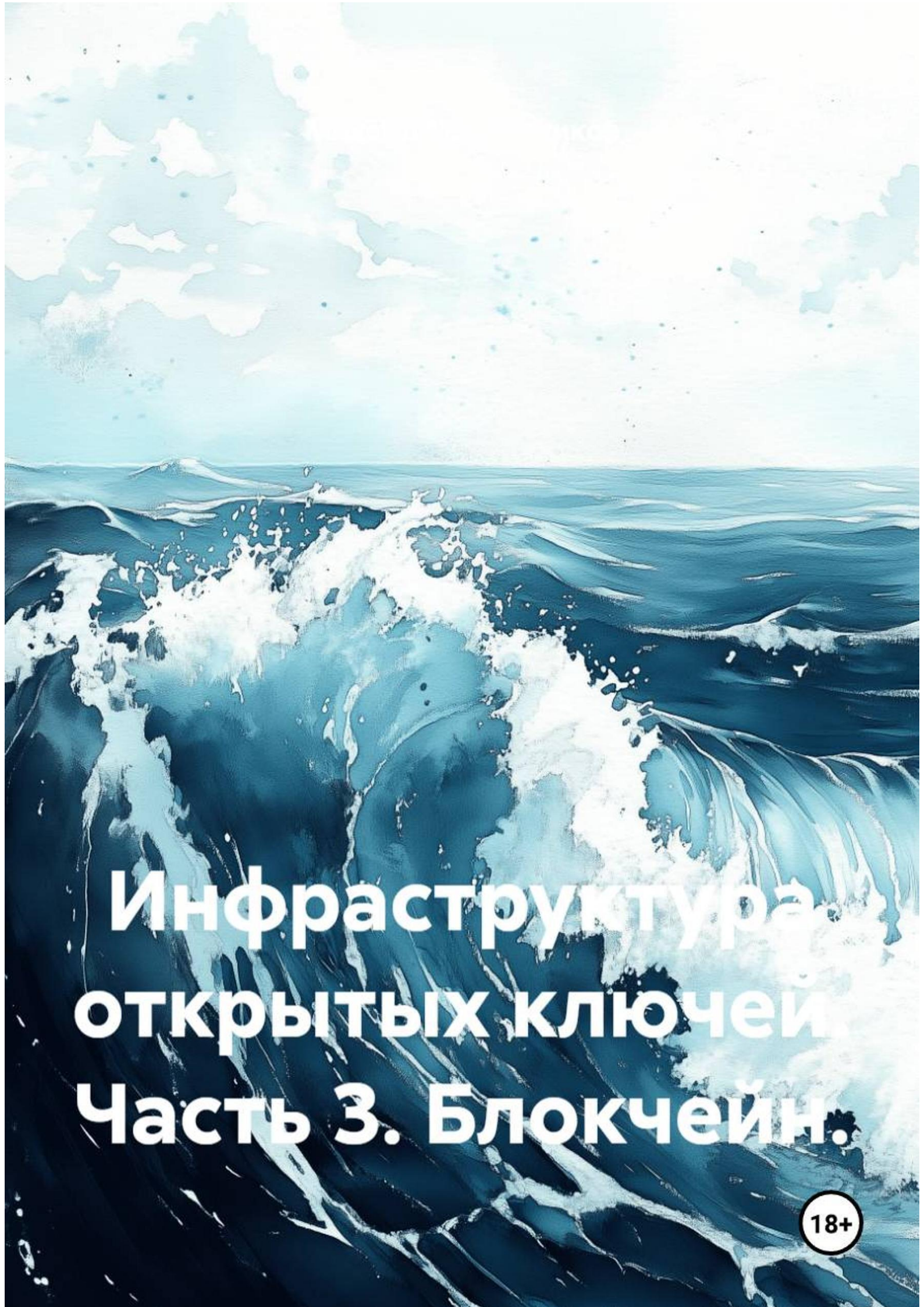




Инфраструктура открытых ключей. Часть 3. Блокчейн.

18+

Михаил Масленников

**Инфраструктура открытых
ключей. Часть 3. Блокчейн.**

«Автор»

2026

Масленников М. Е.

Инфраструктура открытых ключей. Часть 3. Блокчейн. /
М. Е. Масленников — «Автор», 2026

Децентрализованная инфраструктура открытых ключей (dPKI — Decentralized Public Key Infrastructure) — это система управления цифровыми именами, ключами шифрования и сертификатами безопасности, в которой полностью отсутствуют центральные органы управления (такие как удостоверяющие центры, корпорации или государственные реестры). В классической инфраструктуре (PKI) мы вынуждены доверять третьей стороне (например, компаниям вроде Let's Encrypt или VeriSign), которая подтверждает, что данный открытый ключ действительно принадлежит конкретному сайту или человеку. В dPKI эта обязанность переложена на децентрализованный реестр (блокчейн) и математические алгоритмы консенсуса.

© Масленников М. Е., 2026

© Автор, 2026

Содержание

dPKI	5
dPKI vs PKI	7
Proof-of-Work (PoW).	10
Proof-of-Stake (PoS).	13
Конец ознакомительного фрагмента.	16

Михаил Масленников

Инфраструктура открытых ключей. Часть 3. Блокчейн.

dPKI

Наконец-то дошли до современности – децентрализованных PKI. Признаюсь честно: во времена моего обучения (середина 70-х годов прошлого века) на Техническом факультете Высшей Краснознаменной школы КГБ СССР, в том единственном в СССР учебном заведении, где готовили криптографов, ни о каких децентрализованных PKI (да и централизованных тоже) никто практически ничего не знал. Так что при написании этой части книги мы с читателем находимся почти в равных стартовых условиях. Сиречь зовем на помощь наш великий и могучий ИИ!

Вопрос к ИИ: «Что такое децентрализованная PKI?»

ИИ:

Децентрализованная инфраструктура открытых ключей (dPKI — Decentralized Public Key Infrastructure) — это система управления цифровыми именами, ключами шифрования и сертификатами безопасности, в которой полностью отсутствуют центральные органы управления (такие как удостоверяющие центры, корпорации или государственные реестры).

В классической инфраструктуре (PKI) мы вынуждены доверять третьей стороне (например, компаниям вроде *Let's Encrypt* или *VeriSign*), которая подтверждает, что данный открытый ключ действительно принадлежит конкретному сайту или человеку. В dPKI эта обязанность переложена на **децентрализованный реестр (блокчейн)** и математические алгоритмы консенсуса.

Архитектурные принципы dPKI

Инфраструктура dPKI строится на трех фундаментальных технологиях:

Блокчейн как единый источник истины: Вместо баз данных удостоверяющих центров (CA) все связи между пользователями и их открытыми ключами записываются в распределенный реестр. Изменить или подделать эти записи задним числом невозможно.

Криптография с открытым ключом: Пользователь сам локально генерирует свои пары ключей (открытый/закрытый) с помощью математических алгоритмов (например, ECDSA или Ed25519).

Децентрализованные идентификаторы (DID): В dPKI вместо привычных паспортов или доменных имен используются DID — уникальные цифровые адреса, которыми полностью владеет сам пользователь, и которые жестко связаны с его открытым ключом на уровне блокчейна.

Главные отличия от классической PKI

Защита от «точки отказа» (Устойчивость к компрометации): В обычной PKI, если хакеры взломают один крупный Удостоверяющий центр, они смогут выпускать фальшивые

сертификаты для любых сайтов и перехватывать данные пользователей. В dPKI взламывать некого — доверие распределено между тысячами независимых компьютеров (нод) сети.

Абсолютный контроль (Self-Sovereign Identity): Никто не может аннулировать, отозвать или заблокировать ваш цифровой идентификатор или ключ по политическим, экономическим или личным причинам. Вы — единственный хозяин своих ключей.

Автоматизация и скорость: Привязка ключа к идентификатору происходит мгновенно в виде транзакции в блокчейне. Больше не нужно проходить бюрократические проверки, отправлять документы администраторам или платить ежегодные взносы за поддержание сертификата.

Как dPKI решает проблему отзыва ключей?

В традиционных системах для отзыва скомпрометированного ключа используются громоздкие списки отзыва (CRL) или онлайн-протоколы (OCSP), которые часто работают с задержками.

В dPKI отзыв или замена ключа происходит путем **публикации новой транзакции в блокчейне**. Владелец идентификатора с помощью своего старого (или резервного) ключа подписывает транзакцию, которая объявляет старый ключ недействительным и привязывает к профилю новый открытый ключ. Вся сеть мгновенно узнает об изменениях.

Где сегодня применяется dPKI?

Децентрализованные системы доменных имен (DNS): Проекты вроде ENS (Ethereum Name Service) или Handshake. Они заменяют классическую систему доменов, делая невозможным захват или блокировку вашего сайта цензорами.

Web3 и криптокошельки: Вход на сайты и сервисы без паролей с помощью криптографической подписи (авторизация через MetaMask, WalletConnect).

Защищенные мессенджеры: Системы связи нового поколения, где пользователи обмениваются ключами напрямую через распределенную сеть, исключая риск прослушки на центральном сервере.

Аж дух захватывает! Нет привычных УЦ с их генералами, которые могут отозвать ваш сертификат открытого ключа! Не нужны IT-гиганты с их корневыми УЦ, сертификатам которых все должны верить по определению! Нет громоздкой технологии отзыва, использующей всякие CRL и OCSP!

Так почему же тогда молодые dPKI до сих пор не истребили под корень старообрядные централизованные PKI с их CRL, OCSP, списками SCT и прочими заморочками, о которых шла речь в предыдущих частях этой книги?

dPKI vs PKI

А скажи-ка мне, голова с микросхемами и проводами, «Насколько широкое распространение получили dPKI?»

ИИ:

По состоянию на 2026 год децентрализованная PKI (dPKI) пока не получила повсеместного глобального распространения, но находится в стадии **активного перехода от концепции к реальному производственному использованию**.

В то время как классическая PKI (с традиционными удостоверяющими центрами и SSL/TLS-сертификатами) по-прежнему удерживает доминирующие позиции в глобальном интернете, dPKI сформировала мощные ниши и проникает в стандарты веб-безопасности.

Степень внедрения технологии можно разделить по направлениям:

1. Сектор Web3 и криптовалюты (Максимальное распространение)

В этой сфере dPKI фактически стала стандартом дефолта.

Криптографические кошельки и подписи: Сотни миллионов пользователей ежедневно используют dPKI (через интеграции Web3) для подписи транзакций и авторизации на сайтах без паролей, используя свои пары ключей вместо аккаунтов Google или Apple.

Децентрализованные домены: Такие сервисы, как ENS (Ethereum Name Service), управляют миллионами доменных имен, где связка «имя — публичный ключ» полностью защищена блокчейном от цензуры и захвата.

2. Корпоративный сектор и IoT (Начало массового внедрения)

Безопасность Интернета вещей (IoT): Обычная PKI плохо справляется с миллиардами умных устройств из-за перегрузки центральных серверов. dPKI внедряется в промышленные сети и системы умных домов, позволяя устройствам автономно проверять подлинность друг друга без «звонков» на центральный сервер.

Постквантовая криптография (PQC): В 2026 году индустрия сталкивается с переходом на квантово-устойчивые стандарты. Крупные игроки (включая инициативы от Google и Cloudflare) рассматривают **блокчейн-модели для хранения тяжелых квантово-безопасных сертификатов**, что подталкивает классическую PKI к гибридной децентрализации.

3. Государственные и международные стандарты (Стадия стандартизации)

Стандарты W3C DID: Консорциум Всемирной паутины (W3C) официально утвердил стандарт Децентрализованных идентификаторов (DID). Это заложило юридическую и техническую основу для интеграции dPKI в классический веб-браузинг.

Цифровые паспорта и ID: Ряд стран (в рамках концепций Self-Sovereign Identity / SSI) тестируют цифровые документы граждан на базе dPKI, где государство лишь подтверждает факт выдачи паспорта, но сам криптографический ключ и контроль над данными остаются у гражданина.

Что сдерживает повсеместное вытеснение классической PKI?

Проблема утери ключей: В dPKI нет техподдержки. Если пользователь теряет или компрометирует свой закрытый ключ, он безвозвратно теряет доступ к своей цифровой личности. Корпорации боятся такой ответственности.

Масштабируемость и скорость: Запись данных в блокчейн и их синхронизация по всему миру занимают больше времени и требуют больше вычислительных ресурсов, чем обращение к традиционной централизованной базе данных.

Сопrotивление инфраструктуры: Индустрия Web2 инвестировала триллионы долларов в централизованную архитектуру (удостоверяющие центры, аппаратные модули HSM). Полный переход на dPKI требует глобальной модернизации сетевого оборудования.

Итог: dPKI сейчас переживает фазу взросления технологии. Она не заменит традиционный HTTPS завтра, но уверенно становится базовым фундаментом для систем с повышенными требованиями к цензуроустойчивости, безопасности IoT и автономности пользователей.

ИИ, тебе бы в парламенте выступать! Там точно такая же «словесно-облачная» технология.

Но давайте все же попробуем из этого «словесного облака» от ИИ кое-что выделить.

«Дорого, сложно, деньги» - вот, на мой взгляд, три слова, которые дают ответ на вопрос: «Почему мы до сих пор не живем в мире dPKI?»

Цитируем ИИ: «**Запись данных в блокчейн и их синхронизация по всему миру занимают больше времени и требуют больше вычислительных ресурсов, чем обращение к традиционной централизованной базе данных**»

Интуитивно ясно, что традиционные затраты централизованных PKI на операции типа рассылки CRL или обслуживание протокола OCSP по потребляемым вычислительным, и не только вычислительным, но и обычным энергоресурсам – это детский лепет по сравнению с синхронизацией блокчейнов по всему миру. Давайте спросим ИИ.

Вопрос к ИИ: «Какое количество электроэнергии необходимо для синхронизации блокчейна по всему миру?»

ИИ:

Ответ на этот вопрос зависит от того, **какой именно блокчейн** имеется в виду, так как разные сети используют принципиально разные механизмы защиты.

Сам процесс передачи данных и их синхронизации (копирования на компьютеры) между участниками потребляет ничтожно мало — как обычный обмен файлами в интернете. Однако **защита блокчейна от подделки** может требовать колоссальных ресурсов.

Всю мировую индустрию блокчейна можно разделить на две категории:

1. Блокчейны на алгоритме Proof-of-Work (Биткоин и аналоги)

Здесь синхронизация неразрывно связана с **майнингом** (вычислениями для защиты сети). Чтобы добавить новый блок и синхронизировать его по всему миру, тысячи суперкомпьютеров должны непрерывно сжигать электричество.

Общее потребление: По оценкам Кембриджского центра альтернативных финансов (CBEI) и аналитических агентств, сеть Биткоина потребляет около **135–150 тераватт-часов (ТВт·ч) электроэнергии в год**.

С чем это можно сравнить: Это больше, чем годовое потребление всей **Аргентины, Финляндии или Нидерландов**. В масштабах планеты Биткоин забирает около **0,5–0,6%** всего вырабатываемого на Земле электричества.

В пересчете на одну транзакцию: Математически на подтверждение и синхронизацию всего лишь одного перевода в сети Биткоина тратится от **200 до 850 кВт·ч**. Этого электричества хватит, чтобы обычный частный дом бесперебойно работал от нескольких недель до месяца.

2. Блокчейны на алгоритме Proof-of-Stake (Ethereum, Solana, Cardano, TON)

В этих сетях майнинг отсутствует. Безопасность и синхронизация обеспечиваются не мощностью процессоров, а балансом монет на счетах специальных узлов (валидаторов). Для их работы нужны обычные сервера, а не огромные майнинг-фермы.

Ethereum (Эфириум): После глобального обновления (The Merge) сеть снизила свое энергопотребление на **99,95%**. Сейчас весь мировой блокчейн Ethereum потребляет всего около

0,003–0,005 ТВт·ч в год. Это сопоставимо с потреблением энергии несколькими крупными дата-центрами или одного небольшого городка.

Другие современные сети (Solana, TON): Их показатели еще ниже. На одну транзакцию в таких сетях уходит мизерное количество энергии (около **0,0005 кВт·ч**), что даже экономичнее, чем один поиск в Google или стандартный платеж через банковскую систему Visa.

Сводное сравнение затрат энергии

Сеть (Блокчейн)

Тип алгоритма

Потребление энергии в год

Примерный эквивалент

Bitcoin

Proof-of-Work

~138 000 000 000 кВт·ч

Целая европейская страна (Финляндия/Чехия)

Ethereum

Proof-of-Stake

~3 000 000 кВт·ч

Около 300–400 частных жилых домов

Visa (традиционная)

Централизованная

~150 000 000 кВт·ч

Один крупный офисный квартал

Итог: Глобальная синхронизация блокчейнов требует огромного количества энергии только в том случае, если это Биткоин. Современные технологические блокчейны работают на энергоэффективных алгоритмах и практически не создают нагрузки на мировую экологию.

Proof-of-Work (PoW).

А скажи-ка, язык СИ (супер интеллект, по-американски), «Что такое вычисления для защиты сети (майнинг), которые использует биткоин?»

ИИ:

Вычисления для защиты сети в Биткоине (майнинг) — это процесс, при котором тысячи мощных компьютеров по всему миру одновременно решают сложнейшую математическую задачу, чтобы **проверить новые переводы, объединить их в блок и защитить сеть от взлома.**

Майнинг работает по алгоритму **Proof-of-Work (Доказательство работы)**. Компьютеры не просто делают бесполезные расчеты: они соревнуются друг за другом, тратя электричество, чтобы доказать сети свою честность. Тот компьютер, который первым решит задачу, получает право записать новый блок в блокчейн и забирает за это награду — свеже-созданные биткоины.

В чем именно заключаются эти «вычисления»? (Простыми словами)

Представьте, что сеть Биткоина каждые 10 минут собирает все новые переводы со всего мира в одну цифровую коробку (блок). Чтобы закрыть эту коробку и навсегда прикрепить её к цепочке блокчейна, на неё нужно повесить кодовый замок.

Код от этого замка (в криптографии он называется **хэш**) должен соответствовать строжайшему правилу сети: например, начинаться с определенного количества нулей (скажем, 20 нулей подряд).

Тут я немного поспорю с уважаемым мною ИИ. Хеш — это не ключ и не код от замка. Замок подразумевает наличие секретного ключа, а никаких ключей при операции хеширования нет. Майнер не ставит свою ЭЦП под блоком, а просто вычисляет его хеш-функцию по специальному правилу, известному всем.

Продолжайте, пожалуйста, господин ИИ.

Компьютер майнера выполняет одну единственную задачу — **метод перебора (брут-форс)**. Он берет данные всех транзакций, добавляет к ним случайное число (оно называется **nonce**) и пропускает через математическую формулу SHA-256, проверяя результат.

Попытка 1: Код не подошел.

Попытка 2: Снова мимо.

Попытка 100 триллионов: **Код подошел!**

Как только код найден, майнер кричит на всю сеть: «Я нашел решение!». Другие компьютеры мгновенно (за доли секунды) проверяют его результат. Если всё честно, блок закрывается, синхронизируется по всему миру, а победитель получает награду.

Почему это защищает сеть Биткоина?

Майнинг выполняет три важнейшие защитные функции:

Защита от изменения истории (Необратимость):

Каждый новый блок математически намертво привязан к предыдущему через тот самый код (хэш). Если хакер захочет изменить старый перевод пятилетней давности, ему придется заново пересчитать математические задачи для этого блока и **всех последующих блоков**, которые были созданы после него. Для этого потребуется вычислительная мощ-

ность, превышающая мощность половины компьютеров всей планеты, что экономически и технически невозможно.

Опять немного поспорю с ИИ. Почему мощность только половины компьютеров всей планеты? Откуда появилась эта оценка? В Теоретическом отделе Спецуправления 8 ГУ КГБ СССР начальник этого отдела умнейший Вадим Евдокимович Степанов, если бы я написал такие слова в отчете по контрольному криптографическому анализу какой-нибудь шифраппаратуры, моментально выгнал бы меня переделывать такой отчет!

Хотя задача, безусловно, весьма канительная, но в принципе решаемая. И говорить о гарантированной криптографической стойкости такой защиты не приходится. В этой защите нет секретных ключей, вся надежность блокчейна держится на том, что предыдущие блоки расползлись к тому времени по всему миру и изменить их действительно очень сложно.

Защита от «двойного расходования» (Double-spending):

Вычисления гарантируют, что никто не сможет отправить одни и те же биткоины двум разным людям одновременно. Компьютеры-майнеры сверяют каждую транзакцию с историей блокчейна и одобряют только ту, которая была первой.

Защита от спама и ложных данных:

Поскольку вычисления требуют реальных затрат на покупку дорогого оборудования (ASIC-майнеров) и оплату огромных счетов за электричество, майнерам выгодно играть по правилам. Если майнер попытается добавить в блок фальшивую транзакцию (например, нарисует себе миллион монет), сеть мгновенно отвергнет его блок. В итоге обманщик просто сожжет дорогое электричество впустую и ничего не заработает.

Таким образом, Биткоин превратил законы математики и экономическую выгоду в непреодолимый щит, который никто не смог взломать с момента запуска сети.

Не смог взломать, или не пытался? Или смог взломать, но просто помалкивает об этом?

Что-то слышится родное для криптографа – брутфорс! Тотальная переборка! Тупо перебираем случайные числа (попсе), вычисляем хеш SHA-256 от громадной таблицы всех транзакций + попсе и проверяем, не начинается ли этот дурной хеш с нулей.

Бр... Тошнит от одной мысли про майнинг – куча бесполезной работы, бесполезная трата энергоресурсов и ресурсов вычислительной техники! Если нужно первые 20 нулей в хеше, хеш равновероятный, длина хеша SHA-256 равна 256 бит, вероятность того, что первые 20 бит будут нули, равна 2^{-20} . Это примерно 10^{-6} . Следовательно, нужно в среднем миллион раз выполнить абсолютно бесполезные вычисления хеша для того, чтобы получить требуемые первые 20 нулей.

Естественный вопрос к ИИ: «Где в России запрещен майнинг?»

ИИ:

По состоянию на 2026 год в России действует официальный запрет на майнинг цифровой валюты в ряде регионов. Ограничения были введены Правительством РФ (Постановление № 1869) из-за дефицита электроэнергии и делятся на две категории: круглогодичные и сезонные.

Запреты касаются как юридических, так и физических лиц (даже тех, кто зарегистрирован в реестре ФНС).

1. Регионы с полным (круглогодичным) запретом

В этих субъектах РФ майнинг полностью запрещен на период с 1 января 2025 года по 15 марта 2031 года:

Северный Кавказ: Дагестан, Чечня, Ингушетия, Кабардино-Балкария, Карачаево-Черкесия, Северная Осетия — Алания.

Новые регионы: Донецкая Народная Республика (ДНР), Луганская Народная Республика (ЛНР), Запорожская и Херсонская области.

2. Регионы с сезонным запретом (в период пиковых нагрузок)

В этих регионах майнить запрещено ежегодно в зимний период — с 15 ноября по 15 марта (ограничение действует вплоть до 2031 года):

Иркутская область (отдельные части энергосистемы).

Республика Бурятия.

Забайкальский край.

Важное ограничение для физических лиц по всей России

В тех регионах, где майнинг официально разрешен, для обычных граждан (физлиц без статуса ИП) действует жесткий лимит на потребление электричества — **не более 6 000 кВт·ч в месяц**. Если этот лимит превышен, гражданин обязан зарегистрироваться в качестве индивидуального предпринимателя и войти в специальный реестр ФНС, иначе его деятельность будет считаться незаконной.

Итак, майнинг — это олицетворение бесконечной и в основном бесполезной работы со случайными числами: а вдруг получатся требуемые нули в начале? К числу красивых криптографических решений такой метод вряд ли можно отнести, как, к примеру, алгоритмы DH или RSA.

Proof-of-Stake (PoS).

Варварский PoW – майнинг – рассмотрели. А теперь сравним его с алгоритмом защиты Proof-of-Stake (PoS). Друг ИИ! Сделай одолжение!

Вопрос к ИИ: «Что такое блокчейны на алгоритме Proof-of-Stake?»

ИИ:

Блокчейны на алгоритме Proof-of-Stake (PoS / «доказательство доли владения») — это распределенные сети, в которых безопасность и проверка транзакций обеспечиваются участниками, **блокирующими (стейкающими) свои монеты**, а не использующими вычислительную мощность компьютеров (как в Proof-of-Work (PoW)).

В PoS-сетях майнеров заменили **валидаторы**. Чем больше монет пользователь отправляет в стейкинг, тем выше его шанс быть выбранным сетью для создания следующего блока и получения за это награды.

Как работает Proof-of-Stake: Пошаговый процесс

Блокировка средств: Пользователь «замораживает» определенное количество нативной криптовалюты сети в специальном смарт-контракте. Это называется **стейкингом**.

Выбор валидатора: Алгоритм случайным образом (но с учетом размера доли) выбирает валидатора для создания нового блока.

Проверка (Валидация): Выбранный валидатор проверяет транзакции, формирует блок и отправляет его в сеть. Другие валидаторы подтверждают правильность блока.

Награда или штраф:

За честную работу валидатор получает **вознаграждение** (новые монеты или комиссии за транзакции).

За попытку обмана сети или долгий офлайн применяется **слешинг (slashing)** — штраф, при котором часть заблокированных монет безвозвратно сжигается.

Вопрос ИИ: «Как валидатор формирует блок?»

ИИ:

Процесс формирования блока валидатором напоминает работу строгого цифрового нотариуса. Валидатор собирает новые переводы, проверяет их по правилам математики и криптографии, а затем упаковывает в единый реестр.

Вот детальный пошаговый алгоритм, как именно валидатор создает новый блок в PoS-сети:

1. Сбор транзакций из Мемпула (Mempool)

Когда пользователи отправляют кому-то криптовалюту, их транзакции не попадают в блокчейн мгновенно. Сначала они отправляются в **мемпул** — это общая «комната ожидания» или буфер неподтвержденных транзакций.

Выбранный сетью валидатор подключается к мемпулу и выбирает оттуда транзакции для своего будущего блока.

Как правило, валидатор в первую очередь выбирает транзакции с **самой высокой комиссией**, чтобы максимизировать свой заработок.

2. Локальная проверка (Валидация) каждой транзакции

Прежде чем добавить транзакции в блок, валидатор обязан убедиться, что они легитимны. Для этого его программное обеспечение проверяет каждую операцию по жестким правилам:

Проверка баланса: Хватает ли у отправителя монет на счету для перевода и оплаты сетевой комиссии?

Криптографическая подпись: Действительно ли транзакция подписана приватным ключом владельца кошелька (что исключает кражу)?

Защита от двойного расходования: Не пытался ли отправитель перевести эти же самые монеты кому-то еще одновременно?

3. Упаковка в блок и построение дерева Меркла

Проверенные транзакции группируются. Чтобы блок был компактным и безопасным, транзакции внутри него связываются с помощью криптографической функции (хэширования) в специальную структуру — **Дерево Меркла**.

На выходе получается один короткий код — **корень Меркла (Merkle Root)**. Он представляет собой цифровой отпечаток абсолютно всех транзакций в этом блоке. Если в будущем изменить хотя бы один символ в любой транзакции, этот корень полностью изменится, и обман раскроется.

4. Создание заголовка блока (Block Header)

Валидатор формирует «паспорт» блока — его заголовок. Заголовок содержит метаданные, без которых блок не примет сеть:

Хэш предыдущего блока: Ссылка на самый последний блок в сети. Это то, что намертво связывает блоки в неразрывную цепочку (блок-чейн).

Корень Меркла: Тот самый отпечаток транзакций из шага 3.

Временная метка (Timestamp): Точное время создания блока.

Техническая информация: Версия протокола и адрес самого валидатора (чтобы сеть знала, кому выплатить награду).

5. Подписание и трансляция блока в сеть

Валидатор скрепляет сформированный заголовок и тело блока своей **цифровой подписью** (используя свой приватный ключ валидатора). Это доказывает сети, что именно он несет материальную ответственность за этот блок.

После этого валидатор отправляет (транслирует) готовый блок по P2P-сети всем остальным узлам (нодам) и валидаторам для финальной проверки (аттестации). Как только большинство других валидаторов подтверждают, что блок собран честно, он навсегда записывается в общую базу данных.

В централизованной PKI было ASN.1 дерево, а теперь появилось какое-то дерево Меркла.

Вопрос ИИ: «Что такое дерево Меркла?»

ИИ:

Дерево Меркла (Merkle Tree) — это структура данных в криптографии и блокчейне, которая позволяет быстро и безопасно проверять подлинность больших объемов информации.

Проще говоря, это способ свернуть тысячи или миллионы транзакций в **один короткий буквенно-цифровой код (хэш)**. Если в будущем изменится хотя бы одна точка в любой из транзакций, этот итоговый код полностью поменяется, сигнализируя об обмане.

Как устроена эта структура?

Дерево Меркла строится снизу вверх («листья» превращаются в «корень»):

[Корень Меркла] <-- Итоговый хэш блока (записывается в заголовок)

/ \

[Хэш AB] [Хэш CD] <-- Промежуточные хэши (ветви)

/ \ / \

[Хэш A][Хэш B][Хэш C][Хэш D]<-- Хэши отдельных транзакций

||||

Транс. Транс. Транс. Транс. <-- Сами данные (листья дерева)

A B C D

Листья дерева (Транзакции): Берутся исходные данные, например, четыре транзакции: A, B, C и D.

Первое хэширование: Каждая транзакция прогоняется через криптографическую функцию (например, SHA-256), превращаясь в уникальные строки фиксированной длины: Хэш A, Хэш B, Хэш C и Хэш D.

Объединение в пары (Ветви): Хэши соседних транзакций склеиваются друг с другом и хэшируются снова.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.