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.

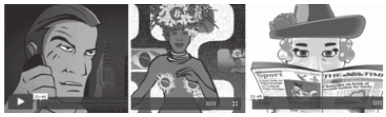

Рисунок П-2. *Рекламные ролики Bitflm*

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 однорангового 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.

---

[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/*

Конец ознакомительного фрагмента.