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 Сатоси 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 Сатоси 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 считаные 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

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 Сатоси 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 Сатоси 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 Сатоси 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 — биткоин (bitcoin, BTC — от англ. bit — минимальная единица информации и coin — монета). Поскольку биткоин 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 биткоины 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 содержимым 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.

Майнинг — процесс эмиссии в блокчейнах

В основу экономической части концепции новой валюты Сатоси Накамото поставил свойства золота. Поэтому выпуск (эмиссию) монет в криптовалютах и подобных им блокчейнах принято сравнивать с добычей драгоценных металлов. Количество биткоинов ограничено, а получение одного биткоина сейчас требует затрат в несколько тысяч долларов, поэтому такая точка зрения более чем справедлива.

По аналогии с добычей полезных ископаемых процесс эмиссии монет (токенов) в классических блокчейнах называется майнингом (англ. mining — добыча полезных ископаемых).

Майнинг в блокчейнах осуществляют так называемые майнеры (англ. miner — шахтер), которые выполняют требуемые для создания новых блоков вычисления и получают за это вознаграждение в монетах того блокчейна, в котором они работают. Кроме того, майнерами называются специализированные устройства для майнинга, например ASIC-майнеры или GPU-майнеры.

В 2011 году был изобретен совместный майнинг в нескольких блокчейнах (merged mining), где вычисления выполняются по одному алгоритму хеширования. Например, наиболее известен совместный майнинг в блокчейнах Bitcoin и Namecoin (алгоритм хеширования SHA256), а также Litecoin и Dogecoin (алгоритм хеширования Scrypt).

Майнинг в блокчейне осуществляется с помощью стандартного или специализированного кошелька, аналогичного кошелькам всех остальных пользователей. Программное обеспечение кошелька предназначено для

выполнения набора правил протокола, установленного разработчиками каждого блокчейна, регулирующих в том числе и майнинг. Протокол обеспечивает согласованное выполнение пользователями блокчейна таких правил, как:

- способы сетевого соединения между узлами;
- прием, проверка и пересылка блоков и транзакций;
- максимальное количество монет в целом и вознаграждение за отдельный блок;
- средний интервал между блоками и механизм регулирования сложности;
- формат составления транзакции и заголовка блока и методы проверки их соответствия стандарту.

Также есть множество менее существенных правил, помогающих сделать работу блокчейна более быстрой, эффективной и безопасной.

Процесс майнинга состоит в подборе хеш-суммы содержимого блока, соответствующей заданным протоколом правилам, алгоритму хеширования и уровню сложности (параметр протокола, определяющий ресурсоемкость вычислений для создания блока). На основе этого хеша происходит сборка нового блока и включение в него транзакций, имеющихся в пуле памяти узла (mempool). Каждый последующий блок прицепляется к предыдущему с помощью хеш-суммы содержимого предыдущего блока, которая включается в заголовок нового. Именно эта последовательность сцепления блоков привела к появлению термина «блокчейн», то есть «цепочка блоков».

При добыче нового блока в нем автоматически создается транзакция, которая отправляет в кошелек майнера некоторое количество новых монет, до этого

не существовавших в блокчейне. Они называются наградой за блок (block reward). К награде присоединяются комиссионные сборы, выплачиваемые пользователями за включение их транзакций в блоки. В блокчейне Bitcoin (и большинства криптовалют) эта награда постепенно уменьшается, что приводит к замедлению эмиссии и вызывает увеличение спроса на монеты. В Bitcoin майнеры первоначально получали 50 BTC, а через каждые 210 000 блоков награда уменьшается вдвое. К 2018 году произошло уже два уменьшения награды, и на момент издания книги майнеры получают только 12,5 BTC и около 1–2 BTC комиссионных сборов. В 2020 году произойдет очередное уменьшение награды, после которого майнеры будут получать только 6,25 BTC за каждый блок, и так далее. Полностью эмиссия биткоинов закончится примерно в 2140 году, но уже задолго до этой даты основной статьей дохода майнеров должны стать комиссионные сборы.

Особенностью майнинга является то, что за единицу времени добывается в среднем фиксированное количество монет, не зависящее от количества и производительности работающих в сети майнеров. При росте суммарной производительности майнеров эмиссия монет на некоторое время ускоряется, но через определенное количество блоков происходит перерасчет сложности, и уже увеличившаяся производительность майнеров приводит к добыче стандартного количества монет. Если майнеры начинают отключаться от сети, процесс корректировки сложности происходит в обратном порядке.

В блокчейне Bitcoin перерасчет сложности происходит через каждые 2016 блоков, на что в среднем требуется две недели. Такой период был признан слишком длинным, так как вызывает достаточно резкие

колебания скорости эмиссии. В новых блокчейнах разработчики устанавливают более короткий период перерасчета сложности, в идеале она пересчитывается после каждого нового блока на основании усредненной скорости добычи последних нескольких сотен блоков.

Все вышеизложенное относится к большинству криптовалютных блокчейнов, применяющих метод Proof-of-Work. Несколько лет назад среди разработчиков блокчейнов появилось новое веяние — так называемый предварительный майнинг, или премайн (premine). Он состоит в том, что при запуске блокчейна в первом блоке задается мгновенное создание монет — сразу всех или доли от запланированного максимального их числа. Эти монеты оказываются в руках разработчиков, которые и занимаются их распределением. В таких блокчейнах влияние майнеров снижается и повышается уровень централизации, поэтому сообщество относится к ним с подозрением. В блокчейнах с альтернативными методами консенсуса (см. ниже) премайн уже стал общей практикой, и во многих из них все монеты (токены) создаются в первом блоке. Такая же практика используется при создании на блокчейнах производных активов — токены выпускаются разработчиками в полном объеме и впоследствии продаются пользователям.

Популярность майнинга росла вместе с распространением и ценой криптовалют. До середины 2010 года майнингом в сети Bitcoin занимались только Сатоси Накамото и немногочисленные энтузиасты, так как будущее криптовалюты было еще туманным и знали о ней не более нескольких тысяч людей во всем мире. И даже для большинства этих «ранних адептов» Bitcoin оставался всего лишь любопытным научным и социальным экспериментом.

В то время майнинг происходил на процессорах обыкновенных ПК или ноутбуков с помощью стандартного кошелька. Сложность майнинга увеличивалась достаточно медленно, поскольку он еще не стал коммерчески выгодным. Но в конце 2010 года новости о криптовалюте появились в крупных СМИ, начали открываться биржи, сервисы и магазины, принимающие оплату в криптовалюте. Цена биткоина активно росла, и майнинг стал экономически выгодным занятием.

После этого количество майнеров и производительность оборудования начали быстро увеличиваться, и уже в 2013 году появились фермы для промышленного майнинга. Сейчас суммарное энергопотребление майнеров всех ведущих PoW-блокчейнов можно сравнить с потреблением крупных европейских стран. В ближайшем будущем майнеры будут потреблять более 1% всей генерируемой в мире электроэнергии.

И еще один любопытный момент, наглядно показывающий ресурсоемкость майнинга. Несколько лет назад широко распространялась информация о том, что вычислительная мощность сети Bitcoin во много раз превышает возможности любого суперкомпьютера в мире. Однако это касается только скорости расчета хешей для формирования блоков. Поскольку майнинг биткоина происходит на специализированном оборудовании, которое не способно выполнять другие операции, подобные сравнения некорректны. И все же в майнинге сейчас задействованы огромные вычислительные ресурсы, которыми не может похвастаться ни одно из научных учреждений мира. Но GPU-майнеры работают на универсальном оборудовании, которое может использоваться для других задач. После того как во II квартале 2018 года прибыльность майнинга значительно снизилась, некоторые

крупные майнеры начали искать дополнительные источники дохода, предоставляя свои майнинговые фермы в аренду для проведения научных или инженерных расчетов, рендеринга видео и других задач, где требуются значительные вычислительные ресурсы.

Учитывая текущие вычислительные мощности, затрачиваемые на функционирование блокчейна Bitcoin, он остается самым безопасным блокчейном в мире и будет таковым до тех пор, пока не появятся и не будут проверены на практике кардинально новые методы обеспечения безопасности транзакций в блокчейне.

Особенности блокчейна

Блокчейн предложил миру новые возможности, и нашлись люди, которые оценили все перспективы их использования в реальной жизни. Поэтому технология, изначально задуманная исключительно как метод хранения истории финансовых транзакций в свободной от контроля и регулирования платежной системе, теперь предлагается к использованию в целом ряде направлений, в том числе не связанных с финансами.

Почему блокчейн пробудил интерес к себе у тысяч предпринимателей, разработчиков, ученых и энтузиастов? Чем эта технология вдохновила на отделение ее от криптовалют и разработку многочисленных проектов в государственном и корпоративном секторе?

Ключевые особенности блокчейна, выделяющие его среди всех ранее созданных аналогов:

- Децентрализация процессов хранения и обработки информации. Уникальность блокчейна в том, что

вся записанная в нем информация хранится у каждого участника сети в полном объеме. Иными словами, блокчейн существует до тех пор, пока функционирует хотя бы один из его узлов. При этом нагрузка на каждый отдельный узел сравнительно невелика, и с хранением всего блокчейна Bitcoin до сих пор справляется обычный офисный компьютер. Эта особенность блокчейна позволяет создавать географически распределенные сети без дорогостоящих дата-центров, централизованных систем хранения данных и резервного копирования, а также обеспечивать локальный доступ к данным для каждого узла сети.

- Доказуемая неизменяемость данных. С самого возникновения систем хранения информации на электронных носителях одной из главных проблем оставалась возможность ее порчи, искажения, подмены или подделки — случайно или по злому умыслу. Блокчейн, как неразрывная последовательность криптографически связанных блоков, позволяет в любой момент времени проверить всю последовательность добавления информации, таким образом исключая возможность внесения любых изменений в отдельные участки цепи без ее полной перестройки.

- Прозрачность операций. В классических одноуровневых блокчейнах все участники сети обладают одинаковыми правами. Они принимают на хранение всю информацию о происходящих в блокчейне операциях. Все содержимое транзакций в публичных блокчейнах доступно для чтения любыми участниками сети, но доступ к изменению чужих

данных невозможен без наличия соответствующего закрытого ключа. Таким образом, блокчейн располагает к абсолютной честности и открытости: каждый может видеть всю историю операций своих контрагентов и она никогда не стирается.

- Безвозвратность транзакций. В публичных блокчейнах транзакции невозвратны, то есть их нельзя вернуть в исходное состояние после подтверждения — включения в блок и формирования последующих блоков. Помимо прочего, это защита от мошенничества с платежами через банки и другие централизованные платежные системы. Возможны такие ситуации, когда мошенник дожидается отправки заказанного товара, а после этого отменяет уже совершенный платеж. В блокчейне подтвержденную транзакцию отменить практически невозможно, а вся история платежей между контрагентами хранится в открытом виде, что исключает необходимость взаимной сверки расчетов.
- Возможность анонимизации участников. Адреса в блокчейне представляют собой уникальные идентификаторы, состоящие из обезличенного набора символов, и блокчейн не содержит никакой информации, позволяющей однозначно связать кошелек с его владельцем. В то же время все платежи в блокчейне сохраняются навсегда, а большинству пользователей время от времени приходится взаимодействовать с биржами, магазинами и другими централизованными сервисами. Таким образом, активного пользователя, не предпринимающего специальных мер безопасности, возможно вычислить с помощью анализа истории

его транзакций. Но, если пользователь соблюдает комплекс мер конфиденциальности, вычислить его даже при использовании открытого блокчейна становится гораздо труднее. В последние годы начинают приобретать популярность блокчейны с повышенным уровнем конфиденциальности, позволяющие скрыть от посторонних ключевые параметры транзакций.

- Отсутствие необходимости в доверии. Пользователи блокчейна при совершении транзакций часто не знают друг друга, но децентрализованная обработка платежей исключает необходимость доверия между участниками сделки — если транзакция корректна и отправлена на правильный адрес, она дойдет по назначению. Однако получатель платежа может взять деньги, не выполнив своих обязательств. Для решения этой проблемы был разработан механизм децентрализованного посредничества, который называется эскроу (escrow). Для использования эскроу существуют транзакции с несколькими подписями (multi signature, или multisig). Чтобы получатель мог воспользоваться отправленными ему средствами, такую транзакцию, кроме отправителя, должен подписать посредник. Типичный случай применения эскроу в блокчейне — продажа товара в другой город за криптовалюту: после того, как покупатель сообщит о поступлении товара, посредник подписывает транзакцию и отправитель получает деньги. Посреднику, как правило, приходится отказываться от анонимности.
- Поддержание работы сети самими участниками. Пользователи блокчейна по праву могут считать

себя полноправными хозяевами своих токенов и другой хранимой в блокчейне информации. Но это накладывает на них и определенный уровень ответственности по поддержанию работы самого блокчейна, так как в публичных блокчейнах нет никакой организации, которая будет делать это вместо них. Как правило, каждый блокчейн поддерживается группой независимых разработчиков, не получающих прямой оплаты за работу. Все разработчики и другие активисты сообщества связаны с блокчейном экономическими или какими-либо личными интересами.

Ключевое отличие блокчейна от традиционных платежных систем состоит в том, что он не имеет единого управляющего центра, который может по своему усмотрению отправлять или задерживать транзакции, генерировать или уничтожать токены, а также осуществлять другие меры регулирования деятельности сети. Благодаря этому никто не может заблокировать транзакции в блокчейне, заморозить средства в кошельке или конфисковать их.

Децентрализация и отсутствие необходимости доверия между участниками в блокчейне достигаются с помощью системы децентрализованного управления, суть которой состоит в аналоге онлайн-голосования, постоянно проводимого всеми узлами сети. В разных блокчейнах это голосование имеет разные формы, но во всех публичных блокчейнах для формирования единственно правильной последовательности блоков необходимо достижение большинства или так называемого консенсуса.

Функционирование блокчейна невозможно без консенсуса, то есть процесса согласования вносимых

изменений. Консенсус в разных блокчейнах обеспечивается несколькими методами:

- Proof-of-Work (PoW) — доказательство работы. Вклад участника в достижение консенсуса определяется выполняемым им объемом вычислений. Метод PoW используется в Bitcoin и блокчейнах, созданных на его основе.
- Proof-of-Stake (PoS) — доказательство доли. Вклад участника в достижение консенсуса определяется долей токенов блокчейна, которыми он владеет, от их общего количества.
- Proof-of-Capacity, Proof-of-Weight, Proof-of-Spacetime — несколько сходных методов, используемых в системах распределенного хранения файлов на основе блокчейна. Эти методы основаны на доказательстве выделения узлами блокчейна ресурсов для хранения файлов или другой информации.
- Proof-of-Authority (PoA) — доказательство полномочий. Находящийся в разработке алгоритм консенсуса, который предполагается использовать в управляемых (частично централизованных) блокчейнах. В этом алгоритме транзакции, подписанные участниками с повышенными полномочиями, будут иметь преимущество.
- Byzantine Fault Tolerance (BFT) — условное название нескольких различных методов консенсуса, которые применяются в корпоративных платформах и частично централизованных проектах распределенного реестра — Hyperledger, Ripple, Stellar и т. д.

Метод Proof-of-Work считается наиболее надежным, но у него есть один существенный недостаток — высокая ресурсоемкость. В первые годы существования криптовалют высокое энергопотребление майнинга не принималось во внимание, но в 2017 году оно начало представлять серьезную проблему. Так, для добычи 50 BTC в январе 2009 года было достаточно 10 минут работы процессора ПК с энергопотреблением около 100 Вт или меньше. Для добычи 50 BTC в середине 2018 года нужны целые сутки работы более полумиллиона ASIC-майнеров, каждый из которых за это время потребляет 33 кВт·ч электроэнергии, то есть в сумме 1,5–2 ГВт·ч, что сравнимо с энергопотреблением достаточно крупного города. Именно необходимость огромного количества энергии, выпуска и поддержки целых парков специализированного оборудования привела к разработке альтернативных методов консенсуса.

На данный момент только некоторые варианты Proof-of-Stake по надежности обещают приблизиться к Proof-of-Work. В 2019 году Ethereum — второй блокчейн по капитализации — планирует переход на PoS. Этот метод консенсуса в собственных вариантах используют и запущенные летом 2018 года платформы EOS и Tezos.

Прочие методы консенсуса имеют специфические характеристики и по большей части пригодны для применения в специализированных блокчейнах.

Возможные уязвимости блокчейна

Несмотря на непревзойденную криптографическую защиту, на любой из блокчейнов могут быть проведены

атаки нескольких видов, поэтому необходимо рассказать о способах защиты от таких нападений.

Наиболее известный способ атаки на блокчейны криптовалют — так называемая «двойная трата» (double spending), то есть возможность потратить одни и те же монеты дважды. Для этого злоумышленнику необходимо отправить крупную сумму в качестве «правильного» платежа, а затем совершить аналогичную транзакцию на собственный адрес и добиться ее включения в блокчейн. В результате, если будет подтверждена вторая транзакция, получатель платежа увидит, что его транзакция исчезла, а реально совершена другая на неизвестный ему адрес. Такая атака может быть успешна в двух случаях:

1. Злоумышленник отправил вторую транзакцию до подтверждения первой, а получатель не дождался подтверждения в блокчейне. Это частный случай, основанный на неизбежной дискретности изменения состояний блокчейна — например, для Bitcoin среднее время между блоками составляет 10 минут. Все добросовестные операторы криптовалютных платежей просят своих клиентов дождаться хотя бы одного подтверждения транзакции. Такая атака не затрагивает работу других пользователей.

2. Злоумышленник обладает более чем половиной мощности хеширования в конкретном блокчейне и способен перезаписать цепочку из нескольких последних блоков, добытых им самим. В таком случае исчезнут все транзакции в замененных блоках, а вместо них появятся только те, что были подтверждены в блоках злоумышленника. Этот вид атаки называется «атака 51%» и опасен для всех