Мелани Свон

БЛОКЧЕЙН

СХЕМА НОВОЙ ЭКОНОМИКИ

РЕВОЛЮЦИЯ НА УРОВНЕ ИНТЕРНЕТА

ТЕХНОЛОГИЯ, КОТОРАЯ ИЗМЕНИТ МИР

Мелани Свон

Блокчейн. Схема новой экономики

«Олимп-Бизнес»

2015

УДК 004:338
ББК 65.050.253

Свон М.

Блокчейн. Схема новой экономики / М. Свон — «Олимп-Бизнес», 2015

ISBN 978-5-9693-0360-7

Блокчейн – это многофункциональная и многоуровневая информационная технология, предназначенная для надежного учета различных активов. Потенциально эта технология охватывает все без исключения сферы экономической деятельности и имеет множество областей применения. В их числе: финансы и экономика; операции с материальными и нематериальными активами, учет в государственных и частных организациях и организациях смешанного типа. По сути, блокчейн – это новая организационная парадигма для координации любого вида человеческой деятельности. Возможно даже, что это наше будущее, о котором полезно узнать уже сегодня. Книга адресована тем, кто интересуется финансовыми инструментами и технологическими инновациями, в частности криптотехнологиями.

УДК 004:338
ББК 65.050.253

ISBN 978-5-9693-0360-7

Содержание

Мелани Свон
Блокчейн
Схема новой экономики

* * *

Об авторе

Мелани Свон – основатель Института блокчейн-исследований (Institute for Blockchain Studies), магистр современной философии Кингстонского университета в Лондоне и Университета Париж VIII, выпускник программы MBA по специализации «Финансы» Уортонской школы бизнеса Пенсильванского университета. Свон стажировалась в финансовой корпорации Fidelity и банке JP Morgan, в качестве предпринимателя и консультанта стартапов GroupPurchase и Prosper приобрела значительный опыт работы на новых рынках, который применила, разработав принципы оценки и учета цифровых активов в виртуальном мире для компании Deloitte. Свон стала одним из первых участников движения Quantifed Self; в 2010 году она основала DIYgenomics – организацию, которая в числе первых занялась исследованиями здоровья, организуемыми по принципу краудсорсинга. Мелани Свон занимает должности преподавателя в Университете Сингулярности (Singularity University) и аффилированного научного сотрудника Института этики и новых технологий (Institute for Ethics and Emerging Technologies). Ее статьи регулярно публикуются на сайте Edge.org в разделе Annual Essay Question.

Предисловие

Блокчейн – это многофункциональная и многоуровневая информационная технология, предназначенная для надежного учета различных активов. Потенциально эта технология охватывает все без исключения сферы экономической деятельности и имеет множество областей применения. В их числе: финансы, экономика и денежные расчеты, а также операции с материальными (реальная собственность, недвижимость, автомобили и т. п.) и нематериальными (права голосования, идеи, репутация, намерения, медицинские данные, личная информация и т. п.) активами. Блокчейн создает новые возможности по поиску, организации, оценке и передаче любых дискретных единиц. По сути, это новая организационная парадигма для координации любого вида человеческой деятельности.

Вполне вероятно, мы находимся на пороге блокчейн-революции. Эта революция началась с появлением новой экономической реальности в интернете – альтернативной валюты под названием биткойн, которая эмитируется и обеспечивается не государством, а пользователями биткойн-сети при автоматизированном достижении консенсуса между ними. Но уникальность этой валюты заключается в том, что ее пользователям не обязательно доверять друг другу. Встроенные в систему алгоритмы саморегулирования предотвращают любые злонамеренные попытки обмана. Если быть точным, то с технической точки зрения биткойн – это цифровые деньги, обращающиеся в децентрализованной, пиринговой электронной платежной системе[1], основанной на публично доступной книге учета, именуемой «блокчейном».

По сути – это новая форма денег, комбинирующая одноранговый обмен файлами[2] подобно BitTorrent, и криптографическую систему с открытым ключом[3,4]. С момента возникновения биткойна в 2009 году у него появился целый ряд подражателей – альтернативных криптовалют, в целом использующих такой же подход, но с некоторыми изменениями и улучшениями. Важно, что блокчейн-технология способна стать органичной экономической оболочкой сети интернет, обслуживающей онлайн-платежи, децентрализованный обмен, заработок и расходование токенов ценности, получение и передачу цифровых активов, а также выпуск и исполнение умных контрактов. Как средство децентрализации эти технологии могут стать следующим фундаментальным прорывом в информационных технологиях – после мейнфреймов, персональных компьютеров, интернета, мобильных и социальных сетей. Они способны коренным образом изменить жизнедеятельность человечества, как это в свое время сделал интернет.

---

[1] Одноранговый, децентрализованный или пиринговый (*англ.* peer-to-peer, P2P – равный к равному) обмен файлами – это обмен файлами в сети, основанной на равноправии участников. Часто в такой сети отсутствуют выделенные серверы, а каждый узел (peer) является как клиентом, так и выполняет функции сервера. В отличие от архитектуры клиент-сервера такая организация позволяет сохранять работоспособность сети при любом количестве и любом сочетании доступных узлов. Участниками сети являются пиры. – *Прим. ред*.

[2] *Kayne, R.,* «What Is BitTorrent?», сайт wiseGEEK, 25 декабря 2014 г., *http://www.wisegeek.com/what-is-bittorrent.htm#didyouknowout*

[3] *Beal, V.,* «Public-key encryption», Webopedia, *http://www.we-bopedia.com/TERM/P/public_key_cryptography.html*

[4] Криптографическая система с открытым ключом (или асимметричное шифрование, асимметричный шифр) – система шифрования и/или электронной подписи (ЭП), при которой открытый ключ передается по открытому (то есть незащищенному, доступному для наблюдения) каналу и используется для проверки ЭП и для шифрования сообщения. Для генерации ЭП и для расшифровки сообщения используется закрытый ключ. – *Прим. ред*.

Валюта, контракты и приложения блокчейн вне финансовых рынков

Потенциальные выгоды от применения блокчейн-технологии лежат не только в сфере экономики – они распространяются на политику и гуманитарные, социальные и научные области. Технологические возможности блокчейна уже задействуются для решения реальных общественных задач. Например, блокчейн может стать средством противостояния политическому произволу за счет внедрения децентрализованных облачных функций, которые ранее управлялись исключительно официальными организациями. Это удобно таким лицам, как Эдвард Сноуден, и таким организациям, как WikiLeaks, в связи с тем, что пожертвования на их адрес через международные платежные системы в ряде стран находятся под запретом.

Преимущества блокчейн-технологий оценили и транснациональные политически нейтральные организации, такие как ICANN[5] и службы DNS. Помимо ситуаций, когда общественные интересы выходят за рамки национальных границ, целые отрасли экономики смогут освободиться от избыточного регулирования и лицензирования, навязанных иерархическими структурами, лоббистами и группами влияния внутри государств. Это позволит создавать новые модели бизнеса, не отягощенные ненужными посредниками. Активно поддерживаемые отраслевым лобби изменения в законодательстве фактически запретили предоставлять рядовым потребителям новые услуги в области генетики[6,7], но новейшие экономические модели, в частности экономики совместного использования (*sharing economy*), реализуемые такими компаниями, как, например, Airbnb и Uber, эффективно противостоят запретительным инициативам властных структур[8].

Вдобавок к экономическим и политическим преимуществам, координация, учет и безотзывность транзакций в блокчейн-технологии могут стать такой же основой для прогресса общества, какой в свое время стали «Великая хартия вольностей»[9] или Розеттский камень. Блокчейн может служить надежным хранилищем имеющих общественную ценность записей, таких как реестры документов и событий, личных данных и активов. В такой системе каждый актив может стать *умным активом* (*smart property*).

Каждый актив в блокчейне кодируется уникальным идентификатором, по которому актив можно отслеживать, контролировать и обменивать, продавать или покупать. Это означает, что любые виды материальных (дома, автомобили и другие) и цифровых активов можно регистрировать и совершать с ними транзакции на блокчейне.

---

[5] ICANN – Internet Corporation for Assigned Names and Numbers, Корпорация по управлению доменными именами и IP-адресами. – *Прим. ред.*

[6] *Knight, H., Evangelista, B.*, «S. F., L. A. Threaten Uber, Lyft, Sidecar with Legal Action», сайт SFGATE, 25 сентября 2014 г., *http://m.sfgate.com/bayarea/article/S-F-L-A-threaten-Uber-Lyft-Sidecar-with-5781328.php*

[7] В частности, речь идет о персональной геномике – разделе науки, связанном с секвенированием и анализом генома человека. После расшифровки генотипа его можно проанализировать для определения вероятности риска заболеваний человека. – *Прим. ред.*

[8] *Knight, H., Evangelista, B.*, «S. F., L. A. Threaten Uber, Lyft, Sidecar with Legal Action», сайт SFGATE, 25 сентября 2014 г., *http://m.sfgate.com/bayarea/article/S-F-L-A-threaten-Uber-Lyft-Sidecar-with-5781328.php*

[9] Великая хартия вольностей (*лат.* Magna Carta, также Magna Charta Libertatum) – политико-правовой документ, составленный в июне 1215 года на основе требований английской знати к королю Иоанну Безземельному и защищавший ряд юридических прав и привилегий свободного населения средневековой Англии. Состоит из 63 статей, регулировавших вопросы налогов, сборов и феодальных повинностей, судоустройства и судопроизводства, прав английской церкви, городов и купцов, наследственного права и опеки. Ряд статей Хартии содержал правила, целью которых было ограничение королевской власти путем введения в политическую систему страны особых государственных органов – общего совета королевства и комитета двадцати пяти баронов, обладавшего полномочиями предпринимать действия по принуждению короля к восстановлению нарушенных прав; в силу этого данные статьи получили название конституционных. – *Прим. ред.*

В качестве примера, которых в этой книге будет еще немало, можно привести использование блокчейн-технологии для регистрации и защиты объектов интеллектуальной собственности (ИС). Новая отрасль так называемого цифрового искусства *(digital art)* предлагает услуги по частной регистрации в распределенном журнале записей точного содержания любого цифрового актива: файла, изображения, медицинской записи или ПО. Блокчейн может дополнить или полностью заменить собой все существующие системы управления ИС.

Работает это таким образом. Для начала к любому файлу применяется алгоритм, сжимающий этот файл в короткий код из 64 символов, называемый «хеш», который уникален для данного документа[10]. Каким бы ни был размер файла – например, объем файла генома составляет 9 ГБ, – на выходе всегда получается уникальный 64-символьный хеш, идентифицирующий, но не позволяющий восстановить исходный файл. Полученный хеш включается в блокчейн-транзакцию с добавлением метки времени – доказательство существования цифрового актива на тот момент. Имея исходный файл, который хранится на компьютере собственника, а не в распределенном журнале записей, всегда можно повторно вычислить его хеш и убедиться, что содержимое файла не подверглось изменению.

Стандартизированные механизмы правового регулирования, например договорное право, стали революционным шагом вперед для всего общества. Стандартизированные операции с интеллектуальной собственностью при помощи блокчейна могут стать следующей поворотной точкой для лучшей координации цифрового общества – по мере того, как все большая часть экономической деятельности приводится в движение идеями.

[10] Нельзя полностью исключить ситуацию равенства хешей у двух разных файлов, но число 64-символьных хешей намного больше числа файлов, которое человечество сможет создать в обозримом будущем. Это похоже на криптографический стандарт, заключающийся в том, что схему можно взломать, но вычисления займут время, которое превышает время существования Вселенной.

Блокчейн 1.0, 2.0 и 3.0

Многие уже начинают понимать, что благодаря своим экономическим, политическим, гуманитарным и юридическим преимуществам биткойн и блокчейн-технологии превращаются в мощнейшую подрывную инновацию, способную коренным образом изменить большинство аспектов жизни общества. Для упорядочения и удобства давайте разделим различные – существующие и потенциальные – технологические аспекты блокчейн-революции на три категории: блокчейн 1.0, 2.0 и 3.0.

Блокчейн 1.0 – это *валюта.* Криптовалюты применяются в различных приложениях, имеющих отношение к деньгам, например системы переводов и цифровых платежей.

Блокчейн 2.0 —это *контракты.* Целые классы экономических, рыночных и финансовых приложений, в основе которых лежит блокчейн, работают с различными типами финансовых инструментов – с акциями, облигациями, фьючерсами, закладными, правовыми титулами, умными активами и умными контрактами.

Блокчейн 3.0 – это *приложения,* область применения которых выходит за рамки денежных расчетов, финансов и рынков. Они распространяются на сферы государственного управления, здравоохранения, науки, образования, культуры и искусства.

Что такое биткойн?

Биткойн – это цифровая наличность. Это одновременно цифровая валюта и онлайновая платежная система, в которой технологии шифрования обеспечивают управление генерацией денежных единиц и подтверждение перевода средств и которая работает независимо от государственных центробанков.

В терминах легко запутаться, потому что слова *«биткойн»* и *«блокчейн»* могут обозначать любую из трех частей концепции: базовую *блокчейн-технологию, протокол* и *клиента,* обеспечивающие выполнение транзакций, и собственно криптовалюту (деньги). Кроме того, эти термины могут применяться для обозначения и концепции криптовалют. Это все равно что называть термином «PayPal» сам интернет, через который работает протокол PayPal, служащий для перевода валюты PayPal. В блокчейн-индустрии эти термины часто смешиваются, поскольку пока не завершился процесс формирования общепризнанного многоуровневого стека технологий.

Биткойн был создан в 2009 году (точная дата – 9 января 2009 г.[11]) неизвестным лицом или группой людей, работавших под псевдонимом Сатоши Накамото (Satoshi Nakamoto). Концепция и подробности работы биткойна изложены в лаконичном и легком для чтения техническом документе «Биткойн: Одноранговая система электронной наличности»[12;13]. Платежи в децентрализованной виртуальной валюте записываются в публичный реестр (*public ledger*), который хранится на многих – потенциально на всех – компьютерах пользователей биткойна и постоянно доступен для просмотра в интернете.

Биткойн – первая и крупнейшая децентрализованная криптовалюта. Существуют сотни других альткойнов (альтернативных криптовалют), например Litecoin или Dogecoin, но на биткойн приходится около 90 % рыночной капитализации всех криптовалют, и он стал фактическим стандартом. Биткойны используются псевдонимно (а не анонимно), то есть для отправки и получения биткойнов и записи транзакций применяются биткойн-адреса – буквенно-цифровые строки длиной 27–32 символов, в чем-то аналогичные адресу электронной почты, а не личная идентификационная информация.

Биткойны создаются как вознаграждение за выполнение математических вычислений. Суть этой работы, называемой *майнингом (mining)* в том, что пользователи предоставляют свои вычислительные ресурсы для верификации адресов и записи транзакций в реестр. В награду за участие в майнинге пользователи получают комиссию за транзакции и вновь создаваемые биткойны. Помимо майнинга, биткойны, как и любую другую валюту можно получить в обмен на обычные (фиатные[14]) деньги, товары и услуги. Пользователи могут отправлять и получать биткойны с помощью *электронного кошелька* через веб-браузер или приложение, установленное на персональном компьютере или мобильном устройстве. В зависимости от размера транзакции с суммы может как взиматься комиссия, так и нет.

---

[11] *Nakamoto, S.,* «Bitcoin v0.1 Released», сайт The Mail Archive, 9 января 2009 г., *http://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html*

[12] «Bitcoin: A Peer-to-Peer Electronic Cash System» (дата публикации неизвестна), *https://bitcoin.org/bitcoin.pdf*

[13] *Nakamoto, Satoshi.* Bitcoin: A Peer-to-Peer Electronic Cash System. – *Прим. ред*.

[14] Фиатные (от лат. *fat* – декрет, указание), они же фидуциарные (от лат. *fducia* – доверие) деньги – деньги, номинальная стоимость которых устанавливается и гарантируется государством, традиционные деньги. – *Прим. ред.*

Что такое блокчейн?

Блокчейн – это технология надежного распределенного хранения записей обо всех когда-либо совершенных биткойн-транзакциях. Блокчейн представляет собой цепочку блоков данных, объем которой постоянно растет по мере добавления майнерами новых блоков с записями самых последних транзакций, что происходит каждые 10 минут. Блоки записываются в блокчейн в линейном последовательно-хронологическом порядке. На каждом полном узле – то есть компьютере, подключенном к сети биткойна с помощью клиента, выполняющего проверку и передачу транзакций, – хранится копия блокчейна, которая автоматически загружается, когда майнер присоединяется к биткойн-сети. В реестре сохраняется полная информация обо всех адресах и балансах, начиная с генезис-блока, то есть самого первого блока транзакций, до самого последнего добавленного блока.

Поскольку блокчейн представляет собой реестр, любое средство просмотра, например сайт *https://blockchain.info*, позволяет легко запросить транзакции, относящиеся к определенному биткойн-адресу. Так, например, в собственном электронном кошельке можно увидеть транзакцию, в которой вы получили свой первый биткойн.

Блокчейн-технология считается главной инновацией биткойна, потому что именно она служит «не требующим доверия» (*trustless*) механизмом верификации всех транзакций в сети. Принципиальное новшество блокчейна заключается в его архитектуре, обеспечивающей возможности децентрализованных транзакций, не требующих доверия. Вместо того чтобы устанавливать и поддерживать доверительные отношения с партнером по транзакции (другим человеком) или сторонним участником-посредником (например, банком), пользователи полагаются на общедоступную распределенную базу данных, хранимых на многих децентрализованных узлах и поддерживаемых «майнерами-бухгалтерами». Блокчейн позволяет избавиться от «доверенных посредников» и полностью децентрализовать транзакции произвольных типов между любыми участниками в глобальном масштабе.

Технически блокчейн-технология представляет собой еще один прикладной уровень, работающий поверх существующего стека интернет-протоколов. Она привносит в интернет совершенно новое звено поддержки экономических транзакций – как моментальных денежных платежей в универсальной криптовалюте, так и более сложных и долгоживущих финансовых контрактов.

В системе, похожей на блокчейн, могут совершаться транзакции с любыми валютами, финансовыми контрактами, материальными и нематериальными активами. Более того – блокчейн может применяться не только для транзакций, но и для фиксации, отслеживания, мониторинга и совершения операций с любыми активами. По сути, мы имеем дело с громадной электронной таблицей для регистрации всех активов и учетной системой для выполнения операций с ними в глобальном масштабе без ограничений по форме активов, типу участников или географическому положению.

Тем самым блокчейн может стать средством регистрации, учета и обмена любых финансовых, материальных (имущество) и нематериальных (права голосования, идеи, репутация, намерения, медицинские данные и другие) активов.

Связанный мир и блокчейн: пятая революционная парадигма вычислений

Одна из моделей познания современного мира основывается на парадигмах вычислений. Новая парадигма возникает примерно каждое десятилетие (рис. П-1). Сначала появились мейнфреймы[15], затем персональные компьютеры (ПК), а следом нашу жизнь принципиально изменил интернет. Мобильные и социальные сети стали следующей – четвертой – парадигмой. Парадигмой для нынешнего десятилетия может стать *связанный мир вычислений (connected world of computing)*, основанный на криптографии блокчейна.

Не исключено, что именно блокчейн-технологии предстоит стать верхним экономическим слоем органично связанного мира разнообразных вычислительных устройств, в числе которых – носимые вычислительные устройства, сенсоры «интернета вещей»[16], смартфоны, планшеты, ноутбуки, цифровые устройства самофиксации (например, Fitbit[17]), умные дома, умные автомобили и умный город. Но реализуемая средствами блокчейна экономика поддерживает не просто движение денег, а перенос информации и эффективное размещение ресурсов, которые эти деньги обеспечивают в масштабах экономики отдельных людей и целых компаний.

Обладая революционным потенциалом, равным потенциалу интернета, блокчейн-технология будет разворачиваться и внедряться намного быстрее благодаря повсеместной доступности интернета и мобильной связи.

Функциональность социальных и мобильных сетей четвертой парадигмы стала настолько естественной, что пользователи теперь ожидают ее от всех технологий. Так, мобильные приложения поддерживают функционал, который раньше реализовывался через веб: отметка «нравится», комментирование, включение в друзья, участие в форумах. Точно так же блокчейн-технология, относящаяся к пятой парадигме, создает у пользователей ожидание, что обмен ценностями должен быть доступен повсеместно.

Функциональность, реализованная в рамках пятой парадигмы, может выглядеть как подключенный интегрированный физический уровень вычислений со многими устройствами, поверх которого находится слой для обслуживания платежей. Но речь идет не просто о платежах, а о микроплатежах, децентрализованной бирже, зарабатывании и трате токенов, получении и передаче цифровых активов, а также о составлении и выполнении умных контрактов – то есть о полноценном экономическом слое, которого в вебе до сих пор не было.

Мир уже готов к всеобщим деньгам, в основе которых лежит взаимодействие в интернете. Apple Pay (использующее токены мобильное приложение электронного кошелька компании Apple) и конкурирующие продукты могут стать той поворотной точкой, с которой начнется мир полнофункциональных криптовалют. Блокчейн при этом становится неотъемлемым экономическим слоем веба.

---

[15] Мейнфрейм (*англ.* mainframe) – большой универсальный высокопроизводительный отказоустойчивый компьютер со значительным объемом оперативной и внешней памяти, используемый для интенсивной обработки данных, как правило, крупными компаниями и государственными организациями. – *Прим. ред.*

[16] Интернет вещей (*англ.* Internet of Things, IoT) – концепция вычислительной сети физических объектов («вещей»), оснащенных встроенными технологиями для взаимодействия друг с другом или с внешней средой. Организация таких сетей рассматривается как явление, способное перестроить экономические и общественные процессы, с тем чтобы частично исключить участие человека. – *Прим. ред.*

[17] Fitbit – лидер рынка фитнес-гаджетов, являющихся частью более широкой темы, так называемого «мобильного здоровья». – *Прим. ред.*

Рисунок П-1. *Революционные парадигмы вычислений: мейнфреймы, ПК, интернет, социальные и мобильные сети, блокчейн*[18]

Сеть биткойн-платежей для поддержки машинной экономики: M2M/IOT

Блокчейн – революционная парадигма для «интернета людей», но она может также стать валютной основой «экономики машин». По оценкам компании Gartner, к 2020 году пространство «интернета вещей» будет насчитывать около 26 млрд устройств, а оборот интернет-экономики достигнет 1,9 трлн долларов[19]. Для управления транзакциями между этими устройствами потребуется «интернет денег»[20] и соответствующая криптовалюта, а микроплатежи между подключенными устройствами могут развиться в новый уровень экономики[21]. По оценкам компании Cisco, количество M2M-подключений *(machine-to-machine,* то есть связь между машинами) растет быстрее любой другой категории, прибавляя по 84 %. И дело не только в оценочном трехкратном росте глобального IP-трафика в период с 2012 по 2018 год, но и в изменении его характера: в сдвиге трафика в сторону передачи мобильных данных, Wi-Fi и M2M-соединений[22]. Как товарно-денежная экономика обеспечивает более качественное, быстрое и эффективное распределение ресурсов на уровне человека, так и машинная экономика предоставляет надежную и децентрализованную систему управления теми же ресурсами, но на уровне машин.

В качестве примера микроплатежей между устройствами можно привести автомобиль, который автоматически согласует скоростное прохождение шоссе в экстренных случаях, компенсируя микроплатежами неудобство, доставленное другим участникам движения. Координация воздушной доставки товаров беспилотными летательными аппаратами – еще один пример сетей микроплатежей между устройствами, где нужна балансировка индивидуальных приоритетов. Сельскохозяйственные датчики – другой пример системы, в которой экономические принципы применяются для отсеивания фоновых малозначимых данных и повышения приоритета других данных, которые подтверждаются достаточно большой группой датчиков, развернутых на местности: например, определенные параметры окружающей среды, такие как уровень влажности.

Децентрализованная модель блокчейн-технологии, предусматривающая одноранговые, не требующие доверия транзакции, на самом базовом уровне означает, что для совершения транзакций не требуются посредники. Однако возможность реализации децентрализованной

---

[18] Вывод сделан на основе: *Sigal, M.*, «You Say You Want a Revolution? It's Called Post-PC Computing», сайт Radar (O'Reilly), 24 октября 2011 г., *http://radar.oreilly.com/2011/10/post-pc-revolution.html*

[19] *Gartner*, «Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020», издательство «Gartner Press», 12 декабря 2013 г., *http://www.gartner.com/news-room/id/2636073*

[20] *Omohundro, S.,* «Cryptocurrencies, Smart Contracts, and Artifcial Intelligence», направлено для публикации в вестнике *AI Matters* («Ассоциация по вычислительной технике»), 22 октября 2014 г., *http://steveomohundro.com/2014/10/22/cryptocurrencies-smart-contracts-and-artifcial-intelligence/*

[21] *Dawson, R.,* «The New Layer of the Economy Enabled by M2M Payments in the Internet of Things», блог «Trends in the Living Networks», 16 сентября 2014 г., *http://rossdawsonblog.com/weblog/archives/2014/09/new-layer-economy-en-abled-m2m-payments-internet-things.html*

[22] *Petschow, K.,* «Cisco Visual Networking Index Predicts Annual Internet Trafc to Grow More Than 20 Percent (Reaching 1.6 Zettabytes) by 2018», пресс-релиз компании Cisco, 2014 г., *http://newsroom.cisco.com/release/1426270*

модели для всех видов взаимодействий (между людьми, между человеком и машиной, между машинами) в глобальном масштабе может требовать совершенно иных структур и способов функционирования общества. Направления таких изменений пока непонятны, но существующие властные отношения и иерархии могут в новых реалиях быстро утратить свое значение.

Повсеместное внедрение: доверие, удобство и простота использования

Идеи биткойна и блокчейна новы и технически трудны, по этому бытует мнение, что криптовалюты слишком сложны для повсеместного внедрения среди обычных пользователей. А ведь то же самое когда-то говорили об интернете – но это не стало серьезным препятствием для его распространения: не надо понимать, как работает протокол TCP/IP, чтобы отправить сообщение по электронной почте.

На заре новых технологий рядовые пользователи всегда интересуются техническими подробностями: «что это?» и «как это работает?». Приложения, основанные на технологических новациях, легко находят путь к рядовым потребителям, если они способны предложить адекватный, удобный в использовании и дружественный интерфейс. В частности, пользователям не обязательно видеть, а тем более вводить вручную маловразумительные буквы и цифры 32-символьного биткойн-адреса. Компании, предлагающие «общедоступный кошелек», такие как Circle Internet Financial и Xapo, разрабатывают пользовательские приложения, специально ориентированные на повсеместное использование биткойна, – разумеется, это делается для того, чтобы стать «Gmail от биткойна», то есть предоставить такое же удобство и завоевать такую же долю рынка, как общеизвестная почтовая служба.

Биткойн, как платежная система, и электронные кошельки оперируют хоть и электронными, но все же деньгами, поэтому приложения для конечных пользователей должны обеспечивать повышенную защиту транзакций. Поэтому, прежде чем удобные биткойн-кошельки завоюют массовое признание, потребуется заслужить доверие потребителей. В частности, придется решить множество вопросов обеспечения безопасности криптовалюты, в том числе: «Как сохранять свои деньги?» или «Что делать при утере закрытого ключа или при получении в транзакции сомнительной (то есть ранее украденной) монеты?».

Специалисты блокчейн-индустрии успешно работают над решением этих вопросов, что позволит альтернативным валютам стать новым этапом развития финансовых технологий, не менее значимым, чем появление банкоматов, банковского обслуживания через интернет и Apple Pay.

Приложения для работы с деньгами, обладающие доверительно-дружественным и удобным интерфейсом, уже близки к массовому внедрению. Но вот повсеместное принятие блокчейн-приложений, выходящих за пределы исключительно денежных отношений, может оказаться намного более трудным делом. Например, казалось бы очевидный вариант – услуги виртуальных нотариусов: их будет просто находить, и они позволят легко, недорого, безопасно, надежно регистрировать интеллектуальную собственность, договоры или завещания. Тем не менее существуют социальные причины, в силу которых люди все равно будут в ряде случаев обращаться к обычным нотариусам, чтобы получить человеческий совет (и немного психотерапии) или для того, чтобы подтвердить дееспособность человека, а это может тормозить распространение технологии.

Но в целом если отрасли биткойна и блокчейна суждено будущее, то, скорее всего, развитие будет происходить поэтапно – примерно так же, как развивался интернет, который в разное время начинал привлекать различные аудитории, «подключавшиеся» к сети по разным причинам. Изначально интернет решал задачу коллективного взаимодействия в четко определенных подгруппах: среди ученых и военных. Со временем в него пришли любители компьютерных игр и развлечений, а затем «подтянулись» и все остальные. Сейчас биткойн находится на этапе участия энтузиастов или ранних потребителей, используя термин модели Эверетта Роджерса – субкультуры людей, интересующихся деньгами и идеологией.

На следующем этапе блокчейн-технологию станут осваивать те социальные группы, для которых она сможет решать реальные практические проблемы, – например, люди из стран с введенной интернет-цензурой. Для них особое значение будет иметь существование децентрализованной системы доменных имен (DNS) на основе блокчейна. На рынке интеллектуальной собственности блокчейн-технологию можно задействовать для регистрации патентов, с ее помощью можно коренным образом изменить судопроизводство, связанное с интеллектуальной собственностью: управление объектами ИС, доступ к ним и установление их принадлежности.

Биткойн-культура: фестиваль Bitfilm

Один из индикаторов масштаба принятия новой технологии обычными людьми – ее след в массовой культуре. Возможно, фестиваль Bitflm, в котором участвуют фильмы, посвященные биткой-ну, может стать первой ласточкой внедрения криптовалют в массовое сознание. Фильмы, отобранные для фестиваля, по-своему интерпретируют биткойн и рассказывают о его влиянии. Фестиваль впервые прошел в 2013 году и получил продолжение в конце 2014 – начале 2015 года в Берлине (где находится штаб-квартира Bitflm), Сеуле, Буэнос-Айресе, Амстердаме, Рио-де-Жанейро и Кейптауне. Естественно, Bitflm позволяет зрителям голосовать за понравившийся фильм биткойнами. Фестиваль продюсирует компания Bitflm. Другое направление деятельности компании – создание роликов, рекламирующих блокчейн (рис. 2).

Цели, методология и структура этой книги

Отрасль блокчейн находится на начальной стадии развития – стадии бурного роста и инноваций. Принципы, терминология, стандарты, основные участники, нормы и отношение к тем или иным проектам – все это очень быстро меняется. Может случиться, что, оглянувшись назад через год-другой, мы сочтем нынешнюю технологию биткойна и блокчейна безнадежно устаревшей, она окажется поглощенной другой технологией или станет артефактом прошлого.

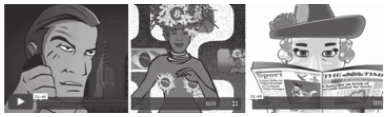

Рисунок П-2. *Рекламные ролики Bitflm*

Приведу один пример: сейчас активно развивается область обеспечения безопасности электронных кошельков потребителей. Это далеко не праздная тема ввиду постоянных атак хакеров, старающихся подорвать основы отрасли криптовалют. Сегодня считается, что стандарт безопасности электронного кошелька должен предусматривать мультиподпись, то есть использование множественных подписей для одобрения транзакции. Между тем большинство пользователей – а это все еще энтузиасты, а не широкая публика – пока не созрели для поддержания такого уровня безопасности.

Эта книга задумана как исследование принципов, возможностей и функциональности технологий биткойна и блокчейна, их потенциальных возможностей и последствий их внедрения. Книга ничего не пропагандирует и не отстаивает, она не дает никаких советов или прогнозов относительно жизнеспособности данной отрасли. Книга готовилась с целью представить на суд читателей наиболее передовые концепции; для изучения основ блокчейна есть много других ресурсов.

Отрасль блокчейна пребывает сейчас на начальном и незрелом этапе своей эволюции, очень многое в ней находится на стадии развития и подвержено множеству рисков. Поэтому, как бы мы ни старались, в тексте могут содержаться неточности, ведь информация имеет свойство устаревать очень быстро, буквально за считанные дни.

Мы старались дать общую картину, описать масштаб, состояние и возможности блокчейн-индустрии. Мы хотели познакомить вас с базовыми технологиями, возможностями их использования, опасностями и рисками, но что еще важнее – с основными принципами и возможностью их дальнейшего развития. Наша задача заключалась в создании всеобъемлющего обзора всего происходящего в отрасли криптовалют и попытке спрогнозировать возможности их широкого применения. Наш обзор, конечно же, неполон и может содержать технические ошибки, несмотря на тщательную проверку текста экспертами. Повторимся: он вполне может оказаться устаревшим в случае провала или, наоборот, стремительного успеха описанных здесь проектов; более того, вся отрасль биткойна и блокчейна в ее текущем состоянии может безнадежно устареть или оказаться поглощенной другими технологическими моделями.

В процессе работы над книгой мы использовали множество источников по теме биткойна и его развития. Основные источники – форумы разработчиков, подгруппы Reddit, технические документы GitHub, подкасты, средства массовой информации, YouTube, блоги и Twitter, в частности материалы отраслевой конференции по биткойну на YouTube и Slideshare, подкасты Let's Talk Bitcoin, Consider This! Epicenter Bitcoin, канал EtherCasts (Ethereum), специализированные новостные каналы по биткойну CoinDesk, Bitcoin Magazine, Cryptocoins News, Coin Telegraph и форумы Bitcoin StackExchange, Quora.

Кроме того, мы встречались с разработчиками, общались по электронной почте и дискутировали с отраслевыми специалистами-практиками, посещали конференции и семинары по биткойну, наблюдали за торговыми сессиями пирингового криптовалютного обмена Satoshi Square.

Структура книги предусматривает обсуждение уже сформировавшихся уровней технологии биткойна и блокчейна: Блокчейн 1.0, 2.0 и 3.0. Сначала мы рассказываем о базовых определениях и принципах технологии биткойна и блокчейна, а также о валютах и денежных расчетах как основе приложений Блокчейн 1.0.

Затем вы узнаете о Блокчейн 2.0 – рыночных и финансовых приложениях, выходящих за рамки валют, в частности о контрактах. Далее обсуждается потенциал Блокчейна 3.0 – применений блокчейна, не укладывающихся в рамки финансовых транзакций, экономики и рынков. В эту обширную область входит применение блокчейна для достижения общественно-полезных целей, например для децентрализации управления, а также для вывода организаций, таких как WikiLeaks и службы ICANN и DNS, из-под репрессивных политических юрисдик-ций с переносом в децентрализованное облако; защита интеллектуальной собственности; проверка цифровой индивидуальности и аутентификация. Мы также остановимся еще на одном классе приложений – Блокчейн 3.0, где блокчейн-технология предлагает преимущества масштабируемости, эффективности, организации и координации в области науки, геномики, здравоохранения, образования, публикации научных статей, разработки, обучения и культуры. Наконец, представлены продвинутые концепции, такие как демереджевые (стимулирующие) валюты и их применение в контексте крупномасштабного развертывания блокчейн-технологий.

Глава 1
Блокчейн: фундамент для криптовалют (Блокчейн 1.0)

Стек технологий: блокчейн, протокол, валюта

Термин «биткойн» (Bitcoin) может ввести в заблуждение, поскольку биткойном принято считать три разные вещи.

Во-первых, биткойн – это базовая платформа блокчейн-технологии.

Во-вторых, биткойном называется работающий на основе этой базовой технологии протокол, описывающий, как именно происходит перевод активов в цепочке блоков.

В-третьих, биткойн – это цифровая криптовалюта, самая первая и самая популярная из известных на сегодня криптовалют.

В таблице 1–1 показано, чем различаются эти понятия. Нижний уровень – это базовая блокчейн-технология. Блокчейн как цепочка блоков транзакций – это распределенный, общедоступный и совместно используемый всеми узлами сети реестр или журнал записей, содержащий данные о транзакциях. Журнал обновляется майнерами и отслеживается всеми желающими, но при этом никем не контролируется. Он подобен гигантской общедоступной таблице, которая периодически обновляется и подтверждает уникальность цифровых операций перевода денежных средств.

Средним уровнем стека является протокол – пакет программ, который переводит средства путем внесения транзакций в блокчейн (журнал записей). Наконец, третий уровень – это сама валюта под названием «биткойн», в транзакциях и на биржах используется обозначение *BTC* или *Btc*. Среди сотни криптовалют биткойн – не только самая первая, но и самая популярная. Среди прочих следует отметить Litecoin, Dogecoin, Ripple, NXT, и Peercoin. Перечень и котировки основных альткойнов можно найти на сайте *http://coinmarketcap.com/*.

Таблица 1–1. Уровни стека блокчейн-технологий на примере биткойна

Криптовалюта	Биткойн (BTC), Litecoin, Dogecoin
Биткойн-протокол и клиент	Программы, выполняющие операции
Блокчейн биткойна	Базовый децентрализованный журнал записей

Важно понимать, что общая структура любой современной криптовалютной системы формируется всеми тремя уровнями (блокчейн, протокол и валюта). Каждая монета представляет собой одновременно валюту и протокол, она может иметь собственный распределенный журнал записей или использовать распределенный блокчейн биткойна. Например, криптовалюта Litecoin использует Litecoin-протокол, работающий с блокчей-ном Litecoin, – по сути, это клон биткойна, в котором слегка изменены некоторые функции.

Отдельный блокчейн означает, что у монеты имеется собственный децентрализованный журнал записей с такой же структурой и форматом, что и распределенный журнал записей биткойна.

Другие протоколы, например Counterparty, имеют собственную валюту (XCP), но используют блокчейн биткойна, то есть транзакции XCP регистрируются в распределенном журнале записей биткойна. Таблицу с описанием характеристик проекта Crypto 2.0 можно найти по адресу: *http://bit.ly/crypto_2_0_comp*.

Двойное расходование и задача византийских генералов

Даже если оставить в стороне потенциал использования биткойна и блокчейн-технологии, биткойн, безусловно, является серьезным фундаментальным прорывом в области информатики – результатом 20 лет исследований в области цифровых валют и 40 лет исследований в области криптографии, над которыми работали тысячи ученых всего мира[23]. Биткойн стал решением давней проблемы цифровых наличных денег – проблемы двойного расходования *(double-spend problem).* До появления криптографии блокчейна цифровую наличность *(digital cash)*[24], как и любой другой цифровой актив, можно было бесконечно копировать – как, например, мы можем сегодня бессчетное количество раз копировать вложение в электронной почте. При этом без специального посредника невозможно было подтвердить, что та или иная партия денег не была уже израсходована ранее. Функцию посредника выполняла доверенная третья сторона: банк или платежная система вроде PayPal, которая хранила журнал записей, гарантирующий, что каждая единица цифровых денег может быть потрачена только один раз, тем самым предотвращая двойное расходование.

Проблема двойного расходования аналогична давно сформулированной математической проблеме – так называемой «Задаче византийских генералов»[25], суть которой состоит в том, что несколько генералов перед сражением, не доверяя друг другу, должны как-то согласовать свои действия[26].

Блокчейн решает проблему двойного расходования, объединяя технологию одноранговго обмена файлами BitTorrent и шифрование с открытым ключом, тем самым создавая новый вид цифровых денег. Собственность на монеты регистрируется в открытом журнале записей и подтверждается криптографическими протоколами и сообществом майнеров. Блокчейн не требует доверия в том смысле, что в процессе транзакции пользователю нет нужды доверять контрагенту или посреднику. Необходимо лишь доверять системе – программной реализации блокчейн-протокола.

«Блоки» в блокчейне представляют собой группы транзакций, которые последовательно записываются в журнал учета транзакций, то есть «добавляются в цепочку». Распределенные журналы записей можно свободно просматривать с помощью браузеров блоков, размещенных на специализированных интернет-сайтах; например, для распределенного журнала записей биткойна – *www.blockchain.info*. Чтобы просмотреть поток транзакций пользователя, нужно ввести его биткойн-адрес, например *1DpZHXi5bEjNn6SriUKjh6wE4HwPFBPvfx*.

---

[23] *Andreessen, M.,* «Why Bitcoin Matters», газета *The New York Times*, 21 января 2014 г., *http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/?_php=true&_ type=blogs&_r=0*

[24] Цифровая наличность (*англ.* digital cash) или электронная наличность (*англ.* e-cash, electronic cash) – термин, который в настоящее время широко используется в платежных системах. Название связано с возможностью совершать электронные платежи аналогично оплате обычными наличными: без обязательного посредничества третьего лица. Первые криптографические протоколы электронной наличности были предложены в 1983 году Дэвидом Чаумом и Стефаном Брэндсом. – *Прим. ред.*

[25] В вычислительной технике под «Задачей византийских генералов» понимают мысленный эксперимент, призванный проиллюстрировать проблему синхронизации состояния систем в случае, когда коммуникации считаются надежными, а процессоры – нет. В криптологии – это задача взаимодействия нескольких удаленных абонентов, которые получили приказы из одного центра. Часть абонентов, включая центр, могут быть противниками. Нужно выработать единую стратегию действий, которая будет выигрышной для абонентов. – *Прим. ред.*

[26] *Lamport, L., Shostack, R., Pease, M.* (1982), «The Byzantine Generals Problem», журнал *ACM Transactions on Programming Languages and Systems*, том 4, № 3, с. 382–401; *Philipp* (псевдоним) (2014), «Bitcoin and the Byzantine Generals Problem – A Crusade Is Needed? A Revolution?», журнал *Financial Cryptography, http://fnancialcryptography.com/mt/archives/001522.html; Vaurum* (псевдоним) (2014).«A Mathematical Model for Bitcoin» (запись в блоге), *http:// blog.vaurum.com/a-mathematical-model-for-bitcoin/*

Как работает криптовалюта

Биткойн – это цифровые наличные деньги, с помощью которых можно покупать и продавать товары через интернет. Цепочка добавленной стоимости биткойна формируется несколькими группами: разработчиками, майнерами, биржами, сервисами обработки платежей, операторами интернет-кошельков и конечными пользователями/потребителями. Для начала работы с криптовалютой пользователю требуется лишь биткойн-адрес, секретный ключ и программа-кошелек. Биткойн-адрес – это идентификатор вроде номера счета, на который другие пользователи могут отправлять биткойны, а секретный ключ – это криптографический ключ, с помощью которого можно отправлять полученные биткойны другим пользователям. Для того чтобы оперировать биткойнами, программа-кошелек устанавливается на компьютере или смартфоне (см. рис. 1–1). При этом не нужно открывать никакого «расчетного счета» в какой-либо компании или банке – после установки программа автоматически генерирует связку из секретного ключа и биткойн-адреса, и вы можете сразу же распоряжаться средствами, привязанными к данному адресу. Кошелек может содержать копию блокчейна – записи всех транзакций, когда-либо выполненных с данной валютой. Это позволяет самостоятельно верифицировать любые транзакции в рамках децентрализованной системы Биткойн. Практические аспекты обслуживания альткойн-кошельков подробнее описаны в Приложении А.

Рисунок 1–1. *Приложение – электронный биткойн-кошелек и перевод биткойнов (изображение предоставлено разработчиками электронного биткойн-кошелька и InterAksyon)*

Сервисы электронных кошельков и криптозащита персональных данных

Криптозащита персональных данных – это новая обширная область знаний. Проблема обеспечения защиты персональных финансовых активов и транзакций в блокчейне весьма актуальна.

Обычным потребителям незнакомы многие особенности блокчейн-технологии и криптозащиты персональных данных – например, необходимость создавать резервную копию кошелька. Сохранение секретного ключа в электронном кошельке на собственном компьютере дает полную финансовую независимость, но также означает невозможность обратиться в службу поддержки для «восстановления пароля». Потеря секретного ключа влечет за собой потерю биткойнов. В этом плане блокчейн-технология пока еще не готова к повсеместному использованию. Данную проблему пытаются решить ориентированные на пользователя биткойн-стартапы вроде Circle Internet Financial и Xapo. Можно разработать стандартизированное приложение или сервис для создания резервных копий (например, если биткойн-кошелек был установлен на потерянных, украденных, вышедших из строя или обновленных смартфонах/ноутбуках/планшетах). Такой сервис помог бы пользователям управлять своими секретными ключами и их резервными копиями, чтобы они могли самостоятельно решить свою проблему или обратиться к сторонним специалистам.

Еще один элемент защиты персональных данных, который рекомендуют специалисты, – это *койн-миксинг* – «перемеши вание» своих монет с транзакциями других пользователей для до стижения максимальной конфиденциальности транзакций. Эту задачу решают такие сервисы, как Dark Coin, Dark Wallet и BitMixer[27]. По мере роста рынка альтернативных криптовалют будет также расти спрос на унифицированный электронный кошелек, который способен работать более чем с одной криптовалютой. Сегодня для большинства сервисов на основе блокчейна требуется установка отдельного кошелька, так что можно просто забить свой смартфон разнообразными электронными кошельками.

Несмотря на то что на сегодня реализация криптовалют громоздка и неэффективна, они обладают множеством важных преимуществ в области криптозащиты персональных данных. Вот одно из таких преимуществ – блокчейн представляет собой *push-технологию* (пользователь самостоятельно инициирует каждую транзакции), а не *pull-технологию* (как в случае с кредитной картой или банком, когда персональные данные пользователя хранятся в файле и используются во время каждой авторизации). Когда создавались технологии кредитных карт, безопасность интернет-платежей вообще не стояла на повестке дня, в то время как при создании блокчейн-технологий она находится в центре внимания.

Pull-технологии не могут обойтись без централизованных хранилищ персональных данных, которые становятся все более уязвимыми для хакерских атак. Вот лишь некоторые из недавних примеров масштабных атак с целью хищения персональных данных, от которых пострадали миллионы пользователей: Target, ChaseBank и Dairy Queen. Возможность оплаты биткойнами услуг десятков тысяч торговцев, принимающих криптовалюту (например, Microsoft, Overstock, New Egg, и Dell Computer; см. *https://bitpay.com/directory#/*), означает, что отныне нет необходимости оставлять личные персональные данные в централизованных базах данных этих компаний. Немаловажно и то, что комиссии для биткойн-транзакций гораздо ниже, чем комиссии центров обработки операций кредитных карт.

Прием биткойна торговыми организациями

На момент создания этой книги основными сервисами, обеспечивающими прием платежей в биткойнах торговыми организациями, были BitPay и Coinbase в США и Coinify в Европе[28]. Небольшим предприятиям, таким как кафе, трудно работать с двумя различными платежными системами (для приема традиционных, фиатных денег и для приема криптовалют), поэтому в будущем целесообразнее будет интегрировать биткойн в уже существующие платежные системы. Для осуществления быстрых покупок за биткойны в торговых терминалах (например, для покупки чашки кофе) надо создать возможность легкой оплаты через мобильный телефон. CoinBeyond и другие компании специализируются именно на мобильных биткойн-платежах. У BitPay и Coinbase также имеются мобильные решения для оплаты заказов. Одним из заметных шагов стало появление возможности принимать платежи в биткойнах с помощью модуля PayByCoin[29] в бухгалтерской программе для малых предприятий QuickBooks компании Intuit.

---

[27] *Cipher* (псевдоним), «The Current State of Coin-Mixing Services», сайт Depp.Dot.Web, 25 мая 2014 г., *http://www.deepdotweb.com/2014/05/25/current-state-coin-mixing-services/*

[28] *Rizzo, P.,* «Coinify Raises Millions to Build Europe's Complete Bitcoin Solution», сайт CoinDesk, 26 сентября 2014 г., *http://www.coindesk.com/coinify-raises-millions-build-eu-ropes-complete-bitcoin-solution/*

[29] *Patterson, J.,* «Intuit Adds BitPay to PayByCoin», блог Bitpay, 11 ноября 2014 г., *http://blog.bitpay.com/2014/11/11/intu-it-adds-bitpay-to-paybycoin.html*

Резюме: практическое использование Блокчейн 1.0

Блокчейн уже занял нишу «валюты интернета», стал глобальной цифровой платежной системой и имеет потенциал развиться в целый «интернет денег», объединяющий финансы так же, как «интернет вещей» объединяет различные устройства. Первой и наиболее очевидной областью применения блокчейна стали денежные расчеты. Смысл существования альтернативных систем денежных расчетов оправдан уже одними только соображениями экономии: снижение комиссий за платежи кредитными картами во всем мире с 3 % хотя бы до 1 % станет огромной выгодой для экономики. Особенно это касается международного рынка денежных переводов объемом в 514 млрд долларов ежегодно, где комиссии за перевод могут составлять от 7 % до 30 %[30]. Кроме того, блокчейн доставляет средства немедленно, пользователи не ожидают перевода несколько дней. Использование биткойна и других криптовалют может привести к полному пересмотру представлений о деньгах, торговле и коммерции. Биткойн – не просто улучшенная версия системы VISA, он позволяет делать то, о чем люди даже не задумывались, ведь валюта и платежи – это лишь первая область его применения[31]. Основная особенность денежных расчетов на основе блокчейна состоит в том, что они позволяют совершать любые сделки через интернет без посредников. С помощью альткойнов можно осуществлять денежные переводы и вести коммерческую деятельность полностью децентрализованным, распределенным и глобальным образом. Поэтому криптовалюта может стать открытой программируемой сетью для децентрализованного обмена любыми ресурсами – даже без учета валюты и платежей. Таким образом, Блокчейн 1.0 как технология денежных расчетов и платежей уже эволюционирует в Блокчейн 2.0, полнее использующий функциональность биткойна как программируемых денег.

Отношение к фиатным деньгам

Возьмем в качестве примера биткойн как наиболее распространенную криптовалюту. Двенадцатого ноября 2014 года биткойн стоил 399,40 долларов. Курс сильно колебался (см. рис. 1–2), от 12 долларов в начале 2013 года до 1242 долларов 29 ноября

2013 года, когда биткойн ненадолго превзошел в цене унцию золота (1240 долларов)[32]. Этот пик был вызван комбинацией воздействия нескольких факторов. Значительный рост спроса был обусловлен банковским кризисом на Кипре (март 2013 года). Кроме того, рост курса подстегнула высокая активность на криптовалютном рынке Китая, которая продолжалась до 5 декабря 2013 года. В этот день правительство страны запретило организациям (не физическим лицам) использовать биткойн, после чего курс упал[33].

В 2014 году курс биткойна постепенно снижался с 800 долларов до приблизительно 350 долларов в декабре 2014 года. Впрочем, по некоторым (хотя и спорным) данным, 70 % торговли биткойнами происходит за китайские юани[34]. По этой цифре трудно оценить масштабы

---

[30] *Hajdarbegovic, N.*, «Deloitte: Media 'Distracting' from Bitcoin's Disruptive Potential», сайт CoinDesk, 30 июня 2014 г., *http://www.coindesk.com/deloitte-media-distracting-bitcoins-dis-ruptive-potential; аноним*, «Remittances: Over the Sea and Far Away», журнал *The Economist*, 19 мая 2012 г., *http://www.economist.com/node/21554740*

[31] *Levine, A. B., Antonopoulos, A. M.,* «Let's Talk Bitcoin! #149: Price and Popularity», подкаст «Let's Talk Bitcoin», 30 сентября 2014 г., *http://letstalkbitcoin.com/blog/post/lets-talk-bit-coin-149-price-and-popularity*

[32] *Kitco News*, «2013: Year of the Bitcoin», журнал *Forbes*, 10 декабря 2013 г., *http://www.forbes.com/sites/kitconews/2013/12/10/2013-year-of-the-bitcoin/*

[33] *Gough, N.*, «Bitcoin Value Sinks After Chinese Exchange Move», газета *The New York Times*, 18 декабря 2013 г., http://www.nytimes.com/2013/12/19/business/international/china-bit-coin-exchange-ends-renminbi-deposits.html?_r=0

[34] *Hajdarbegovic, N.*, «Yuan Trades Now Make Up Over 70 % of Bit-coin Volume», сайт CoinDesk, 5 сентября 2014 г., *http://*

торговли, поскольку китайские биржи не взимают комиссии; следовательно, можно бесплатно обменивать любую валюту, создавая ложный объем. Кроме того, большая часть торговли за юани – это, скорее всего, спекуляции (что касается и торговли биткойнами в целом), так как в Китае существует лишь несколько реальных поставщиков, принимающих биткойны, и лишь небольшое количество потребителей, использующих эту валюту для активного потребления товаров и услуг.

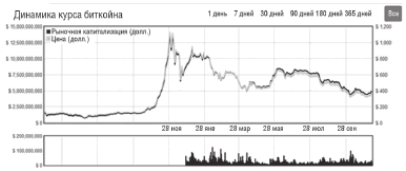

Рисунок 1–2. *Курс биткойна с 2009 года по ноябрь 2014 года (источник изображения: http://coinmarketcap.com/currencies/bitcoin/#charts)*

Есть мнение, что широкому использованию криптовалюты препятствуют волатильность и колебания курса. Чтобы решить эту проблему, был создан ряд проектов с целью снижения волатильности: Bitreserve (депозиты в биткойнах с фиксированным курсом обмена)[35], криптовалюта Realcoin, привязанная к доллару США (USD)[36], и сервис LOCKS от Coinapult, поддерживающий привязку биткойна к курсу золота, серебра, доллара США, британского фунта или евро[37]. Одной из первых крипто-валют, привязанных к доллару, стала XRP/USD от компании Ripple. Еще одна подобная валюта – BitUSD от BitShares. Однако в целом биткойн подвержен волатильности и инфляции в меньшей степени, чем некоторые фиатные валюты (благодаря чему относительная ценность биткойна выше). Кроме того, многие операции с биткойнами представляют собой моментальные переводы с обменом на другие валюты по текущему курсу, для которых волатильность не имеет особого значения.

Капитализация рынка биткойна на ноябрь 2014 года составляет 5,3 млрд долларов (см. http://coinmarketcap.com/). Она была вычислена путем умножения текущей цены (399,40 доллара) на имеющееся количество (13 492 000 биткойнов). Это уже сопоставимо с ВВП небольшой страны (в рейтинге 200 крупнейших экономик биткойн был бы на 150-м месте). В отличие от фиатных валют, для которых правительство может напечатать дополнительные деньги, количество биткойнов растет по заранее определенному графику и в пределе ограничено.

Новые биткойны выпускаются как часть блоков, на регулярной и однозначно предсказуемой основе. На сегодня выпущено 13,5 млн монет, а к 2040 году ожидается рост до 21 млн монет. Целыми биткойнами неудобно оперировать для повседневных покупок, поскольку его курс составляет около 400 долларов за монету. Поэтому цены и курсы обмена обычно выражаются его дробными единицами: миллибитами (одна тысячная биткойна; 1 mBTC = ~0,40 долл.), битами (одна миллионная биткойна; 1 mBTC = ~0,0004 долл.) и сатоши (одна стомиллионная часть биткойна; 1 Satoshi = ~0,000 004 долл.).

---

www.coindesk.com/yuan-trades-now-make-70-bitcoin-volume/

[35] *Vigna, P.*, «CNET Founder Readies Bitreserve Launch in Bid to Quell Bitcoin Volatility», газета *The Wall Street Journal*, 22 октября 2014 г., *http://blogs.wsj.com/moneybeat/2014/10/22/cnet-founder-readies-bitreserve-launch-in-bid-to-quell-bitcoin-volatility/*

[36] *Casey, M. J.*, «Dollar-Backed Digital Currency Aims to Fix Bit-coin's Volatility Dilemma», газета *The Wall Street Journal*, 8 июля 2014 г., *http://blogs.wsj.com/moneybeat/2014/07/08/dol-lar-backed-digital-currency-aims-to-fix-bitcoins-volatili-ty-dilemma/*

[37] *Rizzo, P.*, «Coinapult Launches LOCKS, Aiming to Eliminate Bitcoin Price Volatility», сайт CoinDesk, 29 июля 2014 г., *http://www.coindesk.com/coinapult-launches-locks-tool-elimi-nate-bitcoin-price-volatility/*

Правовой статус

Государственное регулирование – это, вероятно, один из самых существенных факторов, от которого зависит развитие блокчейн-отрасли в полноценную индустрию финансовых услуг. По данным на октябрь 2013 года, биткойн полностью запрещен в ряде стран: Бангладеш, Боливия, Эквадор, Исландия (возможно, запрет сделан для поддержки Auroracoin), Киргизия и Вьетнам[38]. Китай, как было сказано выше, в декабре 2013 года запретил финансовым учреждениям иметь дело с этой виртуальной валютой; правда, это не сказалось на объеме торговли в китайских юанях[39]. Некоторые официальные органы Германии, Франции, Кореи и Таиланда высказались негативно по отношению к биткойну[40].

Европейская служба банковского надзора, Швейцария, Польша, Канада и США продолжают оценивать различные аспекты криптовалют и биткойна[41]. Многие страны пытаются подвести биткойн (и цифровые валюты в целом) к своим существующим регулятивным нормативам, зачастую обнаруживая, что криптовалюты не вполне соответствуют им, и, наконец, приходят к выводу, что криптовалюты имеют много особенностей, поэтому для них может потребоваться новое законодательство. Одни страны, например Великобритания, считают биткойн валютой (и не облагают НДС операции покупки-продажи биткойнов), другие же страны, например Австралия, не смогли определить биткойн как валюту из-за законов об эмиссии и потому облагают операции с биткойнами НДС или налогом на продажу[42].

Налоговое управление США рассматривает биткойн как актив, подобный ценным бумагам, а не как деньги, подразумевая, что транзакции в биткойнах облагаются налогами на прирост капитала[43]. С их точки зрения виртуальные валюты являются активом, а не валютой. Тем не менее почти все остальные правительственные учреждения США, включая FinCEN (Сеть по расследованию финансовых преступлений), регуляторы банковской системы, а также Бюро финансовой защиты потребителей, Комиссия по ценным бумагам и биржам, Комиссия по торговле финансовыми фьючерсами и Министерство юстиции пытаются регулировать биткойн как валюту[44].

---

[38] На момент подготовки этого издания (май 2016 г.) правовой статус биткойна в России окончательно не определен и продолжает активно обсуждаться. – *Прим. ред.*

[39] *Yang, S.*, «China Bans Financial Companies from Bitcoin Transactions», информационное агентство Bloomberg, 5 декабря 2013 г., *http://www.bloomberg.com/news/2013-12-05/chi-na-s-pboc-bans-fnancial-companies-from-bitcoin-transac-tions.html*

[40] *Orsini, L.*, «A Year in Bitcoin: Why We'll Still Care About the Cryptocurrency Even If It Fades», сайт ReadWrite, 30 декабря 2013 г., *http://readwrite.com/2013/12/30/bitcoin-may-fade-2014-prediction*

[41] Bitcoin Embassy, «Andreas M. Antonopoulos Educates Senate of Canada About Bitcoin», видеоролик на YouTube, 8 октября 2014 г., *https://www.youtube.com/watch?v=xUNG-FZDO8mM*

[42] *Robertson, M., Bramanathan, R.,* «ATO Ruling Disappointing for Bitcoin in Australia», сайт Lexology, 21 августа 2014 г., *http://www.lexology.com/library/detail.aspx?g=aee6a563-ab32-442d-8575-67a940527882*

[43] *Hern, A.*, «Bitcoin Is Legally Property, Says US IRS. Does That Kill It as a Currency?», газета *The Guardian*, 31 марта 2014 г., *http://www.theguardian.com/technology/2014/mar/31/bitcoin-legally-property-irs-currency. См. также: http:// www.irs.gov/pub/irs-drop/n-14-21.pdf*

[44] Счетная палата правительства США (2014), «Virtual Currencies: Emerging Regulatory, Law Enforcement, and Consumer Protection Challenges. GAO-14-496», опубликовано: 29 мая 2014 г., выпущено в общий доступ: 26 июня 2014 г., *http://www.gao.gov/products/GAO-14-496*. Во второй главе объясняется, как каждое из соответствующих федеральных агентств (FinCEN, banking regulators, CFPB, SEC, CFTC и DOJ) осуществляет надзор над биткойном или виртуальной валютой или как применяются другие средства контроля. См. также: «Virtual Economies and Currencies: Additional IRS Guidance Could Reduce Tax Compliance Risks», *http://www.gao.gov/prod-ucts/GAO-13-516*

Глава 2
Блокчейн: основа для контрактов (Блокчейн 2.0)

Новые возможности

С самого начала предполагалось, что биткойн будет не просто валютой. В процессе разработки протокола в него была встроена функциональность программируемых денег[45] и контрактов. В 2010 году Сатоши Накамото заявил следующее: «Архитектура [криптовалюты] поддерживает огромное разнообразие транзакций, которые я разработал несколько лет назад – эскроу-транзакции[46], гарантийные контракты, трехсторонний арбитраж, многосторонняя подпись и т. д. Если биткойн станет популярным, то придет время для использования этих функций, но, чтобы они были доступны в дальнейшем, важно было изначально предусмотреть их»[47]. В главе 3 подробно описано применение принципов биткойна не только к финансовым, но и к любым другим сделкам, даже к «виртуальным». Это возможно благодаря тому, что концепции и структура, разработанные для биткойна, очень мобильны и легко расширяются.

Блокчейн 2.0 – вторая важная ступень в развитии блокчейн-индустрии, которая осенью 2014 года все еще была в фазе активного формирования[48]. Так как пространство Блокчейн 2.0 еще разрабатывается, существует множество различных его категорий, описаний и концептуализаций. Стандартные классификации и определения все еще формируются. Некоторые термины, в широком смысле слова относящиеся к пространству Блокчейн 2.0, могут включать в себя Биткойн 2.0, протоколы Биткойн 2.0, умные контракты, умные активы, децентрализованные приложения (Dapps), децентрализованные автономные организации (DAO) и децентрализованные автономные корпорации.

Блокчейн 1.0 предназначен для децентрализации денежных расчетов, а Блокчейн 2.0 – для децентрализации рынков в более широком аспекте. Он поддерживает переводы через блокчейн множества других видов активов помимо валюты, от момента создания любой единицы стоимости до момента ее перевода или деления.

Биткойн можно образно сравнить со стеком протокола интернета. После внедрения базовой технологии и инфраструктуры интернета появилась возможность создавать службы на их основе (например, Amazon, Netfix и Airbnb), которые со временем развиваются, совершенствуя использование базовой технологии. Блокчейн 1.0 аналогичен базовому транспортному протоколу сети интернет TCP/IP, поверх которого создавались протоколы передачи данных: HTTP, SMTP и FTP – их можно называть протоколами 2.0. Протоколы Блокчейн 2.0 либо напрямую используют распределенный журнал записей биткойна, либо создают свои собственные распределенные журналы записей, но при этом они находятся все в той же децентрализованной модели технической архитектуры криптовалюты трехуровневого стека: блокчейн, протокол и валюта.

---

[45] Программируемые деньги означают, что использование биткойнов можно ограничить (запрограммировать) на то, чтобы их можно было потратить в каком-то конкретном городе, стране или даже с какой-то конкретной целью. – *Прим. ред.*

[46] Эскроу (от англ. *escrow)* – контракт, который находится на хранении у третьего лица и вступает в силу при выполнении определенного условия. Эскроу-сделками, таким образом, называют сделки с привлечением третьего лица, т. н. эскроу-агента, обеспечивающего должное исполнение сделки сторонами. – *Прим. ред.*

[47] *Nakamoto, S.*, «Re: Transactions and Scripts: DUP HASH160… EQUALVERIFY CHECKSIG», сайт-форум Bitcointalk, 17 июня 2010 г., *https://bitcointalk.org/index.php?topic=195.ms-g1611#msg1611*

[48] *Swanson, T.*, «Blockchain 2.0 – Let a Thousand Chains Blossom», форум «Let's Talk Bitcoin!», 8 апреля 2014 г., *http://letstalkbitcoin.com/blockchain-2-0-let-a-thousand-chains-blossom/*

Впрочем, важно отметить, что эти «новые вспомогательные уровни интернета» в основном находятся в стадии разработки и любое образное определение может быстро устареть. Это все равно что назвать Chrome «Napster 2.0», а Facebook или AdBlock – «веб-браузер 3.0».

Основная идея состоит в том, что с помощью функции децентрализованного журнала записей транзакций можно регистрировать, подтверждать и передавать все виды контрактов и собственности. В таблице 2–1 перечислены некоторые классы и примеры активов и контрактов, которые можно передавать с помощью блокчейна.

Сатоши Накамото называл сделки эскроу, гарантийные обязательства, трехсторонний арбитраж и многостороннюю подпись. Блокчейн позволяет переопределить все виды финансовых транзакций, включая операции с ценными бумагами, акциями и долями компаний, инструментами краудфандинга, долговыми обязательствами, взаимными фондами, аннуитетами, пенсионными фондами и разного рода производными финансовыми инструментами (фьючерсы, опционы, свопы и прочее).

В распределенный журнал записей можно перемещать и общедоступные документы: свидетельства о праве собственности на земельные участки и недвижимость, свидетельства о регистрации транспортных средств, бизнес-лицензии, свидетельства о браке и свидетельства о смерти. С помощью блокчейна можно подтверждать цифровые удостоверения, например водительские удостоверения, удостоверения личности, паспорта и свидетельства о регистрации избирателя. Можно хранить и частные документы, например долговые расписки, займы, договоры, пари, подписи, завещания, доверенности и эскроу. Посредством блокчейна может выполняться заверение страховых свидетельств, свидетельств о собственности и нотариальное заверение документов.

Таблица 2–1. Блокчейн-приложения помимо валюты (взято из Ledra Capital Mega Master Blockchain List; см. Приложение Б)[49]

Класс	Примеры
Общие	Сделки эскроу, гарантийные обязательства, трехсторонний арбитраж, многосторонняя подпись
Финансовые транзакции	Ценные бумаги, акции компаний, краудфандинг, облигации, взаимные фонды, производные финансовые инструменты, аннуитеты, пенсии
Общедоступные документы	Свидетельства о праве собственности на земельные участки и недвижимость, свидетельства о регистрации транспортных средств, бизнес-лицензии, свидетельства о браке, свидетельства о смерти
Удостоверения	Водительские удостоверения, удостоверения личности, паспорта, свидетельства о регистрации избирателя
Частные документы	Долговые расписки, договоры, пари, подписи, завещания, доверенности, эскроу
Документы, требующие засвидетельствования	Страховые свидетельства, свидетельства о собственности, нотариальное заверение документов
Ключи от материальных активов	Дома, номера отелей, аренда или совместное использование автомобилей
Нематериальные активы	Патенты, торговые марки, авторские права, бронирование, доменные имена

Ключи от материальных активов (речь о них пойдет в главе 3) могут кодироваться в распределенном журнале записей как цифровые активы для управляемого доступа к домам, номе-

[49] «The Mega-Master Blockchain List», опубликовано 11 марта 2014 г., сайт компании Ledra Capital, *http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-block-chain-list*

рам отелей, арендованным или находящемся в совместном пользовании автомобилям (например, Getaround).

Нематериальные активы, например патенты, торговые марки, авторские права, брони и доменные имена, также могут быть защищены и передаваться через распределенный журнал записей. Например, чтобы защитить изобретение, можно вместо регистрации торговой марки или патента закодировать его в распределенном журнале записей, с отметкой даты и времени. Так можно будет подтверждать существование изобретения на определенный момент времени – об этом речь пойдет в главе 3, в разделе «Цифровая собственность: заверение документов в блокчейне (нотариальные службы, защита интеллектуальной собственности)».

Финансовые сервисы

Основная сфера деятельности бизнеса, связанного с блокчейном, – создание интерфейсов для взаимодействия криптовалют с традиционными банковскими и финансовыми рынками. Компания Ripple Labs, которая привлекла серьезное венчурное финансирование, использует блокчейн-технологию для обновления банковских экосистем и предоставления традиционным финансовым учреждениям возможности более эффективного ведения бизнеса. Платежная сеть Ripple позволяет банкам переводить средства и выполнять обмен валют напрямую, без каких-либо посредников[50]. Кроме того, Ripple разрабатывает собственную платформу и язык умных контрактов – Codius. Еще одна возможность симбиоза между традиционной банковской индустрией и биткойном – инвестиции через инновационный фонд испанского банка Bankinter в Coinfeine, стартап на основе биткойн-технологии, цель которого – предоставить конечным пользователям возможность покупать и продавать биткойны напрямую, минуя биржи[51].

Другие компании интегрируют биткойн с традиционными финансовыми и платежными сервисами. Характерный пример – платежная система PayPal. Она имеет много сходств с биткойном; кроме того, планируется, что она и сама будет принимать биткойны. Как и биткойн, система PayPal изначально представляла собой инновационную платежную систему, но затем стала более бюрократизированным предприятием в регулируемой индустрии, собирающим и проверяющим по дробные персональные данные о своих клиентах. Ранее система PayPal считалась инновационной, но со временем она стала весьма централизованной организацией и утратила былое лидерство на рынке. В настоящее время PayPal постепенно внедряет поддержку биткойна. В сентябре 2014 года компания объявила о сотрудничестве с тремя основными платежными биткойн-сервисами: BitPay, Coinbase и GoCoin[52]. Кроме того, по состоянию на сентябрь 2014 года подразделение Braintree компании PayPal, приобретенное в 2013 году, предоставляющее услуги мобильных платежей, разрабатывало функцию, с помощью которой клиенты смогут оплачивать биткойнами аренду недвижимости через Airbnb и услуги такси Uber[53:54].

На пересечении традиционных регулируемых финансовых сервисов и мира биткойна и других криптовалют возникла гибридная концепция «битбанкинга». Так, например, криптовалютная биржа Kraken предоставляет своим пользователям регулируемые финансовые услуги с использованием биткойна в сотрудничестве с банками-партнерами[55]. Очевидно, что есть потребность в адаптации для биткойна стандартных финансовых услуг, таких как сберегательные счета и кредитование; возможно, с предложением пользователям опций по уровню частичного резерва.

---

[50] *Casey, M. J.*, «Ripple Signs First Two U. S. Banks to Bit-coin-Inspired Payments Network», газета *The Wall Street Journal*, 24 сентября 2014 г., *http://blogs.wsj.com/money-beat/2014/09/24/ripple-signs-frst-two-u-s-banks-to-bit-coin-inspired-payments-network/*

[51] *Prisco, G.*, «Spanish Bank Bankinter Invests in Bitcoin Startup Coinfeine», сайт CryptoCoins News, обновлено 17 ноября 2014 г., *https://www.cryptocoinsnews.com/spanish-bank-bankinter-invests-bitcoin-startup-coinfeine/*

[52] *Mac, R.*, «PayPal Takes Baby Step Toward Bitcoin, Partners with Cryptocurrency Processors», журнал *Forbes*, 23 сентября 2014 г., *http://www.forbes.com/sites/ryan-mac/2014/09/23/paypal-takes-small-step-toward-bitcoin-partners-with-cryptocurrency-processors/*

[53] *Bensinger, G.*, «eBay Payments Unit in Talks to Accept Bitcoin», газета *The Wall Street Journal*, 14 августа 2014 г., *http://online.wsj.com/articles/ebay-payment-unit-in-talks-to-ac-cept-bitcoin-1408052917*

[54] Судя по более поздним публикациям, автор имеет в виду продукт v.zero SDK компании Braintree, объявленный в январе 2015 г. и на момент подготовки русского издания этой книги находившийся в состоянии бета-тестирования. – *Прим. ред.*

[55] *Cordell, D.*, «Fidor Bank Partners with Kraken to Create Crypto-currency Bank», сайт CryptoCoins News, обновлено 2 ноября 2014 г., *https://www.cryptocoinsnews.com/fdor-bank-part-ners-kraken-create-cryptocurrency-bank/*

Примером децентрализованного пирингового кредитования на основе блокчейна является платформа BTCjam. Компания Tera Exchange запустила первую биржу биткойн-свопов, регулируемую законодательством США. С ее помощью инвесторы – как юридические, так и физические лица – могут напрямую покупать контракты в биткойнах, используя торговые онлайн-платформы биржи. Помимо этого, Tera предлагает институциональным инвесторам индекс курса биткойна – Tera Bitcoin Price Index, используемый в качестве ориентира для торговых контрактов USD/XBT[56]. Стартап Vaurum, в свою очередь, разрабатывает для финансовых учреждений API, предоставляющий доступ к биткойну брокерам и клиентам банков.

Еще один проект – стартап Buttercoin, торговая платформа и биржа биткойнов для крупных транзакций (200 000–500 000 биткойнов или 70–175 млн долларов), предназначенная для корпоративных клиентов, которым необходимо совершать крупные транзакции в биткойнах [57]. Buttercoin является партнером финансовой компании Wedbush Securities. Эта компания, занимающаяся финансовым анализом, одна из первых стала изу чать биткойн и получать за свои исследования оплату в биткойнах.

Другие блокчейн-компании откровенно нацелены на подрыв доминирования искусственных нерегулируемых монополий на биржевом рынке. К таким монополиям относится, в частности, корпорация National Securities Clearing Corporation (NSCC), подразделение The Depository Trust & Clearing

Corporation (DTCC), занимающееся клирингом[58] и расчетами по ценным бумагам. В частности, такую задачу предстояло решить проекту Medici, инициированному в октябре 2014 года онлайн-ретейлером Overstock и Counterparty, одной из первых платформ Биткойн 2.0[59]. Его целью является создание децентрализованного фондового рынка для ценных бумаг на основе модели блокчейна[60].

---

[56] *Casey, M. J.*, «TeraExchange Unveils First U. S.-Regulated Bit-coin Swaps Exchange», газета *The Wall Street Journal*, 12 сентября 2014 г., *http://teraexchange.com/news/2014_9_12_Tera_WSJ.pdf*

[57] *Rizzo, P.*, «Buttercoin Bids to Take US Business from Global Bit-coin Exchanges», сайт CoinDesk, 5 ноября 2014 г., *http://www.coindesk.com/buttercoin-bids-take-us-business-global-bit-coin-exchanges/*. См. также: *https://www.wedbush.com/sites/default/fles/pdf/2014_11_14_Buttercoin_WEDBUSH.pdf*

[58] Клиринг (*англ.* clearing – очистка) – безналичные расчеты между странами, компаниями, предприятиями за поставленные, проданные друг другу товары, ценные бумаги и оказанные услуги, осуществляемые путем взаимного зачета, исходя из условий баланса платежей. – *Прим. ред.*

[59] В 2015 году Counterparty вышла из проекта Medici. – *Прим. ред.*

[60] *Metz, C.*, «Overstock.com Assembles Coders to Create a Bit-coin-Like Stock Market», журнал *Wired*, 6 октября 2014 г., *http://www.wired.com/2014/10/overstock-com-assembles-coders-build-bitcoin-like-stock-market/*

Краудфандинг

Другой яркий пример обновления финансовых сервисов с помощью децентрализованных моделей на основе блокчейна – это краудфандинг. Его суть заключается в том, что модели одноранговой сбора средств вроде Kickstarter могут устранить необходимость традиционной схемы финансирования стартапов за счет венчурного капитала. Однако если раньше для запуска краудфандинга требовался централизованный сервис наподобие Kickstarter или Indiegogo, то теперь, благодаря краудфандинговым платформам на основе блокчейн-технологии, потребность в посреднике полностью отпадает. С помощью краудфандинговых платформ на основе блокчейна стартапы могут собирать средства, выпуская собственные цифровые валюты и продавая «криптоакции» своим первым инвесторам. Инвесторы при этом получают токены, обозначающие акции того стартапа, который они поддерживают[61].

Одной из ведущих платформ криптовалютного краудфандинга является Swarm – своего рода инкубатор стартапов в области цифровых валют. Эта платформа собрала миллион долларов в процессе собственного краудфандинга, завершившегося в июле 2014 года[62]. Владея собственной криптовалютой инкубатора – Swarmcoin, инвесторы имеют право на дивиденды от стартапов из портфолио инкубатора[63].

В первом наборе финансируемых приложений Swarm уже имеется пять проектов: Manna – разработчик сети персональных дронов; Coinspace – оператор децентрализованного предприятия по майнингу криптовалют; Swarmops – децентрализованная программная платформа управления организациями; Judobaby – децентрализованная игровая платформа; DDP – децентрализованный развлекательный проект танцевальных вечеринок[64].

Еще одна платформа краудфандинга – Koinify, которая имеет на данный момент единственный проект – децентрализованную социальную сеть Gems и привязана к финансовой платформе Melotic[65]. По иронии судьбы, а может быть, как символ эпохи симбиоза, для того чтобы запустить свою краудфандинговую платформу, Koinify привлекла миллион долларов по стандартной схеме венчурных инвестиций[66].

Приложение Lighthouse позволяет реализовывать краудфандинговые инициативы и заключать гарантийные краудфандинг-контракты прямо из биткойн-кошелька. А в Японии в рамках основного сайта краудфандинга fundFlyer был запущен сайт биткойн-краудфандинга bitFlyer[67].

Краудфандинг – популярная тема обсуждения на конференциях биткойн-индустрии, вызывающая ожесточенные споры о легальных аспектах этого способа привлечения средств. Оппоненты ссылаются на то, что в настоящее время невозможно законно заниматься крауд-

---

[61] *Ayral, S.*, «Bitcoin 2.0 Crowdfunding Is Real Crowdfunding», сайт TechCrunch, 17 октября 2014 г., *http://techcrunch.com/2014/10/17/bitcoin-2-0-crowdfunding-is-real-crowd-funding/*

[62] *Hofman, A.*, «Bitcoin Crowdfunding Platform Swarm Announces First Decentralized Demo Day», журнал *Bitcoin Magazine*, 30 сентября 2014 г., *http://bitcoinmagazine.com/16890/bit-coin-crowdfunding-platform-swarm-announces-frst-decen-tralized-demo-day/*

[63] *Casey, M. J.*, «BitBeat: Apple Loves Bitcoin Again, Maybe», газета *The Wall Street Journal*, 30 июня 2014 г., *http://blogs.wsj.com/moneybeat/2014/06/03/bitbeat-apple-loves-bitcoin-again-maybe/*

[64] *Higgins, S.*, «Crowdfunding Platform Swarm Announces First Class of Startups», сайт CoinDesk, 17 октября 2014 г., *http://www.coindesk.com/swarm-first-class-startups-crowdfun-ding-platform/*

[65] *Rizzo, P.*, «How Koinify and Melotic Plan to Bring Order to Crypto Crowdsales», сайт CoinDesk, 14 ноября 2014 г., *http://www.coindesk.com/koinify-melotic-plan-bring-order-cryp-to-crowdsales/*

[66] *Higgins, S.*, «Koinify Raises $1 Million for Smart Corporation Crowdfunding Platform», сайт CoinDesk, 17 сентября 2014 г., *http://www.coindesk.com/koinify-1-million-smart-corpo-ration-crowdfunding/*

[67] *Southurst, J.*, «BitFlyer Launches Japan's First Bitcoin Crowd-funding Platform», сайт CoinDesk, 10 сентября 2014 г., *http://www.coindesk.com/bitflyer-launches-japans-first-bit-coin-crowdfunding-platform/*

фандингом, если сделки на краудфан-динговой платформе предполагают получение доли в акционерном капитале поддерживаемых компаний, поскольку такой краудфандинг так или иначе нарушает различные законы о ценных бумагах. В качестве обходного пути краудфандинговые платформы вроде Swarm и Koinify, а также отдельные краудфандинговые проекты, например Ethereum, продают «виртуальные товары», не являющиеся ценными бумагами, – например, доступ к программам. Однако это является своего рода лукавством, поскольку в большинстве случаев сделки напоминают именно продажу акций. В результате тот, кто фактически вкладывает средства в криптовалютные проекты, с легальной точки зрения всего лишь первым получает доступ к программам с открытым исходным кодом. Необходим более эффективный способ краудфандинга криптовалютных проектов. Он должен быть децентрализованным, но при этом легальным и предлагать более эффективную систему сдержек и противовесов.

Биткойн-тотализаторы

Примерами сочетания новых и старых технологий являются рынки ставок, сделанных в биткойнах, например Predictious и Fairlay[68]. Такие рынки позволяют делать ставки на события в реальном мире: выборы, политическое законодательство, спортивные матчи, выпуски продукции, а также служат хорошим источником информации о развитии индустрии блокчейна. Рынки предсказаний на основе биткойна – это возможность узнать, что инсайдеры думают о будущей динамике курса, успешности различных проектов альткойнов и протокола 2.0, а также об общих вопросах индустрии – например, о вопросах технического развития с использованием биткойна; в частности, когда появится релиз протокола кода, не поддерживающий предыдущие версии, а также об уровне сложности алгоритма майнинга.

[68] *Swan, M.*, «Singularity University Live Prediction Markets Simulation and Big Data Quantitative Indicators», сайт Slideshare, обновлено 11 июля 2014 г., *http://www.slideshare.net/lablog-ga/singularity-university-live-prediction-markets-simula-tion-big-data-indicators*

Умные активы

Блокчейн-технология может быть использована для ведения реестров любых видов, инвентаризации и учета операций с активами в финансовой сфере, различных отраслях экономики и при денежных расчетах; в операциях с реальными (предметы физического мира) и нематериальными (голосования, идеи, репутация, намерения, медицинские данные и информация) активами. Такое использование блокчейн-технологии создает возможности для развития различных классов приложений во всех сегментах бизнеса, связанных с деньгами, рынками и финансовыми сделками. Актив, представленный на блокчейне, становится умным активом, сделки с которым можно совершать посредством умных контрактов.

Основная идея умных активов – осуществление сделок с любой собственностью в моделях на основе блокчейна. Повторимся: активы могут быть как материальными (дом, автомобиль, велосипед, компьютер), так и виртуальными, такими как акции, заказы или авторское право (книги, музыка, иллюстрации и цифровые художественные изображения). Одним из примеров использования блокчейна для управления художественными изображениями с ограниченным тиражом и их передачи является Swancoin, где 121 иллюстрация, выполненная на лакированной фанере размером 30 × 30 см, доступна для покупки и передачи (рис. 2–1)[69]. Все активы можно зарегистрировать в распределенном журнале записей, а собственностью на них могут управлять все обладатели секретного ключа. Владелец может продать актив, передав секретный ключ другому лицу. Таким образом, умный актив – это актив, владение которым регулируется посредством блокчейна с использованием контрактов в соответствии с действующим законодательством. Например, умный контракт, настроенный соответствующим образом, может автоматически передавать собственность на транспортное средство от финансовой компании физическому лицу после выполнения всех выплат по зай му, что автоматически подтверждается другими умными контрактами на блокчейне. Аналогично можно, скажем, изменять процентные ставки по ипотеке в умном контракте на основе блокчейна, проверяя заранее указанный в контракте веб-сайт или элемент данных для получения процентной ставки на определенные даты в будущем.

Рисунок 2–1. *Swancoin: цифровое художественное произведение с ограниченным тиражом (источник изображения: http://swancoin.tumblr.com/)*

Идея умного актива заключается в том, чтобы управлять собственностью и доступом к активу, зарегистрировав его в качестве цифрового актива в блокчейне и имея доступ к секретному ключу. В ряде случаев реальные активы могут в буквальном смысле слова управляться с помощью блокчейна. Смартфон может разблокироваться после подтверждения цифрового удостоверения пользователя, закодированного в блокчейне. Встроенные технологические решения, будь то программный код, датчики, QR-коды, теги NFC, iBeacons, доступ к Wi-Fi или иные решения, обеспечивающие управление доступом в реальном времени, сделают «умными» двери реальных объектов, например автомобилей и домов. Для получения

[69] Не имею никакого отношения к этому автору!

доступа пользователи смогут «предъявлять» свои аппаратные или программные токены. Получив такой запрос на доступ, умный контракт в блокчейне сможет отправить подтверждение или токен доступа физическому объекту – или, например, одноразовый QR-код в электронный кошелек пользователя, чтобы тот смог открыть арендованную машину или номер в отеле. Блокчейн-технология позволяет организовать проверку подлинности удостоверения и верификацию доступа более тонкими, гибкими и настраиваемыми в реальном времени способами, чем те, что используются сейчас. Это достигается путем изящной интеграции существующих аппаратных решений и цифровых программных интернет-технологий[70].

Сделки с умными активами с помощью блокчейна – это совершенно новая идея, к которой пользователи пока еще не привыкли. Закодированные права собственности реализуются с помощью кода. Код запускается автоматически технической инфраструктурой – это значит, что он запрограммирован работать в зависимости от заложенного кода и не может отклоняться от него. Если кодом предусмотрена передача собственности, она не может не произойти. Таким образом, умные активы на основе блокчейна подразумевают возможность реализации распределенных децентрализованных систем управления активами, а также активов, реализуемых с помощью кода. Это может привести к существенной трансформации законодательства в сфере владения собственностью и к упрощению любых операций с собственностью.

Кредитование, не основанное на доверии

Принцип децентрализации журнала записи транзакций, лежащий в основе блокчейн-технологии, – это главный фактор в контексте умных активов и умных контрактов. Придание объекту собственности тех или иных умных свойств дает возможность проводить операции с такими объектами, не требуя высокого уровня доверия. Это снижает затраты на страхование от мошенничества и неправомерных действий, но что еще важнее – это дает возможность оперировать куда более значительными суммами, чем было принято ранее, так как сторонам нет нужды доверять друг другу. Например, можно одалживать деньги через интернет, используя в качестве залога умные активы заемщика, благодаря чему кредитование становится более конкурентоспособным и выгодным[71].

Кроме того, существует вероятность, что благодаря умным контрактам, исполняемым в децентрализованных сетях, может существенно уменьшиться количество судебных споров. Как известно, больше всего судебных процессов приходится на споры, связанные с договорами – 44 % в США и 57 % в Великобритании. Этого можно избежать за счет более высокой точности составления соглашений и внедрения автоматизированных механизмов их исполнения[72]. Ник Сабо, популяризатор криптовалют и теоретик умных контрактов, считает, что проблема контрактов связана с более широкой проблемой неэффективного (то есть иррационального) принятия решений. Данную ситуацию можно исправить с помощью таких автоматизированных механизмов, как умные контракты.

Цветные монеты

Одной из первых реализаций умных активов в блокчейне стали «цветные монеты». В поле «мемо» биткойн-транзакции вносится пометка, «окрашивающая» некоторые биткойны, соответствующие тому или иному активу или эмитенту. С тем же успехом можно написать на долларовой купюре долговое обязательство в отношении другого актива (например, автомобиля). Таким образом, в конкретном биткойне закодирован какой-то другой актив, который

---

[70] *Swan, M.*, «Identity Authentication and Security Access 2.0», блог Broader Perspective, 7 апреля 2013 г., *http://futurememes.blogspot.com/2013/04/identity-authentication-and-se-curity.html*

[71] *Szabo, N.*, «Formalizing and Securing Relationships on Public Networks», журнал *First Monday*, 1 сентября 1997 г., *http://firstmonday.org/ojs/index.php/fm/article/view/548/469* в изложении: *Hearn, M.* (2014); вики Bitcoin, *https://en.bit-coin.it/wiki/Smart_Property*

[72] *Swanson, T.*, «Great Chain of Numbers: A Guide to Smart Contracts, Smart Property, and Trustless Asset Management».

можно безопасно передавать с помощью блокчейна. Впрочем, эта модель требует определенного доверия (актив, обозначенный в поле «мемо», должен использоваться согласно договоренности). Итак, цветные монеты предназначены для использования внутри определенного сообщества. Они выполняют функцию бонусных баллов или токенов, обозначая целый ряд реальных или цифровых товаров и услуг. Основной смысл заключается в том, что эти цветные монеты представляют собой биткойны, помеченные определенными свойствами для обозначения тех или иных цифровых или реальных активов, чтобы можно было совершать с помощью блокчейна более сложные сделки. Сделкой может быть обмен активами, а также выполнение различных видов деятельности – например, голосование, поощрение и комментирование на форумах[73].

[73] *Hajdarbegovic, N.*, «Coinprism Releases Colored Coins Android App for Mobile Asset Transfer», сайт CoinDesk, 20 октября 2014 г., *http://www.coindesk.com/coinprism-mobile-wal-let-colored-coins/*

Умные контракты

Общий смысл умных контрактов на основе блокчейна вытекает из идеи умных активов. В контексте блокчейна контракты или умные контракты означают сделки в распределенном журнале записей, не ограниченные простой куплей-продажей. В них могут быть встроены более сложные инструкции. Контракт – это способ использования биткойна для формирования соглашений посредством блокчейна.

Контракт в традиционном понимании представляет собой соглашение между двумя или более сторонами о выполнении или невыполнении какого-либо действия в обмен на что-то. Каждая из сторон должна доверять другой стороне, чтобы выполнить свою часть обязательств. В отличие от традиционного контракта, умные контракты хоть и выглядят как соглашения о выполнении или невыполнении действий, но при этом они устраняют необходимость доверия между сторонами. Причина в том, что умный контракт как определяется, так и выполняется автоматически, работающим на блокчейне кодом, что не оставляет простора для «человеческого фактора».

Умные контракты обладают тремя главными свойствами: автономность, самодостаточность и децентрализация. Автономность означает, что после того, как контракт запущен, нет необходимости в его дальнейшем взаимодействии с инициатором. Самодостаточность контракта обеспечивает мобилизацию ресурсов и предполагает, что контракты способны собирать средства, предоставляя услуги или выпуская ценные бумаги, и тратить их на необходимые ресурсы, например вычислительную мощность или хранилище. Умные контракты децентрализованы, то есть они не сосредоточены на одном центральном сервере, а распределены по узлам сети, где они самостоятельно и выполняются[74].

Классический пример умных контрактов в виде автоматически исполняемого кода – торговый автомат. В отличие от продавца-человека торговый автомат действует на основе алгоритма. Каждый раз выполняется одна и та же инструкция. После внесения денег и выбора товара автомат выдает этот товар покупателю. Автомат не может «выполнить контракт частично» (если он исправен). Аналогично, умный контракт не может не исполнить заранее предопределенный код. По утверждению Лессига, «код – это закон» в том смысле, что код будет исполняться в любом случае. В зависимости от ситуации это может быть хорошо или плохо. Так или иначе, для общества это новая концепция, которая потребует длительного привыкания, если умные контракты на основе блокчейна станут повсеместно распространены.

Существует множество соображений относительно умных контрактов и криптографически активируемых систем. Они касаются вопроса о необходимости нового свода законов и правил, различающего технически обязательные контракты в коде и более гибкие человеческие контракты, регулируемые законом[75]. Соблюдение или нарушение условий обычных контрактов – это выбор людей, но в случае с блокчейном и любыми другими видами контрактов на основе кода это уже совершенно не так. Кроме того, умные контракты влияют не только на договорное право, но и в широком контексте – на понятие общественного договора среди людей. Необходимо решить и определить, какого рода общественные договоры будут подпадать под закон об автоматическом и потенциально непрерывно исполняющемся коде. Сейчас почти невозможно совместить умные контракты с существующим контрактным правом (например, после запуска контрактного кода им трудно управлять, регулировать или потребовать от него возместить от него ущерб в судебном порядке). Соответственно, нормативно-правовая база, по сути,

---

[74] *De Filippi, P.*, «Primavera De Filippi on Ethereum: Freenet or Skynet? The Berkman Center for Internet and Society at Harvard University», видеоролик на YouTube, 15 апреля 2014 г., *https://www.youtube.com/watch?v=slhuidzccpI*

[75] Там же.

переходит на уровень контракта. В конечном счете это приведет не к беззаконию и анархии, а к тому, что нормативно-правовая база станет более фрагментированной и адаптированной к конкретным ситуациям. Стороны, заключающие контракт, должны выбрать нормативно-правовую базу, уже встроенную в код. Могут существовать несколько известных, проверенных, «готовых к использованию» нормативно-правовых баз, подобно лицензиям Creative Commons, из которых пользователи будут выбирать нормативно-правовую базу в качестве компонента умного контракта. Таким образом, появилась бы возможность достичь разнообразия нормативно-правовых баз, подобно существующему разнообразию валют.

Умные контракты не делают возможным то, что ранее было невозможным, они просто позволяют решать распространенные проблемы, сводя к минимуму необходимость доверия. Зачастую минимум доверия бывает весьма удобным, так как при этом устраняется «человеческий фактор» и обеспечивается полная автоматизация. Примером базового умного контракта является подарок в наследство, который становится доступным на восемнадцатилетие внука либо в день смерти дедушки. Можно создать транзакцию, которая будет находиться в распределенном журнале записей незадействованной, пока не наступит определенная дата или событие. Для того чтобы задать первое условие (когда внук достигнет восемнадцатилетия), программа задает дату инициации транзакции, включающую в себя проверку выполнения транзакции.

Задать второе условие можно, написав программу, которая сканирует онлайновую базу данных реестра смертей, заранее определенную интернет-газету некрологов или любой другой информационный источник, подтверждающий смерть дедушки. После подтверждения факта смерти умный контракт может автоматически отправить деньги[76]. В научно-фантастическом романе Даниэля Суареса «Демон» («Daemon») реализуются именно такие умные контракты, которые исполняются после смерти персонажа.

Еще один вариант использования умных контрактов – настройка автоматических выплат для ставок (подобно лимитным заявкам на финансовых рынках). Можно написать программу или умный контракт, который будет осуществлять выплату по достижении биржевым товаром определенной стоимости либо при получении результата какого-либо события в реальном мире (например, какой-либо новости или победителя в спортивном матче). Можно также развертывать умные контракты в системах краудфандинга, таких как Kickstarter. При этом физические лица делают в режиме онлайн взносы, которые блокируются на блокчейне. Биткойны из кошельков инвесторов разблокируются только после достижения цели по сбору средств; до получения всех средств транзакции осуществляться не будут. Кроме того, по последующим исходящим транзакциям адреса распределенного журнала записей, на который выполнялся сбор средств, можно отслеживать бюджет, расходы и среднемесячные затраты предпринимателя.

[76] GSB Daily Blog, «Bitcoinomics, Chap. 11: The Future of Money and Property or the Gospel Of Layers», сайт GoldSilverBitcoin, 18 августа 2013 г., *https://www.goldsilverbitcoin.com/fu-ture-of-money-bitcoinomic/*

Проекты Блокчейн 2.0

Существует множество проектов развития блокчейн-технологии следующего поколения, которые можно весьма произвольно объединить под заголовком «Проекты Блокчейн 2.0». В таблице 2–2 перечислены некоторые текущие высокоуровневые проекты без подробного описания их технических или концептуальных различий.

Проекты разработки кошельков

Пожалуй, главная категория приложений, создаваемых на основе протоколов блокчейна, – это кошельки. Кошельки, несомненно, являются главным элементом инфраструктуры для криптовалют, поскольку они представляют собой механизм безопасного хранения и переводов биткойнов и других криптографических активов. В таблице 2–3 перечислен ряд различных проектов кошельков и компаний-разработчиков, их названия, URL-адреса, а также базовые платформы, на которых они создаются.

Таблица 2–2. Список образцов проектов Блокчейн 2.0 (расширен Петром Пясеки, *http://bit.ly/crypto_2_0_comp)*

Название и URL-адрес проекта Биткойн 2.0	Описание проекта	Техническое примечание
Ripple *https://ripple.com/*	Платежи, обмен криптовалют, сеть переводов; система умных контрактов Codius	Собственный блокчейн
Counterparty *https://www.counterparty.co/*	Высокоуровневый протокол для выпуска и обмена валют	Поверх блокчейна биткойна
Ethereum *http://ethereum.org/*	Тьюринг-полная вычислительная платформа общего назначения	Собственный блокчейн, виртуальная машина Ethereum
Mastercoin *http://www.mastercoin.org/*	Производные финансовые инструменты	Поверх блокчейна биткойна
NXT *http://www.nxtcommunity.org/*	Альткойн с майнингом по модели proof-of-stake («подтверждение доли»)	Собственный блокчейн
Open Transactions *http://opentransactions.org/*	Неотслеживаемые анонимные транзакции и транзакции без задержек	Распределенный журнал записей отсутствует; библиотека транзакций
BitShares *http://bitshares.org/*	Децентрализованная биржа криптоакций	Отдельный блокчейн
Open Assets *https://github.com/OpenAssets*	Выпуск и кошелек цветных монет	Блокчейн биткойна
Colored Coins *http://coloredcoins.org/*	Маркировка цифровых/реальных активов в биткойн-активах	Блокчейн биткойна

Таблица 2–3. Проекты кошельков криптовалют

Название проекта	URL-адрес	Базовая инфраструктура
Проекты кошельков		
ChromaWallet	*http://chromawallet.com/*	Open Assets
CoinSpark	*http://coinspark.org/*	Open Assets
Counterwallet	*https://counterwallet.io/*	Counterparty
Компании-разработчики		
Coinprism	*https://www.coinprism.com/*	Open Assets
Melotic	*https://www.melotic.com/*	Возможность торговать выбранными цифровыми активами (то есть Storjcoin, LTBCoin) за биткойны
OneWallet	*https://www.onewallet.io*	Рынок и кошелек биткойнов

Платформы и API разработки блокчейна

Помимо проектов протокола Блокчейн 2.0 существует ряд компаний – разработчиков платформ и проектов, предлагающих инструменты для разработки приложений. У Blockchain.info есть ряд API для работы с их сервисом электронных кошельков (это один из крупнейших сервисов электронных кошельков), предназначенных для отправки и получения платежей и выполнения других операций. Компания Chain создала интерфейсы для обращения к данным, содержащимся в полных узлах распределенного журнала записей, и стандартные информационные запросы, например о балансе биткойнов по адресу. Кроме того, можно отправлять уведомления, когда по тому или иному адресу выполняется какое-либо действие. Stellar – это полудецентрализованный (обслуживается организациями-шлюзами, а не майнерами) общедоступный журнал записей и унифицированная среда разработки (API блокчейна, API мультиподписи), привязанная к платежной сети Stripe[77]. Существуют и другие компании, имеющие API-кошельки с многосторонней подписью, – Block.io, Gem и BlockCypher.

Потребуются более унифицированные среды разработки API, в том числе разнообразные и развивающиеся компоненты экосистемы блокчейна (хранение, обслуживание файлов, взаимодействие кошельков, мобильные платежи, подтверждение удостоверений и репутация). Существует возможность привязки среды разработки блокчейна к другим крупным сегментам, например к межмашинной (M2M) коммуникации и инфраструктуре сетей «интернета вещей» для быстрой разработки приложений. Примером подобного развитого интегрированного приложения в отдаленном будущем могут стать интеллектуальные часы, взаимодействующие с датчиками дорожного движения в рамках инфраструктуры умного города, для того чтобы автоматически резервировать и оплачивать полосу движения с помощью умных контрактов в биткойнах.

[77] *Carney, M.*, «Growing Pains: Stellar Stumbles Briefy Amid Its Launch of a New Crypto-Currency Platform», сайт PandoDaily, 5 августа 2014 г., *http://pando.com/2014/08/05/growing-pains-stellar-stumbles-briefly-amid-its-launch-of-a-new-crypto-currency-platform/*

Экосистема блокчейна: децентрализованные хранение, коммуникации и вычисления

Блокчейн-технологии нужна распределенная экосистема, которая обеспечит комплексную операционную поддержку. Блокчейн – это децентрализованный журнал записи транзакций, который является частью более широкой вычислительной инфраструктуры, которая также должна включать в себя много других функций, например хранение, коммуникации, обслуживание файлов и архивирование. Из конкретных проектов разработки решений для распределенной экосистемы блокчейна следует отметить Storj (хранение всех видов файлов – текстов, изображений, аудио, мультимедиа); IPFS (обслуживание файлов, поддержка ссылок и хранение); а также Maidsafe и Ethereum (хранение, коммуникация и обслуживание файлов).

Хранение. Прежде всего необходимо безопасное, децентрализованное хранилище вне блокчейна, предназначенное для хранения объемных файлов, таких как электронные медицинские карты (EMR), геномы или документы Microsoft Word, которые не могут быть упакованы в поле размером 40 байт (40 знаков) OP_RETURN, используемое для комментирования биткойн-транзакций (или даже в 528-значное поле для аннотаций Florincoin). Хранилище файлов может быть либо централизованным (как Dropbox или Google Drive), либо находиться в той же децентрализованной архитектуре, что и распределенный журнал записей. Транзакция блокчейна, которая регистрирует актив, может включать в себя указатель и метод доступа, а также привилегии для файла, хранящегося вне блокчейна.

Обслуживание файлов. Создатели проекта IPFS предложили интересный метод децентрализованного безопасного обслуживания файлов. IPFS означает InterPlanetary File System, что предполагает потребность в глобальной файловой системе с постоянным доступом. Эта система, предназначенная для решения проблемы битых ссылок сайта на файлы, выходит далеко за пределы контекста блокчейн-технологии. Система объединяет технологию однорангового обмена файлами BitTorrent с функциями распределенной системы управления версиями Git, изначально созданной для управления разработкой ПО, но применимой в более широком контексте к любым цифровым активам. Таким образом, IPFS – это глобальная версионированная одноранговая файловая система, однозначно сопоставляющая уникальный файл, где бы он ни находился в сети (вместо использования центрального репозитория), с его хешем (уникальным кодом), который подтверждает целостность файла и отсутствие в нем спама и вирусов[78]. IPFS совместима с технической архитектурой и духом биткойна, для узлов общего доступа к файлам предусмотрено вознаграждение в виде монет Filecoin.

Архивирование. Полная экосистема обязательно должна включать планирование жизненного цикла и окончания срока службы блокчейнов. Вовсе не факт, что распределенные журналы записей будут существовать вечно, и обеспечение их сохранности и доступа к ним – нетривиальные задачи. Для того чтобы архивировать блокчейны, если это потребуется, нужна система наподобие Internet Archive и Wayback Machine. Ведь потребуется не только сохранение блокчейн-транзакций, но также последующее восстановление записанных ранее активов распределенного журнала записей и управление ими – при том, что могут применяться проприетарные алгоритмы хеширования, – поскольку некоторые блокчейны, вероятно, перестанут использоваться. Допустим, кто-то создал свидетельство существования своего завещания в распределенном журнале записей биткойна в 2014 году. Но как удостовериться, что это завещание будет активировано и пройдет проверку подлинности через 60 лет, когда настанет время его прочесть? Если блокчейн-технологиям суждено стать общепринятым механизмом хране-

[78] *Benet, J.*, «IPFS – Content Addressed, Versioned, P2P File System (DRAFT 3)», прочитано в 2014 г. (нет сведений о дате публикации), *http://static.benet.ai/t/ipfs.pdf*

ния всех документов общества, необходимо обеспечить их сохранность, архивирование, регулирование их срока службы и обеспечение доступа. Такие возможности должны быть явным образом встроены в цепочку создания стоимости. Существование подобных инструментов, архивирующих неиспользуемые распределенные журналы записей и обеспечивающие их полный жизненный цикл, поможет широкому распространению блокчейн-технологии.

Конец ознакомительного фрагмента.