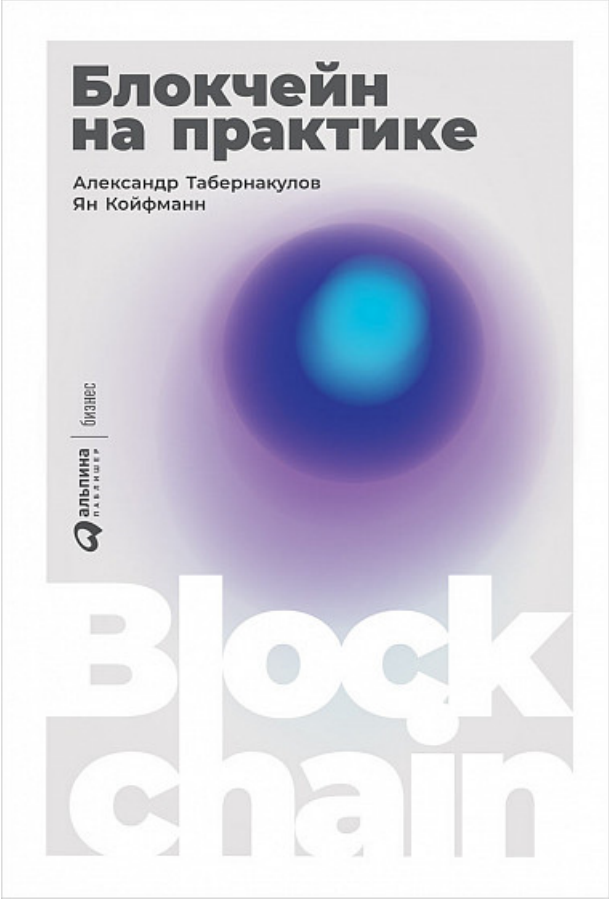
Александр Табернакулов,Ян Койфманн
Блокчейн на практике



Аннотация

Информационный шум вокруг блокчейна не стихает уже несколько лет. Благодаря этой технологии участники криптовалютной золотой лихорадки обогатились феноменально быстро и вне регуляции законом. Но шумиха в СМИ сформировала не совсем корректное представление о блокчейне. Возможности технологии, которую многие эксперты сейчас называют «новым интернетом», гораздо глубже. Она продолжает развиваться и нашла применение уже в 25 отраслях. Государственные услуги, авторское право, финансовые рынки, медицина, страхование, образование — это лишь часть направлений, где применяется блокчейн.

Александр Табернакулов,Ян Койфманн
Блокчейн на практике

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.

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 пользователей блокчейна. Атака 51% может быть применена только в малоизвестных блокчейнах, так как популярные блокчейны, подобные Bitcoin или Ethereum, достаточно хорошо защищены мощностями добросовестных майнеров.

Для предотвращения этого вида атак все поступающие в кошелек транзакции проходят проверку на возможность двойного расходования, и, если такая попытка зафиксирована, кошелек отвергает все транзакции, кроме первой. Но атаке 51% может воспрепятствовать только увеличение мощностей добросовестных майнеров.

Также попытка двойной траты может быть произведена путем проведения противоречивых транзакций на географически удаленных узлах блокчейна, однако она возможна только в случае достаточно длительной изоляции сегментов распределенной сети друг от друга, например, в случае аварии на международных магистральных каналах связи или в результате действий сетевых экранов государственного уровня, подобных китайскому «Золотому щиту».

В подавляющем большинстве ситуаций существующая система защиты блокчейнов, основанная на распределенном майнинге, успешно справляется с угрозами — за все время существования криптовалют не произошло ни одной успешной атаки 51% на популярные блокчейны. Однако во всех случаях двойная трата может быть проведена только со своими монетами — ни при каких обстоятельствах она не может дать доступа к чужим кошелькам.

Блокчейн в политике и экономике

Мало кто из нынешних крупных политиков, финансистов, ученых и бизнесменов еще не успел высказать свое мнение о криптовалютах, блокчейне и перспективах индустрии блокчейна в ближайшие несколько лет. Одни ожидают, что технология блокчейна произведет революцию, подобную интернету, другие сравнивают растущую непомерными темпами отрасль с пузырем доткомов, который вырос и лопнул на американском рынке в течение нескольких лет. Кто из них прав, мы узнаем по прошествии нескольких лет. Однако даже из «пузыря доткомов» родились компании, возглавляющие сейчас технологическую отрасль. То же самое может случиться и с нынешними блокчейн-стартапами. К слову, некоторые из них уже фактически перешли в разряд «единорогов», превысив рубеж капитализации миллиард долларов всего за несколько лет существования, хотя большая часть участников индустрии блокчейна до сих пор не котируется на фондовых биржах. Но так ли это важно на самом деле?

Одной из самых жарких тем дискуссий, сопровождающих становление отрасли блокчейна, остается экономическое обоснование ценности цифровых активов и возможность их встраивания в мировую финансовую систему. В этом споре как сторонники, так и противники криптовалют приводят множество убедительных аргументов. Здесь мы не будем пытаться установить истину, но приведем основные доводы сторон.

Противники криптоактивов заявляют, что децентрализованная денежная система не может существовать, так как:

1. Криптовалюты не обеспечены никакими реальными активами, не имеют внутренней ценности и их стоимость поддерживается только спекулятивным спросом;

2. Децентрализованная эмиссия означает, что ни одна организация не будет поддерживать их стоимость;

3. Криптовалюты не регулируются, поэтому никто не может защитить инвесторов от мошенников;

4. Контролировать операции с криптовалютами невозможно, поэтому они широко используются в противоправных целях;

5. Дефляционные деньги невозможно использовать в реальной экономике, так как они будут снижать экономическую активность и приведут к стагнации;

6. Необратимость изменений в блокчейне может привести к тому, что криптовалюты будут уничтожены при нахождении критической уязвимости в них самих или в базовых технологиях;

7. Блокчейн слабо масштабируется и не может обеспечить потребностей глобальной финансовой системы.

Однако и сторонники криптовалют выдвигают достаточно убедительные аргументы:

1. Криптовалюты обеспечены участием в отрасли десятков миллионов людей и многомиллиардными инвестициями в блокчейн-проекты.

2. Реальное использование криптовалют и их сообщество непрерывно растут во всем мире, что говорит о доверии людей к технологии.

3. Криптовалюты не замкнуты государственными границами и вскоре не будут нуждаться в обмене на другие активы для проведения расчетов.

4. Технология блокчейна обеспечивает криптовалютам значительное техническое превосходство над традиционными валютами в надежности и скорости проведения платежей.

5. Прозрачность операций в блокчейне упрощает защиту от мошенников и противоправного использования.

6. Криптовалютные системы не зависят от политических решений и цензуры.

7. Заложенный в протоколе ограниченный ресурс гарантирует отсутствие неограниченной эмиссии и защищает от инфляции.

На уровне правительств различных стран мира отношение к криптоактивам и подход к их регулированию значительно отличаются. Несмотря на попытки выработать единую позицию на уровне G20, ООН, FATF и других международных организаций, единого подхода в регулировании криптовалют и блокчейна в ближайшее время, очевидно, не появится.

Наиболее активно в этом направлении действуют правительства азиатских стран. В Японии с 1 апреля 2017 года криптовалюты приравнены к иностранным валютам и рассматриваются как законное средство платежа, что позволило бизнесу принимать их наравне с традиционными валютами. Японский криптовалютный рынок, бесспорно, можно

считать крупнейшим в мире. Однако японские биржи криптовалют подвергаются достаточно жесткому регулированию и требуют обязательной идентификации пользователей. Южная Корея после предпринятых в 2017 году шагов к серьезным ограничениям изменила курс и сняла запреты на торговлю криптовалютами и ICO. Однако в Китае и Индии все еще имеются жесткие ограничения, и криптовалютного бизнеса в них практически не существует.

Страны-офшоры, напротив, до предела смягчают политику в отношении криптовалют и стараются привлечь к себе блокчейн-стартапы: Мальта, Сингапур, Гибралтар, Кипр, Гонконг и другие небольшие государства предоставляют криптовалютному бизнесу наилучшие условия, в результате чего многие компании переместились в эти юрисдикции.

Западные государства, в том числе страны Евросоюза, США, Канада, Австралия и другие, все еще сохраняют выжидательную позицию и очень осторожно ведут разработку инструментов регулирования, тем не менее проводя жесткую борьбу с экономическими преступлениями, в которых используются криптовалюты.

Запрет на деятельность с использованием криптоактивов действует в шести странах: Бангладеш, Боливии, Индонезии, Киргизии, Непале и Эквадоре, а вот единственной государственной криптовалютой остается венесуэльская петро, обеспеченная добытой нефтью.

В Государственной думе Российской Федерации на момент издания книги обсуждаются три законопроекта, касающиеся криптовалют и блокчейна: «О цифровых финансовых активах», «О привлечении инвестиций с использованием инвестиционных платформ» и «О цифровых правах». Вероятно, в них еще будут вноситься изменения, но уже можно сказать, что их принятие в той или иной степени наконец легализует операции с криптоактивами и даст возможность российским стартапам не задумываться о выборе юрисдикции.

Глава 2

История развития блокчейна

Количество существующих блокчейн-проектов не поддается точному подсчету, так как многие из них рождаются и умирают в течение нескольких месяцев или даже недель, и далеко не все заслуживают упоминания. Но можно с уверенностью сказать, что живых проектов несколько тысяч. Среди них и крупнейшие криптовалюты, и широко известные компании с миллиардной капитализацией, и небольшие частные инициативы, которые разрабатывает несколько человек без внешнего финансирования.

Чтобы внести какую-то ясность в хаос и научиться ориентироваться в новой отрасли, необходимо классифицировать и разобрать по определенным критериям тысячи стартапов.

Если рассмотреть подробнее, то окажется, что многие из них прекрасно обошлись бы без блокчейна и пришли в новую отрасль исключительно в поисках быстрых инвестиций или просто потому, что это считается модным и перспективным.

Для того чтобы понять, насколько уникальна идея конкретного проекта и способен ли он достичь успеха, необходимо определить его технический уровень и к каким типам блокчейн-проектов его можно отнести.

Краткая хронология развития блокчейн-проектов

Прежде чем говорить о какой-либо преемственности в отрасли блокчейна, следует обозначить основные вехи в ее развитии, связанные с появлением наиболее значимых проектов и технологий.

Как известно, Bitcoin — первое в мире воплощение блокчейна — был запущен 3 января 2009 года, но достаточно долго оставался в безвестности. Причем децентрализованное создание и поддержка равноправными пользователями неизменяемой распределенной цепочки блоков были задуманы только как метод хранения данных, необходимый для обеспечения надежности функционирования системы цифровых денег. О блокчейне как отдельной технологии заговорили через несколько лет, уже после первого бума криптовалют, завоевавших спекулятивные рынки и напугавших регуляторов своей неуправляемостью и анонимностью.

Bitcoin, основанный на открытом исходном коде, недолго оставался единственным в мире блокчейном. Уже в середине 2010 года был запущен его первый форк под названием Namecoin. Он был призван обеспечить работу независимой системы доменных имен, способной в будущем заменить централизованную DNS, которая основана на иерархической модели серверов, в конечном итоге подчиненной правительствам стран, где расположены основные серверы. Первый форк Bitcoin оказался также первым нефинансовым блокчейном, основная функция которого заключалась не в передаче ценности и обеспечении платежей.

Однако концепция оказалась незрелой. Изначально не удалось реализовать защиту от спама и сквоттинга, в результате чего Namecoin сейчас фактически не функционирует, хотя и продолжает котироваться на биржах и сохраняет достаточно надежную сеть. Его место может занять запущенный в 2013 году блокчейн Emercoin, обладающий более совершенной защитой и широкой функциональностью, но и он способен устареть раньше, чем найдет свою нишу на рынке. Так, сервис децентрализованной службы доменных имен работает на блокчейне Ethereum и планируется к запуску на многих новых платформах децентрализованных приложений, таких как EOS, NEO, Cardano и другие. Там он реализуется в виде достаточно простого приложения.

В конце 2010 — начале 2011 года появилось еще несколько форков, основанных на кодовой базе Bitcoin с небольшими вариациями. Из них до сих пор широко известна криптовалюта Litecoin, основанная сотрудником Google — китайцем Чарли Ли. Этот блокчейн с момента создания в 2011 году позиционируется как «цифровое серебро» и не планирует оспаривать лидирующие позиции старшего брата, оставаясь тестовым полигоном для наиболее значимых нововведений. Litecoin предлагает вчетверо большее количество монет и ускоренную в четыре раза генерацию блоков, в остальном не имея существенных отличий от Bitcoin.

Основной идеей Litecoin было внедрение альтернативного алгоритма хеширования, чтобы остановить распространение майнинга на видеокартах, оставив эмиссию криптовалюты уделом центральных процессоров для обеспечения максимальной децентрализации. Однако замысел Чарли Ли провалился, и вскоре лайткоины стали также добываться с помощью видеокарт, а позже и на специализированных ASIC-майнерах. Сейчас уже существуют десятки альтернативных алгоритмов хеширования для PoW-блокчейнов, постепенно проходящих те же стадии: CPU-GPU-ASIC.

Появившаяся в конце 2010 года криптовалюта Peercoin впервые предложила альтернативный метод консенсуса — Proof-of-Stake (PoS). Он исключает необходимость все

более масштабного потребления аппаратных ресурсов. Создание и подпись новых блоков гарантируются не выполнением определенного объема вычислений, а наличием в кошельке как можно большей суммы монет (токенов). Несмотря на ощутимые достоинства в виде экономичного майнинга и отсутствия «гонки мощностей», PoS имеет и ряд недостатков, включая более широкие возможности для атаки 51% и значительную зависимость надежности сети от «китов» — крупных держателей токенов блокчейна.

Этот вид консенсуса, сначала вызвавший волну критики, обрел вторую жизнь в 2016–2017 годах, и сейчас на нем действуют уже несколько крупных проектов. Сегодняшние реализации PoS гораздо более надежны и обеспечивают пропускную способность блокчейна до десятков тысяч транзакций в секунду, чего так и не удалось реализовать с помощью PoW (без учета многоуровневых систем).

Альтернативные блокчейны очень долго оставались в тени Bitcoin. Первый настоящий расцвет альтернативных криптовалют (альткоинов) начался в 2013 году, когда биткоин приобрел всемирную известность и в отрасль устремились миллионы людей со всего мира, а количество криптовалютных проектов начало исчисляться сотнями. Однако большинство альткоинов того времени создавалось в целях быстрой наживы или в качестве эксперимента, поэтому многие из них скоро угасли, просуществовав некоторое время в качестве инструментов для биржевых спекуляций.

Среди альткоинов 2013 года следует упомянуть целую серию «псевдонациональных» криптовалют — на самом деле исключительно частных проектов, никак не взаимодействовавших с правительством. Первый и самый нашумевший из этих форков — Auroracoin, который планировалось распространять среди жителей Исландии. Но все эти проекты были забыты уже через несколько месяцев.

Летом 2013 года американец Джексон Палмер запустил шуточную криптовалюту Dogecoin, символом которой стала собака породы сиба-ину. Dogecoin был копией Litecoin, но с более частыми блоками, которые следовали через одну минуту, и ограничением миллиард монет. Шутка оказалась удачной, Dogecoin стал весьма популярен и несколько лет служил одной из самых востребованных криптовалют для микроплатежей. Он до сих пор часто используется трейдерами, которым нужно быстро переслать монеты с одной биржи на другую, но код Dogecoin почти не обновляется, и его использование продолжает снижаться. Позже децентрализованные приложения с игровой подоплекой возродились на платформе Ethereum, доставив немало проблем разработчикам из-за чрезвычайно высокой активности пользователей. Самая известная игра этого типа — «Криптокотики» (CryptoKitties).

В июле 2013-го на базе Bitcoin была впервые реализована платформа производных криптоактивов (токенов) под названием Mastercoin (в марте 2015 года переименованная в Omni Layer). Она основывалась на технологии, подобной не получившей признания концепции «цветных монет» (colored coins), по сути — транзакций со специальными текстовыми метками. С помощью информации, переносимой этими метками, можно было проводить идентификацию и учет транзакций второго уровня, использующих блокчейн Bitcoin только как транспортную сеть. Вследствие ограничений протокола и появления специализированных платформ проект не имел большого успеха, но на Omni Layer до сих пор базируется проект Tether, выпускающий токенизированный доллар (USDT) и евро (EURT). Капитализация токенов Tether в сентябре 2018 года приблизилась к $2,5 млрд.

В ноябре 2013 года запустился проект NXT (англ. next — следующий), первый, названный «биткоин 2.0». Именно с него началась мода делить блокчейны на поколения. NXT создала группа независимых разработчиков, собравшая через кампанию краудфандинга 21 BTC — на тот момент менее $10 000. Ее же можно считать и одним из первых в истории криптовалют ICO (хотя пальму первенства обычно отдают описанному выше Mastercoin, который собрал гораздо более значительную сумму — почти 5000 BTC). NXT отличался тем, что не являлся надстройкой или доработанным клоном Bitcoin — его код писали с нуля. Проект выпустил сразу все токены (1 млрд, распределенные между разработчиками и первыми инвесторами, и использовал консенсус PoS. При этом майнеры не производили

новых монет, а только получали фиксированную плату за транзакции. Разработчики NXT создали первую многофункциональную платформу в истории криптовалют, на которой можно было выпускать собственные активы и торговать ими через встроенную в кошелек биржу, а также обмениваться сообщениями. Была предпринята и попытка создания магазина цифровых товаров, продаваемых за криптовалюту.

Несмотря на перспективность и ряд новых идей, NXT не удалось достичь коммерческого успеха — недоверие вызвала анонимность разработчиков и непрозрачное распределение токенов. В результате команда потеряла драгоценное время и вскоре была обойдена конкурентами, предлагавшими большую прозрачность и не жалевшими денег на маркетинг. Многие идеи впоследствии использовались в других проектах многофункциональных криптовалютных платформ. NXT существует до сих пор, в 2017 году проект запустил новую сеть под названием Ardor, но его капитализация находится за пределами топ-50 по версии портала Coinmarketcap, а популярность в сообществе оставляет желать лучшего.

2014 год, ознаменовавшийся крупными провалами курса и идейным кризисом для криптовалют, не был отмечен техническими прорывами, но именно тогда появились новые идеи, позже сформировавшие полноценную индустрию блокчейна.

Одной из платформ, зародившихся в 2014 году, стала Ethereum, которую сейчас принято считать образцом блокчейна 2.0. В Ethereum была реализована виртуальная машина для децентрализованного исполнения умных контрактов, или смарт-контрактов, а также первый эффективный механизм краудфандинга на блокчейне, позже названный ICO. Команда Ethereum под руководством Виталика Бутерина и Гэвина Вуда в июле–августе 2014 года провела успешную кампанию краудфандинга, собрав более 31 500 BTC. Блокчейн Ethereum запущен в июле 2015 года и, по данным на 21 января 2019 года, занимает третье место по капитализации. На нем основано уже несколько сотен действующих проектов. (Подробнее о платформе Ethereum и технологии умных контрактов см. в главе 5.)

Следует также отметить платформу Bitshares, запущенную командой под руководством Дэна Ларимера в июле 2014 года. Она представляет собой прообраз децентрализованной биржи и платформы производных криптоактивов, в котором более успешно реализованы идеи разработчиков NXT. В разработке Bitshares участвовал один из создателей Ethereum — Чарльз Хоскинсон, а финансировал проект китайский криптомагнат Ли Сяолай. В процессе разработки этого блокчейна появился доработанный вариант консенсуса DPoS — Delegated Proof-of-Stake, ныне применяемый в большинстве запускаемых блокчейн-платформ, выбравших консенсус PoS. В 2015 году был выпущен новый релиз Bitshares под названием Graphene, по утверждениям разработчиков, способный обрабатывать до 100 000 транзакций в секунду. Это больше, чем может обрабатывать любая из существующих платежных систем. Сам Дэн Лаример сыграл ключевую роль в запуске еще двух популярных блокчейн-проектов: социальной сети Steemit и платформы EOS.

Становление «блокчейна без биткоина»

С развитием криптовалютных платформ и появлением новых, все более отходящих от первоначального замысла Сатоси Накамото, стали появляться публикации, продвигавшие идеологию «блокчейна без биткоина». В 2014–2015 годах эта идеология стала крайне популярной среди политиков и бизнесменов, не понимавших, что делать с криптовалютами, но боявшихся опоздать на поезд инноваций. Споры о дееспособности блокчейна без внутренней передачи ценности продолжаются до сих пор, однако блокчейны прикладного характера, использующие чисто технические токены вместо встроенной криптовалюты, уже нашли применение.

К концу 2015 года государственный и корпоративный сектора начали проявлять усиливающийся интерес не столько к самим криптовалютам, сколько непосредственно к их базовой технологии — блокчейну. Именно тогда были сформированы первые блокчейн-консорциумы Hyperledger и R3, а в отрасль пришли и обосновались в ней такие технологические гиганты, как IBM и Microsoft. С каждым годом количество крупных

компаний, занявшихся разработками в области блокчейна, продолжает расти. В их число вошли и крупнейшие производители корпоративного ПО, такие как SAP и Oracle. В мае 2017 года был сформирован Enterprise Ethereum Alliance (EEA) для совместной разработки корпоративной версии Ethereum, в который входит более 200 компаний.

Растущая популярность блокчейна породила и повышенный спрос на блокчейн-специалистов, а также обозначила будущую сегментацию рынка. Разумеется, для малого бизнеса и транснациональных корпораций существуют совершенно разные ожидания от блокчейна, так же как и разные возможности их реализации. Один из главных вопросов, стоящих перед создателями блокчейн-проектов, звучит так: нужен ли собственный блокчейн или будет достаточно запустить децентрализованное приложение (DApp) на одной из существующих платформ? Плюсы и минусы каждого из подходов достаточно очевидны: собственный блокчейн дает больше гибкости и возможностей настройки под собственный бизнес, в то время как приложение на специализированной платформе значительно снижает издержки на R&D и порог входа в отрасль. Одно можно сказать с уверенностью: при наличии устойчивого спроса блокчейнов хватит на всех, так как выбор растет.

Кроме традиционных криптовалют и открытых платформ криптоактивов уже существуют не связанные с ними достаточно развитые блокчейн-платформы, такие как российская «Мастерчейн», Hyperledger, R3 Corda, Quorum от J. P. Morgan, Exonum от Bitfury Group и другие, предназначенные для выполнения практических бизнес-задач. Более подробно эти платформы будут описаны в следующих главах.

Поколения блокчейнов

В маркетинговых и рекламных материалах очень часто можно встретить такой термин, как «блокчейн 3.0», а летом 2018 года начали появляться проекты, причисляющие себя уже к блокчейнам поколения 4.0. Если доверять такой классификации, то блокчейны 1.0 и 2.0, очевидно, давно и безнадежно устарели. Что все это значит на самом деле и как соотносятся друг с другом все эти цифры?

Каких-либо общепринятых и тем более официально утвержденных стандартов классификации блокчейнов не существует, и, по сути, различные попытки ее создания происходят из субъективных мнений представителей различных проектов, блогеров и СМИ. Рассмотрим наиболее распространенные описания поколений блокчейнов.

1.0

К первому поколению (Blockchain 1.0), как правило, относят Bitcoin и другие классические криптовалюты. Они представляют собой децентрализованные платежные системы и предназначены для безопасной и бездоверительной передачи ценности, проще говоря, для прямых денежных переводов без участия посредников. Обычно в них обращается один внутренний токен (монета), и вся инфраструктура блокчейна строится вокруг обеспечения его безопасности и надежности. Подробно описывать блокчейны первого поколения нет смысла, поскольку они нужны только для сравнения с все более инновационными и прорывными проектами последних поколений.

2.0

С блокчейнами второго поколения несколько сложнее. Наиболее распространены два подхода. В первом случае к блокчейнам второго поколения относят те, в которых имеется возможность выпуска обособленных активов (токенов) поверх основного блокчейна. К таким платформам относятся, например, NXT/Ardor, Bitshares, Waves и другие.

Согласно второму подходу принадлежность к блокчейнам 2.0 означает возможность выполнения произвольного программного кода, как правило, смарт-контрактов или децентрализованных приложений (DApps). Это Ethereum, его форки и аналоги. Впрочем, некоторые авторы относят платформы смарт-контрактов уже к третьему поколению.

Таким образом, для блокчейнов 2.0 характерна двухуровневая структура: первый уровень — блокчейн как база данных и его токен как внутренняя утилитарная система оплаты (топливо). Второй уровень — пользовательские токены или приложения, до определенной степени обособленные друг от друга.

3.0

Определение блокчейна третьего поколения (Blockchain 3.0) еще более размыто. Активнее всего этот термин использовался во время продажи токенов проекта Cardano (ADA). Требования к блокчейнам третьего поколения созданы по большей части командой этого проекта и их последователями, поэтому остановимся на их формулировках. Итак, основные признаки, приписываемые Blockchain 3.0:

- Высокая масштабируемость. Под ней обычно имеется в виду пропускная способность базового блокчейна, измеряемая в тысячах транзакций в секунду, и интервал между сохранением состояний (блоками) в несколько секунд или даже меньше. Однако еще ни один блокчейн, заявивший о наличии таких возможностей, не подвергался нагрузочному тестированию в реальной обстановке.

- Взаимодействие с другими блокчейнами. Работы в этой области ведутся достаточно давно, но еще не достигли уровня технологической реализации. Обычно под таким взаимодействием подразумевается возможность прямого обмена токенами между блокчейнами или совершение транзакций в нескольких блокчейнах с авторизацией только в одном из них. Что интересно, первым популярным блокчейном с возможностью такого взаимодействия, вероятно, станет Bitcoin.

- Устойчивость к атакам. Самое неопределенное из требований, так как совершенного программного продукта не существует, а уязвимости обычно происходят от ошибок программного кода. Напротив, чем сложнее структуры, например многоуровневые блокчейны с возможностью выполнения произвольного кода, тем выше категории риска, которому они подвергаются. А проблемы безопасности блокчейнов первого поколения, такие как атака 51%, пока сохраняются и для всех последующих.

- Конфиденциальность пользователей и транзакций. Эта проблема активно обсуждается с самого появления Bitcoin, но до сих пор наиболее надежно конфиденциальность реализована именно в примитивных блокчейнах первого поколения, таких как Dash, Monero и Zcash.

- Внутреннее самоуправление. Под ним обычно понимается возможность независимого принятия решений с помощью всеобщего голосования пользователей или формирования надежного представительства. Однако блокчейны, о принадлежности которых к третьему поколению было заявлено их разработчиками, так и не предоставили существенно новых механизмов для реализации этого принципа. Методы голосования и децентрализованного принятия решений уже давно существуют и проверены в проектах предыдущих поколений — Dash, Emercoin, Bitshares (Steemit) и других.

Основная сложность состоит в том, что все указанные выше параметры не содержат числовых значений или четких критериев, согласно которым можно было бы однозначно определить полноту соответствия конкретного проекта этим требованиям. Тем более что ни

один из проектов, заявивших о принадлежности к третьему поколению, еще не может похвастаться реальным применением.

Более того, при внимательном рассмотрении оказывается, что блокчейны третьего поколения структурно идентичны второму поколению, но должны обладать более широкими возможностями для работы с высокой нагрузкой и большим количеством пользователей. Провести же четкую грань между ними невозможно.

4.0

Что касается блокчейна 4.0, то к этому поколению себя отнесли команды всего нескольких проектов, что характерно, находящихся в стадии ICO или недавно ее завершивших. Таким образом, определение блокчейна 4.0 еще никем четко не сформулировано.

Среди них, например, стартап Multiverse, планирующий создать «многомерный реляционный блокчейн», способный передавать до 64 000 транзакций в секунду с помощью уникального алгоритма консенсуса PoI (Proof of Integrity) — и все это за $35 млн. Однако будущее этого проекта пока неясно, так как активность команды, по сути, оборвалась в середине июня 2018 года, после сбора половины вышеуказанной суммы.

Прочие претенденты на звание блокчейна 4.0 — стартапы Seele, Metahash, GenEOS и другие, однако разрабатывающие их команды никому не известны, а текущая активность сосредоточена по большей части на проведении ICO и продвижении токенов на биржах. Поэтому серьезно рассуждать о перспективах блокчейнов 4.0 сейчас слишком рано.

Существует ли смена поколений блокчейнов

Стандартизация технологии блокчейна все еще остается делом будущего, так как работа над созданием стандартов находится в теоретической фазе. Крупный бизнес, которому однозначно необходимы подобные стандарты, только пытается понять, может ли блокчейн применяться в основных бизнес-процессах, будет ли его внедрение экономически выгодным и насколько использование блокчейна повысит эффективность работы всей компании. Твердая потребность в стандарте возникнет только тогда, когда появится необходимость налаживать взаимодействие между проектами разных компаний. И деление блокчейнов на плохо определенные поколения скорее запутывает этот процесс, чем облегчает.

Ключевой вопрос здесь — не универсальность, сложность архитектуры и широта спектра возможностей, а целесообразность и необходимая для выполнения поставленных перед проектом задач функциональность. Например, зачем блокчейну, предназначенному для хранения файлов или организации распределенных вычислений, нужны возможности платформы по выпуску и обмену токенов? Точно так же цифровому реестру, хранящему записи кадастра недвижимости или реестр юридических лиц, вовсе не обязательны расширенные возможности программирования и выполнения смарт-контрактов и распределенная виртуальная машина. Такому проекту в первую очередь необходимы максимальные гарантии неизменности записей и жесткий контроль поступающих данных, а все избыточные функции не только не нужны, но даже вредны. Значит ли это, что такие проекты навсегда останутся «устаревшими» блокчейнами 1.0?

Технические возможности блокчейнов далеко не полностью зависят от времени их возникновения и даже первоначальных функций. Блокчейн, как и любой программный продукт, не нечто неизменное, отлитое в металле, его можно совершенствовать в соответствии с требованиями времени, если его команда и пользователи в состоянии поддерживать это развитие.

В качестве наиболее наглядного примера возьмем самый первый, а следовательно, и самый «древний» и «окончательно устаревший» блокчейн — Bitcoin, с которым любят приводить сравнения авторы самых «инновационных» и «прорывных» проектов.

Первая технология для создания производных активов на базе родительского блокчейна, а также первая платформа с их использованием Mastercoin (сейчас Omnilayer) появилась и до

сих пор работает именно на блокчейне Bitcoin, и именно на ней базируется самый популярный из цифровых токенов, эквивалентный доллару США, — USDT, созданный проектом Tether.

Стартап Rootstock (RSK) разрабатывает возможности применения в сайдчейнах («боковых» или дополнительных субблокчейнах) полнофункциональных смарт-контрактов. Вероятно, их функциональность будет несколько уже, чем на специализированных блокчейнах, но более чем достаточной для большинства децентрализованных приложений.

С помощью технологии атомарных свопов, разрабатываемой командой Bitcoin Core (а отнюдь не новейшего блокчейна XXX.0), уже в обозримом будущем станет возможным прямое взаимодействие блокчейнов. Оно представляет собой пересылку защищенных транзакций непосредственно из одного блокчейна в другой, включая обмен криптоактивами без централизованных посредников, таких как криптовалютные биржи. Ни один из новейших проектов даже не приблизился к такой возможности без использования решений от разработчиков Bitcoin.

Самая большая проблема Bitcoin, с точки зрения его критиков, — чрезвычайно низкая пропускная способность и масштабируемость сети, якобы до сих пор остающаяся на уровне пяти транзакций в секунду. Однако технология сети платежных каналов Lightning Network, позволяющая проводить практически неограниченные объемы транзакций мгновенно, с отложенным сохранением их суммарных итогов в публичном блокчейне, уже прошла большую часть этапов тестирования и в течение нескольких месяцев используется в основном блокчейне. С ее помощью будет возможно совершать тысячи транзакций в секунду при сохранении непревзойденной надежности PoW-блокчейнов.

Итак, подытожим: «ветхий» и «никуда не годный» блокчейн поколения 1.0 уже сейчас или в перспективе нескольких месяцев (а не в далеком неясном будущем) способен:

1. Пересылать до нескольких тысяч транзакций с финансовой или любой другой информацией в секунду;

2. Работать в качестве платформы для выпуска производных активов;

3. Поддерживать работу нескольких миллионов пользователей и перспективный рост пользовательской базы;

4. Выполнять простые функции смарт-контрактов напрямую, а с использованием надстроек стать полноценной платформой умных контрактов;

5. Взаимодействовать с другими блокчейнами.

Bitcoin уже много лет остается и еще долго будет самым надежным из существующих блокчейнов, так как консенсус Proof-of-Work при всех его недостатках все еще не имеет конкурентов с точки зрения неизменяемости хранимых данных.

Из всего вышеизложенного можно сделать вывод, что последовательность поколений блокчейнов не отражает действительного прогресса технологии блокчейна и даже искажает реальный ход развития отрасли, основываясь только на некоторых аспектах, вовсе не являющихся необходимыми для любого блокчейна.

Может быть, несовершенство кроется в самой модели преемственности поколений, пытающейся втиснуть индустрию, развивающуюся во многих измерениях, в рамки однонаправленного прямолинейного движения? Действительно ли поколение блокчейна определяется расширением возможностей и возрастающей универсальностью? Ведь давно известно, что для выполнения конкретной задачи универсальные решения всегда проигрывают специализированным, и блокчейн не исключение.

Как делить блокчейны

Исходя из приведенных выше аргументов, приходится остановиться на идее, что наиболее полная классификация блокчейнов не может быть одномерной и одноуровневой. В первую очередь она должна быть основана не на обещаниях будущих преимуществ и инноваций, а на реально выполняемых функциях конкретных блокчейн-решений и их уникальных особенностях. Функциональная классификация дает более ясную картину того, что представляет собой конкретный блокчейн, каковы его специализация и возможности. Более подробно этот подход к классификации и типы блокчейнов будут описаны в следующей главе.

Независимо от принятой классификации или ее отсутствия на момент написания книги уже фактически определились основные направления, в которых применение блокчейна может принести серьезные выгоды в процессе модернизации существующих информационных и финансовых систем:

- Биржевые и финансовые платформы, международные переводы.
- Платформы смарт-контрактов и децентрализованных приложений.
- Государственные и корпоративные реестры.
- Интеллектуальная собственность.
- Краудфандинг и другие формы публичного финансирования.
- Системы распределенных вычислений и хранения данных.
- Сети автономных устройств и интернет вещей.
- Политические выборы и платформы онлайн-голосований.
- Системы управления и контроля версий.

Разумеется, список возможных применений блокчейна этим не исчерпывается, и в будущем могут возникнуть новые направления, где будут необходимы максимально возможные уровни целостности и прозрачности хранения данных.

Глава 3

Какие бывают блокчейны и где они применяются

Как и любой свободный рынок, отрасль блокчейна развивается методом проб и ошибок — путем многочисленных экспериментов, конкурирующих или сотрудничающих друг с другом проектов, из которых постепенно выделяются наиболее жизнеспособные. Одни работают на энтузиазме создателей, другие находят инвесторов, третьи собирают средства на развитие с помощью краудфандинга — разумеется, тоже основанного на блокчейне.

Направленность и масштабы блокчейн-проектов крайне разнообразны — от консорциумов, занимающихся разработкой корпоративных платформ, до проектов энтузиастов для сохранения в блокчейне авторских прав на рисунки или музыкальные

композиции. Как мы уже выяснили в предыдущей главе, классификация блокчейнов может быть только многомерной, то есть производиться по совокупности независимых параметров. Блокчейн-проекты вырастают один из другого, постоянно видоизменяются и совершенствуются и даже пользуются разработками друг друга, так как большинство из них основаны на открытом исходном коде. Это значит, что каждый из блокчейнов практически невозможно отнести к какой-либо группе. Однако почти у любого блокчейна есть свои особенности и признаки, а также достаточно четко очерченные рамки возможного применения.

Публичные и частные

Вероятно, самое очевидное разделение блокчейнов — на публичные и частные или открытые и закрытые, что по сути одно и то же, но с некоторыми нюансами. Каковы основные отличия открытого и закрытого блокчейна и что они значат для пользователей?

Степень открытости блокчейна может зависеть от нескольких факторов. Первый — доступность исходного кода протокола блокчейна (обычно под этим подразумевается наиболее распространенный клиент данного блокчейна). Для Bitcoin таким клиентом является Bitcoin Core. А, например, в системе Ethereum нет одного общепринятого клиента, и пользователи могут выбирать из нескольких вариантов: Geth, Parity, MyEtherWallet и т.д., и все они разрабатываются с открытым исходным кодом.

Криптовалюты создавались как децентрализованные и общедоступные платежные системы, поэтому их исходный код, как правило, открыт с самого начала разработки, и его изменения ведутся на одном из наиболее популярных ресурсов, например на GitHub.

Блокчейны и платформы для корпоративного применения могут быть как с открытым, так и с частично или полностью закрытым исходным кодом. Проект Hyperledger, созданный под эгидой Linux Foundation как открытая блокчейн-платформа для бизнеса, изначально открыл свой исходный код, а разработчики Ripple открыли исходный код своего серверного приложения только через год после запуска. Такие ИТ-гиганты, как Microsoft или SAP, для собственных блокчейн-продуктов, очевидно, будут придерживаться обычной своей политики, и их исходный код останется закрытым.

Что же касается блокчейн-разработок для государственного сектора, то их количество еще слишком мало, используемых в реальных процессах продуктов практически не существует, но следует ожидать, что большинство из них также будут закрытыми.

Второй и наиболее важный показатель — возможность для любого пользователя свободного подключения к сети без получения каких-либо разрешений. Именно это является определяющим отличием публичного блокчейна от частного. Подавляющее большинство известных на сегодня блокчейнов публичны — для подключения к ним достаточно скачать совместимую с текущей версией протокола программу (клиент) и установить связь с другими равноправными узлами сети.

Чтобы полноценно участвовать в работе сети, в частности, проверять и ретранслировать транзакции других пользователей или участвовать в создании блоков, необходимо запустить клиент с функциональностью полного узла. В остальных случаях достаточно легкого клиента с ограниченными возможностями. Однако в публичных блокчейнах уровень участия пользователя всегда определяется им самим и зависит только от его личных (финансовых или аппаратных) ресурсов. Кроме того, никто не может отключить пользователя от распределенной сети, поскольку все участники публичного блокчейна равноправны. В отдельных случаях они могут, например, бойкотировать пользователя, рассылающего некорректные транзакции или пытающегося передать не соответствующую протоколу информацию, но такие инициативы носят исключительно саморегулируемый характер и не вводятся на уровне протокола.

В частных же блокчейнах за подключение к сети новых пользователей (а также за возможность их отключения) могут отвечать выделенные доверенные узлы или группы узлов, имеющие более высокий уровень полномочий по сравнению с остальными

пользователями. Частные блокчейны представляют собой иерархические структуры, состоящие из двух или более уровней. Пары ключей, предоставляющие доступ к системе, выдаются и управляются специальными административными узлами и при необходимости могут быть отозваны. Таким образом, частные блокчейны не реализуют основные принципы технологии — децентрализацию и равноправие участников, так как для корпоративных систем их наличие оборачивается существенными рисками.

Уровни управления блокчейнами

Попытки найти баланс между децентрализацией, безопасностью, конфиденциальностью и разграничением доступа привели к многочисленным экспериментам с механизмами управления блокчейном. Существующие на данный момент блокчейн-системы по уровню управляемости можно разбить на четыре группы.

Публичные децентрализованные системы

Большинство существующих на сегодня криптовалют и проектов на их основе — это блокчейны с одноуровневой структурой. В них все участники теоретически равноправны и консенсус достигается путем опосредованного голосования узлов, выполняющих функции создания блока (майнеров или валидаторов). Механизмы работы классического блокчейна уже многократно описаны, и по сути в нем присутствуют две функции управления:

1. Распространение и проверка транзакций (что косвенно влияет на принятие изменений программного кода протокола). Эту функцию выполняют все подключенные к сети полные узлы.

2. Подтверждение транзакций и формирование единой цепочки блоков. Этим занимаются майнеры (валидаторы), которым для выполнения работы необходимо обладание определенными ресурсами (вычислительными мощностями, монетами в кошельке, свободным пространством на дисках и т.п.).

Децентрализованные системы не накладывают каких-либо ограничений на участие в управлении, и возможности участников определяются только долей имеющихся у них ресурсов от общего количества, например долей вычислительной мощности оборудования конкретного майнера от общей вычислительной мощности всех майнеров блокчейна.

Публичные системы с делегированным управлением

По итогам почти десятилетней эксплуатации блокчейна Bitcoin и несколько меньшей — других популярных криптовалют можно сделать вывод, что полная децентрализация в саморегулируемых, а точнее, стихийно регулируемых системах на практике почти невозможна — все публичные блокчейны рано или поздно сталкиваются с одной из форм централизации. Поэтому была сделана достаточно спорная попытка частично пожертвовать децентрализацией для улучшения функций управления и других показателей блокчейна.

В 2015 году возникли первые публичные блокчейны с двухуровневой структурой, где ведущую роль играли так называемые суперноды, или узлы с расширенными полномочиями. Первым из таких блокчейнов стала криптовалюта Dash, где суперузлы осуществляют функции предварительного подтверждения (для ускорения платежей) и перемешивания транзакций (для повышения анонимности), а также участвуют в голосовании для утверждения изменений кода. За выполнение этой работы суперузлы получают значительную часть эмиссионного вознаграждения (в Dash — 45%), однако для открытия и поддержки работы такого привилегированного узла необходимо держать в кошельке достаточно крупную сумму монет (в августе 2018 года — 1000 Dash, что составляло на тот момент более

$200 000). То есть обладателем суперузла и участником частичного управления блокчейном может стать любой член сети, имеющий необходимое количество монет.

Похожую схему планируется реализовать в Ethereum после выхода версии 2.0 Serenity, когда второй по капитализации блокчейн окончательно перейдет на метод консенсуса Proof-of-Stake. После перехода место обычных майнеров займут валидаторы, и функция подтверждения транзакций перейдет к ним. Валидатором также сможет стать любой пользователь сети, имеющий в кошельке необходимое количество монет ETH. Однако в отличие от классического Proof-of-Stake в Ethereum 2.0 будет предусмотрено параллельное многопоточное подтверждение транзакций (шардинг), а также наказание в виде лишения депозита для недобросовестных валидаторов, уличенных в реализации мошеннических схем.

Еще дальше в осуществлении делегированного управления пошел китайский проект Ontology. В нем реализованы участие держателей токенов в утверждении обновлений кода, система идентификации пользователей и даже взаимодействие с регулирующими органами. Для проведения голосований и других функций управления используется внутренний токен ONT, выпущенный в марте 2018 года.

С Ontology тесно связан «китайский Ethereum» — проект NEO (ранее — Antshares), разработанный той же компанией OnChain. Кроме возможностей платформы децентрализованных приложений в NEO предусмотрена система цифровой идентификации пользователей. На сентябрь 2018 года она еще никак не применялась, однако слухи о сотрудничестве NEO с китайским правительством похожи на правду, и вскоре система управления этим блокчейном может сильно измениться в сторону повышения контроля.

Первым блокчейном с полностью делегированным управлением стал EOS.IO, запущенный в июне 2018 года и используемый в криптовалюте EOS. В отличие от описанных выше проектов, создателем блоков (валидатором) в EOS может стать не каждый участник сети, располагающий необходимой суммой в кошельке. Сначала ему необходимо завоевать авторитет в сообществе и… победить на выборах. Количество валидаторов ограничено — их всего 21, и они выбираются с помощью периодически проводящегося голосования держателей токенов EOS. Действия валидаторов контролируются так называемыми арбитрами — отдельной группой с более высокими полномочиями, которая может менять консенсус, созданный валидаторами. За ввод этой схемы в сообществе EOS поднялась волна критики в адрес разработчиков, и блокчейн практически переходит в разряд контролируемых. Однако эволюция системы управления в EOS еще не завершена, и вполне вероятно, что полномочия арбитров со временем будут урезаны.

Еще одна интересная реализация делегированного управления блокчейном существует в децентрализованной социальной сети Steemit, запущенной в 2016 году на основе технологии Graphene от Bitshares. Что интересно, Bitshares, Steemit и EOS созданы одной командой под руководством Дэна Ларимера. Позже в России стартапом cyber·Fund был запущен локализованный аналог Steemit под названием «Голос», с технической стороны не имеющий существенных отличий.

В Steemit выпущены два типа токенов: кроме обычного Steem существует также голосующий токен Steem Power (SP), распределенный между так называемыми «китами» — основными инвесторами проекта. Именно поддержка крупных владельцев SP играет решающую роль при оценке публикаций пользователей в блокчейне Steemit и определении получаемого ими вознаграждения. Хотя «киты» и не имеют прямого влияния на создание блоков, они голосуют за принятие существенных изменений в работе сети. Что не менее важно, распределение токенов между авторами контента, а соответственно, и получаемый ими доход от публикаций в значительной степени зависят от держателей токенов SP. Эта модель много раз подвергалась критике, и разработчики Steemit пытались ее оптимизировать, однако не достигли успеха, и количество пользователей социальной сети остается небольшим.

Частные контролируемые блокчейны

Наиболее известным корпоративным решением на основе блокчейна является R3 Corda — проект, изначально разработанный банковской группой J. P. Morgan и в 2016 году переданный блокчейн-консорциуму R3 CEV, одним из ключевых инвесторов которого и стала J. P. Morgan. В октябре 2017 года была опубликована платформа Corda 1.0 с открытым исходным кодом. В июле 2018 года представлена платформа Corda Enterprise — решение от R3 для предприятий с закрытым кодом, частично совместимое с открытой Corda. Более подробно этот продукт будет описан в главе 5, здесь же остановимся на его схеме управления и сравнении ее с традиционными блокчейнами.

Собственно, Corda Enterprise и другие корпоративные системы нельзя считать настоящими блокчейнами, их часто называют распределенными реестрами. В таких системах каждый узел имеет предварительно назначенный ему уровень доступа, и, в отличие от публичного блокчейна, данные не всегда общедоступны даже для чтения. Это достигается с помощью так называемого Blockchain Application Firewall, который фильтрует доступ к данным транзакций в соответствии с назначенной администраторами блокчейна политикой. Кроме того, Corda Enterprise заявляет о совместимости с наиболее распространенными типами реляционных СУБД и высоком уровне интеграции блокчейна с корпоративными ИТ-системами.

Управление в корпоративных блокчейнах осуществляется с помощью специальных узлов, обладающих повышенными полномочиями, именно они отвечают за политику распространения данных и идентификацию пользователей и удостоверяют внесение данных в блокчейн. В R3 Corda существует три типа управляющих узлов:

1. Портье, управляющие сетевым трафиком и ограничивающие доступ к данным на основе полномочий пользователя;

2. Нотариальные узлы, подтверждающие транзакции и отвечающие за корректность обновления распределенного реестра;

3. Оракулы, работающие на основе смарт-контрактов и автоматически утверждающие транзакции, которые соответствуют определенным условиям.

Таким образом, при комбинировании этих методов управления возможно построение достаточно гибкой и надежной распределенной системы, которая использует ключевые преимущества блокчейна, при этом позволяя придерживаться корпоративной политики доступа к информации.

Разумеется, Corda не единственный представитель семейства корпоративных блокчейнов, но наиболее яркий из них. Среди его конкурентов необходимо назвать Hyperledger — проект с открытым исходным кодом, работающий под эгидой Linux Foundation. В рамках Hyperledger разрабатывается целый ряд блокчейн-платформ для бизнеса, включая Fabric от IBM, Sawtooth от Intel, Iroha, Indy и другие продукты. На их основе возможно создать настраиваемый блокчейн практически с любым набором параметров (от публичного до полностью контролируемого). Hyperledger предоставляет только фреймворк и набор совместимых инструментов для дальнейшей разработки, а не готовые «коробочные» решения. Банк J. P. Morgan, избавившись от Corda, приступил к работе над новым проектом под названием Quorum, который представляет собой закрытую коммерческую версию Ethereum.

Государственные блокчейны

Распределенные реестры для государственного применения в целом мало отличаются от корпоративных блокчейнов и также требуют контролируемого доступа к информации. Однако у государственных ведомств существуют и особые требования к блокчейну — максимальный уровень неизменности уже добавленной информации и самый строгий

контроль над ее добавлением в блокчейн. При этом уже имеющаяся в блокчейне информация во многих случаях может быть публичной, поскольку государственные органы стремятся к повышению прозрачности своей работы (по крайней мере декларируют это).

Идеальными объектами для использования блокчейна в государственных ведомствах являются различные государственные реестры — от персональных данных граждан до госзакупок, кадастров земель и объектов недвижимости, а также данных налоговых и регулирующих органов.

Обеспечение надежного функционирования государственных реестров, казалось бы, требует специально настроенного для выполнения этих функций контролируемого блокчейна, который используется только для ведения вышеуказанных реестров и больше ни для чего. Первые примеры реализации государственных услуг на блокчейне появились, как ни странно, именно на публичных блокчейнах. Земельный кадастр Грузии, блокчейнизацией которого занималась компания Bitfury, был помещен в самый публичный из всех блокчейнов — Bitcoin, а программа электронного резидентства Эстонии использовала блокчейн Ethereum.

Завоевал популярность блокчейн и в вузах всего мира: начиная с 2017 года более десятка университетов заявили о проведении пилотных программ по размещению дипломов студентов в блокчейне. Причем выбраны были опять же публичные блокчейны. Так, Массачусетский технологический институт (MIT) в своей программе Blockcerts использовал блокчейн Bitcoin, Базельский университет — Ethereum, а Университет бизнеса и технологий в Тбилиси (BTU) — Emercoin.

Однако для государственных сервисов обязательным условием является идентификация пользователя, так как предоставление государственных услуг анонимам — это нонсенс. Поэтому, если идентификация пользователей не будет осуществляться на уровне блокчейна, она будет производиться другими средствами. То есть пользователь сможет получить доступ к прямому взаимодействию с блокчейном только после получения удостоверенной государством цифровой подписи, или же с блокчейном будет работать только государственное ведомство. Оба варианта ограничивают возможности размещения данных государственных реестров в блокчейнах с децентрализованным управлением.

Можно сделать вывод, что государственные сервисы на блокчейне все еще остаются в стадии тестирования, и технологическая блокчейн-платформа для государственных ведомств в разных странах до сих пор не определена. То есть говорить о какой-либо целенаправленной политике блокчейнизации госуслуг еще рано.

Автономные или интегрированные

Первые блокчейны задумывались как полностью самостоятельные системы, потребность которых во взаимодействии с внешним миром была крайне ограниченной, хотя его реализация с помощью API и других программных средств предусматривалась. Большинство публичных блокчейнов не нуждается в плотной интеграции с внешними информационными системами — это касается и универсальных платформ, таких как Ethereum, EOS, NEO и т.д. Для них, по сути, все пользователи, будь то частное лицо или транснациональная корпорация, равноправны и являются только клиентами, имеющими одинаковые средства доступа к блокчейну, даже если создаваемая ими нагрузка и объем данных отличаются на порядки.

Однако современные проекты, особенно для корпоративного или государственного применения, не могут существовать обособленно, и их интеграция в существующие информационные системы планируется изначально. По сути, блокчейну в них отводится роль всего лишь одного из компонентов корпоративной информационной системы (КИС). Его задача состоит в поддержании надежной доверенной среды хранения и распространения данных, не требующей многоуровневой верификации и сложных процедур контроля доступа. Такие проекты, как R3 Corda или Hyperledger, подходят к проектированию блокчейна аналогично традиционным СУБД, разумеется, учитывая особенности технологии, и создают

инструменты для полноценной интеграции распределенных реестров в существующие системы.

Универсальные или специализированные

Еще одним критерием классификации блокчейнов является степень их универсальности, вернее, возможность и целесообразность выполнения на них произвольных пользовательских приложений при отсутствии специализации базового блокчейна.

К универсальным блокчейнам относятся платформы смарт-контрактов или децентрализованных приложений, так как на них можно запускать полноценные программы практически любого типа — от платежной системы до системы онлайн-голосования. Также универсальными блокчейнами можно считать фреймворки для разработки блокчейн-приложений, такие как Hyperledger, в них конечным пользователям доступны любые решения, которые при этом могут базироваться даже на разных блокчейнах.

Все остальные блокчейны следует отнести к разряду специализированных, то есть выполняющих более или менее ограниченный набор функций. Разумеется, блокчейн, как и любой программный продукт, может совершенствоваться и получать новые функции, но в большинстве случаев разработчики не стремятся к их расширению в сторону возможностей, не предусмотренных при создании, чтобы избежать появления новых проблем.

Например, Litecoin или Monero остаются криптовалютами, SIA или Storj — платформами распределенного хранения данных, а Ripple или «Мастерчейн» — блокчейнами для проведения финансовых операций. Специализация помогает усилить основные их функции и при этом избежать затрат на разработку ненужных. Поэтому более широкий набор возможностей блокчейна вовсе не говорит о его превосходстве над другими, а лишь означает, что его эксплуатация сложна и требует больших ресурсов.

Сферы применения блокчейнов

Пришло время поговорить о функциональном делении блокчейнов, которое наиболее объективно учитывает характерные особенности каждого типа блокчейнов и помогает сформулировать технические требования к блокчейну для конкретного проекта. При правильном проектировании именно выполняемые задачи определяют необходимый и достаточный набор инструментов для их реализации, а не наоборот.

Некоторые блокчейны могут выполнять несколько функций из указанных выше, но у всех, за исключением универсальных платформ децентрализованных приложений, одна функция всегда будет основной, а остальные — вторичными. Например, внутренние токены платформ Ethereum, NEO или Steemit помимо прочих функций являются и криптовалютами, но их использование в качестве платежного средства, как правило, менее удобно и имеет определенные ограничения по сравнению с классическими криптовалютами. Однако если на блокчейне Bitcoin будет запущена платформа смарт-контрактов, она не сможет стать настолько же гибкой и функциональной, как на блокчейнах, предназначенных для этого.

Криптовалюты

Среди более 2000 самостоятельных блокчейнов самой многочисленной группой по-прежнему остаются криптовалюты. Несмотря на логотипы всех цветов и различные размеры блока, все они фактически слегка измененные копии прародителя — Bitcoin. Многочисленные эксперименты и попытки противостоять ASIC-майнерам привели к появлению десятков алгоритмов хеширования. Были изобретены различные способы регулирования сложности майнинга, несколько альтернативных методов достижения консенсуса и другие технические улучшения. Но все эти изменения практически не повлияли на сущность криптовалют.

Все криптовалюты объединяет общая философия. Bitcoin был создан в качестве открытой, децентрализованной, не подверженной цензуре платежной сети, каждый участник

которой полностью контролирует средства в своем кошельке и полностью за них отвечает. Все криптовалюты представляют собой публичные одноранговые блокчейны, основанные на децентрализованном механизме принятия решений. Все они автономны и самодостаточны и управляются сообществом. Единственной серьезной угрозой для децентрализации в блокчейнах большинства криптовалют является возможность сосредоточения у ограниченной группы майнеров большей части мощностей хеширования (или большей доли эмитированных монет для блокчейнов с консенсусом Proof-of-Stake), что в перспективе приведет к усилению влияния этой группы на управление блокчейном.

Криптовалюты все еще остаются основным движителем развития отрасли блокчейна, и большая часть перспективных технических новшеств производится независимыми разработчиками криптовалютных проектов. Именно инвестиции в криптовалюты привлекают в сообщество основную часть новых членов и заставляют государства разрабатывать механизмы регулирования новой финансовой технологии. Если взять топ-25 рейтинга рыночной капитализации криптовалют Coinmarketcap, только шесть позиций в списке занимают чистые криптовалюты, и даже в топ-100 их наберется меньше 20. Многие когда-то популярные криптовалюты уже откатились за пределы первой и даже второй сотни. Это значит, что сейчас на рынке более востребованы платформы смарт-контрактов и другие многофункциональные блокчейны. При этом нужно учитывать, что в рейтинге капитализации не участвуют частные блокчейны, так как их ценность невозможно рассчитать на основе биржевой стоимости токенов.

Конфиденциальные криптовалюты

Анонимность транзакций, которая преподносилась как одно из ключевых преимуществ Bitcoin, уже в 2014–2015 годах ставилась под сомнение после закрытия теневого рынка Silk Road и ряда других проектов, платежи внутри которых осуществлялись преимущественно в этой криптовалюте. А существующие сейчас системы анализа больших данных всех основных криптовалют фактически уничтожили анонимность Bitcoin. Многие пользователи, не использующие комплексных мер для обеспечения анонимности, уже идентифицированы, так как в публичном блокчейне вся история платежей доступна для анализа. Из таких систем анализа наиболее известна Elliptic, разработчики которой сотрудничают со спецслужбами США.

Это привело к расцвету криптовалют, использующих различные методы сокрытия деталей транзакций, в первую очередь адресов отправителя и получателя. Возглавляют это направление три проекта:

1. Dash, где любой пользователь за небольшую дополнительную плату может включить механизм перемешивания транзакций, затрудняющий идентификацию сторон, участвующих в платеже.

2. Monero, в котором используется механизм кольцевой подписи, перемешивающий подписи большого количества участников транзакций и таким образом делающий невозможной привязку конкретного адреса к конкретной транзакции. С 2016 года эта криптовалюта стала одной из самых популярных в даркнете.

3. Zcash, маскирующий содержимое транзакции с помощью технологии zk-SNARKs. Все еще находится в стадии доработки, и большая часть транзакций в блокчейне Zcash пока остается публичной.

Технологии анонимизации, разработанные для криптовалют с повышенной конфиденциальностью, тестируются с целью внедрения в другие публичные блокчейны.

Однако противодействие регуляторов может замедлить распространение этих технологий даже в относительно лояльных юрисдикциях.

Платформы смарт-контрактов

Вторая по популярности и капитализации группа блокчейнов (которая в ближайшем будущем может стать первой) — это платформы смарт-контрактов и создаваемых на их основе децентрализованных приложений (DApps).

Широкие возможности, открывающиеся после внедрения с помощью блокчейна автоматически исполняемых с соблюдением определенных условий и фактически не требующих участия человека договоров (контрактов), были оценены по достоинству уже в 2014 году.

В 2015 был запущен первый блокчейн этого типа — Ethereum, а в 2017-м начался настоящий бум смарт-контрактов, и сейчас существует уже несколько десятков запущенных или готовящихся к запуску блокчейн-платформ с возможностью функционирования децентрализованных приложений.

Описание технологии смарт-контрактов и обзор платформ размещены в главе 5.

Финансовые блокчейны, банкчейны

В результате ошеломляющего успеха криптовалют, которые принесли миллионы долларов как энтузиастам, так и спекулянтам, финансовый мир увидел в блокчейне инновационную технологию, способную совершить революционные изменения. После нескольких лет хаотичных исследований и инвестиций в сотни проектов, многие из которых уже закрылись, ажиотаж стих, но интерес к блокчейну в финансовом секторе не ослабевает.

Первыми ласточками среди блокчейн-систем, предназначенных для использования криптовалют традиционными финансовыми учреждениями, стали Ripple и разработанный на его основе протокол Stellar. Это частично централизованные системы, обладающие некоторыми механизмами блокчейна, которые обычно не признают полноценными блокчейнами. Они используют систему доверенных шлюзов, токенизирующих активы и пересылающих их (как правило, это фиатные активы или криптовалюты). Технология xRapid от Ripple тестируется несколькими крупными банками для осуществления трансграничных денежных переводов. Проект Stellar еще достаточно молод и пока не достиг существенных результатов.

Однако для банков и других регулируемых финансовых институтов даже частично контролируемые сети выглядят недостаточно надежными. Это привело к созданию нескольких объединений, или блокчейн-консорциумов, разрабатывающих специальные блокчейны для банков. Такие блокчейны получили название банкчейнов. Самые известные из них — это описанные выше проекты R3 Corda и Quorum. Центральный банк Индии (Reserve Bank of India) в 2017 году создал проект именно с таким названием — BankChain. Проект разрабатывается с помощью нескольких коммерческих банков. К семейству банкчейнов относится и российский «Мастерчейн». Основные функции банкчейнов — перевод на блокчейн межбанковских транзакций и торгового финансирования, выпуск облигаций и другие банковские операции.

Получил признание блокчейн и на фондовом рынке. О разработке блокчейн-проектов в течение последних двух лет заявили Московская биржа (а именно НРД), Гонконгская, Австралийская и Сингапурская биржи, а также американская NASDAQ и фондовые биржи Германии и Турции. На данный момент все эти проекты находятся в стадии разработки и тестирования и, возможно, уже в 2019 году некоторые из перечисленных выше бирж начнут использовать блокчейн в основных бизнес-процессах.

Цифровые реестры

Невозможность изменения данных в блокчейне в сочетании с полной открытостью их просмотра сделали эту технологию крайне привлекательной для применения в любых публичных реестрах, в первую очередь в государственных.

Чтобы получить сведения из какого-либо государственного реестра (например, об объекте недвижимости), обычно требуется личное обращение гражданина, а обработка запроса и получение ответа занимают несколько дней. При этом большая часть сведений в реестрах многих стран до сих пор хранится на бумаге, их сохранность не гарантирована, и всегда существует риск искажения информации или подмены документов. Перенос информации госреестров и различных архивов в блокчейн решит сразу несколько важнейших проблем, ускорит все внутренние процессы и позволит сэкономить значительные средства.

Кроме хранения государственных реестров, блокчейн может пригодиться и в других случаях, когда оцифровка реестров принесет ощутимую пользу. Например, на фондовых рынках, в страховании, нотариате, защите интеллектуальной собственности, медицине и в других отраслях, где крайне важны безопасность хранения информации и гарантия ее неизменности.

О возможностях использования блокчейна в цифровых реестрах и о существующих и разрабатываемых проектах вы узнаете из главы 4.

Децентрализованные хранилища

Если цифровые реестры представляют собой относительно небольшие массивы данных и эффективность применения в них блокчейна достаточно очевидна, то базы данных, файловые архивы и другие хранилища «тяжелой» информации, такой как мультимедийные файлы, на первый взгляд, совершенно не подходят для размещения их в блокчейне. Но даже здесь блокчейны могут быть полезны.

Суть применения блокчейна для хранения больших объемов данных произвольного формата состоит в том, что держать в самом блокчейне весь объем информации вовсе не обязательно. Для того, чтобы доказать, что файл не изменялся после его размещения в блокчейн-системе, не нужно проводить побайтное сравнение его с оригиналом. Достаточно рассчитать и сохранить в блокчейне хеш этого файла, а сам файл хранить отдельно, причем под контролем той же программы, которая отвечает за размещение и учет файлов. При этом файлы необязательно держать в одном месте и даже на одном компьютере. Здесь приходит на помощь технология BitTorrent и ее аналоги, предназначенные для распространения файлов через интернет. Специально для распределенного хранения файлов с помощью блокчейна была разработана так называемая межпланетная файловая система, или IPFS. Она позволяет собрать файл из множества различных источников, которые могут быть разбросаны по всему миру, и проверить его аутентичность с помощью хеша, взятого из блокчейна. На самом деле возможности IPFS гораздо шире, и, если подобный метод хранения сможет завоевать доверие пользователей, через несколько лет IPFS и подобные системы будут способны конкурировать на рынке с уже ставшими привычными облачными хранилищами от популярных централизованных сервисов, ведь блокчейн значительно безопаснее и, в отличие от «облака», его не может отключить владеющая им корпорация.

Проектов распределенного хранения информации с помощью блокчейна уже немало — это Sia, Storj, LBRY, Filecoin и другие, но аудитория их еще незначительна, так как люди, предоставляющие свое дисковое пространство для хранения файлов, ожидают за это вознаграждение, а создать децентрализованное сообщество, готовое платить за надежное хранение своих файлов, — задача не из тривиальных. Поэтому операторы облачных хранилищ пока могут спать спокойно.

Системы голосования

Политические процессы — еще одна сфера, в которой обществу хотелось бы иметь максимальную открытость. Темы фальсификаций и прочих искажений выборов или

результатов других политических голосований очень часто поднимаются во всех концах света, но предъявить какие-либо доказательства часто бывает невозможно из-за того, что многие процессы зависят от конкретных людей, у которых всегда есть искушение использовать предоставленные им возможности в свою пользу. И здесь блокчейн, без сомнения, способен помочь разрешить многие проблемы.

Не раз звучали предложения использовать блокчейн в выборах президента США в 2016 году и президента РФ в 2018-м. Однако эти предложения не нашли поддержки избирательных органов, так как системы проведения выборов крайне консервативны и внесение любых изменений в них требует множества согласований и создает бюрократическую волокиту. Тем более что в данном случае речь идет о радикальных изменениях и возникает ряд проблем технического характера, например необходимость выдачи каждому избирателю электронной подписи, удостоверенной ЦИК, и полного преобразования процедур подсчета и проверки голосов. Поэтому избирательные комиссии предпочитают традиционную, хотя и давно устаревшую, форму голосования.

В июле 2018 года на президентских выборах в Кении применили параллельный подсчет голосов с помощью блокчейна, но его результаты не имели юридической силы. Что же касается других стран, они не могут похвастаться и этим. К сожалению, время для реального применения блокчейна в выборах еще не пришло.

Итоги

Разумеется, сферы применения блокчейна не ограничиваются перечисленными выше. Например, этой многообещающей технологией заинтересовались военные ведомства таких стран, как США и Россия, ее пытаются использовать для обеспечения безопасности критически важных объектов, а также для учета и розничной продажи электроэнергии. Разработки ведутся и в таких направлениях, как учет произведений искусства и драгоценных камней, и даже в сфере благотворительности.

Не все эти эксперименты приводят к ожидаемым результатам, но это не значит, что все они неудачны. Процесс изучения и познания может быть длительным и трудным, но рано или поздно он принесет плоды, и блокчейн займет достойное место среди множества технологий, уже изобретенных человечеством.

Описанная выше система классификации блокчейнов по нескольким признакам может показаться спорной и неоднозначной, как и все прочие. Тем не менее она позволяет, получив ответы на ряд простых вопросов, определить основные характеристики и возможности конкретного блокчейна и хотя бы поверхностно оценить его актуальность и возможности его применения.

Глава 4

Блокчейн как цифровой реестр

В англоязычном сегменте отрасли блокчейн еще несколько лет назад окрестили технологией распределенного реестра (DLT — Distributed Ledger Technology). И хотя это определение охватывает не только классические блокчейны, но и достаточно далекие от них проекты, данная формулировка очень точно отражает основное назначение блокчейна. В архитектуре Bitcoin ему отводится роль реестра финансовых операций, совершаемых в децентрализованной системе.

Поэтому, когда применением блокчейна вне криптовалют заинтересовались государственный и корпоративный сектора, наиболее логичным вариантом стало развитие

блокчейн-решений именно в виде различных цифровых реестров. Основополагающую роль здесь сыграли общеизвестные преимущества блокчейна над традиционными базами данных:

1. Невозможность изменения любых подтвержденных транзакций, записанных в блокчейн. Это, вероятно, самое важное и революционное новшество из всех возможностей блокчейна.

2. Распределенный характер хранения, причем каждый узел блокчейна содержит полную копию всей когда-либо внесенной в блокчейн информации. Таким образом решается проблема резервного копирования.

3. Полная прозрачность, ведь в классическом блокчейне вся история операций доступна любому подключенному к ней узлу. Впрочем, такая открытость подходит не всем, и некоторые проекты целенаправленно ограничивают доступ к данным в блокчейне даже для чтения.

По сути, любой продукт на основе блокчейна (от криптовалют до смарт-контрактов или систем для проведения голосований) можно назвать цифровым реестром. Согласно определению в «Большом энциклопедическом словаре», реестром называется «список, перечень, опись, книга для регистрации деловых документов, имущества и т.п.». Блокчейны криптовалют вполне подходят под это определение, поскольку являются «регистрационной книгой» или просто хронологической записью совершаемых с соответствующей криптовалютой последовательных операций.

Однако в этой главе мы будем употреблять термин «реестр» в более привычных рамках, а именно в пределах блокчейнизации существующих электронных и бумажных реестров. То есть поговорим о применении блокчейн-систем с определенным назначением для ведения учета любых массивов представленных в едином формате данных. Далее внесенные в блокчейн данные с помощью программных интерфейсов могут быть использованы в целях контроля, анализа или отчетности.

Хранилищем данных цифрового реестра может служить любой из публичных блокчейнов, разрешающий сохранять в теле транзакции достаточный объем произвольной текстовой информации. Поэтому первые попытки создания цифровых реестров проводились с помощью наиболее популярных публичных блокчейнов — Bitcoin и Ethereum.

Однако для текстовой информации в каждой транзакции Bitcoin отводится не более 60 байт, поэтому разработчики были вынуждены пойти на ухищрения, размещая необходимые данные путем их кодирования в хешах, элементах подписей и других служебных компонентах транзакции. Такой подход позволяет сохранить в каждой транзакции сотни байт, однако значительно усложняет как генерацию, так и последующую обработку пользовательской информации в блокчейне. С одной стороны, это требует дополнительного объема вычислений для создания подходящих хешей, с другой, использования единой методики кодирования информации для ее помещения в блокчейн. Кроме того, будущие обновления протокола блокчейна (такие как изменение формата подписей, алгоритма хеширования и т.п.) могут нарушить структуру данных и потребуют многократного внесения изменений в клиентские программы для работы с данными цифрового реестра.

Все изложенное выше приводит к тому, что для ведения цифровых реестров в долгосрочной перспективе требуются специализированные блокчейны или как минимум сайдчейны и децентрализованные приложения. Это позволит отвести под полезные данные значительно большую долю объема транзакции, избежать потенциальных конфликтов с другими пользователями блокчейна и технических проблем, связанных с обновлениями протокола публичного блокчейна общего назначения.

Однако разработка, поддержка и обеспечение безопасности такого блокчейна полностью ложатся на команду проекта. Именно поэтому блокчейнов, выделенных для создания цифровых реестров, по сути, не существует, и разработчики приспосабливаются к

ограничениям совместного использования публичного блокчейна или запускают его частную копию с некоторыми модификациями. Если цифровые реестры на блокчейнах все же получат распространение и их начнут использовать в экономически и социально значимых приложениях, развитие специализированных решений станет необходимостью.

Среди различных реестров, которые могут быть оцифрованы и переведены в систему на основе блокчейна, следует выделить несколько групп приложений:

- Государственные реестры недвижимости и других объектов, операции с которыми подлежат государственной регистрации. (Об этой группе поговорим подробнее ниже.)
- Системы идентификации и обработки персональных данных.
- Системы выборов и других публичных голосований.
- Реестры объектов интеллектуальной собственности.
- Реестры акционеров и биржевых операций.
- Технические реестры, такие как системы контроля версий.

Государственные реестры

Наиболее очевидно и перспективно применение блокчейна в качестве цифрового реестра в сфере государственных услуг. Возможно, именно перенос в блокчейны государственных реестров станет стимулом к повсеместному принятию этой технологии. И хотя государственные ведомства, как правило, более консервативны, чем частные компании, привлекательность блокчейна уже была оценена на самых высоких уровнях в США, Китае, России и Евросоюзе (в том числе и в отдельных его странах). Однако разработки каких-либо общих стандартов и методик в ближайшее время ожидать не приходится, так как подходы к работе с государственными реестрами в разных странах значительно отличаются.

Международная организация по стандартизации (ISO) в 2016 году проявила интерес к блокчейну и даже создала рабочую группу по изучению возможностей разработки стандартов для отрасли. Однако необходимо понимать, что подобные инициативы могут привести к практическим результатам через много лет, поэтому ожидать появления стандартов ISO для распределенных реестров в обозримом будущем не следует, и каждому заинтересованному в применении цифровых реестров государству приходится заниматься этим вопросом самостоятельно.

С формальной и технической точки зрения, чтобы перевести любой государственный реестр на блокчейн, требуется всего несколько шагов:

1. Выбрать наиболее подходящий тип блокчейна для хранения и администрирования записей цифрового реестра. Здесь может как использоваться существующая платформа (публичная или частная), так и потребоваться разработка собственного решения.

2. Сопоставить существующую модель данных государственного реестра с моделью данных выбранного блокчейна. Разумеется, для достижения совместимости и наилучшей эффективности придется чем-то пожертвовать с обеих сторон.

3. Разработать политику доступа для внесения записей в реестр и получения информации из него. При всей кажущейся простоте на этом этапе может встретиться наибольшее количество противоречий.

4. Разработать клиентское ПО как для администраторов реестра, имеющих все возможные доступы для добавления и обновления записей, так и для пользователей, которые будут иметь ограниченные возможности не только добавления, но также и чтения информации реестра. Во втором случае могут быть использованы или адаптированы существующие интерфейсы доступа к государственным реестрам, например «Портал государственных услуг», уже широко применяемый в России.

5. Перенести данные из существующего реестра и провести полномасштабное тестирование реестра на блокчейне перед вводом в эксплуатацию. Это самый трудоемкий и ответственный этап, даже если ранее большинство возникших проблем было успешно выявлено и решено. Однако любому опытному инженеру прекрасно известно, насколько обманчивой может быть кажущаяся законченность системы, особенно если речь идет о программном продукте.

На практике процесс, разумеется, гораздо сложнее, и на пути к цели возникнет огромное количество подводных камней, так как открытая для публичного доступа онлайн-система может подвергаться гораздо большему количеству атак, чем закрытое государственное учреждение даже с достаточно высокой степенью автоматизации.

Одна из первых и наиболее очевидных проблем в блокчейнизации государственных реестров — соответствие новой формы хранения и управления данными действующему законодательству. Для внедрения блокчейна в государственные сервисы в первую очередь требуется решить проблемы не технического, а юридического и политического характера, особенно если речь идет об использовании публичных блокчейнов и их модификаций, где данные государственных реестров могут подвергнуться множеству опасных воздействий — от компрометации до подделки.

На данный момент в юридической сфере готовность к полномасштабному внедрению распределенных реестров так же низка, как и в технической. Регулирующее блокчейн законодательство все еще требует доработки.

В ряде штатов Америки смарт-контракты признаны имеющими юридическую силу аналогично традиционным договорным отношениям, а записи в блокчейне могут быть приравнены к нотариальному заверению. Однако прецедентов реального использования распределенных реестров еще слишком мало, как и правоприменительной практики. В Евросоюзе регулирование блокчейна все еще находится на стадии предварительных разработок, хотя в некоторых странах, включая Эстонию, Францию, Великобританию, Испанию и другие, уже имеются отдельные примеры использования блокчейна на государственном уровне. Так, в сентябре 2018 года администрация испанского региона Арагон заключила соглашение со стартапом Alastria о внедрении блокчейна в госуправление, а минюст Великобритании планирует хранить в распределенном реестре базу судебных доказательств.

В России пакет законопроектов по регулированию криптовалют и блокчейна уже внесен в Государственную думу, однако доработки и утверждение различными инстанциями грозят затянуться на много месяцев. В нашей стране также работает несколько развивающихся блокчейн-платформ, которые будут использоваться государственными ведомствами. Это, например, финансируемая «Ростехом» платформа Vostok и поддерживаемая администрацией Амурской области Amurcoin.io, а в Санкт-Петербурге с 2017 года на базе «Сбербанка-АСТ» разрабатывается электронная площадка для госзакупок с использованием блокчейна.

Что касается Азии, то здесь наибольшую заинтересованность в блокчейне проявляет Южная Корея, где правительство финансирует 12 пилотных блокчейн-проектов. Однако совсем по-другому обстоит дело в лояльной к криптовалютам Японии, в пытающемся максимально их ограничить Китае и во многих других странах, где на государственном уровне идея внедрения технологии распределенного реестра все еще носит теоретический характер.

Можно сказать, что и в правовом поле блокчейн пока находится в стадии пилотных проектов, которые уже в ближайшие годы способны при соответствующей поддержке развернуться в реально работающие продукты. Но не следует считать внедрение блокчейна в государственные реестры абстрактной и далекой от воплощения идеей.

В качестве примера реализации этого сценария в России рассмотрим один из самых востребованных у населения государственных реестров — ЕГРН (Единый государственный реестр недвижимости). Что интересно, в конце 2017 года в СМИ уже появлялась информация о проведении в Москве эксперимента по регистрации на блокчейне операций с недвижимостью и даже о запуске альтернативного блокчейн-реестра. Эксперимент организовал Росреестр при поддержке правительства Москвы. В марте 2018 года были оглашены подробности эксперимента, который должен был стартовать в мае с применением публичного блокчейна Ethereum. В июле планировалось проведение второго этапа эксперимента уже с использованием одной из частных блокчейн-платформ: Exonum, Corda или Hyperledger. Завершиться эксперимент должен был в декабре 2018 года.

Однако информация о дальнейшем ходе проекта до сих пор отсутствует. Очевидно, его разработчики встретились с непредвиденными сложностями и не спешат оглашать результаты даже первого этапа, хотя не исключена вероятность того, что проект мог застопориться по другим причинам.

Но и использование публичного блокчейна для регистрации сделок и хранения информации об объектах недвижимости далеко не лучшая идея. Уникальная особенность блокчейнизации ЕГРН или другого госреестра по сравнению с большинством блокчейн-проектов состоит в том, что в данном случае одноуровневая децентрализованная схема управления не сможет работать ни при каких обстоятельствах. У государственного реестра нет необходимости в конфиденциальности пользователя по отношению к уполномоченному государственному органу, но требуется обеспечить конфиденциальность пользователей реестра между собой для соблюдения закона о персональных данных. Таким образом, использование публичных блокчейнов сопряжено с преодолением ряда препятствий, поэтому разработка с нуля специального блокчейна или использование одной из указанных выше платформ может оказаться быстрее и дешевле. Кроме того, наработки этого проекта могут быть использованы и для оцифровки других государственных реестров.

Большая часть данных реестра недвижимости, таких как кадастровый номер, адрес, информация о переходе прав собственности и о самих собственниках, представляет собой однотипные тексты, которые размещаются в транзакциях с присвоением соответствующих идентификаторов. Но в отличие от классического блокчейна, где отправить транзакцию и включить ее в блок может любой участник сети, для государственного реестра одноранговая схема не подходит.

Необходимо принять как факт, что единственным авторизованным поставщиком данных для внесения в блокчейн должен быть Росреестр или другая уполномоченная федеральная служба. Никакой иной вариант просто не может быть достаточно надежным и вызывающим доверие как у правительства, так и у населения. Децентрализованным системам еще предстоит пройти путь в десятилетия успешной работы, чтобы претендовать на доверие в таких сферах, как, например, право собственности на недвижимость или землю. Впрочем, даже при решении менее ответственных задач блокчейну еще нужно будет завоевать доверие как чиновников, так и остальных граждан.

Исходя из этого, организационная структура реестра может оказаться гораздо сложнее и, вероятно, должна будет остаться иерархической. Что практически неприемлемо для публичного блокчейна.

Так, реестру объектов недвижимости необходимо ограничение доступа для чтения, причем доступ должен быть максимально персонифицированным и легко изменяемым. Для этого в системе нужна внешняя или внутренняя аутентификация, определяющая доступ конкретного пользователя к тем или иным записям реестра и даже их элементам в течение определенного периода времени. Разумеется, в теории возможна полная или частичная реализация такой политики доступа в виде смарт-контрактов, но на практике она может столкнуться с огромным количеством атак, и принятие решений человеком будет гораздо эффективнее. Все это приводит к необходимости наличия в системе привилегированных пользователей, а следовательно, и к централизации управления.

В наиболее очевидном варианте все основные операции с цифровым реестром должны визироваться многосторонними подписями сотрудников Росреестра или другого уполномоченного ведомства. Доступ же граждан без дополнительных затрат может осуществляться с помощью действующей на данный момент на сервисах госуслуг технологии электронных цифровых подписей (ЭЦП). Связанная с гражданином персональная ЭЦП дает ему право полного просмотра сведений о принадлежащих ему объектах и подачи запросов на доступ к другим объектам. При этом доступ к просмотру информации о не принадлежащем ему объекте заявитель может получить только после утверждения запроса администратором реестра. Использование этой схемы делает возможной дальнейшую интеграцию блокчейн-платформы с «Порталом государственных услуг» и значительно облегчит применение блокчейна в других сервисах.

Следующим этапом участия граждан в работе цифрового реестра может стать автоматизация проведения операций с объектами недвижимости. Та же ЭЦП обеспечит возможность временной авторизации в блокчейне для проведения сделок с объектом недвижимости. В случае, например, продажи квартиры две стороны сделки удостоверяют договор купли-продажи своими ЭЦП, в результате чего создается транзакция с многосторонней подписью, участниками которой становятся продавец и покупатель. Таким образом они получают возможность разового внесения записи в блокчейн, которая удостоверяется привилегированным пользователем — сотрудником государственного органа.

С использованием этих технологий большинство операций с недвижимостью может быть практически полностью перенесено в блокчейн, что значительно ускорит процесс их оформления, позволит хранить всю информацию об объектах недвижимости и операциях с ними в одном онлайн-реестре, а также значительно снизит затраты государственных служб.

Конечно, у медали есть и обратная сторона: развертывание подобной системы в масштабах страны потребует очень серьезных материальных и человеческих ресурсов и на решение всех проблем безопасности как самого реестра, так и персональных данных пользователей уйдет несколько лет.

В частности, одной из проблем технического характера будет место хранения документов, имеющих достаточно большой объем, из-за чего включать их содержимое в блокчейн было бы затруднительно. Возникает, например, вопрос, будут ли храниться в блокчейне сами правоустанавливающие и сопутствующие документы или только их хеши. Подключение таких технологий, как IPFS, позволит привязывать к записям в реестре любой набор необходимых документов: договор купли-продажи или дарения, технический паспорт, договор ипотеки и прочие многочисленные документы, которыми рано или поздно обрастает любой объект недвижимости. Этот вопрос останется актуальным до тех пор, пока весь документооборот по операциям с недвижимостью не будет переведен в электронную форму.

Исходя из всего многообразия требований, необходимых для полноценного функционирования цифрового реестра, можно сделать вывод, что для реорганизации государственных реестров нужен специализированный блокчейн, созданный с использованием общедоступного конструктора, такого как Hyperledger.

Публичные блокчейны не могут обеспечить достаточно гибкой системы контроля доступа, а кроме того, их ограничивает необходимость учитывать интересы всех остальных пользователей и разработчиков. Например, те могут вовсе не обрадоваться размещению в сети «тяжелого» реестра, который будет занимать много места в блоках и тормозить транзакции пользователей. Не говоря о том, что разработчики могут провести обновление блокчейна, которое изменит формат транзакций, и в результате придется переделывать модель хранения данных государственного реестра.

Единственным на сегодняшний день действующим примером размещения государственного реестра в блокчейне остается эксперимент компании Bitfury, которая с 2015 года начала размещать в блокчейне Bitcoin данные земельного кадастра Грузии. Это привело к созданию существенного трафика, повышению комиссий и, соответственно, недовольству пользователей. Позже Bitfury пошла по пути создания собственной платформ частных блокчейнов Exonum и, вероятно, начнет переводить на нее всех своих клиентов.

Аналогичным образом может быть оцифрован и переведен на блокчейн любой другой государственный реестр, причем для множества реестров можно использовать единый блокчейн, а также единую систему управления данными и идентификации пользователей.

Электронный нотариат

Перевод на блокчейн государственных реестров потянет за собой и блокчейнизацию множества сопутствующих услуг. Одна из них — это нотариат, который также может получить существенные выгоды от использования неизменяемого и доказуемо идентичного блокчейна. Очень похожий на подписание публичных блокчейн-транзакций механизм используют и сервисы удостоверения документов, которые часто называют электронными нотариусами. Таких сервисов пока немного, все они частные и носят экспериментальный характер, в основном из-за того, что в большинстве юрисдикций информация, размещенная в блокчейне, все еще не признается юридически значимой.

Основная функция цифровых нотариусов состоит в предоставлении неопровержимых доказательств, что некий документ в определенный момент времени был удостоверен подписями нескольких человек. Технология блокчейна обеспечивает неизменность подписанного документа. Однако здесь автоматизация процесса удостоверения документов грозит разрушить сложившийся на протяжении нескольких столетий институт нотариата, лишив обычных нотариусов значительной части оказываемых ими услуг. Впрочем, на фоне других изменений, которые обещает принести блокчейн, этот эпизод может стать не самым заметным.

Цифровая идентификация

Любое применение блокчейна в государственных сервисах не будет эффективным без создания так называемых цифровых профилей пользователей реестров, то есть граждан и организаций. И если в отношении организаций решение вопроса может быть более или менее стандартным, поскольку основные данные юридических лиц, как правило, публичны, то с физическими лицами реализовать создание профилей будет сложнее.

Для создания полноценного цифрового профиля гражданина требуется поместить в этот профиль все его основные персональные данные, которые в соответствии с законодательством большинства стран должны оставаться конфиденциальными. И здесь ключевым становится вопрос безопасности хранения этих данных. В обеспечении их неизменности и многократного резервирования в децентрализованной сети технологии блокчейна нет равных, но другое важное преимущество блокчейна — публичность транзакций — в данном случае оказывается скорее недостатком.

Даже наиболее современные методы шифрования в будущем неизбежно устареют и могут быть легко взломаны. Но поскольку каждый пользователь публичного блокчейна имеет его полную копию, то в руках злоумышленников со временем могут оказаться и все когда-то

секретные персональные данные, пусть и в определенной степени устаревшие. Ведь даже если шифрование будет взломано через 20 лет, очень многие из занесенных в систему людей все еще будут живы и их данные окажутся скомпрометированы.

Есть только два способа избежать этого: сделать блокчейн закрытым (только для внутреннего пользования), при этом жертвуя преимуществами полного взаимодействия с пользователями в режиме онлайн, или ввести ограничения на доступ к информации на уровне самого протокола блокчейна. В этом случае на запросы конкретных пользователей должны открываться только небольшие фрагменты данных блокчейна, основная же их часть будет всегда защищена мультиподписными административными ключами.

Для онлайн-взаимодействия государственных сервисов с гражданами необходима идентификация пользователя, а если гражданам придется для получения госуслуг по-прежнему посещать соответствующие ведомства, то внедрение блокчейна утратит многие преимущества. Даже если идентификация пользователей не будет проводиться непосредственно в блокчейне, для нее в любом случае понадобится техническое решение, способное наиболее надежно удостоверить личность пользователя. Здесь возможны два варианта:

1. Классическая ЭЦП, выдаваемая удостоверяющим центром в качестве цифрового сертификата. Она недостаточно надежна для совершения действий с крупными денежными суммами, так как ее носитель может быть похищен или скомпрометирован и, например, сделка по продаже квартиры может быть осуществлена без ведома ее настоящего собственника.

2. Биометрическая идентификация по ряду параметров — от отпечатков пальцев до распознавания лица и сетчатки глаза. Похитить хранящиеся в едином центре идентификации образцы биометрии конкретного гражданина гораздо сложнее, но все же возможность компрометации биометрических данных не может быть сведена к нулю. И в отличие от ЭЦП, которая легко перевыпускается, заменить отпечатки пальцев или сетчатку глаза невозможно. Следовательно, хранение таких данных в блокчейне повышает риски, однако хранение там только их хешей в целях верификации гораздо безопаснее.

Учитывая консерватизм государственных проектов и необходимость многократного тестирования всех внедряемых технических решений, особенно столь инновационных, не следует удивляться тому, что системы идентификации на основе блокчейна до сих пор очень далеки от практической реализации. Впрочем, это касается и корпоративного сектора, для которого подобные системы также представляют интерес.

В 2017 году была создана некоммерческая организация Decentralized Identity Foundation (DIF), которая к маю 2018 года сообщила об увеличении количества ее членов до 56, включая таких грандов индустрии ИТ, как IBM и Microsoft, а также известные блокчейн-компании (Hyperledger, R3, IOTA, Ontology, Civic, Blockstack и другие). Однако о результатах деятельности этой организации до сих пор ничего не известно.

В феврале 2018 года появилась информация о разработке в Microsoft собственного решения для децентрализованной идентификации (DID) с использованием публичных блокчейнов Bitcoin, Litecoin и Ethereum, а также его подключения к системе Microsoft Authenticator (хотя впервые о разработке в Microsoft блокчейн-системы идентификации стало известно еще в 2016 году). Новое направление представил директор по управлению программами идентификации компании Microsoft Алекс Саймонс. Но по прошествии полугода и об этой разработке не появилось никаких новостей.

Еще одним крупным проектом в области обеспечения идентификации на блокчейне можно назвать китайский проект Ontology, запустивший собственный блокчейн в июле 2018 года, но и он еще не представил работающего решения. Поскольку Ontology тесно связан с

«китайским Ethereum» NEO, а тот, в свою очередь, не скрывает сотрудничества с правительством Китая, скорее всего, этот проект останется локальным.

Интеллектуальная собственность

Еще одна развитая отрасль современной экономики, в которой блокчейн может показать все свои возможности, — интеллектуальная собственность, где для технологии распределенного реестра открываются очень широкие перспективы и уже предпринимаются серьезные попытки ее внедрения.

В постиндустриальной экономике суммарная стоимость объектов интеллектуальной собственности компании может значительно превышать все ее материальные активы, но управление цифровыми правами и меры их регулирования все еще сильно отстают от технологического прогресса. Именно блокчейн может стать недостающим звеном, которое обеспечит прозрачное взаимодействие правообладателей с потребителями и регуляторами.

Права на объекты интеллектуальной собственности при всей своей виртуальности обеспечивают высокую внутреннюю стоимость. Набор патентов у многих технологических корпораций очень часто стоит гораздо больше всех остальных разработок и производственных мощностей. Например, когда корпорация Oracle в 2009 году поглотила Sun Microsystems, в первую очередь она стремилась заполучить именно многочисленные патенты Sun в области разработки операционных систем и программного обеспечения, а основная деятельность одного из некогда крупнейших производителей компьютеров и серверов была вскоре свернута.

Предоставление неисключительных прав на музыкальный альбом или фильм, как правило, является основным доходом его правообладателя и в наиболее успешных случаях многократно окупает все затраты на создание контента. При этом информация о правах на объекты интеллектуальной собственности и их использовании в интернете обычно очень слабо контролируется, что дает полный простор пиратам для злоупотреблений.

Однако сфера интеллектуальной собственности вовсе не так едина, как кажется. В ней существует два основных направления, практически обособленных друг от друга:

1. Промышленная интеллектуальная собственность. В нее входят товарные знаки (торговые марки), которые защищают бренд, символику и прочие уникальные атрибуты компании, а также патенты, которые, соответственно, защищают приоритет компании на технологические разработки.

2. Авторское право, или копирайт. К этому направлению относится защита прав на результаты интеллектуальной (творческой) деятельности в искусстве, литературе, а также теоретической науке и разработке программного обеспечения.

Впрочем, эти направления в некоторых случаях достаточно плотно пересекаются. Так, концепция и уникальные особенности какого-либо приложения (например, специализированного протокола блокчейна) защищаются одним или несколькими патентами, в то время как программный код этого приложения является объектом авторского права.

Как же технология блокчейна, а в данном случае ее реализация в качестве цифрового реестра, может быть применена в сфере интеллектуальной собственности и каким образом способна принести в первую очередь экономические выгоды?

Нюансы применения цифровых реестров

Между объектами промышленной собственности и авторского права существует одно кардинальное различие, определяющее взаимодействие правообладателя, регулятора и пользователя.

Объекты промышленной собственности подлежат обязательной регистрации в патентном ведомстве страны, резидентом которой является правообладатель (например, в российском Роспатенте или американском USPTO). Правовая охрана товарного знака или патента начинается только с момента принятия и публикации решения о регистрации, которое фиксируется регулятором (патентным ведомством). Любые существенные изменения в правах на этот объект также проходят через регулятора, в том числе передача прав, сдача объекта в аренду, лицензирование и т.д. Таким образом обеспечивается централизация системы выдачи прав и управления ими в отношении объектов промышленной собственности, при этом основным центром принятия решений всегда является регулятор. Следовательно, при переводе этих операций на блокчейн, как и в случае с прочими государственными реестрами, Роспатент или другой регулирующий орган будет выступать в качестве администратора цифрового реестра объектов промышленной собственности.

Что касается объектов авторского права, то здесь ситуация во многом противоположная. Исключительные права на объекты авторского права возникают непосредственно в момент их создания, и автор становится первым правообладателем своего творения. Причем эти права не нуждаются в какой-либо регистрации. Если автор желает закрепить за собой приоритет на произведение, он проходит добровольную процедуру депонирования, то есть подтверждения того, что именно он создал данное произведение. Депонирование может осуществить уполномоченная организация, такая как РАО (Российское авторское общество), в отношении произведений искусства, или нотариус в отношении любого из объектов авторского права. Программный код, как правило, депонируется в Роспатенте, но процедура опять же носит характер уведомления, а не утверждения — регулятор не может отобрать у автора его права. Позже эти права могут перейти к другому человеку или организации, но передача оформляется с помощью договора произвольной формы, без обращения к каким-либо регуляторам.

Преимущества и препятствия

Исходя из вышеизложенного, система по учету объектов авторского права может быть децентрализованной и не требовать наличия администратора, принимающего решения о регистрации или переходе прав. Размещение цифрового реестра объектов авторского права возможно как в публичном, так и в частном блокчейне, причем большая часть аргументов приводится в пользу первого варианта. Поскольку регулятор в данном случае не нужен, любой пользователь может самостоятельно распоряжаться принадлежащими ему объектами и правами на них. Единственным доказательством обладания правами на интеллектуальную собственность в таком случае становится владение закрытым ключом (подписью), примененным для внесения этого объекта в блокчейн. Именно поэтому практически все попытки создания распределенного реестра для объектов интеллектуальной собственности приходятся на объекты авторских прав.

Главная проблема перехода на блокчейн и вместе с тем мотивация для этого заключается в том, что не существует единой базы данных даже объектов промышленной собственности, и ее появления в ближайшем будущем не предполагается. Что касается авторского права, то создание единой глобальной базы данных даже не обсуждается. Но технологии блокчейна вполне под силу справиться с этой задачей, ведь блокчейн по сути своей глобален, децентрализован и не требует доверия между пользователями для того, чтобы доказать приоритет и аутентичность добавляемой в него информации.

Составление всемирной базы данных всех объектов промышленной собственности на основе блокчейна вполне реально и может совершить прорыв в отрасли. Такая база данных объединит информацию патентных ведомств всех стран и сделает ненужными перекрестные запросы, которыми эти ведомства вынуждены постоянно обмениваться. Этой базой будет возможно пользоваться с любого устройства в каждой точке мира, а при необходимости и хранить ее на собственном компьютере. Информация в такой базе обновляется в режиме онлайн через короткие промежутки времени, и достоверность хранимых данных не вызывает

сомнений, поскольку изменить или удалить их невозможно. В идеале информацию о любом патенте или товарном знаке, когда-либо выданном в любой стране, а также о переходе прав на объект возможно будет получить с помощью простого запроса из веб-интерфейса или локальной программы-клиента.

К сожалению, реализация такого проекта требует принятия международных стандартов хранения и обработки данных в блокчейне, а также участия патентных ведомств всех стран. Кроме того, необходимо и юридическое признание блокчейна. Поэтому создание глобального цифрового реестра объектов промышленной собственности при всех его преимуществах остается делом далекого будущего. Однако в отдельных странах попытки создать его уже предпринимаются. Активная работа в этом направлении ведется и в России при поддержке Роспатента.

Что касается учета объектов авторского права, ситуация здесь еще менее определенная. Государственные органы не занимаются учетом авторских прав, а нарушения в этой области рассматриваются общей судебной системой. РАО и другие подобные организации, разумеется, имеют базу данных зарегистрированных у них объектов, но они не ведут открытого реестра владения авторскими, имущественными и смежными правами. Такую информацию можно получить только по запросу и только если она касается объектов, депонированных в конкретной организации. Поэтому здесь также открываются широкие перспективы для блокчейна.

Область контроля авторских и смежных прав почти не регламентирована и фактически децентрализована. Объекты авторского права крайне разнообразны, а их количество не поддается учету: это литературные произведения, обычные СМИ и интернет-издания, научные работы, исходные коды программ, техническая документация, изображения, звукозаписи, видео и все остальное, что содержит новую уникальную информацию. Все это принято называть контентом. По самым грубым подсчетам, в мире ежедневно создаются сотни тысяч, а возможно, и миллионы единиц контента, хотя доля объектов, представляющих реальную ценность, вероятно, во много раз ниже. Вести полноценный учет всех существующих и вновь создаваемых объектов авторского права — титаническая задача даже с использованием современных технологий.

Примеры проектов

Любая система депонирования авторских прав, в том числе и на блокчейне, будет служить в первую очередь для закрепления приоритета исключительных прав на произведение. Для этого может подойти любой публичный блокчейн, записи в котором будут признаны юридически достоверными.

Следующий этап развития блокчейн-реестра объектов авторских прав — возможность распространения контента и учета его использования. Однако вторую задачу решить будет сложнее — например, если в видео- или аудиофайл достаточно легко встроить контрольные метки, ссылающиеся, например, на хеш в блокчейне, то с текстовыми произведениями эта схема не сработает. Кроме того, всерьез рассматривать возможность продажи контента через блокчейн еще очень рано.

С технической стороны функционирование подобного реестра выглядит достаточно просто до тех пор, пока к нему не будут присоединяться другие приложения для взаимодействия с конечными пользователями. Каждый пользователь полного узла блокчейна хранит у себя весь реестр загруженных на платформу произведений, но не может получить контент без ключа доступа, выдаваемого автором или смарт-контрактом после покупки. В самом блокчейне хранятся только хеши произведений, а контент в зашифрованном виде находится на компьютерах пользователей, предоставляющих свое дисковое пространство за арендную плату (в токенах), или в централизованных хранилищах, если речь идет о государственной или корпоративной системе. Блокчейн реестра объектов интеллектуальной собственности работает аналогично торрент-трекеру: он хранит хеши и права доступа, но не сам контент.

Несмотря на все сложности, уже существуют проекты, стремящиеся реализовать учет и управление контентом с помощью блокчейна, и количество их растет.

Одним из пионеров в области создания реестра авторских прав на блокчейне является стартап DECENT, основанный в 2014 году, а в 2017-м была запущена платформа для распространения цифрового контента. На этой платформе возможно осуществлять депонирование и мониторинг распространения цифрового контента с помощью блокчейна, при этом все операции производятся пользователями напрямую, без посредников. Пользователи могут самостоятельно вносить в реестр записи о своих произведениях, продавать и покупать контент напрямую с уплатой платформе небольшой комиссии. Все операции проводятся с использованием внутреннего токена DCT.

В 2016 году был запущен проект Mediachain, занимавшийся разработкой системы распространения контента с помощью реестра на блокчейне и распределенного хранения в системе IPFS. Однако рабочий продукт так и не появился. С тем же результатом аналогичную задачу пытался решить китайский стартап BlockCDN. Очевидно, что частных инициатив для запуска и раскрутки подобных проектов недостаточно, необходимо участие государства или лидеров индустрии.

Среди прочих проектов необходимо отметить начатую Intel в марте 2018 года разработку способа защиты авторских прав на изображения путем их регистрации в блокчейне. В дальнейшем планируется добавить инструменты, позволяющие обнаружить копирование или изменение контента, и начать работу с видеоконтентом и литературными произведениями.

В августе 2018 года американское информационное агентство Associated Press завило о сотрудничестве со стартапом Civil Media в разработке блокчейн-системы, предназначенной для учета и лицензирования выпускаемых агентством материалов, а также для контроля за их незаконным распространением.

В России в 2017 году был запущен амбициозный проект под названием IPChain, который поставил перед собой цель создать универсальный цифровой реестр для любых объектов интеллектуальной собственности, включая промышленную собственность. Проект разрабатывается на основе открытой платформы Hyperledger Fabric. В числе прочих учредителями проекта стали Всероссийская организация интеллектуальной собственности, фонд «Сколково», НИУ ВШЭ, Российский союз правообладателей, Российское авторское общество, НИУ ИТМО и банк «Новый век». Кроме того, узлы сети и филиалы организации планируется открыть в Азербайджане, Армении, Казахстане и Киргизии. В июне 2018 года о сотрудничестве с IPChain объявили Госфильмофонд и «Союзмультфильм». В декабре 2018 года Российский суд по интеллектуальным правам протестировал платформу IPChain и разместил на ней данные об изменении состава правообладателей ряда торговых марок.

Финансовые рынки и голосования

Из всех попыток использовать блокчейн отдельно от криптовалют, вероятно, наиболее близки к реализации проекты по применению этой технологии на финансовых рынках. Возможно, причина в том, что Bitcoin в свое время взбудоражил в первую очередь именно финансовый сектор, и блокчейну также начали искать применение в смежных областях. А может быть, дело в том, что практически все технические новинки находят первое применение именно в финансовой сфере: так было с телеграфом, радио, компьютерами и даже с модными сейчас большими данными и искусственным интеллектом.

Чем же цифровые реестры могут быть полезны финансовым рынкам? Здесь блокчейн возвращается к своему первозданному смыслу — реестр финансовых операций. Технология, созданная для обеспечения работы децентрализованной финансовой системы, вполне пригодна и для ее централизованных аналогов. Блокчейн возможно применять почти во всех аспектах работы традиционных бирж. На блокчейне могут сохраняться реестры биржевых операций, фиксироваться расчеты по ценным бумагам, проводиться клиринг, контроль маржинальных требований и многое другое. Также блокчейн подходит и для ведения реестра акционеров и надежной фиксации результатов голосований.

Американская компания OMX Group, оператор торговой площадки NASDAQ, начала первые эксперименты с блокчейном еще в 2015 году и с тех пор значительно продвинулась в этом вопросе, проведя пилотные проекты в своих биржевых подразделениях в Эстонии и Швеции. В ближайшее время блокчейн-сервисы могут появиться и на американском фондовом рынке.

Летом 2017 года появилась информация о создании неформальной рабочей группы по внедрению блокчейна, в которой участвуют несколько крупнейших национальных депозитариев: DTCC (США), CDS (Канада), Национальный расчетный депозитарий (Россия), Центральный депозитарий Южной Африки и DCV (Чили). Цель работы группы — создание международного стандарта обмена финансовой информацией с использованием блокчейна.

Национальный расчетный депозитарий России работает над созданием системы голосования акционеров по доверенности на базе Hyperledger Fabric.

Системы для проведения публичных голосований, в том числе выборов, — одна из самых перспективных, но до сих пор неосвоенных сфер применения блокчейна. В основном это объясняется консерватизмом избирательных органов, которые опасаются, что изменения могут привести к искажению и даже фальсификации результатов выборов. В частности, американские машины для голосования, используемые на выборах президента, остаются неизменными на протяжении десятилетий. Поэтому блокчейн еще не скоро сможет активно использоваться в этой сфере.

Системы контроля версий

И наконец, есть еще одна достаточно узкая область, в которой блокчейн появился на свет и также может быть очень полезен, хотя все еще не нашел подходящего применения. Это системы распределенной разработки приложений и контроля версий.

Неизменяемость информации и хронологическая последовательность транзакций делают блокчейн отличным инструментом для депозитариев программного обеспечения. Можно сказать, что возможность сохранения последовательности версий чего бы то ни было, в том числе и программного кода, встроена в него изначально.

В самом деле, поскольку в блокчейн невозможно внести изменения, новые версии не станут перезаписывать старые, а будут только сохраняться как обновления, связанные идентификатором проекта, номером версии и меткой времени.

Программный код состоит из текста, но для крупных приложений он может занимать несколько мегабайт, поэтому целесообразность его хранения в блокчейне остается под вопросом. Код можно хранить как непосредственно в блокчейне, так и отдельно, подобно объектам авторских прав.

Несмотря на перспективность этого направления, на данный момент ни одна из крупных платформ для разработчиков, таких как Github, Gitlab или Bitbucket, не заинтересовалась блокчейном, хотя он способен решить многие проблемы программных репозиториев.

Глава 5

Блокчейн для применения умных контрактов и децентрализованных приложений

Через пять лет после запуска первого блокчейна возродилась еще одна революционная идея, появившаяся задолго до Bitcoin. В 1994 году американский юрист и криптограф Ник Сабо представил концепцию умного контракта, или смарт-контракта (smart contract). Сабо был одним из самых очевидных кандидатов на роль Сатоси Накамото, анонимного создателя Bitcoin. Сабо отрицает, что он и есть Сатоси, хотя опосредованно принимал участие в работе по уточнению концепции первой криптовалюты, включая переписку на форумах.

Возможно, Ник Сабо не предполагал, что всего через несколько лет его изобретение будет тесно связано с технологией блокчейна, а основанные на этом симбиозе приложения

станут применяться во всех сферах жизни. Сейчас платформы смарт-контрактов уже бросают вызов Bitcoin и другим ведущим криптовалютам, а с учетом разработок в корпоративном секторе инвестиции в них, возможно, скоро превысят реальные вложения в криптовалюты. Уже через несколько лет смарт-контракты, вероятно, станут основным применением технологии блокчейна и будут использоваться в комплексе с криптовалютами и цифровыми реестрами, в том числе как связующее звено между ними и другими информационными системами и приложениями.

Определение умных контрактов

В юридическом смысле сущность смарт-контракта состоит в выполнении договора между двумя или более сторонами согласно заранее прописанным условиям. Смарт-контракт работает без непосредственного участия этих сторон путем автоматического проведения финансовых транзакций или других действий, которые могут быть выполнены с помощью программных средств. Результатом работы смарт-контракта может быть не только перевод денег (токенов) от одной стороны контракта другой, но и действия с какими-либо связанными с ним приложениями — например, регистрация (или отказ в регистрации) документа в цифровом реестре или предоставление доступа к объекту виртуального или реального мира, от покупки контента до аренды автомобиля.

Для соответствия требованиям действующего законодательства контракт и документы, свидетельствующие о его исполнении, могут быть продублированы на бумаге. Но в этом случае теряются практически все преимущества умных контрактов, кроме надежного хранения в блокчейне информации о договоре и его исполнении. Поэтому в ряде стран разрабатываются законопроекты о признании юридической силы смарт-контрактов и записей в распределенном реестре (блокчейне).

Легализация выполнения договоров без участия людей открывает широкие перспективы автоматизации многих процессов (от производственных и экономических до повседневных бытовых), но и порождает ряд проблем. В первую очередь это проблемы безопасности — при повсеместном распространении смарт-контрактов технический сбой в программном обеспечении или хакерская атака могут нарушить работу общественных организаций и даже создать угрозу для жизни людей. Поэтому как регулирование, так и внедрение децентрализованных приложений в реальную жизнь будут происходить медленно — возможно, это займет десятки лет.

Основная идея жизнеспособного умного контракта заключается в автоматизации многих простых операций, в том числе договоров и сделок между людьми или организациями, с участием двух и более сторон. Для этого операции необходимо представить в виде алгоритма, а объекты смарт-контракта должны быть доступны для прямого воздействия контракта, то есть исполняться без вмешательства человека. Каждый шаг алгоритма логически описывается и привязывается к выполнению определенных действий.

С технической точки зрения смарт-контракт представляет собой подписанный с помощью криптографических средств или других электронных удостоверений договор между произвольным количеством участников, реализованный в виде программного кода и полностью выполняемый в виртуальной среде распределенной вычислительной сети.

По сравнению с традиционными договорами смарт-контракт имеет следующие преимущества:

1. Автоматическое выполнение договора без вмешательства сторон или третьих лиц при наступлении записанных в алгоритме событий.

2. Условия контракта не могут быть изменены какой-либо из сторон и всегда исполняются в соответствии с заложенным алгоритмом.

3. Условия контракта общедоступны и могут быть верифицированы в любой момент.

4. Для заключения и выполнения смарт-контракта не требуются свидетели или посредники.

5. Автоматизация выполнения договоров и контроля процессов при массовом применении позволяет экономить значительные человеческие и материальные ресурсы.

Смарт-контракт состоит из хранящегося в блокчейне кода и оракулов — исходной информации из внешних источников.

Необходимое отступление

Теоретически любые транзакции в блокчейнах криптовалют, в том числе в Bitcoin, можно считать простыми смарт-контрактами. Они отправляются не конкретному получателю, а в децентрализованную сеть. Получить транзакцию и воспользоваться отправленными в ней биткоинами может любой, кто выполнит заложенные в транзакции условия.

Самый распространенный сейчас тип транзакций (P2PKH — pay to public key hash) основан на предъявлении получателем закрытого ключа, соответствующего отправленному в транзакции в виде хеша открытому ключу. Проверка выполняется любым узлом сети и представляет собой несколько типовых криптографических преобразований (на основе закрытого ключа по соответствующему алгоритму создается открытый ключ, который хешируется и сравнивается с хешем в транзакции). Есть и другие типы транзакций:

- P2IP, то есть платеж на IP-адрес (существовал в первых версиях протокола, но был удален из-за очевидной ненадежности). При использовании этого метода биткоины мог получить узел, прослушивающий сеть с определенного в транзакции IP-адреса.

- P2SH, или платеж по хешу скрипта (pay to script hash), — наиболее гибкий тип транзакций, формально и фактически представляющий собой платежный смарт-контракт. Для получения биткоинов по этому методу могут быть заданы уже более сложные условия: требование нескольких ключей (мультиподпись), пароля, наступление определенного момента времени (timelock) или другие условия, предусмотренные протоколом.

Язык скриптов Bitcoin достаточно примитивен и предназначен только для проведения платежей с набором условий, в то время как на специализированных платформах, где применяются полноценные языки программирования, смарт-контракты могут производить гораздо более сложные действия и даже обеспечивать выполнение многошаговых или интерактивных алгоритмов.

С появлением работающих блокчейн-платформ, осуществляющих работу смарт-контрактов для большого количества пользователей, и с накоплением опыта их эксплуатации концепция умного контракта была расширена и преобразована в концепцию децентрализованного приложения (decentralized application, DApp). Это более широкое понятие, которое включает не только сам код контракта и входящие данные, но и интерфейсы для его взаимодействия с пользователями, другими приложениями и информационными системами.

То есть децентрализованное приложение — это не только некий код, по мере наступления заложенных алгоритмом условий выполняющий определенные действия. Правильно разработанное децентрализованное приложение, как и любое другое, — это законченный программный продукт, сопровождающий пользователей на всем протяжении

бизнес-процесса, от максимально удобного получения вводных данных до предоставления развернутой отчетности по результатам работы.

По мере интеграции в современные информационные системы децентрализованные приложения должны стать серверными узлами для локальных приложений и пользователей, обращающихся к ним через толстые клиенты или веб-интерфейсы.

Как работает смарт-контракт

Рассмотрим основные механизмы работы смарт-контрактов на примере платформы Ethereum, как самой развитой на сегодняшний день. На первый взгляд, архитектура блокчейна Ethereum имеет много общего с Bitcoin — сетевое взаимодействие узлов, кошельки, блоки, транзакции, ключи и подписи не слишком сильно отличаются, у всех блокчейн-платформ много общих деталей.

Но структура Ethereum сложнее, чем кажется на первый взгляд. То, что в криптовалютах является основой их функционирования, в Ethereum — только транспортная инфраструктура для обеспечения базовой безопасности транзакций. Сами же смарт-контракты, а вернее, их данные хранятся, пересылаются и обмениваются информацией внутри обычных криптовалютных транзакций. Токен ETH (ether, эфир) служит для оплаты создания контрактов, работы майнеров и производимых узлами сети при обработке контрактов распределенных вычислений.

Иными словами, платформа Ethereum двухуровневая и состоит из классического криптовалютного блокчейна, а также децентрализованной виртуальной машины для выполнения умных контрактов. На первом уровне архитектуры находится создаваемая майнерами цепочка блоков, которая выполняет функцию децентрализованного хранилища и среды обмена данными. На втором уровне работают сами децентрализованные приложения (контракты), которые через блокчейн получают исходные данные и отправляют результаты своей работы. Обращающиеся на платформе пользовательские токены второго уровня напрямую не связаны с ETH и могут выполнять самые различные функции, заложенные создателем приложения.

Блокчейн Ethereum задуман как децентрализованная виртуальная машина (EVM), которая обрабатывает исполнение смарт-контрактов на множестве подключенных узлов за небольшую плату в газе — микродолях токена ETH.

Контракты представляют собой программный код, который компилируется и загружается в блокчейн с привязкой к кошельку (аккаунту) его создателя. Для разработки контрактов в Ethereum используется собственный высокоуровневый язык программирования Solidity, подобный JavaScript. Перед загрузкой в блокчейн код контракта компилируется в байт-код, поэтому исходный код контракта в блокчейне не хранится, но, как правило, разработчики контрактов публикуют исходные коды для проверки сообществом.

Контракт работает достаточно просто:

1. На зарегистрированный в блокчейне адрес контракта отправляется транзакция, содержащая вводные данные. Для ICO это, например, обычная платежная транзакция с некоторой суммой ETH.

2. Получив входящую транзакцию, контракт «разбирает» ее и обрабатывает вводные согласно своему алгоритму, например вычисляет сумму купленных токенов для отправки.

3. Закончив работу, контракт формирует ответную транзакцию, в которой содержится вычисленная сумма токенов, и посылает ее на адрес, с которого пришла входящая транзакция.

Это самый простой случай работы смарт-контракта, на самом же деле язык Solidity достаточно гибок и может обрабатывать множество дополнительных условий. Самое главное, что контракты работают полностью автономно, то есть не требуют никаких подтверждений от человека — задача разработчиков состоит в том, чтобы написать контракт, скомпилировать и опубликовать в сети. Еще одно преимущество смарт-контракта в том, что его код не может быть изменен никем, кроме владельца аккаунта, но и это действие не может быть осуществлено незаметно для остальных пользователей блокчейна.

Обзор существующих платформ смарт-контрактов

Через 20 лет после публикации работ Ника Сабо его идею подхватил Виталик Бутерин, с группой единомышленников создавший в 2014 году проект Ethereum, который стал первой платформой смарт-контрактов, работающей на основе блокчейна.

К концу 2018 года число платформ для выполнения децентрализованных приложений превысило два десятка, но большинство из них все еще находится в разработке. Ниже приведен обзор наиболее перспективных проектов, включая те, для которых выполнение смарт-контрактов не является основной функцией.

Ethereum

В разговорах о смарт-контрактах чаще всего упоминается платформа Ethereum, разработчики которой первыми в мире заявили о возможности использования блокчейна для работы независимых децентрализованных приложений. Ethereum — пионер и законодатель мод в сфере смарт-контрактов, так же как Bitcoin в криптовалютах. Большая часть новых идей и разработок в этом направлении появляется именно в Ethereum, и на него же приходится большая часть ошибок — проявляются болезни роста.

Впервые идея создания платформы для выполнения умных контрактов была сформулирована Виталиком Бутериным, основателем интернет-журнала *Bitcoin Magazine,* в конце 2013 года, а весной 2014-го уже более проработанная концепция появилась в виде «желтых страниц», написанных Виталиком Бутериным совместно с Гэвином Вудом.

Летом 2014 года команда Ethereum провела самую успешную на тот момент продажу токенов, собрав более 31 000 биткоинов (около $18 млн, и именно тогда был введен в обиход термин «ICO» (см. главу 6).

Через год после завершения ICO, 30 июля 2015 года, командой Ethereum наконец был запущен собственный блокчейн на основе альфа-версии под названием Frontier. Среди участников ICO было распределено более 60 млн монет ETH, после чего был запущен майнинг PoW на GPU и CPU, который продолжается уже более трех лет, хотя стадия PoW была задумана только на полтора года, пока не будет подготовлен переход на консенсус Proof-of-Stake. Однако этот процесс затянулся и до сих пор далек от завершения.

В марте 2016 года вышла первая стабильная версия — Ethereum 1.0 Homestead. На платформе начали появляться десятки, а вскоре и сотни новых проектов, и некоторые из них достигали собственной капитализации в миллионы долларов.

Первое серьезное испытание для Ethereum наступило в июне 2016 года, когда вследствие ошибки кода в проекте TheDAO были украдены токены на сумму более $50 млн. Это вызвало катастрофическое падение курса эфира и заметное проседание большинства других криптовалют.

Сумма была настолько велика, что под давлением инвесторов TheDAO разработчики Ethereum пошли на беспрецедентный шаг: несмотря на возражения значительной части сообщества, был проведен хардфорк с заморозкой украденных токенов. Не согласные с политикой команды Бутерина не приняли хардфорка и образовали собственный блокчейн с копией всех транзакций Ethereum. Новая криптовалюта получила название Ethereum Classic и существует до сих пор.

Спустя три с лишним года после запуска блокчейна основной целью команды разработчиков Ethereum Foundation все еще является переход на метод консенсуса Proof-of-Stake с применением технологии шардинга, названной Casper (параллельной обработки сетью нескольких цепочек блоков с их последующим слиянием в единый блокчейн). Версия Ethereum на основе PoS и Casper носит предварительный номер 2.0 и называется Serenity. Главным нововведением Serenity станет изменение схемы эмиссии, создания блоков и управления децентрализованной сетью.

В концепции PoS Casper созданием блока и эмиссией новых монет ETH вместо майнеров будут заниматься валидаторы, в число которых сможет войти любой пользователь сети, имеющий на балансе аккаунта в блокчейне не менее 1000 ETH (эта сумма может быть изменена при подготовке релиза).

Валидаторы будут иметь потенциально более высокий уровень участия в сети, но он предполагает и определенную ответственность: если валидатора неоднократно уличат в подтверждении некорректных транзакций, попытке двойного расходования или других недобросовестных действиях, его депозит будет ликвидирован и он лишится возможности участвовать в создании блоков.

Однако все эти нововведения остаются далекой перспективой. Проблема масштабирования блокчейна Ethereum обостряется, так как сеть не справляется с наплывом новых пользователей и проектов. На конец февраля — начало марта 2019 года запланирован выход промежуточного релиза Constantinople, второго в серии обновлений Ethereum 1.5 Metropolis. В этом релизе в очередной раз награда майнеров за блок будет снижена (с 3 до 2 ETH), а также в третий раз будет отложено на год включение «бомбы сложности» — механизма, делающего майнинг по методу Proof-of-Work экономически невыгодным путем пошагового экспоненциального роста сложности майнинга через определенное количество блоков. Это обновление не приведет к глобальному увеличению пропускной способности сети, поэтому разработчики и сообщество получат только небольшую передышку. Существенные же изменения следует ожидать во второй половине 2019 года.

Курс внутренней монеты ETH (ether, эфир) менее чем за три года вырос в десятки тысяч раз, повторив успех биткоина. Начав с нескольких центов летом 2015-го, в начале 2018 года курс ETH кратковременно поднимался выше 0.125 BTC (около $1400) и к концу года все еще не смог повторить рекорд. В этот период капитализация Ethereum поднялась выше половины капитализации Bitcoin, и сторонники платформы начали говорить о смене лидера в отрасли блокчейна и о том, что смарт-контракты становятся важнее децентрализованных платежных сетей. Однако оптимизм быстро иссяк, и в свете множащихся проблем с масштабированием инвесторы продемонстрировали нарастающее разочарование в возможностях платформы. В результате начался обвал цены ETH, темпы которого значительно опередили падение других ведущих криптовалют. К началу сентября 2018 года эфир обвалился до $170, то есть в восемь с лишним раз от ранее зафиксированного максимума, тогда как локальный минимум биткоина сохраняется на уровне $5750, что всего в 3,5 раза меньше пиковых значений декабря 2017 года.

Тем не менее взлеты и падения на биржах не всегда отражают более существенную часть развития проекта, то есть именно то, для чего он и был создан. На Ethereum родились и умерли тысячи проектов, но есть несколько десятков действительно успешных, которые уже имеют минимальный рабочий продукт и достаточно хорошие перспективы его развития. Примеры децентрализованных приложений, работающих на блокчейне Ethereum:

- Augur — блокчейн-оракул, предназначенный для предсказания исхода практически любых событий или процессов в реальном мире на основе «мудрости толпы», то есть сбора ставок большого количества пользователей. Во многом похож на банальный тотализатор в новой упаковке, но может быть использован и для более практических целей.

- Golem — сеть распределенных вычислений на блокчейне, в которой пользователи могут сдавать в аренду вычислительные и другие свободные ресурсы оборудования с оплатой в токенах GNT. По сути, блокчейн Ethereum используется только в качестве учетной книги взаиморасчетов между арендаторами и владельцами оборудования. Вся остальная работа происходит с помощью локального приложения, разработанного командой Golem, которое устанавливается на компьютеры пользователей и служит для обмена данными (отправки заданий, обработки полученных результатов, а также учета потребленных ресурсов для оплаты). На данный момент реализована работа одного вида аренды — ресурсов графических процессоров (видеокарт).

- Brave — децентрализованный браузер, разработчики которого поставили цель избавить пользователей от надоедливой рекламы за небольшую плату в токенах или, наоборот, показывать наиболее подходящую пользователю таргетированную рекламу, за просмотр которой ему начисляется небольшая сумма в токенах BAT (Basic Attention Token). Токены выполняют роль внутренней расчетной единицы.

- Cryptokitties, или «Криптокотики», — первая популярная блокчейн-игра, созданная на основе уникальных токенов стандарта ERC-721 и буквально захлестнувшая блокчейн Ethereum в начале декабря 2017 года. Уникальность ее заключается в том, что в алгоритм игры заложен постепенный рост и развитие виртуальных котиков и даже их размножение. Однако все это происходит с помощью транзакций и создает заметную нагрузку на блокчейн. В первые недели ажиотажа редкие коллекционные экземпляры криптокотиков продавались за тысячи долларов, но вскоре это безумие прошло. Однако игра до сих пор существует, и пользователи продолжают выращивать новых котиков.

- 0x — платформа децентрализованного обмена различных токенизированных активов с помощью пересылки токенов. Во многом напоминает систему Ripple. Однако технические сложности пока мешают широкому распространению платформы.

- Maker — одна из первых стейблкоинов, то есть стабильных криптовалют. Внутренний токен MKR привязан не к материальному ресурсу или валюте, а к корзине криптовалют, поэтому зависит от общего состояния криптовалютного рынка. Предполагается использовать Maker для проведения займов и кредитов в криптовалютах.

- TUSD — токенизированный доллар на основе токена стандарта ERC-20, предложенный компанией Gemini братьев Уинклвосс. Выпущен в августе 2018 года и уже пущен в оборот на нескольких биржах.

Технологические наработки Эфириума были использованы не только в его публичных форках, большая часть которых затерялась среди сотен альтернативных криптовалют, но и в нескольких крупных корпоративных проектах:

Американский банк J. P. Morgan в 2016 году занялся разработкой собственной блокчейн-платформы, названной Quorum. Изначально она была скопирована с блокчейна Ethereum, но сразу проектировалась в качестве корпоративного блокчейна с централизованным управлением.

Российский проект «Мастерчейн», созданный в 2016 году Ассоциацией ФинТех по инициативе Банка России и ряда коммерческих банков, основан на протоколе Ethereum, но также имеет собственный частный блокчейн и работает на основе российских стандартов криптографии. Ассоциация планирует открыть исходные коды проекта, а пока платформой

пользуются только ее участники. С 2018 года на «Мастерчейне» было проведено несколько тестовых транзакций с реальными активами, но платформа все еще не применяется для повседневных операций.

В ноябре 2017 года создана некоммерческая организация Ethereum Enterprise Alliance (EEA) для разработки приложений корпоративного уровня на основе протокола Ethereum (но необязательно на его публичном блокчейне). В объединение входят более 100 крупных международных компаний из технологического и финансового сектора, в том числе Microsoft, Intel, AMD, Cisco, Shell, Accenture, Deloitte, Infosys, BBVA, J. P. Morgan, MUFG, Santander, «Сбербанк» и т.д.

EOS

Проект EOS стал результатом нескольких лет работы команды Дэна Ларимера, ранее создавшей имеющие некоторую популярность проекты — платформу криптоактивов Bitshares и децентрализованную социальную сеть Steemit. Впрочем, эти два блокчейна так и не смогли войти в топ-25 криптовалют по капитализации.

В основе функционирования блокчейна EOS лежит оригинальная версия механизма консенсуса PoS — DpoS (Delegated Proof-of-Stake). Она отличается от стандартного PoS тем, что количество майнеров (валидаторов, создателей блоков) в блокчейне ограничено и в состав этой привилегированной группы можно попасть только в результате голосования держателей токенов.

Таким образом управление блокчейном сосредоточивается в руках группы «китов» — делегатов, которым сообщество передоверило функции создания блоков и подтверждения транзакций. В EOS предусмотрено наличие только 21 создателя блоков, все они избираются на периодически проводимом автоматическом голосовании всех активных держателей токенов EOS.

После решения ряда технических и организационных проблем 14 июня 2018 года Блокчейн EOS был запущен по окончании голосования, определившего первого 21 создателя блоков.

Продажа токенов EOS была признана одной из самых успешных в истории — на момент ее окончания 2 июня 2018 года были собраны криптовалюты на $4 млрд, а вскоре после запуска блокчейна каждый токен EOS стоил около $12, что обеспечило всему проекту теоретическую капитализацию $12 млрд, которая вскоре, однако, заметно упала.

Еще одним интересным моментом при запуске EOS стала конвертация токенов на Ethereum в собственные монеты блокчейна EOS. Процедура проводилась в два этапа. Сначала покупатели токенов EOS должны были отправить на адрес смарт-контракта ICO сообщение, подписанное их закрытым ключом, чтобы зарегистрировать свои токены. При запуске блокчейна соответствующее токенам количество монет было разослано на зарегистрированные адреса, соответствующие закрытым ключам, аналогичным использованным в блокчейне Ethereum для покупки токенов. Несмотря на сложность процесса, существенных потерь токенов, в том числе из-за действий мошенников, большинству пользователей практически удалось избежать.

Наиболее интересной деталью в архитектуре EOS является впервые использованная модель делегированного управления: владельцы монет выбирают создателей блоков, которые и занимаются поддержкой работы блокчейна. Однако для разрешения спорных ситуаций потребовалось задействовать так называемых арбитров, имеющих в блокчейне очень широкие полномочия, вплоть до возможности блокировки кошелька и конфискации монет. Это очень заметный шаг в сторону централизации, поскольку сообществу крайне сложно защититься от произвола арбитров, так же как и от сговора создателей блоков, тем более что и те, и другие могут оставаться условно анонимными. Насколько работоспособными окажутся эти механизмы управления, покажет время.

В сентябре 2018 года на блокчейн EOS работало несколько десятков проектов, в основном находящихся на ранних этапах разработки, и активность пользователей была

недостаточна, чтобы говорить о серьезной проверке производительности и безопасности блокчейна. Тем не менее на данный момент EOS — наиболее серьезный противник Ethereum, так как в нем изначально не существует проблемы масштабирования, связанной с консенсусом PoW, а также гонки мощностей и постоянного роста энергопотребления майнерами.

NEO

Этот китайский проект наиболее известен тем, что его прочат в прямые конкуренты Ethereum и часто называют «китайским Эфириумом». NEO был основан еще в 2014 году (первоначально он назывался Antshares) и разрабатывался в тесном контакте с компанией OnChain, а также в партнерстве с Microsoft. С 2016 года проект присоединился к консорциуму Hyperledger. В NEO был разработан оригинальный механизм консенсуса dBFT (delegated Byzantine Fault Tolerance) на основе технологий Hyperledger, предназначенных в первую очередь для частных блокчейнов. Это обеспечивает ему пропускную способность до 10 000 транзакций в секунду. Для платежей за транзакции используются отдельные токены GAS, которые генерируются в кошельках, содержащих токены NEO.

В отличие от Ethereum, для написания смарт-контрактов в NEO могут быть использованы распространенные языки программирования, такие как C#, Python, Java, Javascript и другие. Виртуальная машина NeoVM имеет лучшие характеристики изоляции и безопасности по сравнению с Ethereum и может использовать более широкий набор компиляторов кода. Кроме того, в NEO изначально реализованы несколько дополнительных компонентов, расширяющих возможности платформы:

- NeoFS — сервис децентрализованного хранения файлов на основе протокола IPFS;
- NeoX — собственная реализация атомарных свопов для взаимодействия с другими блокчейнами;
- NEP5 — стандартизированный набор инструментов для разработчиков, облегчающий написание и тестирование децентрализованных приложений.

В 2017 году стало известно, что криптовалюта NEO может быть использована в разрабатываемой OnChain инфраструктуре децентрализованных приложений под названием DNA (Decentralized Network Architecture). Архитектура этой платформы подразумевает применение цифровой идентификации пользователей. Вероятно, для этого будет использован также принадлежащий OnChain проект Ontology. Программа курируется правительственными органами Китая, и, согласно полуофициальной информации от осведомленных источников, NEO может стать китайской национальной блокчейн-платформой.

Разумеется, это принесет проекту блестящие перспективы внутри Китая, но он вряд ли сможет выйти на глобальные рынки, поскольку и независимое сообщество, и правительства других стран будут настороженно относиться к платформе, подконтрольной китайскому правительству.

NEO все еще находится в тестовой стадии, хотя блокчейн уже запущен и располагает небольшим количеством работающих на нем приложений.

Tezos

Проект Tezos провел один из самых успешных ICO в истории, в июле 2017 года собрав монеты эфира на сумму более $230 млн, но едва не стал жертвой внутреннего конфликта. Двое сооснователей, супруги Артур и Кэйтлин Брайтманы, поссорились с управляющим

директором Йоханом Геверсом, который занимался проведением ICO, и добились его ухода из команды.

Это задержало развитие проекта на несколько месяцев и породило ряд судебных разбирательств, которые на момент издания книги не закончены. Кроме того, в июне 2018 года покупателей токенов Tezos (XTZ) «обрадовали» тем, что для получения токенов в основной сети им потребуется пройти процедуру идентификации личности (KYC), хотя во время ICO токены продавались анонимно и ни о каких проверках речь не шла.

Все эти неурядицы подорвали репутацию проекта, а также привели к значительным задержкам, и он смог выйти в свет значительно позже EOS, проиграв гонку одному из основных конкурентов с практически аналогичной функциональностью.

Преодолев все препятствия, блокчейн Tezos был запущен в сентябре 2018 года и почти сразу столкнулся с серьезными неприятностями. Уже через несколько дней после запуска в протоколе был обнаружен баг, который увеличил время создания блоков до 20 минут. Уязвимость была устранена, но такие ошибки на старте забываются не скоро.

Хотя у Tezos очень много общего с EOS, эта платформа использует модификацию консенсуса DPOS под названием LPOS, которая улучшает степень децентрализации сети, так как количество валидаторов в этом методе не фиксируется. Также разработчиками заявлено проведение «мягких» обновлений протокола с помощью голосования держателей токенов, что должно сгладить противоречия в сообществе и избежать раскола сети в результате хардфорков. Для программирования приложений на Tezos используется появившийся в 1996 году язык OCaml.

Lisk

Один из пионеров отрасли смарт-контрактов и, вероятно, первый из известных соперников Ethereum. Создан командой из Германии. Разработчики, собрав на ICO около $6 млн, сосредоточились на технической стороне проекта, не уделив должного внимания маркетингу. При всех плюсах такого подхода они упустили время и затерялись среди конкурирующих проектов, более агрессивно пиаривших свои преимущества.

В отличие от Ethereum, Lisk предлагает обособленную среду выполнения для каждого контракта, поэтому взлом или технические проблемы одного Dapp не повлияют на другие приложения и платформу в целом, что поможет избежать принятия критических мер, таких как хардфорк для восстановления токенов TheDAO. Однако на Lisk до сих пор работает всего несколько десятков небольших проектов, так как большинство предпочитает оставаться на Ethereum как более популярном и проверенном блокчейне.

RChain

Этот проект, находящийся в стадии разработки, создан командой «раскольников», ушедших из других блокчейн-проектов. Во главе его стоят Грег Мередит, ранее бывший сооснователем неудавшейся децентрализованной социальной сети Synereo, и Влад Замфир, один из сооснователей Ethereum и соавтор технологии Casper, не прижившийся в команде Виталика Бутерина.

Эти люди, несмотря на неудобный характер, являются профессионалами своего дела, и, если доведут работу до конца, RChain сможет занять свою нишу на рынке. Команда проекта активно общается в социальных сетях и информирует о ходе разработок. В сентябре 2018 года запущена тестовая сеть. Однако к планируемому весной 2019 года запуску платформы рынок будет уже довольно плотно занят другими платформами, и команде RChain придется подумать, какие преимущества они смогут предоставить пользователям и разработчикам Dapps.

Другие блокчейны с возможностью выполнения смарт-контрактов

Как уже говорилось ранее, любой блокчейн представляет собой программный продукт, который может быть изменен и усовершенствован, причем нередко это делается без сохранения совместимости с предыдущими версиями протокола (так называемый хардфорк). Поэтому после успеха Ethereum разработчики многих блокчейн-проектов задумались о внедрении смарт-контрактов в дополнение к обычным функциям.

Bitcoin

В последние годы сформировалась достаточно заметная группа сторонников «одного блокчейна». Они исходят из того, что один главный, лучше всех развитый и защищенный блокчейн может выполнять все основные функции, сделав остальные вспомогательными или попросту ненужными.

Проект по развертыванию функциональности платформы смарт-контрактов на блокчейне Bitcoin под названием RootStock (RSK) пришел из 2015 года, то есть он появился несколько позже Ethereum. Его разработка продолжается с переменным успехом уже почти три года, но конечный продукт все еще не заработал в полную силу, несмотря на состоявшийся в январе 2018 года запуск в основной сети. Это говорит о сложности развертывания на криптовалютном блокчейне сколько-нибудь функциональных смарт-контрактов. Кроме того, транзакции в сети Bitcoin без применения Ligthning Network традиционно остаются достаточно дорогими из-за высокой цены BTC.

Чтобы избежать этих проблем, для работы смарт-контрактов RSK планирует использовать систему дочерних цепочек (сайдчейнов), а для внутренних расчетов — собственный токен RTC. Консенсус Rootstock применяет собственный метод DECOR+ и основан на совместном майнинге (merged mining) с биткоином. Однако блоки в сайдчейне RSK появляются в 60 раз быстрее — через каждые 10 секунд, что обеспечивает пропускную способность до 300 транзакций в секунду. Что интересно, RSK имеет совместимую с Ethereum виртуальную машину для обработки смарт-контрактов, а сами контракты пишутся на разработанном для Ethereum языке Solidity.

Cardano

Достаточно спорный проект, созданный широко известным в сообществе блокчейна активистом — американцем Чарльзом Хоскинсоном, принимавшим участие в создании ряда проектов, включая Ethereum и Ethereum Classic. Этот проект одним из первых обозначил свою принадлежность к третьему поколению блокчейнов (blockchain 3.0) и провел активную рекламную кампанию в период продажи токенов, что позволило ему обосноваться в топ-10 криптовалют согласно рейтингу Coinmarketcap.

Главное, что вызывает сомнение в успехе Cardano, — это попытка разработчиков «объять необъятное», создать универсальную блокчейн-инфраструктуру, способную выполнять буквально все задачи, в которых предполагается использование распределенных реестров. Разработчики Cardano проектируют многоуровневую архитектуру, в которой каждый уровень будет в достаточной мере изолирован от прочих и способен выполнять только свою специфическую функцию. В качестве образца взята давно принятая в отрасли ИТ семиуровневая модель OSI (Open System Interconnection), в которой на каждом уровне работают специальные протоколы и стандарты (на втором — Ethernet и ему подобные, на третьем — IP, на четвертом — TCP и UDP и т.д.).

В модели Cardano архитектура блокчейна также разделена на уровни, где базовым является уровень транзакций (Settlement Layer), а за смарт-контракты отвечает вычислительный уровень (Computation Layer). В целом Cardano пока мало отличается от других новейших проектов, таких как EOS и Tezos, но его разработчики планируют исправить ошибки (или то, что они считают таковыми), встречающиеся в уже существующих блокчейнах.

Блокчейн Cardano с внутренним токеном ADA был запущен в сентябре 2017 года, но смарт-контракты в нем еще не функционируют и сроки завершения разработки пока неизвестны. Для написания кода контрактов будет использоваться известный еще с 1990-х язык программирования общего назначения Haskell.

Waves

Один из немногих российских блокчейн-проектов, завоевавших международное признание. Блокчейн-платформа Waves основана в 2016 году и первоначально позиционировалась как платформа для выпуска криптоактивов. В марте 2017-го была запущена децентрализованная биржа (DEX), бета-тестирование которой было завершено в июле 2018-го. В течение 2017 года также появились платежные шлюзы для покупки и продажи криптовалют за доллары и евро с регистрацией транзакций в блокчейне.

Проект долго шел к внедрению смарт-контрактов, и в мае 2018 года функциональность смарт-контрактов появилась в тестнете. Это был запуск так называемых тьюринг-неполных смарт-контрактов с ограниченной функциональностью, которая в основном заключается в повышении безопасности токенов путем внедрения мультиподписей и двухфакторной аутентификации. Кроме того, появились атомарные свопы для взаимодействия с другими блокчейнами и механизм оракулов для получения контрактами данных извне. В платформе используется собственный язык программирования контрактов RIDE.

Первая стадия тьюринг-неполных смарт-контрактов была запущена в основной сети Waves в конце сентября 2018 года, тестирование полноценных контрактов все еще продолжается.

Запуск смарт-контрактов на платформе несколько запоздал. Он выглядел бы более логичным в 2017 году, во время продолжающегося бума ICO, но в 2018-м ажиотаж заметно спал и количество новых проектов многократно уменьшилось. Количество ICO на Waves и объемы привлеченных средств не идут в сравнение с показателями Ethereum, в основном это продажи токенов русскоязычных проектов. В частности, это были: проект «Партии роста» Upcoin, токен правительства Амурской области Amurcoin, ZrCoin и другие.

В российском секторе блокчейна Waves как национальная платформа сможет составить конкуренцию платформам западных компаний, таким как Bitfury Exonum, R3 Corda и Hyperledger Fabric. В частности, Waves сотрудничает в рамках тестирования и внедрения блокчейна с такими крупными игроками на российском рынке, как «Газпромбанк», ВЭБ и корпорация «Ростех» (в рамках внедрения блокчейн-платформы Vostok, которая будет работать на Дальнем Востоке).

NXT/Ardor

Первая многофункциональная криптовалютная платформа, запущенная почти на два года раньше Ethereum, и первая присвоившая себе наименование блокчейна 2.0. На NXT были реализованы возможности выпуска токенов, проведения голосований, зашифрованного обмена сообщениями через блокчейн, а также размещена децентрализованная биржа, встроенная в клиент. Однако платформа не получила признания из-за слабой масштабируемости и проблем с безопасностью. С 1 января 2018 года заработала ее усовершенствованная версия под названием Ardor, которая позиционируется как платформа BaaS (Blockchain as a Service) для создания пользовательских сайдчейнов. На Ardor в числе прочего реализована возможность работы облегченных смарт-контрактов, которые могут исполняться на части узлов, а не всей сетью, как в Ethereum. В Ardor смарт-контракты выполняют исключительно служебную роль.

Собственный блокчейн или DApp?

Команде каждого нового проекта, в котором предполагается использовать смарт-контракты, в первую очередь приходится решить вопрос: создавать ли собственный блокчейн или

удовлетвориться разработкой приложения на одной из описанных выше платформ? У каждого подхода есть свои преимущества и недостатки, и их следует оценить перед тем, как сделать окончательный выбор. Для этого можно использовать достаточно простой чек-лист:

- *Объем хранимых данных.* Если проекту требуется обрабатывать и размещать в блокчейне большие массивы текстовой или даже мультимедийной информации, следует задуматься об отдельном блокчейне, так как на публичной платформе существенный трафик обойдется дорого и может даже привести к замедлению всей сети. В ином случае необходимости в запуске собственного блокчейна нет.

- *Уникальная конфигурация данных.* Если применяемый в каком-либо публичном блокчейне формат данных, транзакций и блоков устраивает разработчиков и существенных изменений модели данных не предполагается, то вполне возможно использовать одну из публичных платформ смарт-контрактов.

- *Политика доступа.* Разработка корпоративных блокчейнов началась в том числе из-за того, что вся информация в общедоступных блокчейнах может быть считана любым из пользователей этого блокчейна. И даже шифрование не всегда служит гарантией сохранения конфиденциальности. Поэтому, если проекту нужна иерархическая схема доступа к данным и имеются требования секретности и конфиденциальности, следует обратиться к платформам частных блокчейнов или задуматься о создании собственного.

- *Внутренняя экономика проекта*. Любая из публичных платформ налагает определенные ограничения, которым разработчикам Dapps приходится следовать. Поэтому для применения сложных внутриэкономических схем возможностей публичного блокчейна может оказаться недостаточно, или использование их будет стоить слишком дорого и приведет к значительным расходам при пересылке внутренней или технической информации, поскольку все транзакции требуют определенной платы.

- *Зависимость от сторонних разработчиков.* С технической стороны разработчики Dapp также зависят от политики выбранной платформы. Например, если им потребуется внести какие-либо изменения в протокол, способные затронуть другие проекты, в таких доработках, вероятно, будет отказано. К тому же команда разработчиков платформы работает по собственным планам, учитывая пожелания всего сообщества, а не отдельных пользователей. Поэтому может оказаться, что для сложных приложений даже возможностей платформ с изолированным выполнением Dapps недостаточно, а команда платформы слишком медленна и неотзывчива, что приведет к срыву сроков или ограничению возможностей приложения.

- *Затраты на разработку и поддержку.* Главное преимущество популярных платформ в том, что они предоставляют уже действующую проверенную среду с набором инструментов, достаточным для разработки приложений. Причем здесь идет речь не о функциях самого приложения, а о базовых технических аспектах, включая сетевые протоколы и алгоритмы шифрования. Любая популярная платформа проходит тестирование и постоянно подвергается атакам, а ее код проверяют сотни независимых разработчиков, заинтересованных в нормальном функционировании. В случае же разработки собственного блокчейна решение всех этих вопросов ляжет на команду проекта и увеличит временные и материальные затраты в несколько раз. Поэтому создание и поддержка

собственного блокчейна становятся достаточно дорогим удовольствием, причем в большинстве случаев неоправданным.

Сложности и критика

Действительно ли смарт-контракты ждет блестящее будущее, которое маркетологи описывают инвесторам?

Чаще всего смарт-контракты подвергаются критике за слабые возможности взаимодействия с реальным миром и слишком малый набор условий, которые возможно заложить в контракт, чтобы он оставался достаточно надежным и сохранял быстродействие. Это значительно снижает возможности и сужает сферу применения смарт-контрактов.

Еще один важный момент — юридическая сила и регулирование операций, к этому сложно приспособить публичные платформы. Как разрешить спор в том случае, если человек, продавший дом с помощью смарт-контракта, на следующий день приходит в регистрирующий орган и заявляет, что он не проводил никакой сделки? Какую юридическую силу имеет подпись транзакции в блокчейне и не приведет ли переход на смарт-контракты к многочисленным утечкам информации и полному хаосу?

Может ли программа полностью заменить человека в обработке финансовых транзакций? Ведь даже малейшей ошибки в коде достаточно, чтобы мошенники смогли за считаные секунды вывести миллионы долларов, прежде чем кто-либо сможет вмешаться в автоматизированный процесс. Еще большая опасность заключается в возможности подделки персональных данных или социальной инженерии — там, где человек может заподозрить подвох и перепроверить информацию, даже самая совершенная программа даст добро и переведет деньги хакеру.

Смогут ли автономные программы заменить людей в тех задачах, которые традиционно считаются слишком сложными для алгоритмизации и автоматизации? И даже если все получится, не приведет ли это к потерям десятков тысяч рабочих мест, обрушению рынка труда и социальному взрыву?

Ответы на все эти вопросы слишком сложны и неоднозначны, поэтому регулирование блокчейна до сих пор не принято в большинстве юрисдикций. Законодатели боятся совершить этот шаг, поскольку он может оказаться дорогой в один конец и обойтись значительно дороже, чем игнорирование новых технологий еще десяток-другой лет.

Глава 6

Блокчейн как основа для крауд-фандинга — ICO

В индустрии блокчейна внимание общественности чаще всего привлекали не технические прорывы и революции в финансах или госуправлении, а истории быстрого обогащения или разорения. Биткоин много раз называли как новой мировой валютой, так и пузырем, который вот-вот лопнет. Пока не сбылось ни то, ни другое.

Первые зарегистрированные криптовалютные миллиардеры братья Кэмерон и Тайлер Уинклвосс или владелец обанкротившейся биржи MtGox Марк Карпелес известны широкой публике гораздо больше, чем глава разработки Bitcoin Владимир ван дер Лаан или анонимный разработчик — создатель метода консенсуса Proof-of-Stake, псевдоним которого,

Sunny King, знает лишь небольшая часть сообщества. Осенью 2013 года весь мир облетела история английского инженера Джеймса Хауэллса, выбросившего на свалку жесткий диск с 7500 BTC (в ноябре 2013-го они стоили около $6,5 млн, а в октябре 2018-го — уже почти $50 млн).

«Деньги из воздуха», получаемые майнерами или просто удачно купившими криптовалюту людьми, поражали воображение миллионов, которые понесли свои сбережения в криптовалютную отрасль, часто не пытаясь вникать в подробности. Очень многие становились жертвами мошенников или просто инвесторами-неудачниками, сделавшими покупку на ценовом пике. Многочисленные статьи и репортажи об удачах, провалах и преступлениях в области криптовалют уже несколько лет не сходят со страниц крупнейших СМИ, а ведущие информационные агентства транслируют котировки биткоина наравне с ценами на нефть и золото и с биржевыми индексами.

Вывод банален — возможности легкого заработка интересуют людей гораздо больше, чем будущее блокчейна как технологии или развитие бизнеса на его основе. Самой популярной темой последних лет стали вовсе не дебаты о масштабировании блокчейна или его медленное, но верное просачивание в корпоративный сектор, а продажи токенов на блокчейне, получившие название ICO (Initial Coin Offering), новый метод общественного финансирования, который, как ожидается, заменит классический краудфандинг.

Настоящий бум ICO, случившийся в 2017 году, превзошел все ожидания, а суммы, собранные с помощью продаж токенов через блокчейн, составили миллиарды долларов. Этот новый метод сбора средств уже обсуждают как серьезного конкурента не только краудфандинга, но и венчурного финансирования.

Но и здесь не все так гладко. Бесконтрольные и часто анонимные продажи цифровых токенов, многочисленные кражи и закрытие проектов, собравших миллионы долларов, приняли такой размах, что некоторые правительства были вынуждены полностью запретить их, а другие — ввести ряд ограничений. И эти жесткие меры оправданны, поскольку очередная революционная идея привлекла как энтузиастов, так и преступников, открыв широкий простор для мошенничества.

Неподготовленному человеку сложно не только разобраться в технических особенностях каждого из сотен предлагаемых проектов, но даже в общих чертах оценить его жизнеспособность. Среди вложившихся в первые ICO оказалось немало счастливчиков, увеличивших свои средства в десятки и даже сотни раз и успевших вовремя соскочить с поезда, на всех парах несущегося в тупик. А многие инвесторы очередного громкого проекта часто даже не задумывались о последствиях и теряли большую часть своих денег, а иногда и все без остатка. И даже спустя два года после начала «денежной бури» нельзя сказать, что индустрия ICO стала сколько-нибудь упорядоченной и надежной.

Теперь обо всем по порядку.

Что такое ICO

Новые сферы деятельности всегда порождают множество непонятных слов, часто обозначающих одно и то же. Поэтому для понимания того, о чем пойдет речь дальше, и даже статей в СМИ, необходимо в первую очередь согласовать терминологию. Итак, что же такое таинственный ICO и все, что с ним связано?

Наиболее распространенный термин ICO, или Initial Coin Offering, имеет множество переводов. Буквально его переводят как «первичное предложение монет». Однако аббревиатура ICO далеко не уникальна и скопирована с широко распространенного в финансовом мире термина IPO (Initial Public Offering) — первичное размещение акций компании на бирже.

В случае продаж цифрового актива в качестве биржи обычно выступает специализированная платформа, такая как Ethereum или Waves, роль депозитария ценных бумаг играет блокчейн, а продажу и распределение актива вместо информационной системы и сотрудников биржи осуществляет смарт-контракт.

ICO чаще всего называют децентрализованной моделью краудфандинга. В отличие от сбора средств в фиатной валюте через централизованный сервис, администрация которого гарантирует передачу денег создателям проекта, если будут выполнены определенные условия (например, собрана нужная сумма), ICO управляется децентрализованным приложением (смарт-контрактом), которое автоматически рассылает покупателям токены по заданному алгоритму, а также может заморозить токены разработчиков на определенный срок. Однако большая часть смарт-контрактов ICO никак не управляет собранными средствами.

Тонкости терминологии

Слово «coin» (монета) в словосочетании Initial Coin Offering может ввести в заблуждение, поскольку в криптовалютном сообществе уже фактически общепринято называть монетой единицу, обращающуюся непосредственно в блокчейне (или на его первом, транспортном, уровне), а производные активы, создаваемые поверх базового блокчейна, называются токенами. Поэтому существует более правильный термин — ITO (Initial Token Offering), отражающий суть продаваемых активов. Но он появился слишком поздно и так и не вошел в широкое обращение.

Впрочем, нужно признать, что, когда создатели Ethereum назвали предварительную продажу эфира (ETH) термином ICO, они не отступили от правил, поскольку проданные виртуальные токены при запуске блокчейна Ethereum фактически были сгенерированы как монеты, каковыми и являются до сих пор. Поэтому обозначение ITO правильнее применять к проектам, где конвертация токена в монету не планируется.

В 2017 году некоторые ICO-проекты начали использовать термин TGE (Token Generation Event) для обозначения непосредственно этапа выпуска и распределения токенов. TGE — не полный аналог ICO, а скорее обозначение технической части процесса. Этот термин тоже не получил широкого распространения, но все еще встречается.

С ICO также часто ассоциируется более общий термин «краудсейл» (crowdsale), который ближе к классическому краудфандингу, но чаще употребляется именно в контексте продажи токенов или другого нематериального актива для привлечения публичного финансирования без официальной регистрации в качестве акционерного общества.

Виды токенов для регулирования

Когда индустрия ICO выросла до миллиардных сумм оборота и привлекла внимание регуляторов по всему миру, одним из первых встал вопрос о юридическом признании процесса продажи токенов через блокчейн. Это было вызвано необходимостью защиты инвесторов, поскольку многие проекты анонимны, а децентрализованная эмиссия токенов не дает оснований правоохранительной и судебной системам правильно квалифицировать подобные дела. Кроме того, необходимо было организовать учет и налогообложение полученных организаторами ICO многомиллионных доходов. Еще раньше назрел вопрос о классификации и регулировании криптовалют.

Поэтому финансовые регуляторы развитых стран, в первую очередь США, приступили к систематизации и юридическому оформлению проведения ICO. Комиссия по ценным бумагам и биржам США (SEC) предложила разделить цифровые токены на два вида: токены-акции (security tokens), дающие инвестору право на долю в компании или ее прибыли, и служебные токены (utility tokens), выполняющие в основном техническую функцию. Ко второй категории было отнесено большинство монет криптовалютных блокчейнов, включая ETH в блокчейне Ethereum, обеспечивающую создание и функционирование смарт-контрактов.

SEC предложила определять, к какому типу отнести токен, с помощью теста Хауи (Howey Test), применяемого для классических ценных бумаг. Суть его сводится к определению того, является ли рассматриваемый актив объектом совместных инвестиций и

предусматривает ли владение им участие в получении и распределении прибыли предприятия. Если на эти вопросы даны положительные ответы, токен классифицируется как security (ценная бумага) и подлежит регулированию, аналогичному управлению акциями.

Кроме того, американская юридическая фирма Cooley в конце 2017 года предложила обходной маневр в виде упрощенного инвестиционного контракта под названием «Простое соглашение о будущих токенах», или SAFT (Simple Agreement for Future Tokens). Это соглашение подразумевает продажу токенов только после регистрации их эмитента в SEC, а выпуск токенов и их распределение производятся после запуска готового продукта. Соглашение SAFT оформляется в письменном виде и в случае отказа организаторов проекта от исполнения обязательств с ним можно обратиться в суд.

Главное препятствие для применения SAFT заключается в том, что оно подходит только для аккредитованных инвесторов, которым необходимо раскрыть свою личность и предоставить ряд документов, в то время как для участия в большинстве ICO требуется всего лишь провести транзакцию в блокчейне для оплаты покупки токенов без необходимости отправки организаторам любых документов.

Инфраструктура индустрии ICO

С ростом популярности и увеличением количества ICO в этой среде появилась вполне закономерная конкуренция, в результате чего сложилась определенная техническая и общественная инфраструктура, а также своеобразные стандарты качества, которым вынуждено следовать большинство проектов, претендующих на получение денег инвесторов. Ниже представлен «джентльменский набор», необходимый практически в любом проекте ICO.

Выбор платформы

Создавать собственный блокчейн или другую техническую платформу для проведения продажи токенов слишком долго и затратно, поэтому подавляющее большинство проектов основывается на существующих платформах, предоставляющих все необходимые инструменты. В результате техническая сторона типового ICO может быть подготовлена одним человеком за несколько дней, а при соответствующем опыте и квалификации даже за несколько часов.

В настоящее время практически все ICO базируются на платформе Ethereum, значительно меньше — на Waves, EOS, Lisk и других конкурирующих платформах. Некоторые проекты для расширения охвата инвесторов проводят ICO одновременно на нескольких платформах.

Монопольное положение Ethereum объясняется достаточно просто — он был первым, кто предоставил такую возможность и, что важнее, инвесторам удобнее работать со множеством токенов на одной платформе и оплачивать их единой криптовалютой. Даже несколько крупных взломов, замедление сети в период наибольшей активности ICO летом–осенью 2017 года и удорожание как технической части процесса покупки токенов, так и обслуживания контрактов не отвратили пользователей от Ethereum. Очевидно, что, несмотря на растущую конкуренцию, он останется ведущей платформой для ICO и других приложений на смарт-контрактах в ближайшие несколько лет.

Сайт и документация

Разумеется, любому солидному проекту необходим собственный сайт. И чем профессиональнее и удобнее он сделан, тем больше шансов убедить инвесторов вложить деньги именно в этот ICO. Как правило, сайт представляет собой достаточно стандартный лендинг, на котором описываются все потенциальные преимущества и перспективы ICO, представлена команда проекта (далеко не всегда настоящая) и, разумеется, расписан процесс

участия в ICO (в первую очередь — как максимально быстро, удобно и без лишних сомнений купить токены).

Адрес распределяющего токены смарт-контракта часто указывается на сайте в виде обычного текста, чем не преминули воспользоваться мошенники. Известны несколько случаев, когда в результате взлома сайта подменялся платежный адрес и инвесторы отправляли свои деньги хакерам. Так, летом 2017 года после взлома сайта ICO CoinDash покупатели токенов отправили эфира злоумышленникам на более чем $7 млн, а инвесторы ICO Enigma потеряли более миллиона долларов после взлома не только сайта, но и сервера почтовой рассылки и Slack-канала. Сайт проекта и аккаунты в соцсетях до сих пор остаются наиболее уязвимыми точками любого ICO.

Самый важный, а часто даже единственный документ, вмещающий всю необходимую инвестору информацию о данном ICO, это «Белая книга» (White paper). Обычно он состоит из нескольких десятков страниц и содержит только общую информацию. Впрочем, большинству инвесторов достаточно сайта и White paper, чтобы принять решение о покупке токенов. После того, как проведение ICO было поставлено на поток, появились фрилансеры и даже компании, специализирующиеся на подготовке качественной «Белой книги» и ее переводе на несколько языков. В период бума стоимость разработки «Белой книги» и сопутствующих документов достигала десятков тысяч долларов.

Рекламная кампания

Самый эффективный метод привлечения средств в ICO — это как можно более широкая рекламная кампания. Причем на рекламу и маркетинг часто расходуются десятки процентов от средств, собранных в ходе ICO. Разумеется, для мошенников расходы на рекламу — практически единственная статья расходов, и на нее они не скупятся. Но и добросовестным проектам часто приходится тратить на продвижение миллионы долларов.

Рекламная кампания разворачивается одновременно на нескольких фронтах: публикации в СМИ и блогах, выступления представителей компании на различных тематических конференциях, распространение рекламы о проекте в соцсетях и на форумах. Для стимулирования активности добровольных помощников используются так называемые баунти (bounty) — вознаграждение авторам статей в блогах, сообщений в соцсетях и прочей вирусной рекламы, которая ввиду массовости часто эффективнее статей в самых популярных СМИ, часто помещающих платные материалы в почти не читаемые разделы сайтов.

Рейтинговые агентства и агрегаторы

Когда количество одновременно проводимых ICO стало исчисляться десятками, а уже проведенных или только готовящихся к запуску приблизилось к тысяче, даже опытному инвестору стало сложно разобраться во всей документации многочисленных проектов, а тем более оценить достоверность предоставляемой информации.

Мошенникам достаточно просто переписать под себя профессионально подготовленную документацию вполне респектабельного проекта, и определить подделку сможет только человек, который постоянно вращается в индустрии ICO. Поэтому многие инвесторы начали прибегать к «веерному» финансированию — наиболее эффективной на тот момент методике. Эти люди вкладывали свои деньги во все проекты, в которых при первичной оценке не обнаруживали явных признаков мошенничества. Даже если половина токенов падала в цене после ICO, за счет многократной прибыли от оставшихся инвестор, как правило, оставался в плюсе. Но для максимизации прибыли наиболее эффективно было формировать «портфель токенов» более осознанно, то есть вкладывать в перспективные проекты больше, а в сомнительные — меньше. И это вновь приводило к необходимости проверки информации и углубленного изучения документации.

Решением этой проблемы стало появление агрегаторов (их также называют трекерами, листингами и т.д.) и рейтинговых агентств, специализирующихся на ICO. Эти сервисы

выполняют сходную задачу — сбор на одной площадке информации о многих ICO и оценку проектов.

Преимущество агрегаторов — более широкий охват проектов и возможность быстрого сравнения большого количества ICO, в то время как рейтинговые агентства делают акцент на глубоком и профессиональном анализе небольшого количества проектов и вынесении объективной оценки на основе этого анализа. Также рейтинговые агентства играют роль фильтра, поскольку процедура рейтингования платная для организаторов ICO и требует раскрытия практически всей информации о проекте и его команде. Поэтому для мошенников и слабо подготовленных команд обращение в рейтинговое агентство не имеет смысла.

Из наиболее известных агрегаторов можно назвать ico-list.com, icohotlist.com, icobazaar.com, icodrops.com, tokenmarket.net и другие. Как правило, агрегаторы предоставляют списки активных, прошедших и планирующихся к запуску ICO, структурированную общую информацию о проекте в виде ключевых показателей и собственную оценку надежности проекта на основе публичных данных. Эта оценка обычно носит очень приблизительный характер, не исключены и платные рейтинги.

Рейтинговых агентств гораздо меньше, поскольку этот бизнес требует более серьезных издержек и наличия профессиональной команды. На данный момент наиболее активны две подобные организации: ICORating (https://icorating.com) и Digital Rating Agency (https://digrate.com/ru). В отличие от агрегаторов, рейтинговые агентства не только собирают публичную информацию, но и плотно работают с командами проектов, оценивая их финансовые показатели, востребованность продукта и возможности его реализации. По итогам анализа они составляют развернутые отчеты, как правило, находящиеся в публичном доступе. Но для организаторов ICO это затратный процесс, который продолжается несколько недель и не гарантирует получения высокого рейтинга. Поэтому оценки таких агентств котируются значительно выше, и если они не гарантируют коммерческого успеха проекта, то достаточно эффективно отсеивают мошенников и команды с голыми идеями, неспособные создать работающий продукт.

Первые ICO

Как появилась и сделала первые шаги индустрия ICO? Ее становление, которое и сейчас нельзя назвать законченным, продолжается уже несколько лет, но продажи токенов приобрели массовый характер около двух лет назад, с 2017 года. Причем специализированные платформы, позволяющие продавать токены в автоматическом режиме, с помощью смарт-контрактов, появились не сразу. Первые ICO проводились путем перечисления криптовалюты на опубликованный организаторами адрес в блокчейне, а сами токены (монеты) распределялись через премайнинг в первом блоке или с помощью скрипта, работающего со стандартным криптовалютным кошельком через API (программный интерфейс приложения).

Mastercoin

Первой в истории целевой продажей токенов считается краудсейл проекта Mastercoin, проведенный летом 2013 года. Самого понятия ICO в то время еще не существовало.

На Mastercoin прошла также первая продажа производных токенов — он базировался на блокчейне Bitcoin, используя его транзакции для рассылки метаданных, отображающих движение токенов. Продажа токенов Mastercoin (MSC) началась 31 июля 2013 года и продолжалась месяц, за это время у разработчиков было куплено MSC примерно на 4700 BTC (немногим более $5 млн). К концу года капитализация проекта поднялась до $132 млн, то есть увеличилась в 26,5 раза — весьма достойный показатель даже для криптовалютного рынка того времени. Но успех оказался недолговечным.

В марте 2015 года Mastercoin был переименован в Omni Layer, а главным и единственным его успехом был запуск на нем проекта Tether, который стал первым

эмитентом токенизированных долларов (USDT) и евро (EURT), ныне используемых несколькими крупными биржами криптовалют как нерегулируемая замена доллару. На октябрь 2018 года выпущено более 2,8 млрд USDT, из-за чего у многих членов сообщества возникают сомнения в их реальном обеспечении долларами. Если проект Tether потерпит крах, это станет для отрасли самым сильным ударом после банкротства биржи Mt. Gox, произошедшего в начале 2014 года.

Капитализация же самого Omni Layer продолжает неуклонно снижаться и, по данным на 21 января 2019 года, составляет всего лишь $1,1 млн, то есть меньше, чем летом 2013 года, тогда как криптовалютный рынок за это время вырос более чем в 100 раз.

NXT

Еще проще был организован краудсейл платформы NXT, состоявшийся в полузакрытом режиме в октябре–ноябре 2013 года. Разработчики провели практически всю рекламную кампанию в узком кругу энтузиастов криптовалют на форуме Bitcointalk, где представили свои идеи на одобрение сообщества. С технической стороны процесс выглядел очень просто — инвесторы перечислили биткоины в кошелек разработчиков, а те после запуска блокчейна NXT вручную зачислили соответствующее количество монет NXT в кошельки инвесторов. Сама продажа никак не была автоматизирована, и даже отсутствовало промежуточное звено в виде токена, поэтому краудсейл NXT можно считать прообразом ICO только с точки зрения концепции и логики процесса.

В то время идея создания многофункциональной платформы производных криптоактивов (токенов) была действительно инновационной, поскольку ничего подобного еще не существовало, по крайней мере в работающем коде, хотя концептуально уже были на пороге и Bitshares, и Ethereum. Кроме того, разработчики, причем сохранившие анонимность, запросили достаточно скромную сумму для компенсации своих расходов (всего лишь 21 BTC) и установили максимальное количество инвесторов 70 человек.

Несмотря на то, что сам проект NXT сейчас скорее мертв, чем жив, и даже новая платформа Ardor на нынешнем конкурентном рынке не добилась значимых успехов, первые инвесторы NXT менее чем за полгода получили потенциальные прибыли, с которыми можно сравнить только сверхдоходы первых майнеров биткоинов, сохранивших монеты до осени 2017 года. Полностью реализовать свое богатство инвесторам NXT помешала только низкая ликвидность рынка альткоинов, но значительная доля NXT все же вышла на открытый рынок.

В конце 2013 года биткоин и рынок криптовалют в целом переживали период бурного роста, но еще не достигли локальных максимумов (около $1200). Цена биткоина в период сбора средств разработчиками NXT поднялась примерно с $400 до $800, следовательно, общая сумма краудсейла составила всего $10 000–$12 000, а средний инвестор внес всего 0,3 BTC, то есть около $200. Для жителей Европы и США это сумма бытовых расходов за день-два, и на фоне сборов крупнейших ICO 2017 года, нередко получавших в день десятки миллионов долларов, она выглядит смехотворной. Но если учесть, что первичные инвесторы получили токены NXT по цене в десятые доли цента, а спустя несколько месяцев (после запуска блокчейна) могли их продать уже за несколько долларов, то есть примерно в 3000–5000 раз дороже, то желание смеяться пропадет даже у самых успешных инвесторов в ICO — лучшие из них показали значительно более скромные результаты.

Ethereum

Последний краудсейл до начала формирования ICO как самостоятельного направления отрасли блокчейна — это продажа токенов проекта Ethereum, запуск которого и ознаменовал появление новой индустрии.

Главные соавторы Ethereum, Виталик Бутерин и Гэвин Вуд, опубликовали «желтые страницы» новой платформы в апреле 2014 года, примерно за три месяца до старта продаж, а

обсуждение концепции началось несколькими месяцами раньше, поэтому к началу краудсейла их идеи уже нашли значительную поддержку.

Маркетинговая инфраструктура, характерная для нынешних ICO, в то время еще не была развита, запуск Ethereum и продажа токенов анонсировались через традиционные тогда каналы — отраслевые СМИ, блоги, форумы, такие как Reddit и Bitcointalk. То есть покупателями токенов стали в основном члены криптовалютного сообщества. Продажа токенов проводилась через блокчейн Bitcoin без смарт-контракта, то есть путем обычных транзакций. По сути, для последующего распространения ETH нужен был только список открытых ключей.

Команда Ethereum применила новый метод создания монет ETH, который позже использовался и другими проектами, например EOS. Всего за время ICO было реализовано около 60 млн ETH, созданных в генезис-блоке (первом блоке блокчейна). Адреса для рассылки ETH создавались на основе открытого ключа адреса Bitcoin, с которого покупатель производил оплату. Таким образом, используя тот же закрытый ключ, что и в кошельке Bitcoin, покупатель мог самостоятельно распоряжаться своими ETH без каких-либо дополнительных действий, создающих риск потери монет.

ICO Ethereum начался 22 июля и продолжался до 2 сентября 2014 года, при этом на первые две недели цена была установлена 2000 ETH за 1 BTC, а в последующие дни линейно уменьшалась и в последний день достигла 1337 ETH за 1 BTC.

Несмотря на довольно небольшое количество каналов продвижения, потенциальных инвесторов, ожидавших начала ICO, оказалось немало. Только за первые 12 часов было продано около 7,4 млн ETH на сумму 3700 BTC (на тот момент примерно $2,3 млн). А к концу краудсейла команда Ethereum получила 31 529 BTC (около $18,4 млн по курсу на 2 сентября 2014 года) за 60 102 216 ETH. Таким образом, цена одного ETH на момент окончания ICO составила примерно 30 центов. Если сравнить эту цену с историческим максимумом (около $1350), установленным в январе 2018 года, эфир за 3,5 года подорожал в 4500 раз! Однако за девять месяцев 2018 года он снова опустился до $225. Но даже если взять среднюю цену (около 500$), ICO самой платформы Ethereum стал более успешным, чем всех проектов на ее основе.

Зарождение-2016

Блокчейн Ethereum был запущен 30 июля 2015 года, а первая стабильная версия под названием Homestead, на которой уже можно было запускать работающие смарт-контракты, появилась 14 марта 2016 года. После этого разработчики различных проектов начали официально объявлять о запуске первых децентрализованных приложений и проведении ICO. Собственно разработка и тестирование смарт-контрактов происходили и на тестовой версии Frontier, но большинство разработчиков дожидались выхода стабильной версии, прежде чем запускать свои приложения.

Например, проект децентрализованного рынка предсказаний Augur провел ICO на Ethereum одним из первых (в августе–октябре 2015 года), но опубликовал в блокчейне Ethereum первую бета-версию своего контракта сразу же после запуска Homestead в марте 2016-го.

Так стартовала первая волна краудсейлов, которая характеризовалась повышенным оптимизмом и оторванными от реальности ожиданиями. К июню 2016 года, когда разразилась первая катастрофа, на блокчейне Ethereum базировалось уже несколько десятков DApps, а их суммарная капитализация приблизилась к половине капитализации самой платформы.

В апреле 2016 был запущен смарт-контракт проекта TheDAO, созданного для построения на Ethereum мечты криптоанархистов — «Децентрализованной автономной организации», деятельность которой управляется не советом директоров, а программным кодом. 16 июня 2016 года, всего через два месяца после запуска, этот смарт-контракт был взломан на пике своей капитализации (около $133 млн). С помощью бага в коде контракта

хакер смог вывести 3,5 млн ETH, где они и остались «замороженными». Похищенная сумма составляла почти половину сборов по итогам ICO и даже после обвала курса ETH, вызванного взломом, равнялась $47 млн. Под давлением инвесторов проекта 20 июля 2016 года разработчики провели хардфорк, который отменил перевод эфиров хакеру, но вызвал раскол в сообществе и в блокчейне и привел к созданию нового блокчейна Ethereum Classic.

Как ни странно, этот эпизод, обрушивший курс эфира на треть (с $21,5 до $14) и последовавший хардфорк не подорвали доверия к Ethereum как платформе для ICO, и их количество продолжало расти. В октябре 2016 года капитализация токенов впервые превысила капитализацию эфира, хотя через несколько месяцев тот смог отыграть позиции.

Что интересно, именно первая волна ICO по большей части состояла из жизнеспособных проектов. Многие из них выдержали проверку временем и выросли в самостоятельные проекты, капитализация которых значительно превышает сумму, полученную на ICO.

Наиболее известные проекты, ICO которых прошел в 2016-м — начале 2017 года (приведены только продолжающие работу на октябрь 2018 года):

Название	Токен	Окончание	Сумма, $ млн	Описание
DigixDAO	DGD	Март 2016 г.	5,6	Обеспеченный золотом стейблкоин
Lisk	LSK	Апрель 2016 г.	5,7	Платформа смарт-контрактов (свой блокчейн)
FirstBlood	1ST	Сентябрь 2016 г.	5,5	Платформа для киберспорта
Antshares	ANT/ NEO	Сентябрь 2016 г.	4,5	Платформа смарт-контрактов (свой блокчейн), переименована в NEO
ICONOMI	ICN	Сентябрь 2016 г.	10,6	Управление цифровыми активами
SingularDTV	SNGLS	Октябрь 2016 г.	7,5	Онлайн-телевидение
DECENT	DCT	Октябрь 2016 г.	3,0	Платформа управления контентом (свой блокчейн)
Golem	GNT	Ноябрь 2016 г.	8,6	Платформа децентрализованных вычислений
QTUM	QTUM	Март 2017 г.	15,6	Платформа децентрализованных приложений
iExec	RLC	Март 2017 г.	12,0	Платформа децентрализованных вычислений
Gnosis	GNO	Апрель 2017 г.	12,5	Блокчейн-оракул
Cosmos	ATOM	Апрель 2017 г.	16,8	Интерфейс взаимодействия блокчейнов

Феномен «молниеносных» ICO

Из перечисленных в таблице проектов несколько оказались так называемыми «молниеносными» ICO, показавшими как преимущества автоматизированной модели краудфандинга, так и недостатки самой платформы Ethereum, испытывавшей во время токенсейлов перегрузки и замедление транзакций. Как уже понятно из названия, их особенность в том, что продажа токенов началась и закончилась в буквальном смысле за несколько минут. Насчитывается около полутора десятка таких проектов.

Так, ICO проекта Golem продолжался 20 минут, проекта Gnosis в апреле 2017-го — всего 10 минут, а проведенный 26 сентября 2016 года ICO платформы киберспорта Firstblood

закончился так быстро, что никто не успел сосчитать его продолжительность (называют время от 10 секунд до 5 минут, что вряд ли реально, учитывая пропускную способность блокчейна). Абсолютным же подтвержденным рекордсменом по скорости является прошедший 1 июня 2017 года ICO децентрализованного браузера Brave, который за 30 секунд собрал эквивалент $35 млн в ETH, то есть в среднем каждую секунду проект получал $1,15 млн! Все транзакции поместились в три блока, которые в Ethereum создаются со средним интервалом 15 секунд. Ни классический краудфандинг, ни венчурное финансирование не могут похвастаться такой скоростью перехода денег от инвестора к стартапу, причем из любой точки мира и с ничтожно малой возможностью перехвата финансовых транзакций.

Эти «моментальные распродажи» замечательно характеризуют и безоглядный оптимизм ранних инвесторов, покупавших токены всех выходящих в свет проектов практически не задумываясь. И, как ни странно, именно они оказались в наибольшем выигрыше, поскольку мошенники и некомпетентные команды, привлеченные легкими деньгами, пришли на растущий рынок позже.

Бум-2017

Большая часть ICO 2016 года и первых месяцев 2017-го, хотя и подпитывалась изрядным количеством энтузиастов, заявляла и собирала достаточно скромные суммы в несколько миллионов долларов. Эти ICO проводились в основном в узком кругу сообщества и инвесторов, интересующихся криптовалютами. Но когда курсы криптовалют летом 2017 года начали бить один рекорд за другим, последовал бум майнинга, сопровождающийся исчезновением из магазинов топовых видеокарт. ICO стали известны широкой публике. О быстрых деньгах и рекордных сборах заговорили буквально все крупнейшие СМИ и телеканалы мира, и тут наконец сработал сетевой эффект — в ICO и криптовалюты хлынул поток новичков. Вырос интерес к новой отрасли и у финансовых «китов», включая крупные банки и хедж-фонды.

Резкий рост собранных в ICO сумм и увеличение капитализации токенов начались в марте 2017 года, а уже в мае суммарная стоимость токенов 34 активных проектов превысила на биржах $1,2 млрд, причем только за апрель 2017 года было собрано $100 млн. Рекордсменом апреля 2017 года стал ICO Cosmos, собравший $16,8 млн и вот уже полтора года создающий «интернет блокчейнов». После этого рекордные суммы обновлялись буквально каждый месяц и становились все более впечатляющими.

Именно 2017 год стал звездным для ICO. Он принес как новые рекорды, так и очередные проблемы. Количество только добросовестных ICO проектов составило 842, из них 537 сумели собрать хотя бы минимальную заявленную сумму (hard cap), всего же было проведено более 1000 ICO, но значительная их часть пришлась на мошенников. Называют общую сумму примерно $5,5 млрд собранных в ICO средств за весь 2017 год, из них только на IV квартал пришлось $3,3 млрд! Сумма сборов ICO за 2017 год в разных источниках может отличаться: во-первых, некоторые крупные ICO (такие как EOS) закончились в 2018 году и, во-вторых, многие китайские ICO после введения запретов были вынуждены вернуть средства инвесторам. Возможны и другие расхождения в расчетах.

Но были и отрицательные стороны этого бума: в отрасль пришли орды мошенников, в результате чего власти Китая в сентябре 2017 года полностью запретили проведение ICO в стране. Их примеру последовали и другие азиатские страны — Вьетнам, Таиланд и Южная Корея (последняя позже смягчила запрет). Правительства других стран, включая США, Россию и страны Евросоюза, также начали обсуждать регулирование ICO.

Если рекордными сборами одного ICO в 2016 году стала сумма немногим более $10 млн, в июне 2017 года сборы одного проекта впервые перевалили за $100 млн, а вскоре была взята планка $250 млн. Ниже приведены наиболее крупные ICO, проведенные с мая по декабрь 2017 года, на этот раз не в хронологическом порядке, а по возрастанию собранной суммы (по курсу ETH на день окончания):

Название	Токен	Окончание	Сумма, $ млн	Описание
Brave	BAT	Сентябрь 2017 г.	36	Децентрализованный браузер
SALT	SALT	Август 2017 г.	48	Рынок займов в крипто-валютах
MobileGo	MGO	Май 2017 г.	53	Платформа мобильных игр
WAX	WAX	Ноябрь 2017 г.	68	Платформа онлайн-торговли
TenX	TENX	Июнь 2017 г.	80	Криптовалютные дебетовые карты
Kin	KIK	Сентябрь 2017 г.	98	Децентрализованный мессенджер
Liquid	QASH	Ноябрь 2017 г.	105	Международные платежи
Status	SNT	Июнь 2017 г.	107	Пакет децентрализован-ных приложений
Polkadot	DOT	Октябрь 2017 г.	145	Интерфейс взаимодей-ствия блокчейнов
Bancor	BNT	Июнь 2017 г.	153	Инфраструктура обмена токенов
Sirin Labs	SRN	Декабрь 2017 г.	157	Специализированный блокчейн-смартфон
Tezos	XTZ	Июль 2017 г.	232	Платформа децентрали-зованных приложений (свой блокчейн)
Filecoin	FIL	Сентябрь 2017 г.	257	Децентрализованная система хранения файлов

Угасание или передышка–2018

В конце 2017-го — начале 2018 года были установлены рекорды стоимости основных криптовалют: биткоин практически достиг $20 000, а эфир — $1400, после чего пузырь начал сдуваться и курсы обвалились в несколько раз. Не мог не пострадать и рынок ICO, который ранее служил одним из основных драйверов роста капитализации Ethereum и был в числе главных бенефициаров криптовалютного бума. Кроме того, поток новичков стал иссякать, а более опытные инвесторы, уже наученные горьким опытом, стали внимательнее относиться к объектам вложения денег.

Этот год был отмечен как новыми рекордами по сборам отдельных ICO и рынка в целом, так и постепенным снижением к осени количества успешных краудсейлов и общих сборов. Абсолютный месячный рекорд ($5,5 млрд) был установлен в июне 2018 года, в основном за счет ICO EOS, который продолжался почти год. Проще говоря, результат одного месяца 2018 года практически превысил весь 2017 год.

По данным сервиса CoinDesk ICO Tracker, на конец июля 2018 года сумма сборов через ICO с начала использования этого инструмента превысила $20 млрд, что является внушительной цифрой даже в международном масштабе, хотя и не может соперничать с суммами, привлекаемыми через IPO. Но ICO еще долго останется инструментом для небольших команд и стартапов, которые не могут себе позволить проведение полноценного IPO.

При этом сумма сборов за 2018 год составила более $14 млрд. Объем привлеченных средств среднего ICO в 2018 году почти вдвое превысил значение предыдущего: $31,08 млн по сравнению с $15,98 млн в 2017-м.

Если сравнивать самые выдающиеся ICO 2017-го и 2018 года, то рост объемов и участие корпоративных игроков, включая прежде непричастных к отрасли блокчейна, заметны сразу. Так выглядят пять самых крупных ICO, завершившихся в 2018 году, они же крупнейшие в истории на данный момент:

1. Криптовалютная биржа Huobi, некогда одна из крупнейших в мире, в феврале 2018 собрала $300 млн.

2. Проект блокчейн-экосистемы Dragonchain, который разрабатывается при поддержке гиганта индустрии развлечений Disney, в марте 2018-го собрал $320 млн.

3. Еще один проект платформы развлечений и социальной сети с использованием блокчейна под названием TaTaTu в июне 2018 года смог собрать $575 млн, причем значительная часть суммы была получена от трех крупных инвесторов: люксембургского принца Феликса Леопольда Марии Гийома, соучредителя компании AMBI Моники Бакарди и американского хедж-фонда BlockTower Capital. На открытом рынке обращается менее 1% токенов TTU, все остальные находятся у команды проекта и ключевых инвесторов.

4. Нашумевшая в начале 2018 года продажа токенов мессенджера Telegram так и осталась непубличной, хотя, по полуофициальным данным, во время двух раундов, прошедших в феврале и марте 2018 года, было продано токенов на $1,7 млрд. Однако до сих пор нет полностью достоверной информации ни о самом проекте Telegram Open Network, ни о его дорожной карте, ни об инвесторах. На данный момент это единственный пример масштабного закрытого ICO, где все токены были распределены между крупными инвесторами, на открытый рынок не был выпущен ни один токен. Создатель Telegram и «ВКонтакте» Павел Дуров отказался комментировать это, и большая часть информации была озвучена в интервью сооснователя Qiwi Сергея Солонина, который также не захотел сообщать подробности. Однако позже в результате журналистского расследования стало известно, что токены были выпущены через зарегистрированную в SEC США офшорную компанию, таким образом с юридической стороны ICO Telegram более всего напоминает процедуру SAFT. Сами же токены, очевидно, будут эмитированы только после запуска сервиса.

5. Самый крупный и продолжительный токенсейл в истории — ICO EOS, начавшаяся 26 июня 2017 года и закончившаяся 2 июня 2018-го. В результате продолжавшейся почти год кампании на платформе Ethereum было продано 900 млн токенов, 100 млн EOS остается в руках разработчиков. С учетом того, что на день окончания ICO токен EOS стоил $12, получается неслыханная прежде сумма $12 млрд, но вследствие длительности процесса обычно рассчитывают среднюю цифру по всем 350 раундам, в результате чего расчеты сходятся на сумме $4,2 млрд, по-прежнему оставляющей проект на неоспоримом первом месте. Что интересно, блокчейн EOS был запущен менее чем через месяц после

окончания ICO, и пользователи получили монеты новой платформы. За прошедшее с этого момента время цена упала вместе с рынком и, по данным на 21 января 2019 года, составляет $2,4, снизившись в пять раз. Однако это не мешает EOS уверенно держаться в топ-10 криптовалют.

На фоне всех этих рекордов складывается впечатление, что индустрия ICO мчится вперед и скоро вытеснит централизованные сервисы краудфандинга, а заодно покорит и мировые фондовые биржи. На самом же деле вместе с падением рынка криптовалют истощается и оптимизм инвесторов ICO.

Согласно результатам исследования компании Autonomous Research, опубликованным в начале октября 2018 года, динамика рынка ICO выглядела неутешительной. Во втором полугодии 2018 количество проектов и собранные ими суммы стремительно снизились. Если в январе 2018 года суммарные сборы на ICO достигали $2,4 млрд, то в июле эта цифра была почти вчетверо меньше ($680 млн), и в дальнейшем падение только ускорилось. В августе проекты смогли собрать только $400 млн, а в сентябре — уже $300 млн, то есть в восемь раз меньше, чем в январе! По итогам ноября 2018 года общая сумма сборов ICO-проектов снизилась до $65 млн.

Падение объемов вложений в ICO выглядит просто катастрофическим: с января по сентябрь оно составило почти 90%, и перелома ситуации пока не видно. Компания объясняет это падение разочарованием инвесторов в служебных токенах, которые не дают права на долю в компании и часть ее прибыли, и повышением спроса на токены-акции. Однако доля проектов, эмитирующих токены-акции с регистрацией в регулирующих органах, все еще крайне мала, и возможности продвижения таких токенов среди частных инвесторов вызывают большие сомнения.

Кроме того, нельзя забывать и о результатах работы, проведенной в прошлые годы ICO. А они пока оставляют желать лучшего. Некоторые проекты, такие как EOS, Augur, NEO (Antshares), Lisk, DECENT, Golem и еще несколько, запустили собственные блокчейны или представили минимальный рабочий продукт (MVP).

Однако большая часть проектов все еще находится в стадии разработки и поэтому вынуждена нести серьезные расходы. Поскольку подавляющее большинство ICO проходило на платформе Ethereum, разработчики проектов вынуждены постоянно продавать собранные ими ETH даже на падающем рынке, в результате чего Ethereum оказался под значительно более сильным давлением, чем Bitcoin; если биткоин по сравнению с историческим максимумом упал примерно в три раза (с $20 000 до $6500), то падение эфира было почти семикратным (с $1400 до $220).

Согласно исследованию криптовалютной биржи Bitmex, опубликованному 30 сентября 2018 года, на конец III квартала 2018 года стартапы продали эфира на $5,5 млрд, то есть всю сумму сборов за 2017 год. По мнению исследователей, основная волна продаж уже закончилась, по крайней мере до тех пор, пока продажи не начнут ICO 2018 года, в которые и была реинвестирована большая часть проданных ETH. Впрочем, падение или рост курса эфира никак не повлияет на крупнейшие проекты, такие как EOS или Telegram.

Российские ICO

Несмотря на правовую неопределенность и прямое давление финансовых регуляторов и правоохранительных органов, в России также прошло некоторое количество ICO, хотя собранные ими суммы далеки от мировых рекордов. Главное, что объединяет российские ICO, — то, что почти все они проходили через компании, зарегистрированные за рубежом, поскольку в России все еще не существует регулирования отрасли блокчейна в целом, включая и продажи цифровых токенов. Соответствующий законопроект находится на рассмотрении в Госдуме еще с весны 2018 года, но так и не продвинулся дальше первого чтения. Это вынуждает стартапы усложнять себе жизнь, регистрируя юридическое лицо в

более лояльных юрисдикциях, таких как Швейцария, Сингапур или многочисленные офшоры.

Однако среди рекордсменов ICO 2017 года все же есть один проект с российскими корнями — MobileGo, собравший $53 млн и уже готовящийся к запуску платформы. Кроме него стоит упомянуть следующие проекты:

- RMC (Russian Mining Center) — один из самых скандальных российских ICO. Проект был создан при участии бизнес-омбудсмена Дмитрия Мариничева и бывшего владельца розничной сети Sunrise Сергея Бобылева и нацелен на создание предназначенного для майнинга оборудования нового поколения по уникальной российской технологии «мультиклет». Однако разработка зависла, и мультиклеточные процессоры для майнинга пока не появились. Параллельная программа по выпуску майнеров для биткоина под маркой Sunrise также не оправдала надежд инвесторов, однако проект все еще продолжает работу и надеется окупить вложенные в него средства.

- SONM, который смог всего за четыре дня собрать $42 млн на разработку платформы распределенных вычислений. В частности, планируется привлечь майнеров на GPU, если майнинг станет экономически невыгодным.

- KICKICO собрал $20 млн на создание децентрализованной платформы для краудфандинга, в том числе с помощью ICO. Разработчики планируют создать сервис, способный стать конкурентом Kickstarter.

- ZrCoin, собравший $3,5 млн на строительство завода по производству диоксида циркония на Урале.

- Starta, планирующий запуск акселератора и инфраструктуры для развития стартапов. Собрал $5 млн на платформе Waves.

- И наконец, еще один нашумевший проект — BioCoin фермерского кооператива LavkaLavka, сумевший привлечь более $20 млн. Токены были выпущены в качестве бонусных, за счет чего планировалось обойти юридические проблемы с криптовалютами и токенами на блокчейне. Проект провел широкую рекламную кампанию, заявив о себе как о первом легальном ICO в России. Эксперты обнаружили в его юридической основе множество несоответствий действующему законодательству, тем не менее правоохранительные органы не нашли в его работе нарушений.

Остается надеяться, что вскоре будет принят законопроект для регулирования ICO и все юридические ухищрения останутся в прошлом, а стартапам больше не придется регистрироваться за границей.

Мошенничество в ICO

Все признают, что самая серьезная проблема молодой индустрии ICO — огромное количество мошеннических проектов. Анонимная продажа цифровых токенов, подогреваемая всеобщим ажиотажем, и огромное количество неопытных инвесторов, готовых отдать свои деньги любому, кто предложит красивую идею и составит хоть сколько-нибудь убедительную White Paper, создают весьма благодатную почву для мошенников.

В самом деле, зачем взламывать защищенные сети, подделывать документы, покупать и красть учетные записи в соцсетях, рассылать вирусы и требовать выкуп за возвращение доступа к информации или, наоборот, за сохранение ее в тайне, когда можно обойтись гораздо более простой схемой? Ведь проведение мошеннического ICO может обойтись

гораздо дешевле и принести гораздо больше денег. Достаточно создать посадочную страницу, смарт-контракт, поместить в раздел «Команда» вымышленных специалистов, скопировать и слегка изменить чужую документацию и, наконец, провести небольшую рекламную кампанию через соцсети и форумы. При разумной экономии и наличии технических навыков все это обойдется в жалкие тысячи долларов. И что самое главное, при должном соблюдении анонимности шансы быть пойманными для преступников гораздо ниже, чем в любых других видах онлайн-мошенничества, поскольку все денежные потоки проходят в криптовалютах.

В период бума 2017 года мошеннические ICO так же, как и добросовестные команды, собирали сотни тысяч и даже миллионы долларов. Затем их организаторы продавали полученную криптовалюту и исчезали.

Общие потери инвесторов на мошенничестве в области ICO оцениваются по-разному. Согласно исследованию компании Diar, за первую половину 2018 года мошенники украли у инвесторов ICO около $100 млн, причем только одному проекту, Puyin Blockchain Group, удалось выманить у них $68 млн с помощью трех ICO. А предприимчивые и весьма циничные жулики из проекта Block Broker собрали $3 млн на… борьбу с мошенническими ICO, после чего бесследно исчезли.

Но сумма $100 млн выглядит слишком скромной, реальные потери, разумеется, гораздо больше. Согласно исследованию Satis Group, опубликованному в июле 2018 года, доля мошеннических ICO составляет 81% от общего числа проектов, однако большинству из них не удается собрать значительные суммы. Однако в денежном выражении Satis Group приводит сумму почти $1,5 млрд, которая выглядит более реалистичной. Причем львиная доля потерь пришлась всего на три проекта: вьетнамские Pincoin и Ifan, создатели которых в общей сложности украли $660 млн, и поддельный криптобанк AriseBank, ICO которого был остановлен SEC после того, как ему удалось собрать $600 млн. В этом случае большая часть средств все же была арестована на счетах мошенников.

В июне 2018 года Федеральная торговая комиссия США (FTC) сделала прогноз, что общие потери инвесторов на мошеннических схемах ICO за весь 2018 год могут достигнуть $3 млрд.

Что касается российского рынка, то, по данным РАКИБ, только за 2017 год отечественные ICO собрали $300 млн, из них половина была потеряна в финансовых пирамидах и других мошеннических проектах.

Борьба с мошенниками

Мошенничество — острая проблема, в решении которой участвуют как крупнейшие финансовые регуляторы, так и отдельные энтузиасты, и даже сами организаторы ICO.

Регулятор американского фондового рынка Комиссия по ценным бумагам и биржам (SEC) для этой цели создала отдельный сайт. На нем рекламировался новый «революционный» ICO и были представлены все основные уловки мошенников — от команды из знаменитостей до впечатляющей, но ничего не разъясняющей «Белой книги». Инвесторы, которые не смогли распознать подделку и нажимали кнопку «купить токены», перенаправлялись на страницу сайта, объясняющую, как распознать мошенничество в ICO.

Похожий сайт был создан и правительством Бельгии. Его назвали Too Good to Be True, и на нем опубликована информация о способах незаконного использования криптовалют, включая и мошеннические продажи токенов несуществующих проектов.

В мае 2018 года Ассоциация регуляторов ценных бумаг Канады и США (NASAA) запустила программу международного преследования криптовалютных мошенников под названием Operation Cryptosweep. В качестве вопиющего примера мошеннического ICO они привели техасский проект Wind Wide Coin, который разместил фотографии знаменитостей под видом своих клиентов, включая актрису Дженнифер Энистон и бывшего премьер-министра Финляндии Матти Ванханена.

Помимо традиционных мер по поиску и поимке мошенников, надо признаться, не очень эффективных, борцы с киберпреступниками используют даже юмор. Приведем здесь несколько самых интересных случаев.

В апреле 2018 года разработчики немецкого стартапа savedroid, который на собственном ICO собрал $50 млн, решили попугать своих и чужих инвесторов, для чего устроили не совсем безобидный розыгрыш с собственным ICO. Уже под конец кампании в один прекрасный день сайт стартапа перестал работать, а главная страница была заменена сценой из шоу South Park — «Aannd It's Gone». На следующий день сайт снова заработал в обычном режиме, а генеральный директор компании рассказал, что хотел просветить сообщество, чтобы оно было внимательнее при оценке вложений в ICO. Некоторые горячие головы сочли шутку неудачной и даже собирались подать в суд, но постепенно история затихла.

Но самой тонкой шуткой над бумом ICO, вероятно, стал проект «Бесполезный токен Ethereum» (Useless Ethereum Token, UET), запущенный в июле 2017 года и закрытый в апреле 2018-го. Его создатель поступил противоположно SEC. Он назвал свой проект «единственным честным ICO» и написал на главной странице сайта, что он мошенник, который хочет собрать деньги и не собирается ничего делать. Каждый может купить у него токены, получить их и послать кому угодно, и… все. Больше ни на что они не пригодны, «как и все токены всех ICO». Несмотря на такое весьма красноречивое описание, нашлись люди, которые купили «бесполезных токенов» на 310 ETH, или $62 750. Зачем они это сделали, никто, вероятно, так и не узнает.

Как не стать жертвой мошенников

Как начинающему инвестору не стать жертвой мошенников? Это не так уж сложно, если использовать здравый смысл, не быть слишком доверчивым и не поддаваться жадности.

Самое важное — не верить слишком заманчивым обещаниям и перед покупкой токенов провести собственный анализ, подкрепленный мнениями более опытных людей. Надо соблюсти всего несколько простых правил:

- **Оценить реальность обещаний и действительную востребованность проекта**, а также необходимость использования в нем блокчейна, если таковая заявлена.

- **Проверить проект на наличие в команде известных в сообществе людей** (но не каких-либо знаменитостей). Лучше всего, если ими окажутся разработчики или основатели блокчейн-проектов, и на их реальных страницах в социальных сетях найдется информация о данном проекте.

- **Проверить информацию о проекте на ICO-трекерах или в рейтинговых агентствах**. Разумеется, оценкам трекеров и рейтингам нельзя доверять полностью, но плохая репутация должна быть серьезным аргументом против покупки.

- **Разыскать отзывы о проекте на специализированных форумах, в блогах игруппах соцсетей**. Если положительные отзывы не стоит воспринимать слишком серьезно, то отсутствие отрицательных будет плюсом. Но необходимо проверить, не является ли тема или группа проекта самомодерируемой, из которой негативные отзывы попросту удаляются.

- **Наконец, если вы даже решили купить токены, не следует вкладывать средства в один проект**. Диверсификация спасет от потерь в одной-двух неудачных ICO, если остальные принесут прибыль.

- В конце концов, возможно, следует подождать, пока ситуация утрясется. Покупка токенов на вторичном рынке может быть менее выгодной, но в этом случае появится возможность понаблюдать за развитием проекта. Мошенники обычно исчезают сразу после окончания ICO.

Двигатель любой отрасли экономики — эффективная система финансирования, поддерживающая наиболее перспективные проекты сначала на ранних стадиях, а затем по мере их роста. Для индустрии блокчейна это правило не менее справедливо, чем для всех

остальных. Несмотря на претензии криптовалютных сообществ к децентрализации, приток средств на развитие необходим и децентрализованным сообществам, и частным проектам.

Мир блокчейна и криптовалют часто и вполне справедливо называют «Диким Западом», поскольку сложившиеся в нем правила все еще далеки от норм регулирования, которым подчиняются традиционные финансовые рынки. Анонимные распределенные команды разработчиков сосуществуют с регулируемыми биржами, а никем не контролируемые кампании ICO раз за разом собирают десятки и сотни миллионов долларов, не предоставляя своим инвесторам никаких гарантий. Нерегулируемые продажи токенов показали как перспективы новой глобальной модели краудфандинга, так и слабую защищенность инвесторов, которые каждый раз рискуют потерять все вложенные деньги.

Растет доля государственных и корпоративных блокчейн-проектов и консорциумов, их работа финансируется государственными и частными организациями, банками, технологическими гигантами или инвестиционными фондами.

Попробуем разобраться, как работают различные схемы финансирования криптовалютных и блокчейн-стартапов, какие они имеют преимущества и недостатки и как могут измениться в ближайшем будущем.

Государственные и корпоративные

Блокчейн-проекты, создаваемые под управлением государственных ведомств или корпораций, фактически ничем не отличаются от своих аналогов в других отраслях. Проекты, разрабатываемые для государственных учреждений, финансируются на деньги, выделяемые из бюджета, или средства частных инвесторов при поддержке государства. Примерами таких проектов в России являются, например, «Мастерчейн», IPChain или привязка к блокчейну программы правительства Москвы «Активный гражданин».

Над развитием блокчейн-проектов крупных корпораций работают, как правило, специально созданные подразделения, которые часто размещаются в нескольких офисах по всему миру. В Microsoft, IBM, «Сбербанке» и других крупных компаниях в подобных подразделениях могут работать несколько десятков или даже сотен инженеров, аналитиков и тестировщиков. Сейчас почти в каждом крупном банке, технологической или финансовой компании имеется рабочая группа для исследования и тестирования блокчейна. В некоторых случаях заключаются партнерские соглашения для ведения разработок на аутсорсе. Так, например, поступили Microsoft и ConsenSys или РЖД и Bitfury.

Такие известные консорциумы, как Hyperledger, R3, EWF, Ethereum Enterprise Alliance, создаются и финансируются несколькими десятками или даже сотнями компаний-участников консорциума. К корпоративным проектам относятся и эксперименты с внедрением блокчейна на фондовых биржах, проводимые по всему миру — от Австралии до России, Европы и США.

Децентрализованная разработка (криптовалюты)

Большинство криптовалют является проектами с открытым исходным кодом, и к их команде может присоединиться любой желающий, если обладает необходимой квалификацией и некоторым количеством свободного времени.

Анонимный создатель Bitcoin, известный миру под псевдонимом Сатоси Накамото, не получал никакого стороннего финансирования (по крайней мере об этом ничего не известно) и даже не воспользовался принадлежащей ему по праву наградой — более миллиона биткоинов, полученных им во время почти единоличного майнинга в 2009 году. Обладание такой суммой в ее фиатном эквиваленте вывело бы его во вторую сотню миллиардеров рейтинга *Forbes*, но эти биткоины за 10 лет так и не пришли в движение.

Поэтому довольно широко распространено мнение, что разработчики криптовалют работают практически бесплатно, на общественных началах, или по крайней мере имеют прибыль за счет преимущественного получения монет (токенов) своего проекта на ранних

стадиях. Это было справедливо в первые годы существования криптовалют и до сих пор верно для большинства мелких проектов. Однако ведущие криптовалюты уже давно вышли из стадии хобби-разработки или финансирования за счет пожертвований, как часто бывает с open source проектами.

Команда разработчиков Bitcoin Core состоит из нескольких сотен человек, но за ключевые разработки и поддержку протокола отвечает менее десятка сотрудников, по сути, работающих по обычным контрактам. До 2014 года ведущие разработчики Bitcoin финансировались за счет средств, выделяемых Bitcoin Foundation, но вскоре эта организация утратила свое значение и фактически прекратила существование. На данный момент два программиста, отвечающие за базовую поддержку протокола, сборку и выпуск новых версий Bitcoin Core, Владимир ван дер Лаан и Кори Филдс, получают зарплату от проекта MIT Media Lab, созданного Массачусетским технологическим институтом. Еще одна большая группа работает в частной компании Blockstream, занимающейся разработкой решений на основе Lightning Network и платформы сайдчейнов Liquid. В эту группу входят известные теоретики, эксперты и разработчики Bitcoin: Адам Бэк, Грегори Максвелл, Питер Вулле, Мэтт Коралло, Марк Фриденбах, Самсон Моу, Кристофер Аллен и другие. В 2014–2016 годах Blockstream получила более $75 млн инвестиций от ряда частных инвесторов и венчурных фондов. Вследствие работы значительной части команды Bitcoin Core в одной частной компании проект часто обвиняют в централизации разработки и подчинении развития Bitcoin интересам Blockstream и ее инвесторов.

Несколько иным образом обстоит дело с разработкой Ethereum и других ведущих криптовалют, например EOS, NEO, Dash и т.д. Как правило, за каждой из команд стоит одна организация, отвечающая за финансирование разработки. Для Ethereum это Ethereum Foundation, для EOS — Block.one, для NEO — компания Onchain и т.д. Таким образом, разработку большинства криптовалют нельзя назвать децентрализованной, хотя методы получения финансирования у них самые разные. В основном проекты финансируются частными инвесторами или за счет продажи токенов.

В ноябре 2017 года один из сооснователей Ethereum, Боб Саммервилл, опубликовал информацию о своих доходах во время работы в команде Ethereum Foundation, включая как фиксированную зарплату, так и вознаграждения и гранты в ETH за участие в различных инициативах.

Команды таких известных криптовалют, как Dash, Zcash, Monero и других, получают средства на разработку за счет продажи собственных монет или пассивного дохода (например, от владения суперузлами в сети Dash).

Миллиарды из майнинга

Немногочисленный, но весьма интересный класс «единорогов из шахты» — блокчейн-компании, заработавшие большие деньги на майнинге и впоследствии начавшие развивать проекты в смежных областях.

Bitmain

Самая известная в мире майнинговая компания, китайская Bitmain, была основана в конце 2013 года, когда производство специализированного оборудования (ASIC-майнеров) только начинало вставать на промышленные рельсы. Используя огромные возможности, предоставляемые китайской промышленностью, Bitmain без внешнего финансирования самостоятельно разработала эффективные для своего времени чипы и запустила крупносерийное производство ASIC-майнеров линейки Antminer. Это название известно сейчас любому майнеру, и устройства от Bitmain составляют более половины мощностей всех криптовалют, где применяется специализированное оборудование.

За пять лет только благодаря прибыли от майнинга и продаж оборудования Bitmain стала майнинговой империей, подмявшей под себя рынок и загрузившей заказами крупнейшие в мире фабрики полупроводниковых компонентов.

С 2016 года Bitmain начала разработку оборудования для вычислений в области нейросетей и искусственного интеллекта под названием Sophon. Точная стоимость Bitmain на данный момент неизвестна, но ее выручка за 2017 год превысила $4 млрд.

Bitfury

Еще один гигант индустрии блокчейна, выросший из сотрудничества всего двух человек — украинского инженера, летом 2013 года разработавшего в гараже высокоэффективный чип для майнинга, и латвийского бизнесмена Валерия Вавилова, который организовал его производство и продажу. В течение нескольких лет Bitfury оставалась основным конкурентом Bitmain, выпуская оборудование для майнинга, в основном для собственных ферм или оптовых покупателей. В 2014–2015 годах Bitfury привлекла $60 млн венчурных инвестиций, которые были направлены на новые разработки. По данным *Forbes*, доходы Bitfury от майнинга и продаж оборудования за 2015 и 2016 годы составили $125 млн, что на порядок ниже доходов Bitmain. Очевидно, проигранная «гонка мощностей» заставила компанию переключиться на другие направления.

Уже в 2016 году Bitfury начала отходить от майнинга и занялась разработкой блокчейн-сервисов. В частности, этой компании принадлежит пальма первенства в переносе на блокчейн первого государственного реестра — земельного кадастра Грузии. На счету компании имеются и другие подобные проекты, например участие в украинском проекте электронного правительства Blockchain eGovernance.

Летом 2017 года Bitfury представила собственную блокчейн-платформу Exonum для развертывания частных блокчейнов, которая в перспективе может стать конкурентом Hyperledger Fabric и R3 Corda. Одним из партнеров Bitfury является крупнейшая консалтинговая фирма Ernst & Young.

CEX.IO

Компания CEX.IO не может похвастаться такими внушительными достижениями, как Bitmain и Bitfury. Основанная в 2013 году как оператор крупнейшего в то время майнингового пула GHash.io, оказывающий также услуги облачного майнинга, уже к 2016 году компания была вынуждена сменить сферу деятельности. Вследствие падения рентабельности майнинга в течение 2014–2015 годов пул и сервис облачного майнинга были закрыты. Сейчас CEX.IO — оператор одноименной биржи криптовалют.

Краудфандинг и ICO

Одним из самых известных достижений технологии блокчейна стала новая модель общественного финансирования (краудфандинга), получившая название ICO (Initial Coin Offering). Благодаря ICO блокчейн-стартапы получили возможность сбора средств на развитие без необходимости поиска крупных инвесторов и юридического оформления в качестве акционерного общества.

Бум ICO 2016–2017 годов, описанный в главе 6, выявил серьезные недостатки этого метода финансирования перед более традиционными способами. С помощью ICO менее чем за три года стартапами было собрано более $20 млрд, однако прозрачность и эффективность их использования оказались крайне низкими. Об этом говорят результаты нескольких исследований, обобщающих результаты деятельности проводивших ICO проектов.

Команда исследователей из Бостонского колледжа в июле 2018 года пришла к выводу, что большинство проектов прекращает существование в течение пяти месяцев после окончания краудсейла: после этого срока остаются активными только 44,2% проектов. Причем если проекту не удалось вывести токен на биржи (чаще вследствие того, что не

удалось пройти проверку или заплатить за листинг), то вероятность краха в течение указанного срока повышается до 83%. В то же время активно торгующиеся токены обычно свидетельствуют о дееспособности команды — такие проекты терпят крах только в 16% случаев. В том же месяце появилось исследование Satis Group, согласно которому 81% ICO был организован мошенниками или некомпетентными командами, и с начала 2017 года инвесторы потеряли на таких проектах более миллиарда долларов.

В августе 2018 года рейтинговое агентство ICORating опубликовало собственный анализ, согласно которому во II квартале 2018 года 55% ICO не смогло собрать необходимой суммы, при этом большинство провалившихся проектов не собрало даже $100 000. И только 7% из проектов, начавших продажи токенов, смогли вывести их на биржи. Этот результат выглядит еще более показательным с учетом того, что рынок ICO вырос более чем в 10 раз в сравнении с аналогичным периодом 2017 года. Каждый из наиболее успешных проектов в среднем собирал около $50 млн. При этом 17% проектов смогло собрать от $1 млн до $5 млн, а 12% — от $10 млн до $25 млн. В целом результаты исследования говорят о взрослении рынка и росте требований со стороны инвесторов. Изначально безнадежные проекты не могут собрать даже минимальной суммы, в то время как перспективные достигают более внушительных результатов, чем в прошлые годы.

Согласно исследованию консалтинговой компании Ernst & Young, результаты которого были опубликованы в октябре 2018 года, более 86% токенов ICO, проведенных в 2017 году и ранее, осенью 2018 года торговались ниже своей номинальной цены, а их инвесторы потеряли 66% вложений. При этом 71% проектов до сих пор не имеет работоспособного продукта или хотя бы его прототипа.

Эти весьма плачевные результаты говорят о необходимости государственного контроля сферы ICO, включая регистрацию организаторов кампании и публичное представление первичной документации проекта, что позволит отсеять большинство мошенников и недееспособных команд. Движение в этом направлении уже началось, однако некоторые правительства, включая Китай и Южную Корею, решили запретить проведение ICO до прояснения ситуации.

Однако введение регулирования ICO в крупнейших экономиках мира, вероятнее всего, приведет к ограничению или полному запрету существующей модели анонимных продаж токенов, при которой организаторы ICO не несут практически никакой ответственности и все риски ложатся на инвесторов. Регуляторы, очевидно, станут настаивать на регистрации и лицензировании компаний, проводящих ICO, а частным лицам будет запрещено продавать токены. Разработку и принятие соответствующих законопроектов следует ожидать в 2019–2020 годах.

SAFT и Telegram

Контуры модели токенсейлов, которая устроит большинство регулирующих ведомств, в первую очередь SEC США, уже вырисовываются. Одним из возможных решений мягкого регулирования ICO может стать метод, подобный SAFT (Simple Agreement for Future Tokens — «Простое соглашение о выпуске токенов», по аналогии с SAFE, «Простому соглашению о будущих доходах»), впервые предложенному юридической фирмой Cooley в 2017 году.

Создатели концепции SAFT утверждают, что она может усовершенствовать модель ICO, приведя ее в соответствие с нормативными требованиями SEC. С помощью SAFT можно продавать токены только аккредитованным частным инвесторам и юридическим лицам, в том числе венчурным фондам, при этом позволяя им избегать большей части процедур регистрации в SEC, сбора и подачи документов, а также предоставления финансовых гарантий. SAFT значительно уменьшает риски для инвесторов, поскольку токены выпускаются только при фактическом запуске сети или выполнении других прописанных в контракте условий. При этом организатор ICO самостоятельно определяет тип токена, его технические и финансовые параметры.

По сравнению с ICO SAFT полностью исключает анонимность как организаторов, так и инвесторов. Следовательно, этот способ значительно снижает потенциальную аудиторию проекта, превращая публичную кампанию в закрытую продажу. Он фактически ограничивает круг покупателей инвестиционными компаниями и гражданами США, имеющими статус аккредитованного инвестора, и даже предполагает подписание бумажного контракта. От собственно ICO остается только модель распределения токенов через блокчейн, причем их генерация и распространение происходят без участия смарт-контракта, который в подобной ситуации излишен. Проще говоря, SAFT представляет собой скорее облегченную форму IPO и даже в случае принятия концепции не принесет существенных новшеств на рынки.

Одним из первых и самых крупных проектов, проведших продажу токенов с помощью SAFT, является Filecoin, осуществляющий разработку системы распределенного хранения файлов на базе протокола IPFS. Летом 2017 года Filecoin получил $52 млн от венчурных инвесторов и еще $206 млн при проведении ICO по методу SAFT. До сих пор SEC не предъявила никаких претензий к проекту, следовательно, этот прецедент можно считать успешным.

Канадскому проекту Unicorn, разрабатывающему блокчейн-платформу для ставок на киберспорт, был предъявлен иск по поводу нарушения законов о ценных бумагах США. Токенсейл проекта осенью 2017 года также проходил по смешанной модели: $31 млн был привлечен при помощи классического ICO, а еще $16 млн — через контракты SAFT. Спустя год после окончания ICO стоимость токена UKG упала более чем в 40 раз — с $2 до $0,047.

Это значит, что модель SAFT даже в ее текущем виде вовсе не обеспечивает соответствия регулирующим требованиям и не гарантирует сохранности вложений инвесторов. Саморегулируемая организация брокеров США — Агентство по регулированию финансовых институтов (FINRA) — в августе 2018 выпустила предупреждение для организаторов ICO в США о том, что продажа токенов в соответствии с SAFT не гарантирует отсутствия претензий со стороны SEC, поскольку сама модель обращения токена может быть разработана с нарушениями.

Еще один интересный пример закрытого токенсейла — это ICO проекта TON от создателей мессенджера Telegram, о котором спустя почти год так и не появилось никакой официальной информации.

Первые слухи о разработке проекта TON появились в декабре 2017 года. Согласно данным информированных источников, первоначально планировалось провести в марте 2018 года публичный ICO по методу, подобному SAFT, и в соответствии с требованиями SEC. Однако крупных инвесторов, желающих купить токены, оказалось столько, что сумма предложений более чем вдвое превысила запланированный объем инвестиций. Вследствие этого было проведено только два раунда закрытых продаж, каждый на $850 млн, причем без использования блокчейна, а в общей сложности покупатели предложили братьям Дуровым $3,8 млрд.

Первый раунд продажи токенов TON проходил в первой половине февраля 2018 года, в нем принял участие 81 инвестор. Следующий раунд был проведен во второй половине марта того же года, и в нем участвовали 94 инвестора. Эмитентами выступали TON Issuer Inc. и Telegram Group Inc, зарегистрированные на Британских Виргинских островах. Выпуск ценных бумаг был одобрен[1] регулятором фондового рынка США (SEC).

Среди инвесторов в TON есть и российские: генеральный директор платежной системы Qiwi Сергей Солонин инвестировал $17 млн, сооснователь компании «Вимм-Билль-Данн» Давид Якобашвили — $10 млн. Также в качестве инвестора выступил фонд TMT Investments, сумма вложений неизвестна. Кроме того, появлялись неподтвержденные слухи, что $300 млн в TON инвестировал Роман Абрамович.

Проведенная Telegram закрытая продажа показывает, что SAFT подходит для корпоративных проектов, но никак не решает проблемы небольших команд, так как по-прежнему ставит слишком много юридических барьеров и отсеивает основную массу

розничных инвесторов. Поэтому правильнее называть SAFT и подобные схемы не легализацией ICO, а цифровизацией IPO.

Венчурное финансирование

Исходя из всего вышеизложенного, самой привлекательной и надежной формой финансирования блокчейн-проектов остается привлечение венчурных инвестиций, благо технология сейчас имеет статус прорывной, и от блокчейн-проектов ожидают бурного развития и многократного роста капитализации. И хотя безумный ажиотаж вокруг ICO привел к тому, что децентрализованные продажи токенов собрали больше средств, чем за тот же период выделили венчурные инвесторы, прямое инвестирование гарантирует более высокий потенциал успешности проекта.

При этом венчурное финансирование может оказаться удобнее для небольших, но действительно квалифицированных команд разработчиков. Убедить венчурных инвесторов выделить средства может быть значительно проще, быстрее и дешевле, чем самостоятельно проходить все круги государственной бюрократической машины и проводить продажу токенов в форме, которая не вызовет претензий у регуляторов. Крупные венчурные фонды изначально закладывают риски неудач и финансируют множество проектов в надежде на то, что даже небольшая их часть, которая «выстрелит» и создаст успешный продукт, покроет расходы.

Один из самых известных в мире венчурных инвесторов, Тим Дрейпер, поверил в будущее криптовалют и купил несколько десятков тысяч биткоинов на аукционах Минюста США, чтобы финансировать блокчейн-проекты.

Даже короткая история отрасли блокчейна знает множество проектов, которые смогли встать на ноги с помощью венчурного инвестирования. Самый яркий пример — крупнейший американский оператор криптовалют Coinbase, капитализация которого на конец октября 2018 года достигла $8 млрд. Всего компания получила пять раундов финансирования, каждый из которых был больше предыдущего:

1. Раунд A, май 2013-го: $6 млн.
2. Раунд B, декабрь 2013-го: $25 млн.
3. Раунд C, январь 2015-го: $75 млн.
4. Раунд D, август 2017-го: $108 млн.
5. Раунд E, октябрь 2018-го: $300 млн.

По этим цифрам видно, что вовремя привлеченный венчурный капитал принес значительную прибыль инвесторам и за пять лет превратил небольшой стартап в крупную компанию, заметную даже на американском рынке. А в апреле 2018 года Coinbase сама открыла венчурный фонд для поддержки блокчейн-стартапов.

Может показаться забавным, что даже создатель игры CryptoKitties на блокчейне Ethereum, компания Dapper Labs, в октябре 2018 года получила $15 млн от нескольких венчурных фондов, в числе которых такие гиганты, как венчурные подразделения Google и Samsung. При этом инвестиции следует считать долгосрочными, поскольку постоянная аудитория CryptoKitties пока составляет менее 400 пользователей в сутки. Это в очередной раз демонстрирует заинтересованность крупнейших мировых компаний в перспективных блокчейн-стартапах.

Среди самых крупных раундов венчурного финансирования также можно отметить:

1. 21 Inc — март 2015-го, $75 млн.

2. Digital Asset Holdings — февраль 2016-го, $60 млн.

3. Circle — июнь 2016, $60 млн.

4. R3 — май 2017-го, $107 млн.

5. Robinhood — март 2015-го, $75 млн.

Объемы венчурного финансирования растут вместе с отраслью: по данным Coindesk Blockchain Venture Capital, в 2013 году их сумма достигла $120 млн, в 2015-м — $600 млн, а за 9 месяцев 2018 года — уже $2 млрд. В целом с 2013 года сумма венчурного финансирования составила $4,5 млрд. Это в 4,5 раза меньше, чем суммарные инвестиции в ICO, но эффективность венчурных инвестиций на порядок выше. Если среди ICO-проектов через год выживают менее 20%, то из компаний, получивших более $1 млн венчурного капитала, закрываются единицы, хотя не все проекты демонстрируют стабильный рост и даже выходят в зону прибыли. Несмотря на успехи ICO и краудфандинга в целом, традиционные методы финансирования все еще демонстрируют гораздо лучшие долгосрочные результаты.

Глава 8

Решения, которые делают блокчейн эффективнее

Десять лет эксплуатации криптовалют, а в последние годы и других реализаций блокчейна, выявили основные проблемы технологии, которые со временем будут только обостряться.

В первую очередь это пропускная способность классического блокчейна, ограничения которой стали хорошо заметны в наиболее нагруженных сетях: в Bitcoin во время кризиса 2016–2017 годов и в Ethereum во время бума ICO в течение двух последних лет. Вторая проблема, тесно связанная с первой, — низкая скорость подтверждения транзакций в классических блокчейнах на основе консенсуса Proof-of-Work, в результате чего при повышенной нагрузке на сеть полного удостоверения транзакции без повышенной комиссии

иногда приходится ждать десятки минут или даже часы. Пока эти задачи не будут решены без потери основных свойств блокчейна, а именно гарантированной невозможности изменения данных и надежного распределенного хранения, массовое применение блокчейнов остается невозможным. Попытки решения этой проблемы привели к разработке сетей второго уровня и альтернативных методов консенсуса, способных обрабатывать более значительные объемы транзакций.

Количество блокчейнов постоянно растет, однако они до сих пор остаются изолированными друг от друга. Так, чтобы обменять токены (монеты) одного блокчейна на токены другого, приходится пользоваться сервисами-посредниками, то есть централизованными биржами и обменниками, что повышает риски и увеличивает техническую сложность процесса, а также требует дополнительных расходов. Что же касается возможности прямой передачи нефинансовой информации между блокчейнами, то ее вообще не существует (в основном из-за того, что сейчас она мало востребована). Необходимость прямого взаимодействия между различными блокчейнами не столь остра, как решение вопросов производительности и масштабирования, но постепенно назревает, и ее решение понадобится уже в ближайшие годы. Особенно актуальным прямой обмен данными станет после распространения узкоспециализированных или корпоративных блокчейнов, изначально предназначенных для ограниченного круга пользователей, но требующих взаимодействия как между собой, так и с внешним миром.

Авторитетные команды разработчиков

Несмотря на существование множества действующих и разрабатываемых блокчейн-проектов, большинство из них основано на небольшом количестве технических решений и использует сходные технологии и кодовую базу. Так, почти все криптовалюты до 2013 года были основаны на кодовой базе Bitcoin, а большая часть платформ смарт-контрактов использует концепцию Ethereum с небольшими вариациями. Такая ситуация сложилась потому, что разработка с нуля оригинальной платформы и кодовой базы требует высоких компетенций и трудовых затрат, и отдельным разработчикам или небольшим группам крайне сложно написать и протестировать полностью уникальный код, а также выявить баги и проблемы стабильности при высоких нагрузках и безопасности. Кроме того, большинство блокчейн-проектов основано на открытых лицензиях, позволяющих свободно использовать и модифицировать код.

В итоге в отрасли блокчейна образовалось небольшое количество сильных команд разработчиков (условно назовем их первым эшелоном), которые способны решать ключевые проблемы и определять пути стратегического развития. Все остальные вынуждены в большей или меньшей степени использовать их наработки и зависят от эффективности основных групп разработчиков.

К первому эшелону разработчиков блокчейна относятся:

1. Bitcoin Core и примыкающие к ней Blockstream и Lightning Labs. Этот сложившийся еще в 2012–2014 годах коллектив разработчиков обладает наибольшим влиянием в отрасли и отвечает за развитие платформы Bitcoin. Именно разработчики Bitcoin Core (многие из которых работают в компании Blockstream) задают вектор развития большинства криптовалют и смежных проектов.

2. Ethereum Foundation, или команда Виталика Бутерина, наиболее влиятельна в сфере смарт-контрактов. Она разрабатывает платформу Ethereum и сопутствующие технологии, такие как Casper, Raiden, шардинг и другие. Несмотря на то что новые платформы могут показаться технически более продвинутыми, они, как правило, используют разработки команды Ethereum,

поэтому несут меньшие затраты и избавлены от груза проблем совместимости и поддержки имеющейся инфраструктуры.

3. Block.one, или команда Дэна Ларимера, создавшая такие громкие проекты, как Bitshares, Steemit и EOS. Несмотря на то что Ларимера часто упрекают в непоследовательности и привычке бросать уже запущенные проекты на полпути, наработки его команды также часто копируются другими. Например, метод консенсуса DPoS (делегированное доказательство доли) и его модификация LPoS уже применяются в ряде блокчейнов, а децентрализованная соцсеть Steemit имеет несколько форков, включая российский проект «Голос».

Здесь не указаны коллективы разработчиков, финансируемые крупными финансовыми и технологическими компаниями, такие как R3 и Hyperledger, поскольку они образованы совместно работающими корпоративными группами, принадлежащими разным компаниям. Кроме того, их технологии, как правило, запатентованы и могут использоваться другими проектами лишь с существенными ограничениями.

Технологии для решения выявленных проблем

Сложившаяся обстановка позволяет говорить о том, что 2018–2019 годы могут стать переломными в переходе на новый уровень использования блокчейна. Тестируется несколько различных технологий, способных решить проблемы масштабирования, взаимодействия и управления. Ниже они будут рассмотрены более подробно.

Еще не для всех обозначенных выше проблем найдены пути решения, но некоторые ведущиеся в этом направлении разработки уже входят в фазу эксплуатации. Как правило, эти разработки направлены не только на решение одной проблемы и имеют различные варианты применения. Обычно они покрывают несколько смежных областей и в каждом конкретном блокчейне могут использоваться частично или в разных комбинациях:

- Сети второго уровня, основанные на транзакциях вне базового блокчейна (off-chain), предназначены для вывода за пределы блокчейна основной массы небольших и повторяющихся платежей. Таким образом достигается значительное повышение производительности и снижается нагрузка на всю децентрализованную сеть за счет локализации распространения этих транзакций между их непосредственными участниками. Это достигается через снижение децентрализации и прозрачности проведения расчетов. К решениям такого типа относятся Lightning Network, Raiden и их аналоги.

- Альтернативные алгоритмы консенсуса, из которых наиболее известны Proof-of-Stake (PoS) и Byzantine Fault Tolerance (BFT), второй чаще применяется в частных проектах. Переход крупных блокчейнов на PoS во много раз снизит энергопотребление при обеспечении работы блокчейна, ускорит подтверждение транзакций, а также позволит использовать параллельное подтверждение блоков (шардинг), что даст возможность многократно ускорить обработку потока транзакций и довести пропускную способность блокчейна до тысяч транзакций в секунду с возможностью дальнейшего роста при увеличении размера сети. Кроме того, в альтернативных методах консенсуса заложена возможность проведения различных видов голосований, что повышает гибкость управления блокчейнами.

- Технология боковых цепей, или сайдчейнов, предназначена для создания древовидной структуры блокчейнов, в которой в отдельные цепочки выводятся определенные виды транзакций и возможно создание собственных токенов с обеспечением монетами материнского блокчейна. Изоляция

специализированных цепочек позволяет создать в каждой из них собственную среду — фактически отдельный блокчейн с определенным набором правил. Наиболее известна система сайдчейнов Liquid, которая создается компанией Blockstream на базе блокчейна Bitcoin. Используются сайдчейны и в еще нескольких проектах, включая платформы смарт-контрактов Rootstock (RSK) и Lisk.

- Технология атомарных свопов (atomic swaps) наиболее эффективно и безопасно решает проблему взаимодействия блокчейнов самых разных типов. Причем в перспективе становятся возможны не только обмен токенами для организации децентрализованных бирж, но и передача внутри этих транзакций произвольных данных.

Развитие систем голосования и идентификации пока еще не распространено и в публичных блокчейнах не получило четкого направления. Тем не менее имеется некоторый прогресс, и многие новые проекты уже приступили к непосредственному решению вопросов управления. Среди них можно назвать платформы EOS, Tezos, а также связанные между собой проекты NEO и Ontology. Более радикальные решения вопросов идентификации и управления планируется применить в проекте Telegram Open Network (TON), запуск которого ожидается в 2019 году.

Lightning Network и внесетевые транзакции

Вывод за пределы блокчейна мелких и периодически повторяющихся транзакций — один из путей решения проблемы масштабирования, которая начала проявляться в сети Bitcoin еще в 2014 году. Именно эта идея стала основой технологии внесетевых транзакций (off-chain transactions) и сети второго уровня с возможностью проведения мгновенных платежей без подтверждения майнерами. Технология получила название Lightning Network. Разработка и внедрение соответствующих решений потребовали нескольких лет и вызвали споры в сообществе, которые продолжались более двух лет и едва не привели к его расколу.

Сама идея надстройки над блокчейном Bitcoin, или построения платежной сети второго уровня, родилась за пределами команды Bitcoin Core, но быстро была ею подхвачена и принята в качестве основного пути развития на несколько лет.

Впервые концепция сети мгновенных транзакций была опубликована в 2015 году Джозефом Пуном и Тадеушем Драйя, а в январе 2016 года они представили «Белую книгу», в которой описали основные принципы Lightning Network. Именно в это время начал назревать кризис масштабирования блокчейна Bitcoin. Вследствие недостаточной пропускной способности механизма майнинга, способного подтверждать в среднем 5–7 транзакций в секунду, в сети начали расти очереди транзакций, ожидающих подтверждения, что привело к многократному повышению комиссий и замедлению работы многих сервисов, в первую очередь бирж и обменников. Кризис масштабирования фактически поставил крест на микроплатежах и розничных покупках с использованием биткоинов. Эти операции, и так немногочисленные, начали перетекать в другие блокчейны.

Разработки Lightning продолжались в течение всего 2016 года, и к концу его были представлены прототипы кошельков, работающие в тестовой сети. Проверка на небольшом количестве узлов их работоспособности прошла вполне успешно, однако настоящего нагрузочного тестирования в действующем блокчейне они не проходили — эта задача была отложена до разрешения конфликта разработчиков и майнеров, которого пришлось ждать до конца 2017 года. Только в сентябре 2017 года была активирована технология Segregated Witness, которая устраняла баг пластичности транзакций и делала функционирование сети Lightning более безопасным. Таким образом, запуск узлов Lightning в основном блокчейне Bitcoin состоялся только в декабре 2017 года, когда вышла версия 1.0 протокола этой технологии. Сейчас разработкой основной версии протокола занимается компания Lightning

Labs, возглавляемая Элизабет Старк. Главный продукт компании — Lightning Network Daemon (LND) без графического интерфейса и мобильная платформа Neutrino. В ближайшем будущем ожидается включение поддержки Lightning Network в основном кошельке Bitcoin Core, а затем и в других распространенных кошельках. Только после этого транзакции в сети второго уровня могут стать действительно массовыми.

К концу января 2018 года величина сети второго уровня впервые достигла 1000 узлов, но к этому времени в ней курсировало всего… 4 BTC, то есть она использовалась исключительно для тестирования работы каналов и микроплатежей. К середине октября 2018 в сети Ligthning работало уже более 3700 узлов и почти 10 000 каналов, но обращающиеся суммы были по-прежнему невелики — около 110 BTC (примерно $700 000). Текущую статистику сети можно увидеть на сайте https://1ml.com//.

Столь незначительное использование Lightning Network объясняется отсутствием в настоящий момент в блокчейне каких-либо перегрузок и завышенных комиссий, так как после сдувания пузыря, образовавшегося в конце 2017 года, объемы транзакций в сети упали в несколько раз, и для работы с минимальными комиссиями и временем подтверждения сейчас достаточно пропускной способности базового блокчейна. Однако теперь Bitcoin и другие криптовалюты гораздо лучше подготовлены к массовому использованию и уже, по крайней мере в теории, могут выдержать несколько сотен или даже тысяч транзакций в секунду, если более 95% будет проходить через сеть второго уровня с периодической фиксацией в блокчейне только взаимозачетов по совершенному массиву транзакций. Фактически Lightning Network уже готова к полноценной работе, но разработчики пользуются предоставленным затишьем для ее тестирования и выявления программных ошибок.

Как работает Lightning Network

На самом деле технология Lightning Network разрабатывается не только для Bitcoin. Ее копии или аналоги имеются еще в нескольких криптовалютах: Litecoin, Zcash (под названием Bolt), Ethereum (под названием Raiden) и NEO (под названием Trinity). Однако версии платежной сети второго уровня в альткоинах находятся на более ранних стадиях развития и гораздо слабее проработаны и протестированы, поэтому далее будет рассматриваться только Lightning Network как уже запущенная в эксплуатацию.

С технической точки зрения Lightning Network основана на технологии многосторонних подписей (multisig) и простых смарт-контрактов, встроенных в Bitcoin и работающих с помощью скриптового языка, интерпретируемого любым кошельком сети. Сеть образуется множеством виртуальных каналов между узлами (кошельками) Bitcoin. Канал состоит из скрепленного двусторонней подписью адреса, на который помещается так называемый залог, или сумма в биткоинах, необходимая для закрытия канала и подведения баланса между сторонами. Проще говоря, эта заблокированная сумма равна задолженности одного участника канала перед другим по совокупности всех совершенных ими транзакций. Если одна из сторон принимает решение о закрытии канала, остаток залога получает под свой контроль тот участник, который отправил по каналу больший объем биткоинов. При этом сумма транзакций, которую может передать по каналу кошелек, не может превышать сумму, определенную его владельцем для этого канала.

Функционирование канала Lightning Network во многом похоже на работу соединения по протоколу TCP, применяемого в современных компьютерных сетях. В Lightning Network между двумя узлами сети Bitcoin сначала происходит первичное согласование путем обмена открытыми ключами и создания общего залогового адреса, затем открывается постоянный виртуальный канал, по которому можно передавать транзакции в обе стороны.

Канал может быть закрыт в любой момент, при этом остаток на залоговом адресе передается в тот кошелек, в котором образовался недостаток средств. В теории канал может существовать практически неограниченное время, но такая практика годится разве что для крупных сервисов, непрерывно пересылающих биткоины своих клиентов и партнеров. Для

обычного же пользователя постоянно открытый канал неудобен, так как блокирует в его кошельке определенную сумму. Поэтому тем, кто не пользуется каналом для постоянного двустороннего обмена, придется время от времени проводить процедуру сведения баланса и закрывать ненужные каналы, при этом в базовом блокчейне будет совершаться итоговая парная транзакция. Таким образом, если в канале передана 1000 транзакций, то в блокчейне произойдет только две пары транзакций — на открытие и закрытие канала и комиссии майнерам будут выплачены лишь за эти две транзакции. Реальная экономия на комиссиях будет зависеть от передаваемых сумм и конечного соотношения балансов при закрытии канала.

Классический пример работы канала Lightning Network:

Алиса и Боб открыли канал, в котором Алиса зарезервировала 10 BTC, а Боб — 5 BTC. Это значит, что на залоговом адресе с помощью открывающей пары транзакций была заморожена сумма 15 BTC. Допустим, канал использовался в течение месяца, за это время Алиса передала Бобу 50 транзакций на общую сумму 5 BTC, а Боб передал Алисе 100 транзакций на общую сумму 9 BTC. Таким образом, на момент закрытия канала у Боба образовалась задолженность в 4 BTC, и эта сумма уйдет Алисе в результирующей транзакции через публичный блокчейн. При этом сторонний наблюдатель увидит не 150 разнонаправленных транзакций между двумя кошельками, а всего четыре (две пары на открытие и закрытие канала):

1. Перевод 5 BTC от Боба и 10 BTC от Алисы на залоговый адрес;

2. Перевод с залогового адреса 14 BTC Алисе и 1 BTC Бобу;

3. В случае, если залог открывала одна сторона либо при закрытии канала, все средства остаются у одной стороны, транзакций будет меньше.

Пока еще каналы образуются только между двумя узлами, но каждый узел может иметь почти неограниченное число каналов — для их работы нужно только наличие необходимой суммы в биткоинах. В будущем, возможно, появятся и каналы с участием множества узлов, на момент написания книги образование сети происходит с помощью создания необходимого количества каналов. Узлы с большим количеством открытых каналов являются шлюзами, или хабами, пропускающими через себя множество транзакций других пользователей. В основном такие узлы выгодно открывать биржам, платежным операторам и другим сервисам для работы с криптовалютами на розничном рынке. На время тестовой эксплуатации в Lightning не принято брать комиссию за транзакции, но, когда сеть войдет в рабочий режим с проведением серьезных сумм, участники сети, и особенно крупные узлы, неизбежно придут к необходимости ввода комиссий, хотя эти комиссии определенно будут во много раз меньше, чем в базовом блокчейне.

Преимущества и недостатки технологии

Механизм работы Lightning Network создавался прежде всего для решения проблемы масштабирования, поэтому она успешно выполняет следующие задачи:

- Значительно снижает комиссии при использовании потоков транзакций, особенно двунаправленных.

- Многократно увеличивает скорость прохождения транзакций — фактически поступление можно увидеть уже через секунды, и оно не зависит от подтверждений майнерами.

- В публичном блокчейне видны только процессы открытия и закрытия канала, что повышает конфиденциальность сторон.

- В блокчейн помещается значительно меньше транзакций, что во много раз уменьшает скорость его роста и снижает аппаратные требования к узлам.

К сожалению, идеальных технологий не бывает, и пользователям Lightning Network также придется мириться с ее недостатками:

- Сеть второго уровня избыточна для одиночных транзакций, то есть не принесет никакой выгоды пользователям, совершающим редкие операции с разными контрагентами, особенно в одну сторону.

- Блокировка средств в канале удобна не всем пользователям, особенно владеющим небольшими суммами.

- Массовый переход на Lightning приведет к неизбежной зависимости от крупных хабов, предлагающих более выгодные условия и связанных со множеством контрагентов. Это увеличит централизацию сети и вызовет миграцию пользователей в централизованные веб-кошельки.

- Одним из постулатов Сатоси Накамото была прозрачность и отслеживаемость платежей в блокчейне. Уход транзакций в каналы приведет к их сокрытию от всех, кроме непосредственных участников.

Как бы то ни было, Lightning Network решает одну из самых острых на сегодня проблем блокчейна, повышая пропускную способность и снижая комиссии. Возможно, найдется ее применение и в нефинансовых блокчейнах.

Альтернативные методы консенсуса

Процесс майнинга по методу доказательства работы (Proof-of-Work) критикуют за наличие очень многих недостатков. В первую очередь это огромное и постоянно растущее энергопотребление майнеров. Кроме того, классический майнинг не позволяет создавать блоки чаще, чем через определенный промежуток времени, равный примерно 10–15 секундам, а комфортный интервал, не приводящий к постоянному конфликту блоков и перезапуску расчетов, начинается от минуты. PoW-цепочка для надежного сопротивления атаке 51% и двойным тратам постоянно надстраивается только в один поток. Все это приводит к медленной по современным меркам работе и избыточному потреблению ресурсов. Достаточно напомнить, что майнеры, обеспечивающие только блокчейн Bitcoin, потребляют десятки тераватт-часов в год (столько расходует страна с населением в несколько миллионов человек без крупных промышленных комплексов), и из-за гонки мощностей их энергопотребление постоянно растет, невзирая на появление все более технологичных и экономных устройств. Нельзя также списывать со счетов майнинг Ethereum и других блокчейнов, потребляющих еще несколько тераватт-часов в год. При этом аппаратный майнинг требует и множества накладных расходов на техническое обеспечение и обслуживание оборудования, помещений и электросетей. По сути, уже сейчас многие промышленные майнеры балансируют на грани рентабельности, а прибыльный домашний майнинг становится искусством, доступным только знатокам этого дела.

Что касается Bitcoin как средства сохранения стоимости и уже общепринятого резервного актива для отрасли блокчейна, то для него высочайшая безопасность PoW-майнинга и отсутствие необходимости многократного масштабирования снижают остроту этой проблемы (за исключением роста энергопотребления). Однако для других блокчейнов

аппаратный майнинг становится все более тяжелой ношей и повышает риск атаки 51%, так как они не могут обеспечить таких мощностей, как Bitcoin и Ethereum. Это вынуждает разработчиков искать более эффективные механизмы достижения консенсуса. Наиболее популярным и универсальным считается метод PoS (Proof-of-Stake, или доказательство доли). Конкуренцию в секторе частных блокчейнов ему стремится составить BFT (Byzantine Fault Tolerance). Прочие методы не получили широкого распространения.

Попытки модификации PoW

Прежде чем приступить к рассмотрению консенсуса PoS, необходимо упомянуть о попытках улучшения метода Proof-of-Work, устраняющих хотя бы часть его недостатков. Наиболее известны две такие разработки.

Во-первых, это технология Instant Send, появившаяся в 2015 году в криптовалюте Dash. В ее блокчейне существует два вида узлов (кошельков): обычные и так называемые суперузлы (masternodes). Для работы суперузла необходимо иметь на балансе не менее 1000 Dash (можно назвать это отсылкой к PoS). Основная функция суперузлов — ускоренное подтверждение транзакций пользователей без ожидания их включения в блок. Если не учитывать риск того, что большинство суперузлов попадет под контроль злоумышленников, этот метод достаточно надежен. Его недостаток в том, что он не увеличивает реальную пропускную способность блокчейна, так как транзакции Instant Send все равно рано или поздно должны быть включены в блок, как и все прочие. Однако этот метод очень хорошо подходит для сглаживания пиковых нагрузок: в случае многократного роста объемов транзакций за короткий период, например после выхода важных новостей, транзакции будут подтверждаться суперузлами мгновенно, а в блоки они могут быть включены значительно позже, когда активность уже спадет и очередь транзакций рассосется. Но Instant Send не сможет справиться с постоянной перегрузкой блокчейна.

Второй способ улучшения Proof-of-Work, названный Bitcoin NG (next generation), был предложен также в 2015 году профессором Корнеллского университета Эмином Гюн Сирером. Он состоит в том, что майнеры каждые 10 минут борются за право генерировать блоки, а не собирают в блоки уже отправленные в сеть транзакции. Победитель этого «конкурса», собравший на основе лучшего хеша так называемый ключевой блок, не содержащий транзакций, на 10 минут получает право создавать неограниченное количество микроблоков, включающих сами транзакции. Количество и размер этих микроблоков фактически неограниченны и диктуются только текущей нагрузкой на сеть. Теоретически этот метод может улучшить объем обрабатываемых транзакций, но технически он сложнее, повышает уязвимость сети перед атакой 51% и несет гораздо большее количество рисков безопасности по сравнению с обычным майнингом. Кроме того, он не устраняет «гонки мощностей» и постоянного роста энергопотребления майнеров. Поэтому Bitcoin NG не получил практического применения, единственный эксперимент с ним поставил российский проект Waves, в конце 2017 года запустивший его модификацию Waves NG. Однако блокчейн Waves работает на технологии Proof-of-Stake, поэтому Waves NG будет правильнее рассматривать как временное решение, на смену которому идут новые технологии масштабирования в современных PoS-блокчейнах.

Особенности Proof-of-Stake

Метод Proof-of-Stake был первой альтернативой Proof-of-Work и ненамного моложе его — он был создан анонимным разработчиком, известным под псевдонимом Sunny King, еще в 2010 году. Первичная реализация PoS была не очень надежной и не получила распространения. Современные разработки обеспечивают этому методу уровень безопасности, сравнимый с PoW, при значительно лучшей скорости и масштабируемости, однако не могут устранить некоторые архитектурные недостатки.

Консенсус PoS основан на экономичном майнинге, в котором вместо мощности хеширования учитывается количество монет в кошельке майнера. На основании псевдослучайного выбора права на создание блока получает один из работающих в сети майнеров. В среднем за длительный период времени (например, за год) доля созданных майнером блоков с ничтожной погрешностью равна его доле монет от их общего количества в сети. В остальном же стандартный PoS-майнинг идентичен PoW-майнингу.

Преимущества PoS:

- Низкое энергопотребление и близкие к нулю эксплуатационные расходы.
- Отсутствие «гонки мощностей» и другой непродуктивной конкуренции.
- Гибкость к изменению основных параметров, включая частоту блоков.
- Возможность многопоточной обработки транзакций.

Недостатки PoS:

- Экономическая модель вынуждает хранить, а не тратить монеты, выводя их из оборота. Это ведет к низкой активности пользователей и завышению цены токена.
- Распределение долей пользователей в блокчейне крайне статично, изменение соотношения возможно только путем передачи (продажи) монет, что в перспективе ведет к их концентрации у небольшой группы «олигархов».
- Отсутствие затрат на майнинг облегчает атаку 51% и другие недобросовестные действия майнеров, которые приводят к необходимости введения в протокол административных наказаний.

Именно перечисленные выше проблемы замедляют массовое принятие PoS, поскольку их сложно решить на уровне протокола, а внешнее администрирование децентрализованной сети неэффективно.

Несмотря на то что первые реализации PoS были не очень надежны, начиная с 2014 года популярность этого метода росла из-за все более очевидно проявлявшихся проблем PoW. В 2015–2016 годах сложились следующие направления развития PoS:

- Delegated Proof-of-Stake (DPoS), разработанный командой Дэна Ларимера. Применяется в платформах Bitshares, EOS, Tezos, Lisk и их аналогах. В 2014 году появился Tendermint — созданная для проекта Cosmos модификация DPoS.
- Casper — технология для масштабирования Ethereum, которая все еще находится в разработке. В 2017 году разделилась на две ветви: Casper FFG создается командой Виталика Бутерина для Ethereum) и Casper CBC (разрабатывается командой Влада Замфира в проекте RChain).

Во всех новых реализациях Proof-of-Stake майнеров принято называть валидаторами, в EOS их именуют создателями блоков, в Tezos — «пекарями». Однако по сути их функции аналогичны майнерам в PoW-сетях — формирование цепочки (блокчейна) путем подтверждения корректности транзакций и помещения их в блоки.

DPoS

Изначально протокол DPoS был задуман для устранения одного из недостатков первых реализаций PoS — каждый кошелек должен был майнить отдельно, только свои монеты. DPoS позволяет владельцам небольших сумм делегировать монеты более крупным держателям, создавая таким образом подобие майнинговых пулов, объединяющих множество майнеров.

В DPoS количество валидаторов ограничено, они выбираются голосованием всех владельцев монет или другим способом, предусмотренным протоколом конкретного блокчейна. Для обновления списка валидаторов голосование, как правило, происходит на периодической основе, и в нем могут принять участие все владельцы токенов блокчейна. Такая схема работает, например, в EOS и Lisk. В Tezos, где применяется собственный алгоритм LPoS, количество валидаторов теоретически неограниченно, необходимо только иметь на балансе 10 000 XTZ. Валидаторы аналогично майнерам работают на псевдоконкурентной основе, право создания блока время от времени получает каждый из них.

В протоколе Tendermint (который часто называют BFT-PoS) каждый блок подписывается несколькими валидаторами с помощью их закрытых ключей, при этом для подтверждения блока за него должны проголосовать не менее 2/3 всех имеющихся валидаторов. Предложить сформированный блок на утверждение может любой из них. Каждый блок предлагается в ходе так называемого раунда, и, если необходимое количество подписей валидаторов не набирается, начинается новый раунд. Это продолжается до тех пор, пока не будет набран кворум в 2/3 подписей, после чего блок присоединяется к основной цепи и открывается раунд для предложения следующего блока. Подписи валидаторов на блоке можно идентифицировать в публичном блокчейне с помощью открытых ключей.

На сегодняшний день консенсус Tendermint применяется только в проекте Cosmos, который проводит достаточно закрытую политику и почти не информирует сообщество о ходе разработок. Кроме того, на Tendermint предположительно основан проект братьев Дуровых Telegram Open Network, который, по неофициальной информации, планируют запустить в марте 2019 года. Точная дата пока неизвестна.

Casper

Теоретические разработки протокола Casper, также называемого Ethereum 2.0, появились летом 2016 года, когда план перехода на консенсус Proof-of-Stake был опубликован командой Виталика Бутерина в «Лиловой книге» (Mauve Paper). Реализация в коде и запуск Casper в основной сети Ethereum первоначально планировались на лето 2017 года, но с тех пор многократно переносились. В сентябре 2018 года разработчики Ethereum заявили, что полноценная реализация Casper появится только в конце 2019 года, а промежуточная, с комбинированным майнингом, не раньше середины года, хотя основные элементы протокола были протестированы к первой половине 2018 года.

Один из ключевых элементов Casper, который теоретически даст Ethereum почти неограниченные возможности масштабирования, — это шардинг, метод распределения базы данных по множеству серверов в виде блоков (шардов), уже достаточно давно применяемый в классических СУБД. В спецификации Casper шардингом называется многопоточная обработка транзакций, в которой единый блокчейн разбит на множество частей (шардов), причем с каждой из них будет работать отдельная группа валидаторов. По сути, блокчейн будет разбит на множество параллельных цепочек, формирующих и подтверждающих (финализирующих) собственные блоки. Надежная синхронизация этих цепочек и создание из них виртуально единого блокчейна с помощью перекрестных ссылок между шардами остается главным камнем преткновения в применении концепции шардинга в протоколе Casper. Эффективное и достаточно безопасное решение до сих пор не найдено, поэтому сроки релиза продолжают переноситься.

На данный момент готовится к выпуску промежуточная версия Casper FFG без шардинга, технически находящаяся посередине между DPoS и Tendermint, — с майнингом

единой цепочки всеми валидаторами. Сначала Casper пройдет стадию гибридного майнинга, когда часть блоков будет создаваться PoW-майнерами, а остальные — валидаторами PoS. Для того чтобы стать валидатором, пользователю придется заморозить некоторую сумму ETH в смарт-контракте (точный размер депозита еще не определен).

Блоки в Casper FFG планируется создавать каждые четыре секунды, при этом PoW-майнерам достанется примерно один из четырех или пяти блоков. Через определенное количество блоков будет создаваться чек-пойнт, дальше которого блокчейн невозможно будет откатить — это один из методов противодействия картельному сговору валидаторов и другим распространенным атакам.

Еще одна версия Casper CBC разрабатывается Владом Замфиром (сейчас он работает в проекте RChain). Эта концепция действует на чистом PoS, причем в ней не предусмотрена общая окончательная финализация блоков — каждый валидатор самостоятельно устанавливает для себя порог неизменяемости. CBC — более гибкий протокол по сравнению с FFG, но более уязвим к разделению цепочки (форку). Запуск проекта Rchain на основе Casper CBC намечен на II квартал 2019 года.

BFT

Название метода BFT (byzantine fault tolerance) может ввести в заблуждение. «Задача византийских генералов» была сформулирована еще до появления Bitcoin и означает способ нахождения консенсуса между сторонами, которые не могут доверять друг другу. Эту модель использовал и Сатоси Накамото, она применяется и в PoW, и в PoS. Однако блокчейн-консорциум Hyperledger, а также другие блокчейны для корпоративного рынка, включая Ripple и Stellar, используют свой альтернативный метод консенсуса именно с таким названием. В этом разделе описан именно BFT как метод консенсуса для определенного вида блокчейнов, а не решение «задачи византийских генералов» в общем виде.

В Hyperledger Fabric используется консенсус под названием Practical Byzantine Fault Tolerance (PBFT), аналогично DPoS основанный на фиксированном количестве валидаторов, однако здесь они не выбираются, а назначаются администраторами блокчейна. Валидация транзакций происходит через смарт-контракт (chaincode). Транзакция считается верной, если количество валидаторов, подтвердивших ее, окажется втрое больше, чем отвергнувших.

В Ripple и Stellar применен Federated Byzantine Agreement (FBA): каждый из валидаторов ведет и подтверждает собственную цепочку транзакций, причем в Ripple валидаторы также назначаются Ripple Foundation, а в Stellar валидатором может стать любой узел. Консенсус формируется с помощью групп узлов, образующих кворум, достаточный для подтверждения транзакции. В большой сети кворум разбивается на части, или слайсы (quorum slices), образующие федерацию, причем один узел может входить в несколько слайсов. Транзакция подтверждается слайсом, которому доверяет отправивший ее узел, в спорных случаях кворум расширяется включением в него других слайсов. Узлы-нарушители могут быть блокированы и исключены из кворума.

Эта группа методов консенсуса отличается тем, что узел блокчейна может самостоятельно выбирать валидаторов для своих транзакций и присоединяться сразу к нескольким группам, также выступая в качестве валидатора.

Сайдчейны

Технология боковых цепей, или сайдчейнов, предусматривает создание древовидной структуры дочерних цепочек, созданных на основе более надежного материнского блокчейна с помощью двусторонней привязки. Концепция сайдчейнов была разработана еще в 2014 году, но технические сложности ее реализации и далеко не очевидные преимущества тормозят появление крупных проектов.

Сайдчейн представляет собой практически самостоятельную цепочку блоков со своими узлами, токенами и консенсусом, однако токены (монеты) сайдчейна выпускаются только на

основе монет базового блокчейна, замороженных на специальном адресе. Готовность монет к использованию в сайдчейне определяется группой узлов, которая называется федерацией. Членов федерации может выбирать создатель адреса.

Монеты базового блокчейна служат для обеспечения ценности монет сайдчейна, причем их использование возможно только при выводе эквивалентного количества из обращения в сайдчейне. Для функционирования сайдчейна необходимы собственные майнеры или валидаторы, независимые от материнского блокчейна (может отличаться даже метод консенсуса или алгоритм хеширования).

Сейчас технологию сайдчейнов разными способами используют всего несколько проектов, так как она достаточно затратна и технически сложнее создания собственного блокчейна, а тем более производного криптоактива (токена). Основные варианты применения сайдчейнов — тестирование каких-либо функций основного блокчейна, создание обособленной среды для работы смарт-контракта, а также выпуск автономного актива с обеспечением монетами какого-либо популярного блокчейна.

Ниже представлены основные платформы и сервисы, применяющие сайдчейны.

Liquid

Проект Liquid, разработанный компанией Blockstream, основан на сайдчейне, привязанном к блокчейну Bitcoin. Разработка Liquid началась в январе 2017 года, когда была опубликована «Белая книга» проекта. Сайдчейн начал работать в июле 2018 года, а официальный запуск платежей в системе произошел в октябре.

Liquid был задуман как автономная альтернатива Lightning Network для операций с крупными суммами и представляет собой платежную сеть на основе отдельного актива L-BTC, обеспеченного связанными в сайдчейне биткоинами и выпускаемого в соотношении 1:1. В Liquid также задействован механизм Strong Federations — развитие идеи многоподписных адресов (multisig), средствами которых могут распоряжаться только члены федерации (пользователи, имеющие один из закрытых ключей, привязанных к адресу). Для совершения транзакций необходим кворум из достаточного количества закрытых ключей.

В отличие от Lightning Network, которая позиционируется в качестве сети для небольших повседневных платежей и предназначена для массового рынка с большим количеством пользователей, Liquid нацелена на небольшое количество максимально безопасных и конфиденциальных транзакций. Разработчики Blockstream описали этот проект как транзакционную сеть между биржами и другими представителями крупного криптовалютного бизнеса.

Технология Strong Federations должна усилить надежность платежей и взаимное доверие участников, а также исключить крупные взломы бирж, поскольку для кражи L-BTC злоумышленнику придется не только добыть нужное количество закрытых ключей, принадлежащих разным компаниям, но и вывести L-BTC из сайдчейна, обменяв их на биткоины. Такая задача едва ли под силу даже крупнейшим хакерским группировкам.

Пока еще сложно говорить о будущем Liquid. Несмотря на то что уже 23 крупные блокчейн-компании участвовали в запуске и изъявили желание воспользоваться сервисом, реальные объемы транзакций в Liquid неизвестны, а использование этого сайдчейна без достаточной ликвидности не имеет смысла. Тем не менее, это на сегодня самое крупное применение технологии за четыре года ее существования.

RSK

Платформа Rootstock (RSK), также основанная на блокчейне Bitcoin, представляет собой пока единственную попытку реализовать на первом в мире блокчейне возможности полнофункциональных смарт-контрактов.

Потенциал встроенного языка скриптов Bitcoin очень скромен и позволяет в лучшем случае определять способ и время получения транзакции, но для сложных сценариев, тем более связанных с внешним миром, его недостаточно.

Эту проблему и пытаются решить разработчики Rootstock, хотя преимущества для исполнения смарт-контрактов более современных специализированных платформ очевидны. Скорее, этот проект — отголосок желания ортодоксов Bitcoin видеть реализацию всех возможностей технологии блокчейна на первой и самой защищенной цепи, невзирая на возникающие препятствия.

Проект Rootstock появился в конце 2015 года и сумел собрать инвестиции на несколько миллионов долларов, но до сих пор не вышел из стадии тестирования, а целесообразность его завершения вызывает много вопросов.

Запустить полноценные смарт-контракты непосредственно в блокчейне Bitcoin невозможно без его полной перестройки, поэтому разработчики RSK решили использовать сайдчейн с собственными правилами протокола, во многом аналогичными Ethereum. Более того, децентрализованные приложения RSK совместимы с Ethereum и поддерживают язык Solidity. Тем не менее сайдчейн все еще находится на этапе бета-версии, доступной только для разработчиков.

Ardor

Блокчейн Ardor, запущенный в 2017 году разработчиками NXT как следующее поколение этой платформы, основан на концепции PoS и использует технологию, похожую на сайдчейны (здесь они называются дочерними цепочками, childchains).

В этих отдельных цепочках обращаются созданные на платформе производные токены. В отличие от NXT, где транзакции токенов передавались в базовом блокчейне, в Ardor они имеют больше самостоятельности за счет использования подчиненных цепочек. Все функции NXT, такие как децентрализованная биржа, голосования, система сообщений, облачное хранилище и платежная сеть, работают на Ardor в автономных дочерних цепочках. Создатели платформы позиционируют ее как основу для развития бизнеса на блокчейне, предлагая создание самостоятельного сайдчейна, который будет поддерживаться инфраструктурой базового блокчейна.

Блокчейн Ardor все еще находится в разработке, поэтому на нем полноценно функционирует только одна дочерняя цепочка под названием Ignis, демонстрирующая возможности платформы для бизнеса. Запуск большей части функций Ardor, включая расширенные возможности управления дочерними цепочками, планируется в первой половине 2019 года.

Lisk

Один из ранних конкурентов Ethereum, проект Lisk, провел ICO в 2016 году, собрав $6,5 млн, и уже к концу года запустил собственный блокчейн на консенсусе DPoS. Однако разработка платформы значительно отстает от первоначальных планов, и, несмотря на оригинальную концепцию, сейчас она практически затерялась среди конкурентов.

Основная особенность Lisk заключается именно в использовании сайдчейнов. По замыслу разработчиков каждое децентрализованное приложение (смарт-контракт) должно работать в собственном сайдчейне. Такой подход позволяет достичь сразу нескольких целей.

Во-первых, DApps независимы друг от друга и от базовой платформы, и взлом или сбой одного из них не затронет остальные — сайдчейн может быть даже полностью уничтожен без ущерба для всей платформы. Во-вторых, каждое приложение получает в свое распоряжение практически полноценный блокчейн и может настраивать правило консенсуса под себя, без необходимости приспосабливаться к общим ограничениям. Наконец, в-третьих, приложения могут даже сами выпускать как производные токены, так и привязанные к токену LSK.

Однако разработчики Lisk переоценили свои возможности: несмотря на то, что в августе–сентябре 2018 года было проведено несколько важных обновлений, в работе сети часто возникают сбои, и до построения надежной экосистемы DApps на сайдчейнах, вероятно, пройдет еще много месяцев.

Атомарные свопы

Прямое взаимодействие блокчейнов уже в ближайшем будущем может стать одной из самых востребованных пользователями функций. Этот механизм становится все более необходимым, поскольку количество как публичных, так и частных блокчейнов растет. Первым нужно надежное средство обмена криптоактивов, вторым — организация прямых информационных потоков без привлечения сторонних систем.

Хорошая новость состоит в том, что такое решение уже есть — оно называется атомарными свопами (atomic swaps). Этот термин пришел из среды баз данных, где существует понятие атомарности транзакции (atomicity): ряд действий с базой данных, совершаемых в рамках транзакции, либо выполняется целиком, либо не должен производиться вовсе. В случае ошибки в одном из элементов транзакции все ранее выполненные действия отменяются, и база данных откатывается на состояние до начала транзакции. Термин «своп» (swap) наиболее распространен на финансовых рынках и обозначает прямой обмен одного актива на другой.

Механизм работы атомарного свопа достаточно прост и технически похож на работу канала Lightning Network с той разницей, что в свопах проводится только одна операция без сохранения открытого канала. В его основе лежит простой смарт-контракт, использующий транзакции P2SH и метод Hash-Time-Lock-Contracts (HTLC) — блокировку по времени и хешу. С помощью блокировки по хешу обеспечивается надежный двусторонний обмен, а блокировка по времени нужна для отката транзакции через установленный интервал, если одна из сторон откажется от свопа.

В качестве примера рассмотрим гипотетический обмен между блокчейнами Bitcoin и Litecoin.

Алиса (инициатор свопа) хочет обменять у Боба 1 BTC на 100 LTC. Для этого Алиса и Боб устанавливают друг для друга условия обмена через многоподписные адреса в каждом блокчейне.

1. Алиса создает обменный (депозитный) адрес в блокчейне Bitcoin, для получения средств с которого нужна подпись Боба и секретная фраза, которую Алиса генерирует и затем хеширует.

2. После этого Алиса отправляет 1 BTC на депозитный адрес с условием разблокировки по предъявлению прообраза хеша (секретной фразы).

3. Боб аналогично отправляет на свой депозитный адрес 100 LTC, но для того, чтобы Алиса могла забрать из него лайткоины, необходима подпись Боба.

4. Получив 100 LTC от Боба, Алиса открывает ему секретную фразу.

5. Используя секретную фразу, Боб подписывает транзакцию свопа, тем самым получая биткоины и открывая Алисе доступ к своим лайткоинам.

Если Боб или Алиса в течение заданного в контракте интервала не завершили какой-либо из перечисленных выше шагов, то срабатывает отмена блокировки по времени и обе стороны остаются при своих.

Атомарные свопы в теории были описаны еще в 2013 году, но реализация в коде появилась далеко не сразу. Их широкое обсуждение началось в конце 2016 года, а к концу

2017-го уже были проведены первые экспериментальные транзакции между Bitcoin и несколькими альткоинами, в число которых вошли Ethereum, Litecoin, Zcash, Decred, Vertcoin и еще несколько криптовалют.

Плюсы внедрения атомарных свопов в процесс обмена криптоактивами более чем очевидны:

1. Исключение доверенных посредников в лице криптовалютных бирж и всех связанных с ними технических и юридических проблем.

2. Ускорение обменов, так как не приходится ждать зачисления средств на баланс и вывода в кошелек. Обмен можно осуществлять непосредственно через кошелек, и все операции будут проводиться под полным контролем пользователя.

3. Минимальные комиссии за обмен, ограничивающиеся вознаграждением майнеров (валидаторов) за подтверждение транзакций в блокчейне.

На основе атомарных свопов может появиться абсолютно новое поколение децентрализованных бирж, где не нужны регистрация, прохождение процедуры KYC и прочие бюрократические процедуры. Основной проблемой таких площадок остается сложность формирования курса и книги ордеров (например, невозможно функционирование удобных крупным трейдерам скрытых заявок), а также низкая скорость непосредственно торговых операций — такие биржи не годятся для спекулянтов.

Из децентрализованных бирж на основе атомарных свопов наиболее известны 0x и Altcoin DEX, в разработке находятся еще несколько проектов этого типа. Но ни одна децентрализованная биржа пока не может похвастаться высокой ликвидностью. Кроме того, они технически не способны работать с фиатными валютами.

У атомарных свопов, несомненно, большое будущее, так как именно эта технология позволит создать интернет блокчейнов, где операции между блокчейнами будут проводиться без каких-либо посредников и их даже можно будет автоматизировать. Появятся и универсальные мультичейновые кошельки, способные обрабатывать атомарные свопы в графическом интерфейсе одного приложения. Это сделает мир криптоактивов доступным для массового использования и обеспечит частные блокчейны надежным инструментом обмена информацией.

Глава 9

Время экспериментов пройдет. В каких областях блокчейн найдет применение

Спустя 10 лет после появления первого блокчейна эта технология во многом все еще остается экспериментальной. Пока сложно с уверенностью прогнозировать будущее отрасли блокчейна и самой технологии, но определенные его контуры уже вырисовываются.

Ортодоксы Bitcoin уверены, что блокчейн сам по себе никому не нужен, а все попытки использования распределенных реестров без криптовалют не оправдают надежд и будут прекращены или же их доработки приведут к отказу от основных принципов блокчейна. Их противники, в основном представляющие банки или госструктуры, напротив, заявляют, что криптовалюты и большинство публичных блокчейнов через несколько лет исчезнут и

будущее останется за стандартизированными и непременно регулируемыми распределенными реестрами.

Реальность вряд ли оправдает все надежды идеалистов или будет полностью соответствовать ожиданиям скептиков: сумма всех усилий приведет к определенному компромиссу, и блокчейн займет свое место среди прочих достижений человечества. Попытаемся сформулировать позитивные и негативные факторы, которые будут влиять на развитие отрасли в обозримом будущем.

Bitcoin появился в 2008 году как реакция свободного общества на растущие возможности государства в регулировании финансовых потоков. Переход развитых стран на безналичные расчеты и постепенный отказ от наличных денег делают все доходы и расходы людей видимыми для банковской системы, а через нее и для регуляторов. Если передачу даже больших сумм наличных денег скрыть несложно, то любые безналичные операции до появления криптовалют могли проходить только через посредников в виде банков и платежных систем. Посредник же имеет все возможности не только отследить, но и отменить транзакцию, заморозить или даже конфисковать средства гражданина, всего лишь заподозренного в незаконной деятельности. Но даже в повседневной деятельности наличие посредников замедляет операции и приводит к повышению расходов. С развитием глобальных сетей коммуникаций старая финансовая система становилась все более тяжеловесной и все сильнее отставала от технического прогресса.

Потребность общества в новых деньгах с лучшими возможностями привела к появлению криптовалют (почти сразу после финансового кризиса 2008 года, который пока остается крупнейшим в XXI веке). Они дали людям возможность полностью контролировать свои операции, избавиться от посредников и не считаться с границами. В отличие от чемодана с наличными, любая сумма в криптовалюте передается в любую точку мира за считаные секунды, и транзакция не может быть заблокирована банком или регулятором. Поэтому появление биткоина произвело настоящую революцию в умах и через несколько лет вызвало новую «золотую лихорадку».

Неопределенность сохраняется

С новым типом денег появился и новый букет проблем. На высокой волатильности расцвели спекулятивные пузыри, многие слабые и зачастую созданные любителями системы безопасности криптовалютных бирж оказались уязвимы для хакеров, а анонимность и неподконтрольность криптовалют привлекли мошенников: с их помощью начались продажи нелегальных товаров, частыми стали случаи уклонения от уплаты налогов и отмывания денег. Регуляторы, обеспокоенные неподконтрольностью растущих финансовых потоков, начали бить тревогу и вводить ограничительные меры — от полного запрета криптовалют в ряде стран до попыток контролировать операции с ними.

Тем временем, пока в обществе бушевал ажиотаж вокруг криптовалют и зарождающихся платформ смарт-контрактов, росла заинтересованность бизнеса не столько в новой финансовой системе, сколько в блокчейне — базовой технологии, позволяющей решить проблемы, назревшие как в финансовом секторе, так и в производстве, логистике, энергетике, госуправлении и даже в медицине.

На самом деле блокчейн представляет собой нишевое решение и неспособен полностью заменить существующие СУБД или международные платежные системы, но может быть интегрирован с ними.

Однако в 2016–2017 годах в деловой среде сформировался странный и, возможно, более опасный пузырь, который уже неоднократно сравнивали с бумом доткомов (интернет-компаний), который зародился на волне распространения интернета. Пузырь доткомов лопнул на рубеже тысячелетий и унес с собой не только большинство неудачных стартапов, но и сотни миллиардов долларов, вложенных в них инвесторами.

С 2016 года блокчейн пытаются применить буквально везде, даже там, где его внедрение совершенно не нужно и не даст никакого экономического эффекта. В стартапы вкладываются

десятки и сотни миллионов долларов только потому, что в их названиях присутствует слово «блокчейн», а также часто из-за пустых обещаний, не подкрепленных ни профессионализмом коллектива разработчиков, ни проработанной и обоснованной концепцией. И это происходит не только в нерегулируемых ICO, но и с публичными компаниями, акции которых торгуются на фондовых биржах США.

Весьма характерен случай, произошедший с производителем напитков, компанией Long Island Iced Tea, в I квартале 2018 года. Ее капитализация на бирже NASDAQ только из-за ребрендинга в Long Blockchain за один день выросла более чем в четыре раза! После того как биржа провела расследование и установила, что компания на самом деле не планировала разработку блокчейна, ее акции были сняты с торгов и обвалились в 10 раз. То же самое вскоре случилось с компанией Longfin, которая заявила о покупке блокчейн-стартапа и добавила в название слово blockchain. Акции компании за несколько дней поднялись на 1342%, но итог был аналогичным: снятие с торгов, обвал котировок и арест активов.

Тем не менее даже подобное безумие приносит плоды, и развитие отрасли становится все более упорядоченным. В последнее время усиливаются призывы к разработке способов глобального регулирования блокчейна и криптовалют. Основную активность проявляет FATF — международная организация, занимающаяся созданием стандартов в сфере борьбы с отмыванием денег и финансированием терроризма. В сентябре 2018 года в России было принято решение отложить утверждение законопроектов о криптовалютах и дождаться рекомендаций FATF, которые могут стать основой глобального регулирования отрасли блокчейна.

Международная организация по стандартизации (ISO) также сформировала рабочую группу для создания стандартов в сфере блокчейна, но практических результатов ее работы следует ожидать в 2019 году. Возможно, принятие технических стандартов будет отложено до прояснения юридических вопросов. Таким образом, отрасль блокчейна перейдет на стадию взросления уже относительно скоро, и в 2020-х годах определится ее облик и решится судьба большинства существующих блокчейн-проектов.

Направления развития

Уже сейчас постепенно определяются два основных направления, которые с течением времени, вероятно, будут все больше обособляться друг от друга: децентрализованные публичные блокчейны и управляемые частные блокчейны. Поскольку их отличия друг от друга фундаментальны, со временем взаимодействие между проектами разных направлений будет все менее возможным.

Во второй половине 2018 года много писали о хороших перспективах управляемых (то есть частных и государственных) блокчейнов. Действительно, решения на основе Hyperledger, Corda, Exonum и других проектов управляемых блокчейнов могут принести все те преимущества, которых от них ожидают. Они позволят снизить затраты в процессах согласования и принятия решений, обеспечить более безопасную среду обмена информацией и повысить доверие между контрагентами. При этом централизованные решения не допускают анархии децентрализованных систем, оставляя принятие ключевых решений не за безликим сообществом рассеянных по всему миру анонимов, а за четко определенной группой или организацией, осуществляющей управление блокчейном.

Правильнее будет называть подобные сети не блокчейнами, а частными распределенными сетями с элементами блокчейна. Из трех основных характеристик Bitcoin и других публичных блокчейнов (неизменяемость, децентрализация, открытость) в управляемых блокчейнах, по сути, сохраняется только первая, и то условно:

1. Неизменность данных в контролируемом блокчейне не гарантирована для рядовых пользователей, так как при наличии единого управляющего центра такой блокчейн может быть остановлен с проведением отката до нужного блока, при этом узлы, не имеющие административных полномочий, никак не

могут предотвратить или отменить такое изменение. Здесь происходит частичный возврат к привычной клиент-серверной архитектуре с балансировкой нагрузки.

2. Понятие децентрализации в управляемом блокчейне исключено на уровне концепции. В нем изначально существуют узлы с разными уровнями полномочий, поэтому даже при распределенном хранении и обработке данных (для чего блокчейн вовсе не обязателен) его структуру правильнее рассматривать как иерархическую с наличием двух или более уровней.

3. Принцип открытости управляемого блокчейна (то есть возможности для любого участника сети видеть всю историю транзакций всех пользователей) может быть заложен или отвергнут при его создании в зависимости от функциональных особенностей. Однако для корпоративных сетей всегда будет характерна политика разграничения доступа к информации — как ее чтения, так и добавления в систему и внесения изменений. Государственным сервисам полная открытость также противопоказана, хотя бы из соображений защиты персональных данных пользователей, наличия различных уровней секретности и т.д.

Все это означает, что архитектурные и технические различия между публичными и частными блокчейнами будут усиливаться и со временем, возможно, приведут к полностью обособленному их развитию, даже если будут приняты стандарты, обеспечивающие совместимость. При этом обмен технологиями может стать односторонним — все удачные решения, найденные разработчиками публичных блокчейнов, смогут на основании открытых лицензий использоваться в частных проектах. В то же время корпоративные разработки, без сомнения, будут патентоваться, а их стороннее использование станет возможным только при заключении лицензионных договоров и соответствующих отчислений.

Однако конфликтов с этой стороны, вероятно, не будет. Если публичные сервисы ввиду открытости исходного кода будут оставлены на попечение неформальных коллективов разработчиков, как это практикуется сейчас, то разработка частных блокчейнов сосредоточится в руках ИТ-корпораций, в число которых будет трудно пробиться новым игрокам. Однако, как и в случае с Linux и многим другим открытым ПО, разработки даже бесплатных продуктов с открытым исходным кодом часто спонсируются корпорациями и впоследствии используются в их продуктах. По сути, этот процесс уже идет: в разработке частных блокчейнов участвуют IBM, Microsoft, Oracle, SAP, Intel, Baidu, Cisco, Hitachi и другие гранды отрасли. Из сколько-нибудь серьезных самостоятельных игроков нового поколения, ставших «единорогами», можно отметить только Bitfury с их проектом Exonum. Но и эта компания, если даже ей удастся вывести на рынок свой продукт, может проиграть битву с гигантами или просто быть поглощена.

Вероятно, наибольшим разочарованием для блокчейн-энтузиастов станет отказ от мечты о «мировой революции», которую якобы должна принести децентрализация и прозрачность обмена информацией. Революции совершаются в сознании общества, а технологии только помогают их воплощению. Но публичные блокчейны не смогут преодолеть политических барьеров, а в частных технологиях используются вполне утилитарно.

На корпоративном рынке от блокчейна можно ожидать эволюционных процессов, таких как снижение затрат и переход на новый уровень взаимодействия между контрагентами, но вряд ли последуют действительно революционные изменения. В конце концов, с технической точки зрения блокчейн (или то, что от него останется после всех модификаций под нужды корпоративного рынка) — это всего лишь еще одна технология распределенных баз данных, причем только для определенной ниши. Технология блокчейна будет так же поглощена рынком, как и все прошлые технические прорывы. Блокчейн получит мировое признание и

повсеместное применение, но вряд ли результат будет соответствовать ожиданиям криптоанархистов и энтузиастов криптовалют.

То же самое касается и юридических аспектов: если частные блокчейны будут введены в правовое поле и должным образом стандартизированы (без этого ни одна крупная организация не пойдет на их внедрение), то давление на публичные блокчейны станет усиливаться. Точечные запреты или ограничения на определенные виды деятельности вроде существующих в Китае будут систематизированы и введены на международном уровне. Возможно, победит более конструктивная японская модель, которая ненамного мягче. Формально криптовалюты в Японии легализованы и приравнены к иностранным фиатным валютам, однако все операции с ними требуют регистрации и идентификации пользователя. Это фактически нивелирует большинство описанных ранее преимуществ нового вида денег.

Что касается регулирования собственно технологии блокчейна, то в нем фактически нет необходимости. В регулировании нуждаются, возможно, некоторые аспекты применения технологии, касающиеся политики и финансов, но не она сама. Здесь роль регуляторов сыграет разработка единых мировых стандартов.

Какие проблемы придется решить

Кроме описанных в главе 7 чисто технических проблем масштабирования и взаимодействия блокчейнов, уже скоро придется заняться и социальными.

И в публичных, и в частных блокчейн-платформах все более актуальным становится вопрос управления как ключевыми изменениями в системе, так и повседневной активностью. Чем больше пользователей находится в децентрализованной системе, тем сложнее организовать эффективное принятие решений. Если в частных блокчейнах возможность управления с помощью привилегированных узлов закладывается изначально, то в открытых системах ее приходится строить «на ходу» и с гораздо меньшей эффективностью, поскольку необходимо исключить возможность влияния небольшой группы пользователей. Существующие виды управления были описаны в главе 3, однако вопрос развития механизмов управления в блокчейнах разных типов и назначений все еще остается открытым.

Отдельно следует рассмотреть еще одну проблему, а именно обеспечение анонимности транзакций в блокчейне. С одной стороны, ведется работа по повышению анонимности транзакций в публичных блокчейнах, с другой — попытки введения механизмов идентификации и процедуры KYC в корпоративных версиях блокчейнов и других проектах, стремящихся продемонстрировать правительствам возможности регулирования и контроля операций. Как правило, задача идентификации пользователей блокчейна решается внешними средствами. То есть либо перед созданием учетной записи в блокчейне, либо, напротив, путем анализа транзакций пользователя, записанных в блокчейн (так, например, ведутся расследования противоправной деятельности). Если же блокчейны найдут массовое применение, то идентификация учетных записей пользователей на уровне блокчейна при сохранении полной или частичной анонимности транзакций будет востребована в корпоративных и государственных проектах, в той или иной степени применяющих блокчейн. Сейчас можно выделить два проекта, вплотную занявшихся совмещением блокчейна и механизмов регулирования. Это Ontology, связанный с китайской блокчейн-платформой NEO, и все еще не представленный общественности проект TON (Telegram Open Network), который задействует для идентификации пользователей блокчейна уже существующую технологию Telegram Passport. Запуска работающих продуктов этих двух проектов следует ожидать в 2019 году.

Прогнозы развития отрасли

Исходя из вышеизложенного, в перспективе ближайших двух-трех лет, скорее всего, будут принимать решения, которые определят будущее блокчейна как минимум на десятилетие.

Займет ли он узкую нишу прикладной технологии или скоро блокчейны будут буквально везде, оставаясь незаметными для рядового пользователя гаджетов и сетевых сервисов? В каких отраслях применение блокчейна будет эффективным, а где он, вероятно, не принесет весомых преимуществ? Как могут измениться в будущем существующие блокчейн-проекты?

Будущее публичных блокчейнов

Многообразие публичных блокчейнов, разросшихся на буме криптовалют и ICO, произошедшем в 2017 году, вскоре, вероятно, ждет значительное уменьшение. Общая капитализация отрасли продолжает падать, и первыми жертвами массового исхода инвесторов станут самые слабые проекты, в которые вкладывались «на всякий случай», пока они росли вместе со всем рынком. В самом деле, кому могут понадобиться десятки копий Bitcoin и Ethereum, которые не способны предложить никаких уникальных разработок или имеющих коммерческую ценность изменений? Не смогут выдержать «гонку на истощение» в период нестабильности и некоторые крупные проекты, не сумевшие сформировать лояльное сообщество. Вероятно, сфера применения публичных блокчейнов сузится до нескольких направлений, где централизованные решения не смогут быть эффективными.

Криптовалюты

Несмотря на множество мрачных прогнозов, исходящих от видных политиков, бизнесменов и ученых, включая нобелевских лауреатов, Bitcoin остается локомотивом отрасли, самым популярным, дорогим и защищенным блокчейном в мире. Это значит, что идеи Сатоси Накамото, пусть нам и не известно, кто скрывается под этим псевдонимом, нашли отклик в обществе и потребность в независимой денежной системе действительно существует.

Если в конце концов появятся государственные цифровые валюты и корпоративные платежные системы со сходными или даже превосходящими характеристиками, альтернатива им в виде децентрализованной криптовалюты, однажды появившись, уже не исчезнет. Помешать этому может разве что запрет частных денег во всем мире, что выглядит маловероятным.

Многим представителям старой экономической школы, особенно среди чиновников, хочется верить в крах «криптовалютного эксперимента», но факты пока говорят об обратном. Несмотря на сдувание спекулятивного пузыря, жесткую риторику многих регуляторов и даже разочарование частных инвесторов, понесших убытки, интерес крупного бизнеса и институциональных инвесторов к криптовалютам продолжает расти.

Так, американские товарные биржи CME и CBOE, в 2017 году запустившие фьючерсы на биткоин, вовсе не собираются сворачивать этот инструмент, а, напротив, сообщают о росте объемов торговли. Оператор Нью-Йоркской фондовой биржи, компания ICE, при поддержке Microsoft разрабатывает платформу торговли криптовалютами Baktt. Возможно, на ней будут торговаться фьючерсы на биткоин и эфир (включая поставочные контракты), а также криптовалютные ETF в случае их одобрения регуляторами. В октябре 2018 года крупная инвестиционная компания Fidelity Investments заявила о запуске криптовалютной платформы для институциональных инвесторов, а председатель Комиссии по торговле товарными фьючерсами США (CFTC) Кристофер Джанкарло заявил, что именно приход крупных инвесторов поможет рынку криптовалют стать зрелым.

Однако если будущее Bitcoin выглядит обнадеживающим, то большинство других криптовалют, вероятно, уже в ближайшие годы ждет постепенное увядание. Когда разработчикам Bitcoin Core удастся окончательно разобраться с масштабированием и постоянным ростом блокчейна, исчезнут даже те мнимые преимущества, на которых все еще держится большинство альткоинов. Основная их масса не может предложить сообществу ничего уникального, и такие проекты в ближайшие годы потеряют большую часть аудитории. За 2018 год почти все альткоины подешевели относительно биткоина в несколько раз, и эта тенденция сохраняется. Поэтому уже через пять лет количество криптовалют с

капитализацией выше 1–2% от капитализации Bitcoin можно будет пересчитать по пальцам одной руки. В первую очередь это относится к чистым криптовалютам, не имеющим иных функций, кроме проведения платежей через блокчейн.

Платформы децентрализованных приложений

Как уже было упомянуто в главе 5, платформы децентрализованных приложений (смарт-контрактов), позволяющие воспользоваться всеми преимуществами децентрализации и распределенных вычислений без необходимости запуска собственного блокчейна, уже уверенно конкурируют с криптовалютами (кроме Bitcoin), а вскоре могут и превзойти их в популярности.

Несмотря на конкуренцию со стороны частных платформ, публичные блокчейны для выполнения смарт-контрактов находятся в начале пути своего развития. Количество платформ со временем неизбежно уменьшится из-за ухода недееспособных проектов, но лидеры при этом будут расти и становиться все более универсальными, добавляя новые возможности и повышая качество кода.

Публичные платформы остаются наилучшим выбором для небольших команд и для проектов, направленных на массовую аудиторию. Сдувание пузыря ICO, которое, вероятно, завершится в течение 2019–2020 годов, окажет на основные платформы смарт-контрактов скорее положительное влияние и оздоровит рынок, избавив его от слабых команд и явных мошенников, в то время как сильные проекты с реальным потенциалом будут стимулировать рынок. О зрелости этого сектора можно будет говорить тогда, когда суммарная капитализация приложений с реально работающими продуктами превысит капитализацию самих платформ. Ожидать этого можно в перспективе трех-пяти лет.

В этом секторе Ethereum пока сохраняет лидерство, и потенциал его технического развития остается самым большим, так как основная часть ключевых разработок появляется именно в этом проекте, а заинтересованность в платформе участников консорциума Enterprise Ethereum Alliance увеличивает его долгосрочную стабильность. Однако задержка командой Виталика Бутерина разработки протокола Casper, перехода на PoS и создания новой системы управления может разочаровать основных инвесторов. Если этот вопрос не будет разрешен ко второй половине 2020 года, проекту может угрожать крах или потеря лидерских позиций. Ближайший конкурент Ethereum — EOS — нацелен на развитие снизу, то есть за счет децентрализованного сообщества, создание которого только начинается. О результатах усилий его разработчиков также можно будет судить по прошествии примерно двух лет. За это время прояснится и судьба растущих проектов, таких как NEO, Tezos, Waves, Cardano, Lisk, Rchain и т.д. Поэтому 2020 год может стать решающим в определении дальнейшего курса развития этого сектора отрасли блокчейна.

Распределенное хранение и вычисления

Еще один нишевый, но перспективный продукт, который более всего подходит для реализации на публичном блокчейне, это системы децентрализованного хранения файлов. Рядом с ними можно упомянуть также сервисы для организации распределенных вычислений на блокчейне, бросающие вызов популярным облачным сервисам, таким как Amazon AWS, Microsoft Azure и Google Cloud. Среди множества провальных и сомнительных ICO именно перечисленные проекты нарушают общую тенденцию падения и даже подают признаки роста. Это значит, что они действительно востребованы и имеют шансы на успех.

В качестве перспективных систем хранения файлов можно назвать Storj, Filecoin, Sia, Decent и т.д. Распределенные вычисления на блокчейне все еще слабо развиты и представлены очень малым количеством проектов, продукты которых находятся в начальных стадиях развития. К ним относятся, например, Golem, iExec, SONM.

Общая проблема всех этих проектов — необходимость набора аудитории и клиентской базы, способных вывести их хотя бы на самоокупаемость разработки и компенсацию прочих

постоянных расходов, не говоря уже о прибыли. К февралю 2019 года они не могут похвастаться безоблачными перспективами, так как общее падение публичного интереса к криптовалютам и сфере блокчейна в целом затронуло и их.

Если в ближайшие год или два поднимется новая волна интереса к блокчейну, проекты распределенного хранения и вычислений могут продемонстрировать опережающий рост. В первую очередь на подобную динамику способны те из них, которые смогут вовремя представить полноценный продукт, пригодный для освоения даже пользователями без технических навыков. В противном случае без внешнего финансирования эти проекты не выдержат конкуренции с продуктами крупных корпораций, а найти его на стагнирующем рынке будет непросто. При таком развитии событий большая часть независимых проектов, вероятнее всего, в течение нескольких лет уйдет с рынка.

Будущее частных блокчейнов

Если относительно будущего публичных блокчейнов еще остаются сомнения, в первую очередь связанные с правовыми рисками и общим снижением рынка, то распространение частных блокчейнов с каждым годом выглядит все более неизбежным. Вопрос уже не в том, будут ли они существовать вообще, а в том, в каких формах будет проходить их внедрение и сколько еще времени займет тестирование и стандартизация. Судя по ускорению процесса и вовлечению в него большинства правительств и наиболее авторитетных международных организаций, долго ждать не придется. Уже несколько отраслей ожидают от блокчейна решения практических задач.

Универсальные платформы

Из всех частных блокчейнов наибольший потенциал роста имеют платформы для бизнеса, которые сегодня разрабатываются при участии крупнейших технологических корпораций мира. В первую очередь это уже много раз упоминавшиеся ранее Hyperledger Fabric, R3 Corda, Bitfury Exonum, а также менее публичные продукты от Microsoft, SAP, Oracle и других ИТ-гигантов.

Эти платформы способны предложить малому и среднему бизнесу как готовые «коробочные» решения, так и инфраструктуру и набор инструментов для самостоятельной разработки, тестирования и оптимизации решений на блокчейне, рассчитанные на нужды конкретного бизнеса. Корпорации имеют штат собственных профессиональных разработчиков, тестировщиков, юристов и необходимых специалистов различного профиля. В то же время технические и финансовые возможности корпораций несравнимы с возможностями небольших публичных проектов, к тому же они имеют различные рычаги влияния на регулирующие и контролирующие ведомства. Поэтому блокчейн для них — всего лишь еще одна перспективная технология, которую необходимо изучить и использовать наилучшим образом и с самой высокой эффективностью. Именно согласованные усилия крупных компаний в конце концов приведут к принятию единых технических стандартов для блокчейна.

Иными словами, вероятно, оптимальное решение для небольших организаций и частных лиц, планирующих использование блокчейна в собственном бизнесе, — это дождаться выхода на рынок корпоративных продуктов и выбрать наиболее подходящий из них. А конкуренция только подстегнет вендоров улучшать свои продукты и предоставлять клиентам все более выгодные условия.

У корпоративных продуктов есть и свои недостатки. Bitcoin и Ethereum уже показали, что независимые разработчики и сообщество могут добиться успеха и создать вполне конкурентоспособный продукт, при этом конечный пользователь имеет полную свободу в распоряжении средствами и инструментами на своей стороне и может свободно использовать платформы и их исходные коды.

Что же касается корпоративных продуктов, то и в области блокчейн-решений вряд ли удастся избежать пресловутого vendor lock-in, то есть привязки к продуктам одного производителя. Корпорации более консервативны и инертны, чем динамичные команды энтузиастов, и часто переносят в новые продукты свои старые баги и «заплатки», а также шлейф совместимости со старыми версиями своих программ. Корпоративные продукты нередко получаются слишком громоздкими и перегруженными ненужными для пользователя функциями. Исходные коды корпоративных приложений в большинстве случаев закрыты, и для доработки конкретного решения клиенту, скорее всего, придется заплатить немалые деньги.

Исходя из этого можно ожидать, что частные платформы найдут свою аудиторию и будут конкурировать скорее между собой, чем с публичными блокчейнами. Этот процесс, вероятно, оформится в течение трех-пяти лет.

Финансовые рынки

Пожалуй, единственная отрасль, где полезность блокчейна и его способность принести реальные изменения безусловны, это финансовые рынки и вся сфера их функционирования, от межбанковских операций до биржевой торговли. Блокчейн уже продемонстрировал высокую эффективность в ходе ряда пилотных проектов, проведенных банками, фондовыми биржами, депозитариями и регуляторами по всему миру.

Блокчейн все чаще рассматривается крупными фирмами как средство повышения эффективности платежных и расчетных систем. В этом плане можно указать несколько основных направлений использования блокчейна.

Системы межбанковских расчетов, в том числе международных, которым требуется наивысшая безопасность и надежность. Примером использования блокчейна в такой системе является российский «Мастерчейн».

На биржевых платформах блокчейн может быть использован в разных направлениях: для ведения реестров акционеров и организации голосований, хранения реестров торговых и посттрейдинговых операций, проведения расчетов между участниками торгов. В этой сфере прилагаются усилия одновременно во множестве стран, и в ближайшие годы они неизбежно приведут к общему знаменателю.

В октябре 2018 года блокчейн-стартап SETL получил лицензию регулятора фондовых бирж Франции на управление центральным депозитарием ценных бумаг. Аналогичными разработками занимаются фондовые биржи Австралии, Сингапура, Турции, Гонконга, Центральный банк Южной Африки и Банк Канады.

Госуправление

Возможности использования блокчейна в оказании государственных услуг и в процессах управления — тема поистине неисчерпаемая, и блокчейн здесь может раскрыться в полную силу. Одна из серьезных проблем, возникающих при взаимодействии государства с гражданами, — низкий уровень прозрачности, а иногда и взаимного доверия. Блокчейн может принести существенную пользу и способствовать сокращению расходов на ведение всех видов государственных реестров, проведение выборов и других голосований и регистрацию прав собственности (включая недвижимость и объекты интеллектуальной собственности).

Основной проблемой внедрения блокчейна в государственный сектор остается отсутствие правового статуса и международной стандартизации, поэтому практически в каждой стране, правительство которой заинтересовано в применении блокчейна, ведутся собственные разработки и эксперименты, а значит, многократно повторяются одни и те же ошибки. Однако по политическим причинам взаимодействие государств и согласование разработок в этой сфере крайне ограничено. Для приведения всех этих процессов к общему знаменателю потребуется много лет.

Логистика

Возможностью использования блокчейна в грузоперевозках крупные операторы заинтересовались еще в 2016 году. Эта технология, гарантирующая максимально быстрое распространение подтвержденной информации среди всех подключенных к сети контрагентов, была оценена по достоинству такими гигантами, как Maersk, UPS, Lloyd's Register и РЖД. В разработке и тестировании блокчейн-систем для цепочек поставок отметились IBM, Samsung SDS и китайский гигант Alibaba.

Поскольку морские, железнодорожные и авиационные грузоперевозки — одна из важнейших отраслей мировой экономики, в ее улучшение и в оптимизацию расходов вкладываются огромные средства. Поэтому внедрение блокчейна в логистику набирает обороты по всему миру.

Порты Абу-Даби, Антверпена, Роттердама и британский портовый оператор ABP независимо друг от друга начинают вести реестры операций на блокчейне. В сентябре 2018 года британское морское регистрационное общество Lloyd's Register представило блокчейн-платформу для повышения эффективности регистрации судов и грузов. В железнодорожных перевозках пионером стало ОАО «Российские железные дороги». Компания запустила пилотный блокчейн-проект для учета подвижного состава и запчастей. В авиаперевозках блокчейн внедряют российская S7 Airlines, немецкая TUI Airs, а также Air France и Air Canada.

По сути, процесс скоро станет необратимым, и препятствовать ему может только отсутствие совместимости между применяемыми системами, что является еще одним доводом в пользу международной стандартизации блокчейна, появление которой в ближайшие годы становится все более очевидным.

Заключение

Несмотря на всеобщий интерес к блокчейну, необходимо признать, что технология распределенных реестров — вовсе не панацея. Блокчейн пока не годится для оперативной обработки больших объемов данных, особенно видео и аудио, и для использования в быстро меняющейся среде.

Блокчейн идеален для долгосрочного и максимально надежного хранения редко изменяющейся информации. Поэтому технология перспективна для фиксации данных о клиентах банков, медицинских учреждений, страховых и логистических компаний. Распределенный реестр сделок принесет пользу патентным бюро и кадастровым палатам. Технология подходит правоохранительным и налоговым органам для учета персональных данных. Брокерским и инвестиционным компаниям блокчейн пригодится в качестве реестра биржевых операций.

Нынешние возможности технологии — это только промежуточный этап. Постоянное совершенствование блокчейна открывает перспективы для его применения в новых и новых отраслях. В своем развитии любая технология должна преодолеть стадию недоверия со стороны тех, кто консервативен и не привык быстро меняться. Блокчейн уже прошел этот этап и поэтому будет развиваться дальше.

[1] https://www.sec.gov/Archives/edgar/data/1729650/000095017218000060/xslFormDX01/primary_doc.xml

Редактор *А. Новресли*
Технический редактор *Н. Ратьков*
Главный редактор *С. Турко*
Руководитель проекта *А. Деркач*
Корректоры *Е. Аксёнова, Ю. Сычева*
Компьютерная верстка *К. Свищёв*
Художественное оформление и макет *Ю. Буга*

Табернакулов А.
Блокчейн на практике / Александр Табернакулов, Ян Койфманн. — М.: Альпина Паблишер, 2019.

ISBN 978-5-9614-2408-9