in such situation people started to panic, started to sell Bitcoin in mass (Panic Sale) resulting in an increase of trade that ultimately froze the trade engine!» Задержка исполнения и 75 000 счетов — Buterin V. The Bitcoin Crash: An Examination. Bitcoin Magazine, 14.04.2013. Mt. Gox в начале апреля жаловалась и на DDoS-атаки, но 10–11 апреля объясняла сбой нагрузкой. Минимум 12.04.2013 — 54,25 доллара у Бутерина, 55,59 по Wikipedia (P. Waldie, «Bitcoin exchange halted after panic “froze the trade engine!”», The Globe and Mail, 11.04.2013, https://www.theglobeandmail.com/report-on-business/international-business/bitcoin-exchange-halted-after-panic-froze-the-trade-engine/article11097521/; V. Buterin, «The Bitcoin Crash: An Examination», Bitcoin Magazine, 14.04.2013, https://bitcoinmagazine.com/markets/the-bitcoin-crash-an-examination-1365911041; Buterin, Bitcoin Magazine, 14.04.2013 — задержка и 75 000 счетов; заявление Mt. Gox — The Globe and Mail, 11.04.2013; The Globe and Mail, 11.04.2013; Singularity Hub, «Bitcoin Exchange Mt. Gox Suspends Trading As Prices Crash», 11.04.2013, https://singularityhub.com/2013/04/11/bitcoin-exchange-mt-gox-suspends-trading-as-prices-crash/; минимум после возобновления — Buterin, 14.04.2013).

[1277] The Globe and Mail, 11.04.2013; Singularity Hub, «Bitcoin Exchange Mt. Gox Suspends Trading As Prices Crash», 11.04.2013, https://singularityhub.com/2013/04/11/bitcoin-exchange-mt-gox-suspends-trading-as-prices-crash/; минимум после возобновления — Buterin, 14.04.2013.

[1278] G. Hileman, «2013 Bitcoin Trading Volume: The Winners and Losers», CoinDesk, 24.12.2013, https://www.coindesk.com/markets/2013/12/24/2013-bitcoin-trading-volume-the-winners-and-losers.

[1279] Hileman G. 2013 Bitcoin Trading Volume: The Winners and Losers. CoinDesk, 24.12.2013, по данным bitcoincharts: 16.04.2013 «Mt. Gox alone equaled 572,186 BTC (90% of the total of the three exchanges)»; 18.12.2013 Bitstamp проторговала 137 070 BTC, Mt. Gox — 109 723, BTC China — 93 934. Выборка — три биржи, не весь рынок, и доля относится к одному дню. Часто повторяемую цифру «70% мировой торговли» в первоисточнике найти не удалось (G. Hileman, «2013 Bitcoin Trading Volume: The Winners and Losers», CoinDesk, 24.12.2013, https://www.coindesk.com/markets/2013/12/24/2013-bitcoin-trading-volume-the-winners-and-losers; Wikipedia, «Mt. Gox» (ссылается на Wired, 11.2013, и исследование 2014 года), https://en.wikipedia.org/wiki/Mt._Gox).

[1280] Wikipedia, «Mt. Gox» (со ссылкой на TechCrunch, 16.05.2013, и WSJ), https://en.wikipedia.org/wiki/Mt._Gox.

[1281] Wikipedia, «Mt. Gox» (со ссылкой на TechCrunch, 16.05.2013, и WSJ), https://en.wikipedia.org/wiki/Mt._Gox; Decker C., Wattenhofer R. «Bitcoin Transaction Malleability and MtGox». arXiv:1403.6676, 26.03.2014, https://arxiv.org/abs/1403.6676.

[1282] G. Hileman, «2013 Bitcoin Trading Volume: The Winners and Losers», CoinDesk, 24.12.2013, https://www.coindesk.com/markets/2013/12/24/2013-bitcoin-trading-volume-the-winners-and-losers.

[1283] Bitstamp API, дневные свечи BTC/USD: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=12&start=1385337600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=15&start=1420416000.

с ним работать, а частным лицам разрешено торговать им на свой риск[1284].[1285] Регулятор отрезал мост между биткоином и юанем, а сам биткоин не тронул.

Mt. Gox продержалась ещё два месяца. 7 февраля 2014 года она остановила вывод биткоинов, а 10 февраля объяснила это ошибкой в протоколе самого биткоина, которую называли «податливостью транзакций»[1286].

Подпись в переводе биткоина можно было записать чуть иначе, не делая её недействительной. Суммы и получатели оставались прежними, но у перевода менялся отпечаток, по которому его ищут. Посторонний мог перехватить отправленный перевод и, пока тот не записан в страницу, разослать по сети изменённую копию, и отправитель, который следил только за старым отпечатком, мог решить, что перевод не прошёл, и выслать деньги ещё раз[1287].

Двое исследователей из Швейцарской высшей технической школы Цюриха проверили данные сети за год до краха. Проблема, по их выводу, реальна, но массовых атак через неё до закрытия Mt. Gox не было[1288].[1289] Биржа списала свою дыру на тетрадку, а тетрадка, которую может проверить каждый, этого не подтвердила.

24 февраля сайт Mt. Gox перестал работать, и в тот же день в сети появился внутренний документ, по которому бирже не хватало 744 408 BTC; подлинность документа биржа тогда не подтверждала[1290]. 28 февраля Mt. Gox подала в Токио заявление о защите от банкротства и сообщила о потере 850 000 BTC, из них 750 000 клиентских, около 477 млн долларов по тогдашнему курсу. Карпелес на пресс-конференции поклонился, извинился и сказал по-японски, что биткоины потеряны «из-за слабостей в системе»[1291].[1292] Через месяц биржа сообщила, что нашла в кошельке старого формата почти 200 000 BTC, и пропавшими стали считать около 650 000[1293].

Биржа не знала, сколько у неё монет, а общая тетрадка знала это всё время. Каждая монета Mt. Gox была записана в ней за каким-то ключом, и найденные 200 000 никуда не

[1284] официальный текст — сайт НБК: http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/2804576/index.html (найден поиском, не открылся — обрыв соединения); содержание — Dorsey & Whitney LLP, «Bitcoin — Could Beijing Make or Break It? — Part Three», декабрь 2013, https://www.dorsey.com/newsresources/publications/2013/12/bitcoin–could-beijing-make-or-break-it–part-th__.

[1285] Уведомление ###2013#289# от 05.12.2013: Народный банк Китая, Министерство промышленности и информатизации и регуляторы банков, ценных бумаг и страхования. Биткоин — «#######», «##################»; частным лицам — «##################» (текст сверен по перепечаткам) (официальный текст — сайт НБК: http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/2804576/index.html (найден поиском, не открылся — обрыв соединения); содержание — Dorsey & Whitney LLP, «Bitcoin — Could Beijing Make or Break It? — Part Three», декабрь 2013, https://www.dorsey.com/newsresources/publications/2013/12/bitcoin–could-beijing-make-or-break-it–part-th__).

[1286] Wikipedia, «Mt. Gox» (ссылки на Bloomberg, Reuters, Wired), https://en.wikipedia.org/wiki/Mt._Gox.

[1287] Decker C., Wattenhofer R. «Bitcoin Transaction Malleability and MtGox». arXiv:1403.6676, 26.03.2014, https://arxiv.org/abs/1403.6676.

[1288] Decker C., Wattenhofer R. «Bitcoin Transaction Malleability and MtGox». arXiv:1403.6676, 26.03.2014, https://arxiv.org/abs/1403.6676.

[1289] Decker C., Wattenhofer R. Bitcoin Transaction Malleability and MtGox. arXiv:1403.6676, 26.03.2014: «The encoded signature is valid in both cases but the hash identifying the transaction is different» (разд. 2); «…while the problem is real, there was no widespread use of malleability attacks before the closure of MtGox.» Программа узла Bitcoin Core атаке не подвержена, потому что считает баланс по самой тетрадке, а не по отпечаткам своих отправленных переводов (разд. 2.2) (Decker C., Wattenhofer R. «Bitcoin Transaction Malleability and MtGox». arXiv:1403.6676, 26.03.2014, https://arxiv.org/abs/1403.6676).

[1290] Wikipedia, «Mt. Gox», https://en.wikipedia.org/wiki/Mt._Gox.

[1291] TechCrunch, «Mt.Gox Files For Bankruptcy Protection, Says 850,000 Bitcoin Lost», 28.02.2014, https://techcrunch.com/2014/02/28/mt-gox-files-for-bankruptcy/.

[1292] TechCrunch, 28.02.2014: «…apologized with a bow, saying in Japanese that the Bitcoin was lost „due to weaknesses in the system.“» Долги биржи — около 63,6 млн долларов. Находка марта 2014 года — 199 999,99 BTC (TechCrunch, «Mt.Gox Files For Bankruptcy Protection, Says 850,000 Bitcoin Lost», 28.02.2014, https://techcrunch.com/2014/02/28/mt-gox-files-for-bankruptcy/; CoinDesk, 21.03.2014, https://www.coindesk.com/markets/2014/03/21/mt-gox-confirms-discovery-of-200000-btc-in-old-format-wallet; Wikipedia, «Mt. Gox» (дата 20 марта), https://en.wikipedia.org/wiki/Mt._Gox).

[1293] CoinDesk, 21.03.2014, https://www.coindesk.com/markets/2014/03/21/mt-gox-confirms-discovery-of-200000-btc-in-old-format-wallet; Wikipedia, «Mt. Gox» (дата 20 марта), https://en.wikipedia.org/wiki/Mt._Gox.

пропадали. Потерялась запись в собственной тетрадке биржи, где она вела балансы клиентов, и сверить эти две тетрадки было некому.

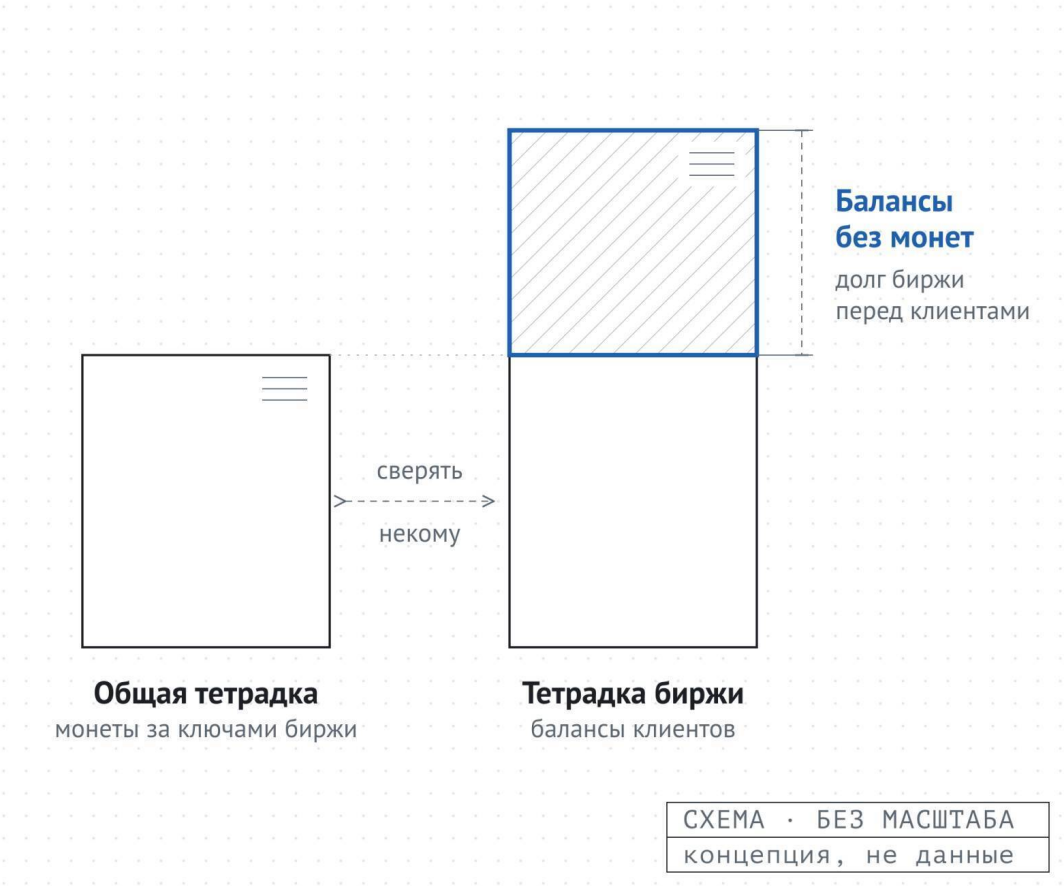


Рисунок 8.1. Две тетрадки Mt. Gox

Вопросы, которые я в первой главе советовал задавать любым деньгам, на тетрадке биржи дают другие ответы, чем на тетрадке биткоина. Кто ведёт запись? Одна компания, и копии у клиентов нет. Кто может дописать строчку? Тот, у кого есть доступ к базе, а в 2011 году, как мы видели, им оказался посторонний со служебной учётной записью. Кто может заморозить чужой баланс? Биржа, и в июне 2013 года она приостановила вывод долларов[1294]. Общая тетрадка отвечала на эти вопросы так же, как в 2009 году, но клиенты Mt. Gox жили не в ней.

В седьмой главе держатель частной банкноты XIX века зависел от того, что лежит в сундуке выпустившего её банка и кто это проверяет[1295]. Баланс на Mt. Gox был такой же банкнотой, помеченной именем биржи, и у него тоже была котировка. Вершину цикла цена на Mt. Gox показала выше, чем на Bitstamp[1296], а доллары с этой биржи с лета 2013 года почти невозможно

[1294] Bitcoin Wiki, «History», https://en.bitcoin.it/wiki/History; Wikipedia, «Mt. Gox» (со ссылкой на Ars Technica, 15–19.06.2011), https://en.wikipedia.org/wiki/Mt._Gox; Wikipedia, «Mt. Gox» (со ссылкой на TechCrunch, 16.05.2013, и WSJ), https://en.wikipedia.org/wiki/Mt._Gox.

[1295] A. J. Rolnick, W. E. Weber, «New Evidence on the Free Banking Era», American Economic Review 73(5), 1983, pp. 1080–1091, https://www.jstor.org/stable/1814673.

[1296] Bitstamp API, дневные свечи BTC/USD: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=12&start=1385337600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=15&start=1420416000.

было вывести[1297]. По-моему, одно следует из другого: доллар, который нельзя забрать, стоит меньше доллара на руках, и за монету на такой бирже его приходится отдавать больше. Эта разница и была котировкой банкноты с именем Mt. Gox, вроде тех, что печатали справочники XIX века, и рынок назначил её сам, задолго до краха.

Что происходило внутри, восстановили позже. WizSec в апреле 2015 года пришла к выводу, что биржа была неплатёжеспособна как минимум с 2012 года и к середине 2013 года практически лишилась биткоинов[1298].[1299] Монеты уходили на чужие адреса без записей о выводе в журнале биржи. Торговый бот Willy, который, по версии расследования, покупал биткоины за доллары, которых у биржи не было, появился в 2013 году, когда большая часть монет уже пропала, и нехватку биткоинов он превращал в нехватку долларов[1300].

Кто вывел монеты, суд до сих пор не установил. В 2023 году Министерство юстиции США обвинило двух граждан России в том, что они с сообщниками с сентября 2011 по май 2014 года похитили из Mt. Gox не меньше 647 000 BTC[1301]. Это обвинение, приговора по нему нет. Самого Карпелеса Токийский окружной суд в 2019 году признал виновным в фальсификации данных (он завышал балансы) и приговорил к 30 месяцам заключения условно, а по обвинению в растрате оправдал[1302]. Версии о краже снаружи и о сокрытии внутри друг другу не противоречат. Опровергнутой данными оказалась только версия самой биржи об ошибке протокола.

Рост 2013 года, выходит, шёл через биржу, которая уже была пуста, и балансы на её экране были строчками в долг без покрытия. Само по себе это решало только, кто заплатит на расчистке. Но если версия WizSec о боте верна, биржа ещё и покупала биткоины за доллары, которых не было, а такой спрос из ниоткуда действует на цену так же, как кредит, только кредиторов о нём никто не спросил. Это второй случай третьего этапа, чужие деньги, пущенные в оборот. Размер такого спроса никто не измерил, и вывод этот мой.

Остаётся вопрос, как биржа с дырой в кассе почти три года продолжала работать. Ответ даёт простая арифметика (пример условный, числа круглые). Допустим, клиенты числят на бирже 100 монет, а у неё есть 60. На подъёме каждый день приходят новички и приносят 7 монет, а уходят старые клиенты с 5. Приток больше оттока, запас даже растёт, и дыру в 40 монет никто не видит, потому что каждый, кто просит свои монеты, их получает.

Теперь цикл разворачивается. Новички приносят 2 монеты в день, а уходящие забирают 8, и запас тает на 6 монет в день. Через десять дней от 60 монет не остаётся ничего, и биржа закрывает вывод. Дыра за всё это время не выросла ни на монету, изменилось только направление потока.

Подъём прячет дыру посредника, а разворот цикла её обнаруживает.

На Mt. Gox это правило видно лучше всего. Вывод биткоинов она остановила через два с небольшим месяца после вершины[1303], и в модели это начало пятого этапа, только принудительно продавать тут было уже нечего.

[1297] Wikipedia, «Mt. Gox» (со ссылкой на TechCrunch, 16.05.2013, и WSJ), https://en.wikipedia.org/wiki/Mt._Gox.

[1298] WizSec, «The missing MtGox bitcoins», 19.04.2015, https://blog.wizsec.jp/2015/04/the-missing-mtgox-bitcoins.html.

[1299] WizSec (Kim Nilsson). The missing MtGox bitcoins, 19.04.2015: «MtGox was technically insolvent since at least 2012»; «by mid-2013… there are practically no (spendable) bitcoins left at all in MtGox». Прямо отслежено около 300 000 BTC, при широких критериях — до 800 000 (WizSec, «The missing MtGox bitcoins», 19.04.2015, https://blog.wizsec.jp/2015/04/the-missing-mtgox-bitcoins.html). Обвинение Министерства юстиции США от 09.06.2023: «…allegedly caused the theft of at least approximately 647,000 bitcoins from Mt. Gox»; вина судом не установлена (IRS Criminal Investigation / DOJ, «Russian nationals charged with hacking one cryptocurrency exchange and illicitly operating another», 09.06.2023, https://www.irs.gov/node/123336; https://justice.gov/usao-ndca/pr/russian-nationals-charged-hacking-one-cryptocurrency-exchange-and-illicitly-operating).

[1300] WizSec, «The missing MtGox bitcoins», 19.04.2015, https://blog.wizsec.jp/2015/04/the-missing-mtgox-bitcoins.html.

[1301] IRS Criminal Investigation / DOJ, «Russian nationals charged with hacking one cryptocurrency exchange and illicitly operating another», 09.06.2023, https://www.irs.gov/node/123336; https://justice.gov/usao-ndca/pr/russian-nationals-charged-hacking-one-cryptocurrency-exchange-and-illicitly-operating.

[1302] Wikipedia, «Mt. Gox» (ссылки на Financial Times, Bloomberg, CNN), https://en.wikipedia.org/wiki/Mt._Gox.

[1303] Bitstamp API, дневные свечи BTC/USD: https://www.bitstamp.net/api/v2/ohlc/btcusd/?

Расчистка заняла больше года. Дно цикла пришлось на 14 января 2015 года — 152,40 доллара на Bitstamp, на 87% ниже вершины и через 410 дней после неё[1304]. Крах главного посредника рынок пережил, и объяснение, вероятно, в данных о торговле конца 2013 года. К тому времени Mt. Gox уже делила рынок с Bitstamp и китайскими биржами[1305], и когда она закрылась, торговать было где. К январю 2015 года, по данным CoinDesk, около 65% сделок с биткоином приходилось на юань[1306], так что запрет для китайских банков торговлю частных лиц не остановил.

Почему выплаты Mt. Gox идут до сих пор

Банкротство Mt. Gox началось в 2014 году, а последний срок выплат по нему назначен на 31 октября 2026 года[1307]. Первые семь лет ушли на выбор процедуры и разбор претензий. Биржа просила о гражданской реабилитации, потом дело перевели в банкротство, потом снова в реабилитацию, и план кредиторы одобрили только в октябре 2021 года[1308]. Часть монет управляющий продал ещё на стадии банкротства, в 2017–2018 годах, а оставшиеся, по его словам, до начала выплат не продавал[1309]. Раздавать биткоины он начал в июле 2024 года через криптобиржи в разных странах, и к концу марта 2025 года выплаты получили больше 19 500 кредиторов[1310].

В октябре 2025 года управляющий сообщил, что многие кредиторы денег так и не получили: одни не прошли нужных процедур, у других возникли сложности при самой выплате. С разрешения суда он перенёс срок на год, и перенос был уже третьим[1311].[1312] Когда я пишу эти строки, срок ещё не наступил, и что с ним стало, смотрите в приложении Б.

---

step=86400&limit=12&start=1385337600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=15&start=1420416000; Wikipedia, «Mt. Gox» (ссылки на Bloomberg, Reuters, Wired), https://en.wikipedia.org/wiki/Mt._Gox.

[1304] Bitstamp API, дневные свечи BTC/USD: https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=12&start=1385337600; https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=15&start=1420416000.

[1305] G. Hileman, «2013 Bitcoin Trading Volume: The Winners and Losers», CoinDesk, 24.12.2013, https://www.coindesk.com/markets/2013/12/24/2013-bitcoin-trading-volume-the-winners-and-losers.

[1306] CoinDesk, «Bitcoin Price Continues to Fall, Breaking Through $200 Barrier», 14.01.2015, https://www.coindesk.com/markets/2015/01/14/bitcoin-price-continues-to-fall-breaking-through-200-barrier; пик ~$1 150 — Wikipedia, «History of bitcoin», https://en.wikipedia.org/wiki/History_of_bitcoin.

[1307] MtGox Co., Ltd., «Notice Concerning Change of Repayments Deadline», 27.10.2025, https://www.mtgox.com/img/pdf/20251027_1cc36334-e8b2-4fe4-8135-97d9a149e4f7_announcement_en.pdf.

[1308] TechCrunch, «Mt.Gox Files For Bankruptcy Protection, Says 850,000 Bitcoin Lost», 28.02.2014, https://techcrunch.com/2014/02/28/mt-gox-files-for-bankruptcy/; CoinDesk, 21.03.2014, https://www.coindesk.com/markets/2014/03/21/mt-gox-confirms-discovery-of-200000-btc-in-old-format-wallet; Wikipedia, «Mt. Gox» (дата 20 марта), https://en.wikipedia.org/wiki/Mt._Gox; Wikipedia, «Mt. Gox», https://en.wikipedia.org/wiki/Mt._Gox.

[1309] MtGox Co., Ltd., Rehabilitation Trustee Nobuaki Kobayashi, «Notice regarding Repayment in Bitcoin and Bitcoin Cash through Designated Cryptocurrency Exchange, etc. (6)», 27.03.2025, https://www.mtgox.com/img/pdf/20250327_50441ef4-dc28-473a-9fd2-495db2da4bbd_announcement_en.pdf.

[1310] MtGox Co., Ltd., Rehabilitation Trustee Nobuaki Kobayashi, «Notice regarding Commencement of Repayments in Bitcoin and Bitcoin Cash», 24.06.2024, https://www.mtgox.com/img/pdf/20240624_announcement_en.pdf; MtGox Co., Ltd., Rehabilitation Trustee Nobuaki Kobayashi, «Notice regarding Repayment in Bitcoin and Bitcoin Cash through Designated Cryptocurrency Exchange, etc. (6)», 27.03.2025, https://www.mtgox.com/img/pdf/20250327_50441ef4-dc28-473a-9fd2-495db2da4bbd_announcement_en.pdf.

[1311] MtGox Co., Ltd., «Notice Concerning Change of Repayments Deadline», 27.10.2025, https://www.mtgox.com/img/pdf/20251027_1cc36334-e8b2-4fe4-8135-97d9a149e4f7_announcement_en.pdf.

[1312] MtGox Co., Ltd., Rehabilitation Trustee Nobuaki Kobayashi. Notice Concerning Change of Repayments Deadline, 27.10.2025: «However, many rehabilitation creditors still have not received their Repayments because they have not completed the necessary procedures for receiving Repayments. Additionally, a considerable number of rehabilitation creditors have not received their Repayments due to various reasons, such as issues arising during the Repayments process.» Цепочка сроков: 31.10.2023 → 31.10.2024 → 31.10.2025 → 31.10.2026. Выплаты идут в биткоинах и Bitcoin Cash, часть кредиторов получает деньги от продажи монет. О продажах 2017–2018 годов в марте 2018 года сообщал сам управляющий (по Wikipedia). По дан-

Клиент Mt. Gox за двенадцать лет так и не вышел из роли кредитора. Пока монеты лежали на бирже, у него была строчка в её тетрадке, то есть требование к должнику. Когда должник рухнул, требование превратилось в место в очереди кредиторов, и очередь шла через японский суд, управляющего и биржи в разных странах. Даже вернуть монеты клиентам управляющий смог только через других посредников.

Отсюда проверка, которую можно сделать на любом посреднике, которому вы доверяете деньги сегодня. Чьи ключи держат ваши монеты в общей тетрадке, и может ли кто-нибудь со стороны сверить эту запись с балансом, который показывает вам посредник? Выпускает ли он свои строчки, будь то токены, «цифровые доллары» или баланс с процентом, и чем они покрыты? В какой стране и по какой процедуре вы окажетесь в очереди кредиторов, если он рухнет? Ни один из этих вопросов не говорит, что посредник плох. Они говорят, какой вид доверия вы ему выдали, а монеты под собственным ключом в такой очереди не стоят вовсе (как их хранить и чем опасно хранение у себя, разберём в главе о безопасности).

ным аналитической компании Arkham, в ноябре 2025 года на кошельках Mt. Gox оставалось около 34 700 BTC; управляющий эту привязку кошельков не подтверждал (D. Park, «Mt. Gox moves $956 million worth of bitcoin to unmarked wallet address: Arkham», The Block, 18.11.2025, https://www.theblock.co/post/379197/mt-gox-956-million-bitcoin). В 2017 году Япония поправками к закону о платёжных услугах ввела специальные правила для криптобирж (об ответе государств на такие крахи — в главе 11) (Wikipedia, «Mt. Gox», https://en.wikipedia.org/wiki/Mt._Gox). На 27.09.2026 новых уведомлений на сайте управляющего нет; свежие данные — в приложении Б (Wikipedia, «Mt. Gox», https://en.wikipedia.org/wiki/Mt._Gox; MtGox Co., Ltd., Rehabilitation Trustee Nobuaki Kobayashi, «Notice regarding Commencement of Repayments in Bitcoin and Bitcoin Cash», 24.06.2024, https://www.mtgox.com/img/pdf/20240624_announcement_en.pdf; MtGox Co., Ltd., «Notice Concerning Change of Repayments Deadline», 27.10.2025, https://www.mtgox.com/img/pdf/20251027_1cc36334-e8b2-4fe4-8135-97d9a149e4f7_announcement_en.pdf; MtGox Co., Ltd., Rehabilitation Trustee Nobuaki Kobayashi, «Notice regarding Repayment in Bitcoin and Bitcoin Cash through Designated Cryptocurrency Exchange, etc. (6)», 27.03.2025, https://www.mtgox.com/img/pdf/20250327_50441ef4-dc28-473a-9fd2-495db2da4bbd_announcement_en.pdf).

Конец ознакомительного фрагмента.