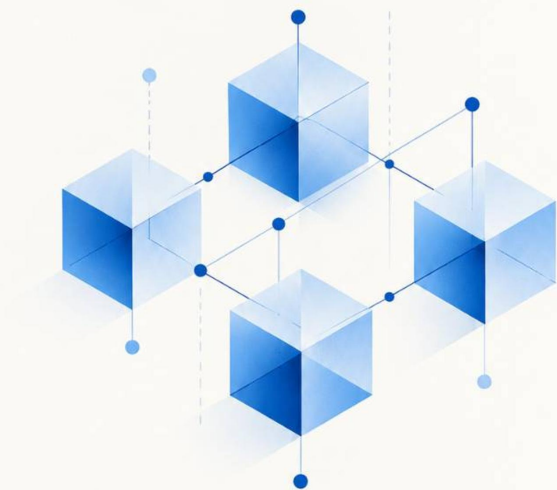


Блокчейн простыми словами

Технология биткоина и криптовалют



Ливай Гиллард

Ливай Гиллард

Блокчейн простыми

словами. Технология

биткоина и криптовалют

<https://litres.ru/74693963>

SelfPub; 2026

Аннотация

Прежде чем покупать криптовалюту, купите себе понимание того, за что собираетесь платить.

Блокчейн, смарт-контракты, NFT, DeFi: за этими словами может стоять полезная технология, а может скрываться красивая упаковка пустого проекта. Как отличить одно от другого, если каждый объясняет ещё непонятнее предыдущего?

Здесь всё начинается с обычного блокнота, в котором друзья записывают долги. От этого простого примера вы дойдёте до цифровой собственности, финансов без банков и устройства криптопроектов. Разберётесь, что система действительно умеет, где у неё ограничения и какие риски прячутся за громкими обещаниями.

Читайте, чтобы в следующий раз задавать неудобные вопросы, а не кивать на незнакомые слова.

Содержание

Введение	5
Глава 1. Что такое блокчейн?	9
Глава 2. Децентрализация — устранение посредников	21
Глава 3. Смарт-контракты — программирование доверия	37
Глава 4. Прозрачность и неизменяемость — записи, которым можно доверять	54
Конец ознакомительного фрагмента.	63

Ливай Гиллард Блокчейн простыми словами. Технология биткойна и криптовалют

Правовая информация

Дух самоотдачи

Введение

Представьте, что в 1990 году вам нужно было кому-то объяснить, что такое интернет. Скорее всего, вы сказали бы: это глобальная сеть, соединяющая компьютеры по всему миру и позволяющая людям обмениваться информацией в режиме реального времени. Но такое описание не передало бы того, чем интернет станет в будущем, и не объяснило бы, почему он так важен.

Сегодня мы сталкиваемся с похожей задачей, когда пытаемся объяснить технологию блокчейна.

Услышав слово «блокчейн», большинство сразу вспоминает биткойн. И не зря: биткойн действительно использует блокчейн. Но сводить блокчейн к биткойну — всё равно что сводить интернет к электронной почте. Так мы упускаем главное.

Блокчейн — это новый способ хранить и проверять информацию без доверенных посредников, таких как банки, государственные органы или компании. Благодаря ему незнакомые люди могут сотрудничать и обмениваться ценностями, не полагаясь друг на друга или на централизованные организации.

Если пока это звучит слишком абстрактно, не волнуйтесь. Дальше мы разберём, что это значит и почему это важно, на конкретных примерах применения.

Почему блокчейн так важен

Мы живём в цифровом мире, построенном на доверии. Покупая что-то в интернете, вы рассчитываете, что банк правильно обработает платёж. Публикуя фотографии в социальных сетях, вы доверяете платформе их хранение и отображение. Подписывая цифровой документ, вы верите, что никто не изменит его без вашего разрешения.

Но что, если создать цифровую систему, которой не нужно такое доверие? Что, если незнакомые люди смогут сотрудничать, обмениваться ценностями и заключать соглашения без банков, платформ и других посредников, проверяющих каждое действие?

Это не просто теория: подобные системы уже существуют благодаря блокчейну.

Чем отличается эта книга

В этой книге мы рассмотрим блокчейн с практической стороны. Начнём не с абстрактных понятий и технических спецификаций, а с проблем, которые он помогает решать. А затем разберёмся, как именно он это делает.

Мы будем опираться на то, что вы узнали из первой книги серии. Если вы понимаете, как работает биткоин, то уже знакомы с основами блокчейна. Теперь мы расширим эти знания и посмотрим на технологию в более широком контексте.

Каждая глава посвящена одному ключевому понятию и его практическому применению. Мы будем говорить не только о теоретических примерах, но и о реальных проектах и

компаниях, использующих блокчейн.

И да, я по-прежнему намерен сдержать обещание: обходиться без лишнего жаргона, не усложнять объяснения ради самой технологии и не требовать от вас знаний сверх того, что мы разобрали в первой книге.

Структура книги

Сначала мы разберёмся, что такое блокчейн и как он связан с биткоином. Затем рассмотрим его ключевые свойства: децентрализацию, прозрачность и неизменяемость.

После этого перейдём к применению за пределами криптовалют: смарт-контрактам, управлению цепочками поставок, цифровой идентификации и многому другому. Поговорим и об ограничениях технологии: понимать их не менее важно, чем знать о её возможностях.

В заключение мы заглянем в будущее технологии блокчейна и подготовимся к следующей книге из этой серии, в которой мы подробно рассмотрим Ethereum и смарт-контракты.

Между ажиотажем и реальностью

Вокруг блокчейна постоянно возникает ажиотаж. Одни уверяют, что он изменит всё. Другие считают его бесполезным решением, которое лишь создаёт проблемы.

Правда, как правило, лежит где-то посередине.

Блокчейн действительно способен решать конкретные задачи. Но это не волшебство и не универсальное средство. Чтобы разобраться в технологии, важно научиться отличать

обоснованные способы её применения от проектов, которые лишь следуют моде и на самом деле не нуждаются в блокчейне.

Эта книга поможет вам научиться проводить такое различие. Мы рассмотрим успешные проекты и неудачные эксперименты, а также обсудим, как понять, действительно ли конкретный проект использует преимущества блокчейна.

Глава 1. Что такое блокчейн?

Если вы читали первую книгу из этой серии, то знаете, что биткоин — это цифровая валюта, не требующая участия банков. Но вы, возможно, задаётесь вопросом: как это вообще возможно? Как система может функционировать без централизованного управления?

Ответ — технология блокчейна.

Блокчейн можно представить как особый реестр, которым пользуются многие участники и который не контролирует ни один человек или организация. В нём фиксируются транзакции, соглашения и другая информация, которую важно надёжно сохранить.

От традиционных реестров блокчейн отличается рядом свойств, которые обеспечивают высокую надёжность и безопасность без необходимости назначать единственного ответственного за систему.

Понимание основных концепций

Начнём с простой аналогии. Представьте, что вы с друзьями учитываете, кто кому должен деньги. В обычной системе кто-то один записывает все долги в блокнот. Остальные доверяют ему и рассчитывают, что записи будут точными.

Но что, если этот человек потеряет тетрадь? Что, если он допустит ошибку? Что, если он намеренно подделает записи в своих интересах?

Теперь представьте, что у каждого участника есть копия такого блокнота. Когда кто-то хочет внести запись о новом займе, он сообщает об этом группе. Все сверяются со своими записями, проверяя, может ли этот человек одолжить нужную сумму. Если большинство признаёт сделку действительной, каждый записывает её в свой блокнот.

Эта система обладает следующими преимуществами:

Отсутствие единой точки отказа. Даже если кто-то потеряет свой блокнот, у остальных сохранятся копии записей.

Прозрачность. Каждый может видеть все транзакции, поэтому обмануть систему очень сложно.

Консенсус. Сделку записывают только после того, как участники согласуют её действительность.

Неизменяемость. Как только что-то записано в тетрадах всех участников, это трудно изменить или удалить.

Примерно так и устроен блокчейн. Только вместо блокнотов здесь компьютеры, а вместо друзей — участники сети по всему миру.

От тетради к блокам

Вернёмся к аналогии с блокнотом. Вы, вероятно, записывали бы по несколько сделок на странице, а затем переходили к следующей. В блокчейне роль страниц играют блоки.

Каждый блок содержит набор транзакций или других записей. После формирования он связывается с предыдущим блоком и становится частью цепочки. Отсюда и название «блокчейн»: цепочка блоков, каждый из которых связан с

предыдущим.

Главное здесь в том, что изменить уже добавленный блок чрезвычайно трудно. Если кто-то попытается подделать старую транзакцию, другие узлы сети обнаружат несоответствие и отвергнут изменённые данные.

Именно это и обеспечивает так называемую неизменяемость — информация, однажды записанная, не может быть легко изменена или удалена.

Роль криптографии

Возможно, вы спросите: если у каждого своя копия реестра, как предотвратить подделку транзакций или попытку выдать себя за другого человека?

На помощь приходит криптография — область знаний, в которой математические методы применяются для защиты информации. В блокчейне она решает несколько задач:

Цифровая подпись подтверждает, что транзакцию разрешил владелец средств. Отправляя кому-то биткоины, вы подписываете транзакцию закрытым ключом, который храните в секрете. Остальные могут проверить подпись с помощью открытого ключа, но без закрытого ключа подделать её не смогут.

Хеш-функции создают своеобразный «отпечаток» данных каждого блока. Такая функция преобразует данные любого объёма в строку фиксированной длины. Даже небольшое изменение исходных данных приводит к изменению хеша, поэтому подделку легко обнаружить.

Дерево Меркла позволяет эффективно организовывать и проверять большие объёмы данных внутри блока. Оно помогает убедиться, что отдельная запись не была изменена, без проверки всех остальных записей.

Если термины пока кажутся сложными, не беспокойтесь. Главное — понять, что криптография помогает участникам блокчейн-сети проверять данные и предотвращать подделки без единого контролирующего органа.

Децентрализованная сеть

Традиционные системы часто централизованы: данные хранятся на серверах одной организации, которая ими управляет. Если центральная система выходит из строя, её сервисы могут стать недоступны.

Блокчейн-сеть распределена между компьютерами, которые называют узлами. Многие из них хранят копии блокчейна. Даже если часть узлов отключится, сеть сможет продолжить работу.

У такого устройства есть несколько преимуществ:

Устойчивость: сеть способна выжить даже в случае выхода из строя большого числа узлов.

Устойчивость к цензуре: ни один отдельный субъект не может отключить или контролировать сеть.

Глобальная доступность: любой человек, имеющий подключение к интернету, может принять участие.

Снижение риска «точки отказа»: отсутствие центрального сервера, который хакеры могли бы атаковать.

Механизм консенсуса

Это один из самых интересных вопросов: как распределённая сеть договаривается о том, какие данные считать верными?

Помните аналогию с блокнотом, о которой мы упоминали ранее? Каждый должен прийти к согласию, прежде чем записывать транзакцию. Сеть блокчейна использует механизм консенсуса для автоматического достижения согласия.

В системе Биткоин механизм консенсуса называется доказательством работы. Специализированные компьютеры, называемые майнерами, соревнуются в решении математических задач. Тот, кто первым решает задачу, может добавить следующий блок в цепочку и получить вознаграждение. Все остальные узлы проверяют правильность решения, прежде чем принять новый блок.

На первый взгляд кажется, что вычислительные мощности расходуются впустую: компьютеры лишь решают задачи. Но эта работа защищает сеть. Чтобы переписать историю транзакций, злоумышленнику пришлось бы сосредоточить огромную вычислительную мощность, а это очень дорого.

Другие блокчейн-сети используют иные механизмы консенсуса. Например, при доказательстве доли владения (PoS) участники блокируют часть своих монет в качестве залога, чтобы участвовать в подтверждении транзакций. Существуют и гибридные подходы.

Суть в том, что эти механизмы позволяют множеству ком-

пьютеров согласовывать состояние блокчейна без единого управляющего центра.

Смарт-контракты: код как закон

Традиционные договоры составляют на обычном языке, а их исполнение обеспечивают правовые механизмы. Смарт-контракты — это программы, записанные в блокчейне, которые автоматически исполняют заданные условия.

Например, предположим, что вы хотите арендовать квартиру с помощью смарт-контракта. Вы могли бы написать следующий код: «Если Рикардо заплатит 1000 долларов и предоставит подтверждение страхования, то передайте Рикардо код доступа к квартире и перечислите деньги арендодателю».

После размещения в блокчейне смарт-контракт выполнит предусмотренные кодом действия при соблюдении заданных условий. Для автоматической части сделки не потребуется ручное вмешательство, однако споры о реальной аренде всё равно могут потребовать юридического решения.

Благодаря смарт-контрактам блокчейн-сети способны реализовывать гораздо больше, чем просто переводы средств. Они позволяют автоматически выполнять сложные соглашения, создавать новые типы организаций и разрабатывать приложения, функционирующие без какого-либо централизованного контроля.

В следующих главах мы подробно поговорим о смарт-контрактах. Пока достаточно помнить, что это программы, ра-

ботающие в блокчейн-сети и автоматически выполняющие предусмотренные кодом действия.

Публичные и частные блокчейны

Не все блокчейн-сети открыты для всех. Существуют следующие типы блокчейн-сетей:

Публичные блокчейны, такие как Биткоин и Ethereum, открыты для всех. Любой желающий может присоединиться к сети, просматривать транзакции и участвовать в поддержании её работы. В таких сетях особое значение имеют децентрализация и устойчивость к цензуре.

Частные блокчейны контролируются одной организацией. Они могут обеспечивать совместное ведение записей и прозрачность для участников, но уступают публичным сетям в децентрализации. Такой подход используют компании для внутренних задач.

Консорциумные блокчейны управляются группой организаций. По степени децентрализации они занимают промежуточное положение между частными и публичными сетями. Их используют там, где нескольким компаниям нужно обмениваться записями без полного раскрытия информации.

Каждый тип имеет свои преимущества и недостатки. Публичные цепочки более безопасны и устойчивы к цензуре, но при этом работают медленнее и потребляют больше энергии. Частные цепочки работают быстрее и эффективнее, но требуют доверия к контролирующим органам.

Проблема двойной траты

Одна из важнейших задач, которые решает блокчейн, — предотвратить двойную трату. Цифровые данные легко копировать: фотографии, документы и музыку можно дублировать практически без ограничений.

Но с деньгами так не может быть. Если бы цифровую валюту можно было копировать, она стала бы бесполезной, поскольку у каждого было бы неограниченное количество цифровой валюты.

Раньше для предотвращения двойной траты в электронных денежных системах обычно требовался доверенный посредник, например банк. Он отслеживал остатки на счетах и не давал потратить одни и те же средства дважды.

Блокчейн позволяет решать эту задачу без доверенного посредника. Распределённый реестр содержит записи о средствах, а правила проверки транзакций и механизм консенсуса предотвращают их повторное расходование.

Этот подход сделал возможным появление децентрализованных цифровых валют.

За пределами денег: другие применения

Хотя биткоин является первым и самым известным применением технологии блокчейна, её основные концепции можно применять к решению многих других задач:

Отслеживание цепочки поставок: фиксирование всего пути продукта от производителя до потребителя, обеспечение подлинности и предотвращение подделок.

Цифровая идентичность: создание безопасной и прове-

ряемой цифровой идентичности, которой человек может управлять самостоятельно, не полагаясь на централизованные органы.

Системы голосования: обеспечение прозрачных и поддающихся проверке выборов, при которых каждый может убедиться в правильности подсчёта голосов.

Учет недвижимости: ведение прозрачных и неизменяемых записей о праве собственности и передаче недвижимости.

Права интеллектуальной собственности: простановка временных меток на творческих произведениях для определения времени их создания и владельца.

Медицинские записи: предоставление пациентам контроля над своими медицинскими данными при одновременном обеспечении безопасного доступа к этим данным уполномоченным медицинским организациям.

Все эти примеры опираются на основные свойства блокчейна: децентрализацию, прозрачность, неизменяемость и возможность проверять записи без доверенного посредника.

Революционный потенциал

Чтобы понять блокчейн, важно увидеть в нём не только технологию, но и новый способ организовывать сотрудничество.

На протяжении большей части истории человечества для сотрудничества в широких масштабах требовалась иерархическая структура. Если вы хотите перевести деньги, вам ну-

жен банк. Если вы хотите заключить соглашение, вам нужен суд для его исполнения. Если вы хотите проголосовать, вам нужно правительство, которое организует голосование и подсчитывает голоса.

Блокчейн позволяет людям напрямую взаимодействовать, заключать соглашения и обмениваться ценностями, не полагаясь на обязательное доверие друг к другу или посредникам.

Однако это не значит, что банки, суды и государства исчезнут. У нас появился другой способ проверять действия и записи: опираться на математические доказательства, а не только на репутацию организаций.

Ограничения и вызовы

Несмотря на преимущества, у блокчейна есть серьёзные ограничения:

Масштабируемость: большинство блокчейн-сетей могут обрабатывать лишь ограниченное количество транзакций в секунду. Биткоин обрабатывает около 7 транзакций в секунду, тогда как традиционные платежные системы — до нескольких тысяч.

Энергопотребление: доказательство работы требует значительных затрат электроэнергии. Энергопотребление сети Биткоина сопоставимо с потреблением целых стран.

Сложность использования: людям без технической подготовки бывает трудно безопасно пользоваться блокчейн-приложениями. Утрата закрытого ключа может привести к без-

возвратной потере доступа к средствам.

Регулирование: правительства всё ещё изучают, как регулировать блокчейн-приложения, что создаёт неопределенность для пользователей и разработчиков.

Необратимость: хотя неизменяемость обычно является преимуществом, она также означает, что ошибки и мошенничество нельзя легко исправить.

Понимание этих ограничений имеет решающее значение для оценки того, подходит ли блокчейн для конкретного применения.

Путь вперед

Технология блокчейна продолжает быстро развиваться: разработчики стремятся преодолеть существующие ограничения, а новые приложения появляются постоянно.

Некоторые блокчейн-сети экспериментируют с различными механизмами консенсуса, чтобы снизить энергопотребление. Другие сети внедряют масштабируемые решения для обработки большего количества транзакций. Усовершенствования пользовательского интерфейса также способствуют более широкому принятию блокчейн-приложений обычными пользователями.

При этом организации и государственные органы начинают применять блокчейн там, где его преимущества перевешивают ограничения.

Ближайшие годы покажут, какие способы применения блокчейна приживутся на практике, а какие останутся инте-

ресными экспериментами.

Подготовка к следующему шагу

Теперь, когда вы ознакомились с основами технологии блокчейна, можно приступить к изучению конкретных приложений и сценариев использования. В следующих главах мы рассмотрим применение блокчейна в различных отраслях, проанализируем примеры успехов и неудач, а также обсудим, как оценивать новые блокчейн-проекты.

Мы также подготовимся к следующей книге серии, посвящённой Ethereum — блокчейн-платформе, на которой реализованы многие инновации, выходящие за рамки простых криптовалютных переводов.

Но сначала давайте подробно рассмотрим, как блокчейн реализует одну из своих важнейших характеристик: децентрализацию. Понимание децентрализации является ключом к пониманию того, почему технология блокчейна является настолько революционной и почему она способна переосмыслить то, как мы организуем цифровые системы.

Переход от централизованных систем к децентрализованным — не просто техническое изменение. Он меняет представления о доверии, контроле и сотрудничестве в цифровую эпоху.

Глава 2. Децентрализация — устранение посредников

В повседневной жизни нас окружают посредники. Банки обрабатывают платежи, социальные сети хранят наши публикации, государственные органы выдают удостоверения личности, а интернет-магазины помогают совершать покупки.

Эти посредники оказывают полезные услуги, но зависимость от них создаёт дополнительные расходы и риски. Блокчейн предлагает другой подход: участники системы могут взаимодействовать напрямую.

Эта концепция называется децентрализацией и является одним из самых революционных аспектов технологии блокчейна.

Понимание централизации

Большинство привычных нам систем централизованы: у них есть единый центр управления.

Возьмем, к примеру, ваш банковский счет. Все записи о ваших транзакциях, остаток на счете и личные данные хранятся на серверах банка. Когда вы хотите перевести деньги другу, вы отправляете запрос в банк. Банк проверяет, достаточно ли средств на вашем счете, затем списывает сумму с вашего счета, зачисляет её на счет вашего друга и обновляет

остатки на счетах обеих сторон.

Эта система во многих отношениях работает хорошо. Банки располагают передовыми системами обнаружения мошенничества, службами поддержки клиентов и страховкой для защиты ваших вкладов. Если вы допустили ошибку, вы можете позвонить в банк и, возможно, отменить транзакцию.

Однако централизованность также создаёт некоторые проблемы:

Единственная точка отказа: если в банковской системе произойдет сбой, вы не сможете получить доступ к своим средствам или совершать транзакции.

Цензура: банк может по любой причине заморозить ваш счет или заблокировать транзакцию.

Высокие затраты: банкам приходится содержать дорогостоящую инфраструктуру и платить сотрудникам. Эти расходы отражаются на комиссиях для клиентов.

Ограничения доступа: не каждый может открыть банковский счёт. Требования к документам, минимальному остатку и кредитной истории могут становиться препятствием.

Медленные расчёты: международные переводы порой занимают несколько дней, поскольку проходят через множество посредников, увеличивающих сроки и комиссии.

Проблемы с конфиденциальностью: банки собирают и хранят подробную информацию обо всех ваших финансовых операциях.

Контроль: на самом деле вы не контролируете свои средства — вы полагаетесь на разрешение банка для доступа к ним и их использования.

Децентрализованная альтернатива

Децентрализованная система распределяет управление между множеством участников. В децентрализованной блокчейн-сети нет единого сервера и органа, который мог бы единолично устанавливать правила.

Давайте продолжим с примером банка, но представим его децентрализованную версию:

Вместо одного банка множество компьютеров по всему миру хранят и сверяют записи о переводах и остатках.

Когда вы хотите перевести деньги, вы рассылаете транзакцию по этой сети. Компьютеры проверяют, достаточно ли у вас средств и действительна ли ваша цифровая подпись.

Если транзакция является законной, она будет включена в следующий блок и добавлена в постоянный реестр. Ваш баланс уменьшится, а баланс вашего друга увеличится, и копии реестра у всех участников будут обновлены соответствующим образом.

В идеале ни один участник не может единолично контролировать этот процесс. Действия сети определяются правилами протокола, которые участники поддерживают совместно.

В сущности, именно так работает биткоин, демонстрируя силу децентрализации финансовой системы.

Виды децентрализации

Децентрализация — не вопрос выбора между двумя крайностями. У неё есть разные стороны и степени:

Архитектурная децентрализация: из скольких физических компьютеров состоит система? Сколько компьютеров могут выйти из строя в любой момент, прежде чем система перестанет функционировать?

Политическая децентрализация: сколько людей или организаций контролируют компьютеры, образующие систему?

Логическая децентрализация: воспринимается ли система как единое целое или как совокупность независимых частей?

Давайте рассмотрим каждый из этих типов:

Архитектурная децентрализация

Биткоин архитектурно децентрализован, поскольку сеть работает на множестве компьютеров по всему миру. Если часть узлов отключится, остальные могут продолжить работу.

Архитектура Facebook централизована, поскольку она работает на серверах, принадлежащих и контролируемых Meta. Если эти серверы выйдут из строя, Facebook перестанет функционировать.

Некоторые системы архитектурно распределены, но политически централизованы. Например, Amazon Web Services (AWS) размещает вычислительные мощности в разных странах, однако управляет ими одна компания — Amazon.

Политическая децентрализация

Биткоин политически децентрализован: ни одна отдельная организация не управляет всей сетью. Изменение правил требует согласия участников, а присоединиться к сети может любой желающий.

Сеть в некоторой степени является политически децентрализованной. Хотя ни одна организация не может контролировать весь интернет, такие организации, как ICANN, оказывают значительное влияние на инфраструктуру интернета.

Традиционные банки являются политически централизованными. Каждый банк, независимо от количества филиалов или банкоматов, контролируется своим руководством и акционерами.

Логическая децентрализация

Биткоин логически централизован: участники опираются на единый согласованный реестр. При этом архитектура и управление сетью остаются децентрализованными.

Электронная почта с логической точки зрения является децентрализованной. Различные почтовые сервисы могут взаимодействовать друг с другом, но не существует единой глобальной адресной книги или журнала сообщений.

Большинство блокчейн-сетей логически централизованы: их участники поддерживают согласованное состояние реестра.

Преимущества децентрализации

По сравнению с централизованными системами децентрализованные системы обладают несколькими важными преимуществами:

Отказоустойчивость

В централизованной системе возможна единая точка отказа: сбой центрального сервера может остановить работу сервиса. Распределённая система способна продолжать работу даже при отключении части узлов.

В 2021 году Facebook, Instagram и WhatsApp простояли шесть часов из-за ошибки в настройках. Это затронуло миллиарды пользователей по всему миру. Биткоин никогда не сталкивался с подобными сбоями, поскольку у него нет центрального сервера.

Устойчивость к атакам

Атаковать централизованную систему гораздо проще, чем децентрализованную. Злоумышленнику достаточно атаковать одну цель, чтобы вывести из строя централизованную систему, тогда как для успешной атаки на децентрализованную систему необходимо атаковать сразу несколько узлов.

Чтобы атаковать Биткоин, злоумышленнику необходимо контролировать вычислительную мощность, превышающую совокупную мощность всей сети — это и дорого, и сложно. А для атаки на традиционный банк злоумышленнику может потребоваться всего лишь взломать один сервер или базу данных.

Сопротивление цензуре

Централизованная организация может ограничить доступ пользователей или заблокировать отдельные операции. В децентрализованной системе ни один участник не должен иметь возможность единолично вводить такие ограничения.

Правительства разных стран уже закрывали социальные сети, блокировали платежные системы и арестовывали банковские счета. Но они не могут закрыть биткоин и не могут помешать людям совершать транзакции с биткоинами, если только не отключить всю сеть.

Снижение зависимости от контрагента

В централизованной системе вы должны верить, что центральный орган власти будет действовать честно и эффективно. В децентрализованной системе вам не нужно доверять ни одной из сторон.

Размещая деньги в банке, вы полагаетесь на его платёжеспособность, соблюдение законов и готовность вернуть средства. Владея биткоинами через собственный кошелёк, вы самостоятельно контролируете доступ к ним.

Цена децентрализации

Децентрализация даёт важные преимущества, но требует компромиссов:

Эффективность

Децентрализованные системы обычно работают медленнее и менее эффективно, чем централизованные. Биткоин обрабатывает около 7 транзакций в секунду, тогда как Visa может обрабатывать тысячи транзакций в секунду. Это свя-

зано с тем, что децентрализованной системе требуется время, чтобы множество узлов достигли согласия по каждой транзакции.

Централизованные системы не нуждаются в механизме консенсуса, поэтому позволяют оптимизировать эффективность. Централизованные базы данных могут мгновенно обрабатывать транзакции, поскольку существует только одна авторитетная копия данных.

Управление

Управление децентрализованной системой сложно: нет единого органа, который мог бы быстро принять решение. Например, обсуждение размера блока в сети Биткойна продолжалось несколько лет, поскольку сообщество не могло договориться, как повысить пропускную способность.

Централизованные системы могут быстро адаптироваться к новым требованиям или решать проблемы благодаря наличию четко определённых полномочий по принятию решений.

Пользовательский опыт

Децентрализованными сервисами часто сложнее пользоваться, особенно без технической подготовки. Потеряв закрытый ключ от биткойнов, вы не сможете обратиться в обычную службу поддержки, чтобы восстановить доступ.

Централизованные системы могут предоставлять поддержку клиентов, восстановление паролей, защиту от мошенничества и другие услуги, что позволяет обычным поль-

зователям использовать систему проще и безопаснее.

Потребление энергии

Механизм доказательства работы, который использует Биткоин, требует значительных затрат электроэнергии. При этом не всякая децентрализованная система основана на таком механизме.

Централизованные системы могут быть более энергоэффективными, поскольку им не нужно дублировать данные между тысячами узлов или запускать алгоритмы консенсуса.

Степень децентрализации

Большинство реальных систем находятся в диапазоне между полной централизацией и полной децентрализацией. Даже системы, называющие себя «децентрализованными», часто содержат некоторые централизованные компоненты.

Рассмотрим Ethereum. Сеть децентрализована по сравнению с традиционными финансовыми системами, но некоторые её компоненты могут зависеть от относительно небольшого числа участников:

Распределение узлов: узлы Ethereum распределены по всему миру, что обеспечивает отказоустойчивость и устойчивость к цензуре.

Разработка: разработка Ethereum частично координируется сообществом и организациями, в том числе Ethereum Foundation, которая влияет на дорожную карту проекта.

Валидация: при доказательстве доли владения часть стейкинга может сосредотачиваться у крупных операторов, со-

здавая риск централизации.

Приложения: многие приложения Ethereum содержат централизованные компоненты, такие как веб-интерфейсы или ключи управления, позволяющие обновлять код контрактов.

Такой подход делает Ethereum гибким и функциональным, сохраняя многие преимущества децентрализации.

Децентрализация на практике

Давайте посмотрим, как децентрализация работает в нескольких реальных приложениях на основе блокчейна:

Хранение файлов

Традиционные облачные хранилища, такие как Google Drive или Dropbox, являются централизованными. Ваши файлы хранятся на серверах компаний, а доступ к ним осуществляется через их приложения.

Децентрализованные системы хранения, например IPFS (InterPlanetary File System) и Filecoin, позволяют хранить и распространять данные между разными узлами, снижая зависимость от одного поставщика.

Преимущества: отсутствие единой точки отказа, устойчивость к цензуре, возможное снижение затрат.

Недостатки: сложность использования, непостоянная скорость поиска, относительно молодая экосистема.

Социальные сети

Традиционные социальные сети, такие как Twitter и Facebook, являются централизованными. Компании контролируют ваш контент в ленте, могут удалять посты или блоки-

ровать пользователей, а также владеют всеми данными, созданными пользователями.

Децентрализованные социальные сети, такие как Mastodon, или децентрализованные протоколы, построенные на блокчейне, распределяют контроль между множеством серверов или узлов.

Преимущества: нет единого субъекта, способного подвергать цензуре всех пользователей; пользователи получают больший контроль над своими данными и защищены от закрытия платформы.

Недостатки: более сложный пользовательский интерфейс, сложность достижения сетевого эффекта, проблемы с модерацией.

Система доменных имён

Традиционная система доменных имён (DNS) преобразует удобочитаемые для человека доменные имена (например, «google.com») в IP-адреса, понятные компьютерам. Эта система имеет иерархическую структуру и в конечном итоге контролируется ICANN и правительствами разных стран.

Системы именования на основе блокчейна, например Ethereum Name Service (ENS) и Handshake, предлагают децентрализованный способ учёта прав на доменные имена.

Преимущества: устойчивость к цензуре доменных имён, контроль над правом собственности со стороны пользователей, интеграция с адресами криптовалют.

Недостатки: ограниченное внедрение, проблемы с совме-

стимостью с традиционными браузерными, высокие транзакционные издержки.

Сетевой эффект и децентрализация

Одним из главных вызовов для децентрализованных систем является достижение сетевого эффекта, то есть ситуации, когда чем больше людей использует продукт, тем выше его ценность.

Социальные сети, платёжные системы и торговые площадки выигрывают от сетевого эффекта. Facebook ценен тем, что им пользуются ваши друзья; банковские карты удобны, потому что их принимают продавцы; Amazon — потому что на площадке много товаров и продавцов.

Централизованным системам проще добиться сетевого эффекта: они могут согласованно продвигать продукт, поддерживать единый интерфейс и быстро принимать решения. Кроме того, они могут привлекать первых пользователей за счёт субсидий.

Децентрализованные системы сталкиваются с проблемами координации. Кто будет оплачивать расходы на маркетинг? Кто обеспечит высокое качество пользовательского опыта? Кто будет принимать решения об обновлении протокола?

Биткоин решил эту проблему, предоставив участникам экономические стимулы. Майнеры получают вознаграждение за поддержание безопасности сети, что привлекает огромные вычислительные мощности и закладывает проч-

ную основу безопасности Биткойна.

Другие децентрализованные системы пробуют использовать другие подходы:

Стимулирование с помощью токенов: ранние пользователи получают вознаграждение в виде токенов, стоимость которых может расти по мере развития сети.

Управление сообществом: предоставление держателям токенов права голосовать по вопросам обновления сети и распределения ресурсов.

Субсидии разработчикам: финансирование разработчиков для улучшения пользовательского интерфейса и добавления новых функций.

Межсетевая совместимость: возможность запуска децентрализованных приложений в нескольких блокчейн-сетях.

Будущее децентрализации

Степень децентрализации бывает разной. Она зависит от потребностей конкретной системы.

Некоторые приложения получают значительные преимущества от полной децентрализации:

Валюта и платежи: устойчивость к цензуре и глобальная доступность децентрализованных валютных систем дают очевидные преимущества.

Связь без цензуры: в регионах, где действуют правительственные ограничения, децентрализованные системы связи имеют решающее значение для свободы слова.

Децентрализованные автономные организации: организа-

ции, функционирующие в соответствии с запрограммированными правилами, не требующие ручного управления.

Другие приложения могут извлечь выгоду из гибридного подхода, сочетающего некоторые преимущества децентрализации и некоторые преимущества централизации:

Отслеживание цепочки поставок: использование блокчейна для обеспечения прозрачности при одновременном сохранении централизованного управления для повышения эффективности.

Цифровая идентификация: предоставление пользователям контроля над своей идентичностью при одновременном обеспечении услуг по верификации со стороны организаций.

Рынки прогнозов: использование децентрализованных систем для прозрачных и устойчивых к цензуре ставок при одновременной интеграции с централизованными источниками данных.

В других приложениях может оказаться, что централизация в целом работает лучше, а блокчейн используется только для определенных компонентов, таких как аудит, отслеживание или межорганизационная координация.

Выбор в пользу децентрализации

При оценке блокчейн-проекта или принятии решения о замене централизованных сервисов децентрализованными альтернативами следует учитывать следующие вопросы:

Какие конкретные преимущества децентрализации есть для данного сценария использования? Не все приложения

могут извлечь выгоду из децентрализации.

Каковы затраты и компромиссы? Децентрализованные системы обычно требуют уступок в плане эффективности, пользовательского опыта или функциональности.

Насколько система децентрализована на практике? Многие проекты заявляют о децентрализации, но сохраняют важные централизованные компоненты.

Является ли эта система устойчивой? Децентрализованные системы нуждаются в экономической модели, способной стимулировать долгосрочное участие.

Каковы риски централизации? Подумайте, что произойдёт, если централизованный сервис закроется, подвергнется взлому или начнёт действовать против интересов пользователей.

Подготовка к смарт-контрактам

Понимание децентрализации важно для изучения смарт-контрактов, о которых пойдёт речь в следующей главе. Смарт-контракты — программы, работающие в блокчейн-сети и автоматически выполняющие заданные условия без доверенного посредника.

Децентрализация позволяет запускать смарт-контракты без единого оператора, которому нужно доверять их исполнение. В централизованной системе такой оператор может вмешаться в работу программы. В децентрализованной сети исполнение определяется правилами протокола и кодом контракта.

Сочетание децентрализации и программируемости открывает новые возможности. Оно позволяет создавать автоматизированные системы, действующие по заранее заданным правилам без постоянного участия централизованных организаций.

Как мы увидим в следующей главе, это имеет революционное значение для нашего понимания протоколов, организаций и автоматизированных систем.

Глава 3. Смарт-контракты — программирование доверия

Представьте, что можно написать программу, которая автоматически выполняет условия соглашения без посредника. Именно такую задачу решают смарт-контракты.

Это не научная фантастика. Такие программы уже существуют сегодня, и они называются смарт-контрактами.

Смарт-контракты — одно из важнейших применений блокчейна. Они позволяют задавать условия соглашения в программном коде, а их исполнение обеспечивается блокчейн-сетью.

Что такое смарт-контракт?

Смарт-контракт — это программа, размещённая в блокчейне и выполняющая действия при наступлении заранее заданных условий. Представьте торговый автомат: вы оплачиваете покупку, выбираете товар — и автомат выдаёт его без участия продавца.

Однако смарт-контракты способны выполнять гораздо более сложные функции, чем автомат. Они могут хранить средства, отслеживать права собственности, исполнять многосторонние соглашения, а также создавать совершенно новые типы организаций и финансовых инструментов.

Термин «смарт-контракт» предложил специалист по ин-

форматике Ник Сабо (Nick Szabo) ещё в 1990-х годах, задолго до появления блокчейна. Он предполагал, что программное и аппаратное обеспечение сможет сделать нарушение условий соглашения сложным или слишком дорогим.

Блокчейн позволил приблизить эту идею к реальности. программы можно выполнять в распределённой среде, где их сложнее подделать или незаметно изменить.

Как работают смарт-контракты

Обычные договоры составляют на естественном языке, а их исполнение обеспечивается правовой системой. Если одна из сторон нарушает условия, другая может обратиться в суд за компенсацией или принудительным исполнением.

Смарт-контракты работают иначе: их условия записаны в виде кода, который исполняется в блокчейне. Если попытка провести операцию не соответствует правилам контракта, она отклоняется.

Рассмотрим пример. Алиса хочет купить у Боба цифровое произведение искусства за криптовалюту на сумму 100 долларов. Для сделки они могут использовать смарт-контракт.

Алиса и Боб согласуют условия: Алиса переводит криптовалюту на сумму 100 долларов, а Боб передаёт ей цифровой актив.

Затем они создают смарт-контракт с правилом: «Если Алиса отправит в контракт криптовалюту на сумму 100 долларов, цифровой актив перейдёт ей, а средства будут перечислены Бобу».

Алиса отправляет криптовалюту в смарт-контракт. После подтверждения операции контракт передаёт ей цифровой актив, а Бобу — платёж.

Алисе и Бобу не обязательно доверять друг другу при проведении такой сделки: им нужно убедиться, что код контракта делает именно то, о чём они договорились, а сеть выполняет его корректно.

Компоненты смарт-контракта

Смарт-контракт состоит из нескольких ключевых компонентов:

Логика кода

Основа любого смарт-контракта — программная логика: набор правил, определяющих его поведение. Код задаёт условия, при которых выполняются различные операции.

Например, смарт-контракт для краудфандинговой кампании может содержать следующую логику:

«Если к концу срока сбора средств достигнута целевая сумма, деньги перечисляются создателю проекта».

«Если срок истёк, а целевая сумма не собрана, участники могут вернуть свои взносы».

Переменные состояния

Смарт-контракты могут сохранять данные между операциями. Так называемые переменные состояния содержат, например, балансы, записи о праве собственности или результаты голосования.

Простой контракт на токены может иметь следующие пе-

ременные состояния:

Общий объем предложения токенов

Количество токенов, принадлежащих каждому адресу

Кто имеет право выпускать новые токены

Функции

Функции — это части программы, которые вызывают для взаимодействия со смарт-контрактом. Некоторые доступны всем, другие — только определённым пользователям.

Контракт токена может иметь следующие функции:

`transfer(получатель, сумма)`: перевод токенов с одного адреса на другой

`approve(spender, amount)`: разрешить другому счету тратить токены от вашего имени

`mint(to, amount)`: выпуск новых токенов (только для уполномоченных адресов)

События

При возникновении важных событий смарт-контракт может генерировать события. Эти события записываются в блокчейн и могут отслеживаться внешними приложениями.

Например, каждый раз, когда токены переводятся с одного счёта на другой, контракт токена может генерировать событие «Transfer». Это позволяет кошелькам и блокчейн-браузерам отслеживать движение токенов без необходимости проверки каждой отдельной транзакции.

Ethereum: платформа для смарт-контрактов

Хотя Биткоин поддерживает простые программируемые

операции, Ethereum изначально разрабатывался для выполнения более сложных смарт-контрактов.

Ethereum включает виртуальную машину Ethereum Virtual Machine (EVM), которая выполняет код смарт-контрактов. Её вычислительная модель обладает полнотой по Тьюрингу: в теории она позволяет реализовать любые вычисления, которые можно описать алгоритмом.

Смарт-контракты Ethereum обычно пишут на языке Solidity. Его синтаксис напоминает языки программирования общего назначения, но при разработке контрактов необходимо отдельно учитывать риски безопасности.

В Solidity очень простой смарт-контракт может выглядеть следующим образом:

```
```solidity
contract SimpleStorage {
 uint256 storedData;
 function set(uint256 x) public {
 storedData = x;
 }
 function get() public view returns (uint256) {
 return storedData;
 }
}
```
```

Этот контракт позволяет сохранять число и позже считывать его. Даже в таком простом примере видны переменная

состояния `storedData` и функции `set` и `get` для работы с ней.

Применение смарт-контрактов на практике

С помощью смарт-контрактов можно реализовывать приложения, создание которых с помощью традиционных технологий затруднительно или невозможно:

Децентрализованные финансы (DeFi)

Приложения DeFi используют смарт-контракты для воссоздания традиционных финансовых услуг без участия традиционных финансовых учреждений.

Кредитные протоколы: смарт-контракты позволяют пользователям предоставлять криптовалюту в долг под проценты или занимать её под залог. Если залог становится недостаточным, протокол может автоматически ликвидировать позицию.

Децентрализованные биржи: смарт-контракты позволяют пользователям напрямую обмениваться криптовалютами друг с другом без участия операторов централизованных бирж.

Автоматический маркетмейкер: механизм на основе смарт-контракта, позволяющий торговать через пул ликвидности и определять цены по заданной формуле.

«Фарминг доходности»: смарт-контракты, вознаграждающие пользователей за предоставление ликвидности или участие в различных протоколах DeFi.

Невзаимозаменяемые токены (NFT)

NFT — уникальные цифровые токены, выпускаемые с

помощью смарт-контрактов. Они могут использоваться для учёта цифровых произведений искусства, коллекционных предметов, виртуальной недвижимости и других уникальных объектов.

Смарт-контракт может определять:

Кто является владельцем каждого NFT

Как происходит передача NFT

Роялти, получаемые автором от вторичной продажи

Метаданные, связанные с каждым NFT

Децентрализованная автономная организация (DAO)

DAO — это организация, функционирующая на основе правил, заложенных в смарт-контрактах, а не в рамках традиционной иерархии управления.

DAO может использовать смарт-контракты для:

управления финансами и принятия решений о расходах путём голосования участников

автоматического распределения прибыли между держателями токенов

управления обновлениями протокола и изменением его параметров

учёта участников и их права голоса

Страхование

Смарт-контракт может автоматически выплачивать страховое возмещение, если данные из проверенного внешнего источника подтверждают наступление страхового случая.

Страхование задержки рейсов: смарт-контракт получает данные о рейсе от внешнего сервиса и автоматически выплачивает компенсацию при выполнении заданных условий.

Страхование урожая: если определенные условия указывают на повреждение урожая, смарт-контракт выплачивает фермерам компенсацию на основе данных о погоде.

Страхование по параметрам: страхование с автоматической выплатой компенсации при достижении заданных параметров, не требующее оценки ущерба.

Преимущества смарт-контрактов

По сравнению с традиционными договорами смарт-контракты обладают рядом значительных преимуществ:

Автоматизация

Смарт-контракты автоматически исполняются при выполнении условий. Это устраняет необходимость ручной обработки и сокращает время между срабатыванием события и исполнением контракта.

Выполнение без необходимости доверия

Сторонам не нужно полностью полагаться друг на друга или на посредника: достаточно проверить, что код правильно отражает условия сделки и выполняется сетью.

Прозрачность

Код смарт-контрактов, как правило, является открытым и хранится в публичном блокчейне, что позволяет любому точно проверить, как работает контракт.

Неизменяемость

После развёртывания смарт-контракт обычно трудно изменить. Это помогает сохранить правила, о которых заранее договорились стороны.

Глобальная доступность

Любой человек, имеющий доступ к интернету, может получить доступ к смарт-контрактам без разрешения банков, правительства или других организаций.

Экономическая эффективность

Смарт-контракты позволяют исключить многих посредников и ручные процессы, что может снизить затраты на выполнение соглашений.

Ограничения и риски

У смарт-контрактов есть и существенные ограничения, о которых пользователям необходимо знать:

Ошибки в коде

Смарт-контракты — это программы, а в программах могут встречаться ошибки. В отличие от традиционного программного обеспечения, ошибки в смарт-контрактах нелегко исправить после развёртывания, и они могут привести к безвозвратной потере средств.

Хакерская атака на DAO в 2016 году наглядно продемонстрировала этот риск. Уязвимость в смарт-контракте позволила злоумышленникам похитить эфир на сумму около 60 миллионов долларов, что в конечном итоге привело к спорному хард-форку сети Ethereum.

Проблемы с оракулами

Смарт-контракты могут обращаться только к информации, хранящейся в блокчейне, и не имеют прямого доступа к внешним данным, таким как котировки акций, информация о погоде или события на практике.

Это приводит к «проблеме оракулов» — как внедрить достоверные внешние данные в смарт-контракт. Оракул — это сервис, предоставляющий внешние данные смарт-контрактам, однако он вводит элементы централизации и требует доверия.

Неизменяемость

Хотя неизменяемость может быть преимуществом, она также означает, что после развертывания внести полезные изменения или исправить ошибки бывает сложно или невозможно.

Некоторые смарт-контракты содержат механизмы обновления, но они, как правило, требуют доверия к разработчикам, контролирующим ключи обновления.

Масштабируемость

Многие блокчейн-сети обрабатывают ограниченное число операций в секунду. При высокой нагрузке исполнение смарт-контрактов может замедляться, а комиссии — расти.

Правовое признание

Во многих юрисдикциях правовой статус смарт-контрактов по-прежнему остаётся неопределённым. В случае непредвиденного поведения смарт-контракта может быть неясно, какие правовые меры защиты можно применить.

Пользовательский опыт

Взаимодействие со смарт-контрактами обычно требует технических знаний в области блокчейн-транзакций, комиссий за газ и управления кошельками. Такая сложность ограничивает их внедрение на массовом рынке.

Безопасность смарт-контрактов

Поскольку смарт-контракты обычно обрабатывают ценные активы и после развертывания их невозможно легко изменить, безопасность имеет решающее значение. Разработчики используют различные методы для повышения безопасности смарт-контрактов:

Аудит кода

Перед публикацией специалисты по безопасности проверяют код смарт-контрактов на уязвимости. Аудит бывает дорогим и не гарантирует, что будут найдены все ошибки.

Формальная верификация

Математические методы, позволяющие доказать определенные свойства кода смарт-контракта. Этот подход более строгий, чем традиционное тестирование, но при этом более сложный и дорогостоящий.

Вознаграждения за обнаружение уязвимостей

Программы вознаграждения исследователей за обнаруженные уязвимости помогают привлекать больше специалистов к проверке безопасности и поощряют ответственное раскрытие ошибок.

Поэтапное внедрение

Сначала размещают смарт-контракты с ограниченными возможностями и небольшими объёмами средств, а затем, по мере проверки надёжности кода, постепенно расширяют функциональность.

Контроль с помощью мультиподписи

Требование одобрения ключевых действий несколькими сторонами снижает риск возникновения единой точки отказа.

Несмотря на эти меры безопасности, уязвимости смарт-контрактов по-прежнему могут приводить к значительным убыткам. Пользователи должны осознавать, что взаимодействие со смарт-контрактами (особенно с новыми или неаудированными) сопряжено с рисками.

Экономика смарт-контрактов

Исполнение смарт-контрактов в блокчейн-сети требует оплаты. В Ethereum вычислительные операции оплачиваются комиссией, размер которой выражается в единицах газа (gas).

Эти комиссии служат нескольким целям:

Предотвращение спама: введение платы за транзакции позволяет предотвратить переполнение сети бесполезными транзакциями.

Вознаграждение валидаторов: комиссии за транзакции выплачиваются майнерам или валидаторам, обеспечивающим безопасность сети.

Распределение ресурсов: более сложные операции требу-

ют большего количества «газа», что обеспечивает эффективное использование ресурсов сети.

Стоимость газа колеблется в зависимости от нагрузки на сеть. В периоды высокой активности в сети стоимость газа может стать чрезвычайно высокой, что приводит к недоступности некоторых приложений на основе смарт-контрактов.

Это привело к развитию решений второго уровня и альтернативных блокчейн-сетей, которые обеспечивают более низкие комиссии и более высокую скорость обработки транзакций.

Разработка смарт-контрактов

Создание безопасных смарт-контрактов требует специальных знаний и внимания к вопросам безопасности. Обычно разработка включает следующие этапы:

Анализ требований

Определение требований к контракту и выявление нестандартных ситуаций и рисков безопасности.

Проектирование

Создание общей архитектуры и выбор подходящих шаблонов проектирования. К распространённым шаблонам относятся контроль доступа, механизмы обновления и аварийная остановка.

Реализация

Написание кода, например на Solidity для Ethereum или Rust для других платформ.

Тестирование

Проведение модульных, интеграционных и сценарных тестов. Во многих проектах используют также инструменты автоматического создания тестовых сценариев и формальной проверки свойств контракта.

Аудит

Перед развертыванием в основной сети код должен быть проверен внешними экспертами по безопасности.

Развертывание

Размещение контракта в блокчейне и проверка его работы.

Мониторинг

Постоянное наблюдение за поведением контракта, возможными уязвимостями и необходимыми улучшениями.

Решения второго уровня и смарт-контракты

Из-за высоких комиссий и ограниченной пропускной способности основных блокчейн-сетей появились решения второго уровня. Они обрабатывают часть операций вне основной цепочки, используя её для подтверждения результатов и обеспечения безопасности.

Такие решения позволяют проводить операции со смарт-контрактами дешевле и быстрее:

Каналы состояния: стороны обмениваются сообщениями вне блокчейна, а итоговое состояние фиксируют в основной сети.

Сайдчейны: независимые блокчейны, подключенные к основной сети через мосты.

Роллапы: объединяют множество операций и передают данные или подтверждения их результатов в основную сеть.

Эти подходы помогают сделать смарт-контракты удобнее для повседневного использования, хотя их свойства безопасности различаются.

Интероперабельность и межсетевые смарт-контракты

С появлением множества блокчейн-сетей растёт интерес к смарт-контрактам, способным работать на разных блокчейнах.

Межсетевые мосты помогают перемещать активы между блокчейнами и использовать ликвидность разных сетей.

Межсетевые протоколы позволяют смарт-контрактам одной сети инициировать действия в другой, создавая более сложные приложения.

Будущее смарт-контрактов

Технология смарт-контрактов продолжает быстро развиваться. Следующие тенденции определяют её будущее:

Усовершенствованные языки программирования

Новые языки программирования помогают упростить разработку безопасных смарт-контрактов и анализ их поведения.

Улучшенные инструменты разработки

Интегрированные среды разработки, тестовые фреймворки и инструменты отладки упрощают разработку смарт-контрактов.

Формальная верификация

Методы математического доказательства свойств программ становятся доступнее и находят более широкое применение при разработке смарт-контрактов.

Смарт-контракты с защитой конфиденциальности

Доказательства с нулевым разглашением и другие криптографические методы позволяют выполнять смарт-контракты в конфиденциальном режиме без раскрытия конфиденциальной информации.

Интеграция искусственного интеллекта

Исследователи изучают способы сочетать искусственный интеллект и машинное обучение со смарт-контрактами для создания более гибких автоматизированных систем.

Оценка проектов по смарт-контрактам

Если вы собираетесь использовать приложение со смарт-контрактами или инвестировать в такой проект, оцените несколько обстоятельств:

Прошел ли код аудит со стороны авторитетной компании, специализирующейся на безопасности?

Является ли код открытым и доступен ли он для проверки?

Как долго проект работает без серьезных проблем?

Существует ли механизм обновлений? Кто им управляет?

Что произойдет, если команда проекта исчезнет или с ней потеряется связь?

Как защищаются источники информации оракула и кто их

предоставляет?

Каковы экономические стимулы для всех участников?

Подготовка к следующей главе

Смарт-контракты позволяют перейти от ручного исполнения соглашений к выполнению правил, закреплённых в коде. Вместо того чтобы во всём полагаться на организацию-посредника, участники могут проверять программу и её исполнение.

Этот переход имеет далеко идущие последствия для того, как мы организуем экономическую деятельность, создаём организации и координируем масштабное сотрудничество людей.

В следующей главе мы поговорим о прозрачности и неизменяемости записей — ещё одном важнейшем свойстве блокчейна. Посмотрим, как оно помогает в управлении цепочками поставок, при голосовании и в других областях, где особенно важны проверяемость и подотчётность.

Понимание сути смарт-контрактов и принципа прозрачности позволит нам в последующих главах изучить конкретные отраслевые применения и увидеть, как эти технологии можно внедрять для решения реальных проблем.

Глава 4. Прозрачность и неизменяемость — записи, которым можно доверять

Представьте, что важные записи хранятся так, что изменить или удалить их крайне сложно, а проверить подлинность может каждый. Что вы можете проследить путь товара от производства до покупки или убедиться, что результаты выборов нельзя незаметно переписать.

Это не просто мечта. Блокчейн уже позволяет создавать системы с таким уровнем прозрачности и защиты записей.

Два ключевых свойства блокчейна — прозрачность и неизменяемость. Первое означает, что данные в публичном блокчейне доступны для просмотра. Второе — что однажды внесённую запись крайне сложно изменить или удалить.

Вместе эти свойства позволяют участникам проверять записи и обнаруживать попытки переписать историю операций.

Как работает неизменяемость

Неизменяемость не означает абсолютной невозможности исправить данные. Скорее, чем больше времени проходит после записи, тем труднее и дороже её изменить.

Вот как это работает:

Каждый новый блок содержит криптографический хеш

предыдущего. Подобно отпечатку пальца, этот хеш связан с содержимым блока и позволяет обнаруживать изменения.

Если кто-то попытается изменить данные в старом блоке, он тем самым изменит и хеш этого блока. Однако следующий блок уже содержит исходный хеш, поэтому такое изменение будет немедленно обнаружено.

Чтобы подделать старую запись, злоумышленнику пришлось бы изменить соответствующий блок, а затем пересчитать связанные с ним последующие блоки. Чем глубже блок в цепочке, тем сложнее такая атака.

В блокчейнах с алгоритмом доказательства работы, таких как Биткоин, злоумышленнику необходимо контролировать вычислительную мощность, превышающую совокупную мощность остальной части сети, чтобы успешно переписать историю.

По мере добавления новых блоков изменить старые записи становится всё труднее. Недавнюю транзакцию теоретически ещё можно отменить при определённых условиях, но переписать историю многомесячной давности чрезвычайно сложно.

Сила прозрачности

Прозрачность блокчейна устроена иначе, чем привычная нам открытость организаций. В традиционной системе мы доверяем тем, кто публикует сведения. Публичный блокчейн позволяет независимо проверить сами записи.

Рассмотрим следующие примеры:

Государственная отчётность: когда власти публикуют бюджетные данные, гражданам приходится полагаться на полноту этих сведений. При этом неудобные детали могут быть опущены, а выводы — представлены односторонне.

Прозрачность блокчейна: если данные записаны в публичный блокчейн, их можно проверить независимо от того, кто их опубликовал. Криптографические механизмы помогают убедиться, что записи не изменились.

Корпоративная отчётность: инвесторы анализируют финансовые отчёты компаний и полагаются на работу бухгалтеров и аудиторов. Однако отчёты не исключают ошибок или мошенничества.

Цепочки поставок: записи в блокчейне могут помочь покупателям проследить происхождение товара и проверить документы о его качестве и подлинности.

Такая проверяемость может повысить подотчётность организаций и укрепить доверие к информации.

Уровни прозрачности

Не все блокчейн-системы одинаково прозрачны. Существуют разные уровни открытости:

Публичные блокчейны

Публичные блокчейны, такие как Биткоин и Ethereum, открывают доступ к истории транзакций и активности сети. Это облегчает независимую проверку, но одновременно создаёт риски для конфиденциальности.

Частные блокчейны

В частных блокчейнах доступ ограничен уполномоченными участниками. Они могут совместно проверять записи, не раскрывая их широкой публике.

Сети с ограниченным участием

В некоторых блокчейнах любой может читать данные, но добавлять записи или участвовать в консенсусе разрешено лишь определённым участникам. Так сочетаются публичная проверяемость и контроль доступа.

Системы с нулевым разглашением

Криптографические методы могут позволять проверять определённые свойства транзакции, например её действительность, не раскрывая подробностей, таких как сумма или данные участников.

Прозрачность на практике

Рассмотрим несколько примеров того, как используется прозрачность блокчейна:

Отслеживание цепочки поставок

Традиционные цепочки поставок часто непрозрачны. Покупая товар, вы обычно не знаете, откуда поступило сырьё, в каких условиях его производили и можно ли доверять заявлениям об экологичности.

Блокчейн помогает фиксировать путь товара по этапам:

Сырьё: источник материалов, сертификаты качества и сведения о воздействии на окружающую среду.

Производство: условия труда, потребление энергии и результаты контроля качества.

Транспортировка: способ, сроки и условия перевозки.

Розничная торговля: проверка подлинности и доступ покупателей к истории товара.

Например, Walmart использует блокчейн для отслеживания пути продуктов от фермы до магазина. При обнаружении загрязнения это помогает быстрее определить его источник и сократить объём отзываемой продукции.

Благотворительные пожертвования

Благотворительные организации тоже сталкиваются с вопросами доверия. Жертвователи хотят знать, на что пошли их деньги, но обычно располагают лишь общей информацией.

Благотворительные платформы на основе блокчейна могут обеспечить полную прозрачность:

Отслеживание пожертвований: запись времени переводов и сведений о жертвователях с учётом требований конфиденциальности.

Распределение средств: сведения о том, какие суммы направлены разным проектам и получателям.

Оценка результатов: фиксация измеримых итогов и их связи с конкретными пожертвованиями.

Административные расходы: разбивка затрат на работу организации и реализацию проектов.

Такая прозрачность укрепляет доверие доноров и может способствовать увеличению общего объёма благотворительных пожертвований.

Системы голосования

Традиционные выборы требуют доверия к избирательным комиссиям, техническим системам и подсчёту голосов. Избирателю трудно самостоятельно убедиться, что его голос учтён правильно, а итоговый результат точен.

Системы голосования на основе блокчейна стремятся сочетать прозрачность с защитой тайны голосования:

Регистрация: каждый голос фиксируется в виде записи, которую можно проверить.

Личная проверка: избиратель может убедиться, что его голос учтён, не раскрывая свой выбор другим людям.

Общественная проверка: независимые наблюдатели могут сверять записи и проверять итоговый подсчёт.

Защита от подмены: попытки изменить уже записанные голоса должны выявляться средствами проверки.

При этом блокчейн не снимает проблем безопасности голосования, сохранения тайны выбора и удобства системы для избирателей.

Реестры недвижимости

Учёт прав на недвижимость важен для экономики, но традиционные реестры не всегда защищены от ошибок, потери документов и мошенничества:

бумажные документы могут быть утеряны, повреждены или подделаны;

Централизованные базы данных могут быть взломаны или повреждены.

Передача собственности часто требует множества проверок, из-за чего сделки затягиваются и дорожают.

Реестр на основе блокчейна может обеспечить:

Историю владения: последовательные записи о прежних владельцах и сделках.

Защиту от мошенничества: криптографические доказательства делают подделку документов о праве собственности практически невозможной.

Упрощение передачи права собственности: автоматизированные проверки могут сократить сроки и расходы.

Глобальная доступность: возможность доступа к записям о собственности и их проверки из любой точки мира.

Ряд стран, таких как Эстония и Грузия, уже внедрили систему регистрации собственности на основе блокчейна и добились обнадеживающих результатов.

Образование

Поддельные дипломы — серьёзная проблема: их нетрудно купить в интернете, а проверка подлинности документов иногда занимает много времени.

Система проверки дипломов на основе блокчейна может помочь решить эту проблему:

Защита от подделок: криптографическая подпись помогает отличить подлинный диплом от фальшивого.

Быстрая проверка: работодатели могут проверить происхождение диплома без обращения в выдавшее его учебное заведение.

История обучения: записи о квалификации можно собирать из разных учебных заведений.

Контроль со стороны выпускников: владелец диплома решает, кому предоставить доступ к своему сертификату.

Массачусетский технологический институт (MIT) уже опробовал дипломы на основе блокчейна, а несколько других университетов также изучают возможность внедрения аналогичных систем.

Проблемы прозрачности

Прозрачность полезна, но у неё есть и свои ограничения:

Конфиденциальность

Полная открытость данных может противоречить требованиям защиты персональной информации, финансовых операций и коммерческой тайны.

Для защиты конфиденциальных данных можно использовать несколько подходов:

Доказательства с нулевым разглашением, позволяющие проверять утверждения, не раскрывая самих данных.

Блокчейны с защитой конфиденциальности, скрывающие детали транзакций при сохранении возможности проверки.

Гибридные системы, в которых публично доступна только часть сведений, а остальные данные защищены.

Информационная перегрузка

Избыточная открытость тоже может мешать. Человеку без технической подготовки трудно разобраться в исходных данных блокчейна и выделить главное.

Эффективная система прозрачности требует:

удобного для пользователя интерфейса, четко представляющего информацию;

Инструментов поиска и фильтрации, помогающих быстро находить нужные сведения.

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.