
Оглавление

Предисловие	5
Введение	9
Глава 1. Обзор технологии блокчейн	13
Глава 2. История развития блокчейна	41
Глава 3. Какие бывают блокчейны и где они применяются	61
Глава 4. Блокчейн как цифровой реестр	87
Глава 5. Блокчейн для применения умных контрактов и децентрализованных приложений	117
Глава 6. Блокчейн как основа для краудфандинга — ICO	149
Глава 7. Как финансируются блокчейн-проекты	185
Глава 8. Решения, которые делают блокчейн эффективнее	203
Глава 9. Время экспериментов пройдет. В каких областях блокчейн найдет применение	237
Заключение	259



Предисловие



Блокчейн продолжает развиваться за пределами криптовалют. По данным ежемесячного журнала *Rising blockchain*, технология распределенного реестра нашла применение еще в 24 отраслях. Мы с Яном Койфманн написали эту книгу, чтобы поделиться опытом, накопившимся за время работы в блокчейн-индустрии. Нам как непосредственным участникам и свидетелям развития технологии блокчейна важно рассказать о многолетних наблюдениях, чтобы избавить читателей от иллюзий, созданных информационным шумом.

На протяжении четырех лет я занимался контент-маркетингом по заказу финтех- и блокчейн-стартапов. С большинством компаний сотрудничал от имени коммуникационного агентства при блокчейн-платформе Waves, в котором работал главным редактором. Я изучил продукт и бизнес-модель каждого проекта: 50% обладали прорывными идеями, но туманными перспективами выхода в прибыль. Эти компании использовали ICO как инструмент проектного финансирования и вместе привлекли более \$80 млн. В данной книге я делюсь выводами, сформулированными мною благодаря опыту работы с 30 блокчейн- и финтех-компаниями.

Я рассматриваю эволюцию блокчейна в масштабах мира, а не только российского рынка. Помимо работы в коммуникационном агентстве я три года выпускал

ежемесячный «Дайджест мировых финансовых технологий», который создал в январе 2016 года. В эту книгу вошли результаты исследования, проведенного мною в процессе ежемесячного мониторинга и анализа событий мировой блокчейн-отрасли.

В ноябре 2017 года я вошел в состав участников Экспертного совета по законодательному обеспечению развития финансовых технологий при Госдуме РФ. Вместе с блокчейн-разработчиками, венчурными инвесторами, юристами, топ-менеджерами банков и госслужащими обсуждал способы регулирования ICO и криптовалютного рынка. Содержание Федерального закона «О цифровых финансовых активах», принятого Госдумой в первом чтении в мае 2018 года, сильно отличалось от рекомендаций представителей криптоиндустрии. Этот опыт помог мне рассмотреть будущее блокчейна в связке с законотворческим процессом.

В этой книге мы с Яном делимся собственным видением эволюции блокчейна и подвергаем сомнению распространенную классификацию поколений данной технологии. Вы узнаете, каких результатов уже удалось достичь благодаря блокчейну, о существующих проблемах развития этой прорывной технологии и о том, какие усовершенствования необходимы для дальнейшего ее прогресса.

Подготовка книги была бы невозможна без участия технического редактора и консультанта Николая Ратькова. Его экспертиза в IT и глубокое понимание устройства блокчейна позволили взглянуть «под капот» и оценить работоспособность технологии.

Особое внимание мы с Яном уделили блокчейну как технологии, способствовавшей феноменально быстрому и не регулируемому законом обогащению участников

«криптовалютной золотой лихорадки», пик которой пришелся на 2017 год.

Александр Табернакулов



Дорогие читатели, последние годы в мировом сообществе наблюдается повышенный интерес к блокчейну. Предприниматели пытаются внедрить в свой бизнес эту технологию, не понимая, что она необходима не в каждом бизнес-процессе.

При написании этой книги я использовал свой 18-летний опыт работы ведущего специалиста в сфере формирования и использования вычислительной техники в информационных системах и инновационных технологиях в различных бизнес-областях. Объединив знания с опытом моего друга Александра Табернакулова, мы подготовили книгу, которая, надеюсь, поможет применить блокчейн на практике.

В нашей книге мы рассказываем о технологии распределенного реестра, об актуальности и перспективах, а также о технических особенностях блокчейна за пределами криптовалют.

Мы не преподносим блокчейн как идеальную технологию, а рассматриваем ее преимущества и недостатки. В отличие от многочисленных сборников публичных заявлений вперемешку с компиляциями чужих статей наша книга предлагает читателю разносторонний анализ развития технологии с 2008 года.

Ян Койфманн



Введение

1 ноября 2018 года платежная сеть Bitcoin отметила юбилей. Десять лет назад некто под псевдонимом Сатоши Накамото опубликовал статью «Bitcoin: A Peer-to-Peer Electronic Cash System» («Биткоин: система электронной пиринговой наличности»), описывающую электронную валюту нового поколения. Юбилей отметил не только биткоин. Самая известная и лидирующая по капитализации криптовалюта принесла с собой технологию распределенного реестра — блокчейн. Его возможности за 10 лет вышли далеко за пределы операций с биткоинами и альткоинами. Блокчейн не только открыл новые перспективы, но и стал причиной массового помешательства, острых конфликтов и многомиллионных афер. В этой книге мы расскажем о причинах популярности технологии и результатах ее развития.

Творение Сатоши Накамото открыло миру широкие возможности:

- доказуемую неизменяемость данных,
- прозрачность операций,
- безвозвратность транзакций,
- поддержание работы сети ее участниками.

Возможности блокчейна Bitcoin развили другие платформы, такие как Ethereum, NEO, EOS, Lisk и Waves. Эти распределенные реестры пригодились не только для операций с криптовалютами, но и для создания государственных баз данных, систем цифровой идентификации, регистрации прав интеллектуальной собственности и бухгалтерского учета.

В 2014 году Виталик Бутерин представил Ethereum — первую блокчейн-платформу смарт-контрактов. Умные контракты стали связующим звеном между распределенными реестрами, криптовалютами, различными информационными системами и приложениями.

2017 год заслуживает названия «криптовалютная золотая лихорадка». Сверхприбыли и появление первых биткоиновых миллиардеров создали ажиотаж и превратили в трейдеров даже тех, кто до этого не воспринимал криптовалюты всерьез. В декабре 2017 года биткоин стоил \$20 000, а эфир — \$1400. Количество запросов «биткоин» в «Яндексе» достигло 8,5 млн.

В это время компании привлекали аномально легкие деньги благодаря криптовалютному краудфандингу — ICO. С его помощью стартапы, у которых не было ничего, кроме идеи, за считанные дни, а иногда и за несколько минут собирали миллионы долларов. Эта инвестиционная аномалия была бы невозможна без блокчейн-платформ, создавших фундамент для ICO.

Разбогатевшие на растущем рынке владельцы криптовалют без сомнений вкладывали биткоины и альткоины в любые стартапы, которые выглядели перспективными. Дошло до того, что ICO стали противопоставлять венчурному капиталу. Средства доставались настолько легко, что криптовалютным краудфандингом вскоре заинтересовались и мошенники.

Происходящее привлекло внимание регуляторов со всего мира. Флагманом выступила SEC — Комиссия по ценным бумагам и биржам США. Американский регулятор приступил к юридическому оформлению ICO и грозил уголовной ответственностью основателям стартапов, нарушающим его требования.

В марте 2018 года консалтинговая компания Satis Group LLC опубликовала исследование, согласно которому около 81% ICO-проектов обладали признаками мошенничества, 6% завершились провалом, 5% прекратили существование. Компании, которые успешно провели ICO и попытались выполнить обязательства перед инвесторами, поняли, что деньги — это еще не всё. Оказалось, что вложенные миллионы долларов вовсе не гарантируют успех продукта и выход в прибыль.

Появление платформ вроде NXT, Ethereum, Lisk, Waves, EOS и Tezos не только подогрело всеобщий ICO-ажиотаж. Они доказали миру, что блокчейн предлагает реестр для учета данных и среду для создания умных контрактов. Поэтому наша книга больше, чем просто анализ происходящего и экскурс в историю. Это авторский взгляд на будущее технологии.



Глава 1

Обзор технологии блокчейн

Blockchain



Технический прогресс ускоряется, и сейчас новые изобретения и решения появляются в темпе, немыслимом еще 50 лет назад. Важнейшую роль в этом процессе играет многократное ускорение обмена информацией, ставшее возможным благодаря развитию интернета и международных каналов связи.

За последний десяток лет разработка проектов командами, участники которых находятся в разных странах и никогда не видели друг друга в реальности, стала обычным делом. Вслед за интернетом надвигается следующая информационно-технологическая волна, одним из важнейших компонентов которой станет технология блокчейна, то есть цепочек блоков, которую все чаще называют революцией в хранении и распределенной обработке информации.

Менее 10 лет потребовалось для того, чтобы в мировой экономике появилось новое направление — пока еще молодое и только начинающее развиваться, но в которое уже вложены десятки, а возможно, и сотни миллиардов долларов.

Инвестиции в блокчейн-проекты делаются по всему миру, и не всегда они осуществляются в рамках классических инвестиционных процессов. Кроме того, значительная доля этих вложений происходит в цифровых

валютах, курсы которых изменяются гораздо быстрее, чем валют, выпускаемых центробанками. Поэтому произвести точный подсчет стоимости всех блокчейн-компаний и частных проектов невозможно.

Индустрия блокчейна все еще очень молода и на самом деле гораздо моложе, чем принято считать. Ее уже нельзя отождествлять с криптовалютами, а капитализацию отрасли вычислять по суммарной стоимости всех криптовалют и производных активов. Ведь все большее количество блокчейн-проектов разрабатывается без внутренней финансовой составляющей.

Возникновение блокчейна

Все началось 1 ноября 2008 года, когда была опубликована анонимная статья под названием «Bitcoin: A Peer-to-Peer Electronic Cash System», подписанная псевдонимом Сатоши Накамото. В ней были описаны теоретические основы создания электронной валюты нового поколения: децентрализованной, прозрачной, независимой от центробанков и регуляторов. Однако она не получила широкого распространения и в первые месяцы обсуждалась в академических кругах — среди криптографов, математиков и программистов.

Bitcoin, первый в мире блокчейн, являющийся воплощением концепции этой статьи, был запущен 3 января 2009 года и успешно функционирует уже почти 10 лет. За это время появилось несколько тысяч блокчейнов, как повторяющих Bitcoin с незначительными вариациями, так и мало похожих на своего прародителя.

Личность Сатоши Накамото до сих пор неизвестна, так как он отошел от разработки Bitcoin в 2010 году и никогда

не раскрывал ни своего имени, ни даже страны, в которой он живет. Исследователи и журналисты выдвигали множество версий о том, кто такой Сатоси, но ни одна из них не подтвердилась. Также не раз появлялись самозванцы, называющие себя Сатоси Накамото, но ни один из них не смог привести достаточных доказательств для подтверждения своих притязаний. На сегодняшний день общественность, вероятно, примет только один способ подтверждения личности Сатоси: владение биткоинами, добытыми им в 2009–2010 годах. Сатоси приписывают капитал размером более миллиона биткоинов, которые до сих пор ни разу не приходили в движение, за исключением нескольких тестовых транзакций, отправленных для доказательства работоспособности блокчейна. В частности, первую в истории транзакцию в блокчейне на сумму 10 BTC Сатоси отправил известному криптографу Гарольду (Хэлу) Финни, который активно участвовал в дискуссии по созданию теоретических основ Bitcoin.

Однако, хотя вся слава создания Bitcoin как первого в мире работоспособного блокчейна, бесспорно, принадлежит Сатоси Накамото, блокчейн появился не как обособленное открытие, возникшее ниоткуда, на пустом месте. По сути, блокчейн представляет собой результат обобщения нескольких направлений развития информационных и финансовых технологий, объединенных прозрением Сатоси Накамото, кто бы он ни был. Среди технологий и решений, на основе которых появились Bitcoin и блокчейн, обычно называют:

1. Виртуальную денежную систему BitGold, созданную в теории криптографом Ником Сабо еще в 1998 году — более чем за 10 лет до появления Bitcoin. BitGold так и не была реализована на практике,

но ее концепция в некоторых аспектах работы децентрализованной платежной сети почти идентична Bitcoin. Ника Сабо не раз «возводили на пьедестал», объявляя, что он и есть Сатоши Накамото, но сам Сабо отрицает это. Ему же принадлежит и авторство термина «умный контракт» (smart contract). Умный контракт был воплощен с помощью криптовалют и еще много раз встретится в этой книге.

2. Метод доказательства работы Proof-of-Work, созданный криптографом Адамом Бэком в 2003 году для защиты от спама в сервисе электронной почты HashCash. В системе HashCash пользователю для отправки электронного письма было необходимо выполнить определенный объем вычислений на своем компьютере. Это избавляло систему от массовых рассылок, которые чаще всего являются коммерческим или вредоносным спамом. Метод Proof-of-Work был использован в блокчейне Bitcoin для процесса подтверждения блоков транзакций, одновременно обеспечивающего эмиссию новых монет.
3. Криптографию открытого ключа, появившуюся еще в прошлом веке для обеспечения безопасности электронных коммуникаций, в том числе и финансовых транзакций. В Bitcoin используется криптография на основе эллиптических кривых (ECDSA), а отправка транзакций и создание адресов обеспечиваются с помощью классической ключевой пары, состоящей из закрытого (private) и открытого (public) ключей. Фактически владение биткоинами, как и токенами любого другого блокчейна,

аналогично владению закрытым ключом, необходимым для их отправки другому участнику сети.

4. Технологию хеширования, то есть получения уникального «отпечатка» исходного набора символов по определенному алгоритму. При этом теоретически невозможно получить одинаковый хеш для двух различных наборов символов (так называемая коллизия) или исходный набор символов из хеша. В блокчейне Bitcoin используется широко распространенный стандарт хеширования SHA2–256, в других блокчейнах часто применяются другие алгоритмы хеширования. С помощью дерева хешей формируется заголовок блока, а расчет хеша необходимой сложности является вычислительной задачей, выполнение которой необходимо для создания нового блока и генерации биткоинов (майнинга).
5. Технологию одноранговой сети распределенного хранения и передачи файлов BitTorrent. Метод распространения блоков в сети Bitcoin во многом повторяет распространение файлов с помощью торрентов. Кроме того, пиринговые (P2P) файлообменники также не имеют единого управляющего центра, за исключением исходного контента и файла торрента.

С каждым годом индустрия блокчейна становится все более зрелой, и многие новые проекты создаются с учетом выявленных проблем эксплуатации первопроходцев, таких как Bitcoin и Ethereum.

Кроме термина «блокчейн» также часто используется словосочетание «распределенный реестр» (distributed ledger). На самом деле между ними существует некоторое

концептуальное различие, так как распределенный реестр более широкое понятие. Можно даже сказать, что блокчейн — частный случай распределенного реестра. В рамках государственных и корпоративных проектов часто создаются распределенные реестры не с одноранговой, а с иерархической структурой, где некоторые узлы обладают более высоким уровнем полномочий и способны влиять на работу всей сети и принимать решения без поддержки большинства. Более подробно типы блокчейнов будут рассмотрены в главе 3.

Как работает блокчейн

Классический блокчейн во многом подобен существующим электронным платежным системам (ЭПС) и межбанковским сетям передачи финансовых сообщений (таким как SWIFT), но имеет ряд отличий в методах передачи информации и управления.

Узлы такого блокчейна, называемые кошельками (wallets), представляют собой аналоги банковских счетов, точно так же адрес в сети Bitcoin аналогичен номеру счета клиента в банке или идентификатору банка в системе SWIFT. Кошелек блокчейна — это экземпляр программного обеспечения для доступа к блокчейну и операций в нем. Кошелек может быть запущен практически на любом электронном устройстве с операционной системой, включая сервер, ПК, ноутбук или смартфон.

Кошелек блокчейна имеет сходство с онлайн-банкингом, который обеспечивает доступ к деньгам на банковском счете, однако пользователь блокчейна обладает единоличным и полным контролем над своими деньгами и может самостоятельно завести любое количество

кошельков, не предоставляя свои персональные данные и документы какой-либо организации. В то же время за все действия пользователя с кошельком отвечает только он сам, и все технические и юридические проблемы ему придется решать самостоятельно.

В блокчейне обращаются виртуальные учетные единицы, которые могут использоваться в качестве денег или выполнять определенные технические функции. В системе Bitcoin эти единицы получили одноименное название — биткойн (bitcoin, BTC — от англ. bit — минимальная единица информации и coin — монета). Поскольку биткойн задумывался как электронный эквивалент золота, по аналогии с металлическими наличными деньгами денежные единицы криптовалют обычно называют монетами, в то время как для нефинансовых блокчейнов стал применяться более широкий термин «токен», уже давно используемый в ИТ-системах и играх.

После усложнения блокчейн-систем и появления многоуровневых сетей сложилась более или менее устоявшаяся терминология:

- Учетные единицы, которые обращаются непосредственно в блокчейне, по-прежнему называют монетами (coins).
- Производные единицы, которые передаются внутри транзакций основного блокчейна, то есть используют его как транспортную среду, называются токенами.
- В случае обобщений токенами могут называться все виртуальные учетные единицы, обращающиеся в блокчейне, независимо от того, на каких уровнях они применяются.

В каждом кошельке имеется один или множество адресов — идентификаторов, на которые могут быть отправлены монеты (токены). Каждый адрес уникален и вероятность создания двух одинаковых адресов в разных кошельках практически равна нулю.

Перемещение монет (токенов) между кошельками в блокчейне удостоверяется уникальным закрытым ключом пользователя, с помощью которого он делает криптографическую подпись транзакции, таким образом удостоверяя свои полномочия как владельца кошелька. Закрытый ключ кошелька — единственное подтверждение владения токенами, и любой, кто получит копию этого ключа, будет иметь в блокчейне точно такие же возможности, как и владелец исходного кошелька. Поэтому для безопасности закрытых ключей необходимо обеспечить наивысший ее уровень из возможных.

Взлом сети Bitcoin извне сейчас практически не обсуждается, так как ее надежность подтверждена многолетним функционированием. Однако взломы индивидуальных кошельков или централизованных сервисов, оперирующих криптовалютами и токенами, исключать нельзя. Также кошелек может быть потерян после аппаратного сбоя или стихийного бедствия. Кошелек или закрытые ключи можно хранить в любом количестве экземпляров, если удастся обеспечить их безопасность. Если же будут потеряны все копии кошелька, то все связанные с ним биткойны навсегда останутся недвижимыми в блокчейне, так как закрытый ключ — единственный гарант возможности их перевода. Поэтому владелец узла (кошелька) должен полностью отвечать за сохранность своих активов.

Для передачи монет (токенов) в блокчейне производятся так называемые транзакции — списание средств

с одного адреса с зачислением на другой в финансовых блокчейнах или передача информационных сообщений с различным содержанием в блокчейнах других типов.

Каждая транзакция представляет собой составленное по установленным правилам финансовое сообщение, подписанное криптографическим ключом отправителя. В транзакции содержится сумма передаваемых монет (токенов), подпись отправителя и адрес получателя, созданный на основе его открытого ключа. Для возможности использования переданных в транзакции монет необходим закрытый ключ, парный с указанным в ней открытым ключом.

После передачи в сеть транзакция должна быть подтверждена, то есть записана в блок, являющийся частью блокчейна и распространяемый по всем узлам одноранговой сети Bitcoin. Блок содержит заголовок для передачи технической информации и список транзакций, в которых передаются пользовательские данные — платежные или любые другие операции.

Блокчейн состоит из последовательно соединенных блоков. В заголовок каждого последующего блока включается хеш предыдущего. Таким образом составляется неразрывная цепь. Разорвать или изменить ее возможно, только если пересчитать все заголовки блоков и собрать цепочку заново с точки разрыва. Для этого необходимо использовать вычислительные ресурсы, эквивалентные или большие, чем те, что были затрачены при сборке оригинальной цепи. Это значит, что безопасность классического блокчейна в долгосрочной перспективе зависит от суммарной вычислительной мощности. Наибольшим доверием пользуются блокчейны, для взлома которых требуются затраты ресурсов, несопоставимые с полученной выгодой.