

Мелани Свон

БЛОК ЧЕЙН

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

© Свон М., 2015
© Олимп-Бизнес, 2015

Содержание

Об авторе	7
Предисловие	8
Валюта, контракты и приложения блокчейн вне финансовых рынков	9
Блокчейн 1.0, 2.0 и 3.0	11
Что такое биткойн?	12
Что такое блокчейн?	13
Связанный мир и блокчейн: пятая революционная парадигма вычислений	14
Повсеместное внедрение: доверие, удобство и простота использования	17
Цели, методология и структура этой книги	19
Глава 1	21
Стек технологий: блокчейн, протокол, валюта	21
Двойное расходование и задача византийских генералов	23
Как работает криптовалюта	25
Резюме: практическое использование Блокчейн 1.0	28
Глава 2	32
Новые возможности	32
Финансовые сервисы	36
Краудфандинг	38
Биткойн-тотализаторы	40
Умные активы	41
Умные контракты	44
Проекты Блокчейн 2.0	46
Проекты разработки кошельков	47
Платформы и API разработки блокчейна	50
Экосистема блокчейна: децентрализованные хранение, коммуникации и вычисления	51
Ethereum: Тьюринг-полная виртуальная машина	53
Децентрализованные приложения, организации, компании и общества: все более автономные умные контракты	55
Блокчейн как путь к искусственному интеллекту	61
Глава 3	62
Блокчейн-технология – новая и высокоэффективная модель организации деятельности	62
Распределенные организационные модели, устойчивые к цензуре	65
Namecoin – децентрализованная система доменных имен	67
Цифровая идентификация	70
Цифровая собственность: службы аттестации блокчейна (нотариальные службы, защита интеллектуальной собственности)	73
Блокчейн-правительство	80
Глава 4	89
Наука на блокчейне: Gridcoin, Foldingcoin	89

Блокчейн и геномика	92
Блокчейн и здравоохранение	96
Блокчейн-обучение: MOOC биткойна и умные контракты на обучение	99
Научные публикации в блокчейне: Journalcoin	101
Блокчейн может не все	104
Баланс между централизацией и децентрализацией	105
Глава 5	106
Терминология и концепции	106
Валюта, токен, токенизация	108
Множественность валют: монетарные и немонетарные валюты	113
Демередж валюты: побуждение к действию и перераспределение	114
Глава 6	117
Технические сложности	118
Возможные улучшения	121
Сложности бизнес-модели	123
Скандалы и восприятие обществом	124
Государственное регулирование	126
Проблемы конфиденциальности персональных данных	128
Итог: тенденции к децентрализации сохраняются	129
Глава 7	130
Блокчейн как информационная технология	131
Приложение А	135
Краткий экскурс в асимметричную криптографию	136
Приложение Б	138
Приложение В	141
Благодарности	142

Мелани Свон Блокчейн Схема новой экономики

© 2015 Melanie Swan. All rights reserved.

© Перевод на русский язык, оформление, издание. Издательство «Олимп – Бизнес»,
2017

* * *

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 Quantified 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 системе¹, основанной на публично доступной книге учета, именуемой «блокчейном».

По сути – это новая форма денег, комбинирующая одноранговый обмен файлами² 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 пираты. – *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.webopedia.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 ICANN⁵ 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 структур⁸.

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 гено типа 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 документа¹⁰. 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, залоговыми, 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 онлайн-вая 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-технология*, *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 (фиатные¹⁴) 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. *fiducia* – 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 мейнфреймы¹⁵, 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, Fitbit¹⁷), 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, блокчейн¹⁸

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 долларов¹⁹. Для управления транзакциями между этими устройствами потребуются «интернет денег»²⁰ и соответствующая криптовалюта, а микроплатежи между подключенными устройствами могут развиваться в новый уровень экономики²¹. 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-соединений²². 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 кото-

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 Artificial 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-artificial-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-enabled-m2m-payments-internet-things.html>

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

рой 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 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 дружелюбный 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-дружелюбным 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-технологии 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-технологии 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 Bitfilm, в котором участвуют фильмы, посвященные биткойну, 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 Bitfilm), Сеуле, Буэнос-Айресе, Амстердаме, Рио-де-Жанейро и Кейптауне. Естественно, Bitfilm позволяет зрителям голосовать за понравившийся фильм биткойнами. Фестиваль продюсирует компания Bitfilm. 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 *Bitflect*

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 юрисдикций 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 блокчейном 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 мира²³. 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 действия²⁶.

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.

«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

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://financialcryptography.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/>

реть поток транзакций пользователя, нужно ввести его биткойн-адрес, например *1DpZHXi5bEjNn6SriUKjh6wE4HwPFBPvfx*.

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 биткойн-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 компью-

тере 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 Харо. 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* – «перемешивание» своих монет с транзакциями других пользователей для достижения максимальной конфиденциальности транзакций. Эту задачу решают такие сервисы, как Dark Coin, Dark Wallet и BitMixer²⁷. 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-технология* (пользователь самостоятельно инициирует каждую транзакцию), а не *pull-технология* (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 Европе²⁸. 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 терми-

²⁷ CIPHER (псевдоним), «The Current State of Coin-Mixing Services», сайт Depp.Dot.Web, 25 мая 2014 г., <http://www.deppdotweb.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/>

налах (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 PayByCoin²⁹ в бухгалтерской программе для малых предприятий QuickBooks компании Intuit.

²⁹ Patterson, J., «Intuit Adds BitPay to PayByCoin», блог Bitpay, 11 ноября 2014 г., <http://blog.bitpay.com/2014/11/11/intuit-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 развиваться 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 экономики: 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 применения³¹. 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 упал³³.

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 юани³⁴. По этой цифре трудно оценить мас-

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/kitcone-ns/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://www.coindesk.com/yuan-trades-now-make-up-over-70-of-bit-coin-volume/>

штабы 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.

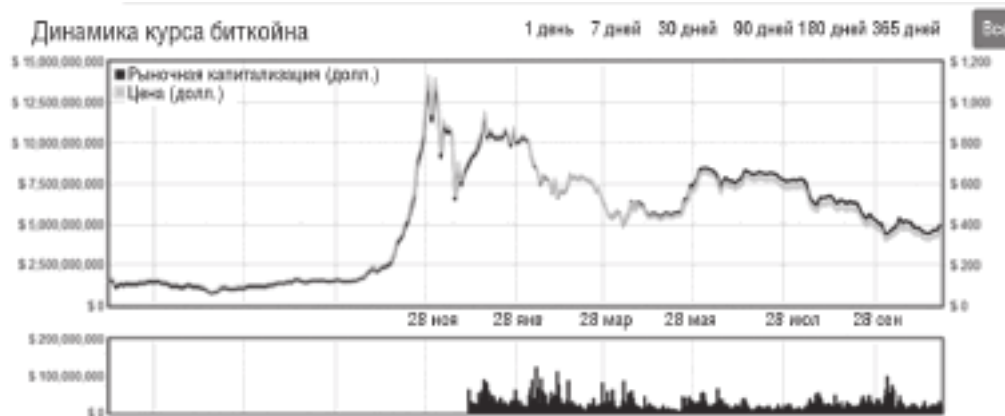


Рисунок 1–2. Курс биткойна с 2009 года по ноябрь 2014 года (источник изображения: <http://coinmarketcap.com/currencies/bitcoin/#charts>)

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 евро³⁷. 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 пределах ограничено.

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-bit-coin-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/dollar-backed-digital-currency-aims-to-fix-bitcoins-volatility-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-eliminate-bitcoin-price-volatility/>

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.).

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 Auorgacoïn), Киргизия и Вьетнам³⁸. 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 юанях³⁹. Некоторые официальные органы Германии, Франции, Кореи и Таиланда высказались негативно по отношению к биткойну⁴⁰.

Европейская служба банковского надзора, Швейцария, Польша, Канада и США продолжают оценивать различные аспекты криптовалют и биткойна⁴¹. 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 продажу⁴².

Налоговое управление США рассматривает биткойн как актив, подобный ценным бумагам, а не как деньги, подразумевая, что транзакции в биткойнах облагаются налогами на прирост капитала⁴³. 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 валюту⁴⁴.

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-financial-companies-from-bitcoin-transactions.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/products/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 денег⁴⁵ и контрактов. В 2010 году Сатоши Накамото заявил следующее: «Архитектура [криптовалюты] поддерживает огромное разнообразие транзакций, которые я разработал несколько лет назад – эскроу-транзакции⁴⁶, 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 формирования⁴⁸. 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, Netflix 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

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/>

же децентрализованной модели технической архитектуры криптовалюты трехуровневого стека: блокчейн, протокол и валюта.

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

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>

Класс	Примеры
Общие	Сделки эскроу, гарантийные обязательства, трехсторонний арбитраж, многосторонняя подпись
Финансовые транзакции	Ценные бумаги, акции компаний, крауд-фандинг, 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, номерам отелей, арендованным или находящимся 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-технологии 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 посредников⁵⁰. 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 биржи⁵¹.

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 GoCoin⁵². 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-партнерами⁵⁵. Очевидно, что есть потребность в адаптации для биткойна стандартных финансовых услуг, таких как

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-first-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://on-line.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/fidor-bank-part-ners-kraken-create-cryptocurrency-bank/>

сберегательные счета и кредитование; возможно, с предложением пользователям опций по уровню частичного резерва.

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/XBT⁵⁶. Стартап Vaugum, 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 биткойнах⁵⁷. Buttercoin является партнером финансовой компании Wedbush Securities. Эта компания, занимающаяся финансовым анализом, одна из первых стала изучать 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 клирингом⁵⁸ и расчетами по ценным бумагам. В частности, такую задачу предстояло решить проекту Medici, инициированному в октябре 2014 года онлайн-ритейлером Overstock и Counterparty, одной из первых платформ Биткойн 2.0⁵⁹. Его целью является создание децентрализованного фондового рынка для ценных бумаг на основе модели блокчейна⁶⁰.

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/files/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 однорангового 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 поддерживают⁶¹.

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 года⁶². Владея собственной криптовалютой инкубатора – Swarmcoin, инвесторы имеют право на дивиденды от стартапов из портфолио инкубатора⁶³.

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 вечеринок⁶⁴.

Еще одна платформа краудфандинга – Koinify, которая имеет на данный момент единственный проект – децентрализованную социальную сеть Gems и привязана к финансовой платформе Melotic⁶⁵. 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 инвестиций⁶⁶.

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 bitFlyer⁶⁷.

Краудфандинг – популярная тема обсуждения на конференциях биткойн-индустрии, вызывающая ожесточенные споры о легальных аспектах этого способа привлечения

⁶¹ Ayal, 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-first-decentralized-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-crowdfunding-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-to-bring-order-to-crypto-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-corporation-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/>

средств. Оппоненты ссылаются на то, что в настоящее время невозможно законно заниматься краудфандингом, если сделки на краудфандинговой 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 Predictionous и Fairlay⁶⁸. 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-simulation-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 займу, 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/>)

⁶⁹ Не имею никакого отношения к этому автору!

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 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-технологий⁷⁰.

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 выгодным⁷¹.

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 испол-

⁷⁰ Swan, M., «Identity Authentication and Security Access 2.0», блог Broader Perspective, 7 апреля 2013 г., <http://futureimes.blogspot.com/2013/04/identity-authentication-and-security.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

нения⁷². 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 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 форумах⁷³.

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

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-wallet-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 выполняются⁷⁴.

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 законом⁷⁵. 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

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.

или потребовать от него возместить от него ущерб в судебном порядке). Соответственно, нормативно-правовая база, по сути, 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 бабушки. 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 онлайн-базу данных реестра смертей, заранее определенную интернет-газету некрологов или любой другой информационный источник, подтверждающий смерть бабушки. После подтверждения факта смерти умный контракт может автоматически отправить деньги⁷⁶. 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 разворачивать 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/future-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 Stripe⁷⁷. Существуют и другие компании, имеющие API-кошельки с многосторонней подписью, – Block.io, Gem и BlockCypher.

Потребуется 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 Briefly 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 вирусов⁷⁸. 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 требуется, нужна система наподобие Internet Archive и Wayback Machine. Ведь потребуются 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

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>

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 хранения 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.

Ethereum: Тьюринг-полная виртуальная машина

Блокчейн-технология объединяет концепции и операции из разных областей, включая вычисления, сети коммуникаций, криптографию и искусственный интеллект (ИИ). В первоначальном плане Сатоши Накамото было три этапа, и только два из них были реализованы в Биткойн 1.0: блокчейн (децентрализованный общедоступный журнал записей транзакций) и протокол Биткойн (система транзакций для перемещения стоимости без участия третьей стороны), что позволило вести денежные расчеты. Но для приложений следующего уровня сложности Блокчейн 2.0, например для записи и передачи умных активов и умных контрактов, необходим третий этап: более мощная система языка скриптов на блокчейне и, в конечном счете, полнота по Тьюрингу этого языка. Это даст способность запускать любую монету, протокол или блокчейн. Накамото предполагал не только отправку денег из точки А в точку Б, но и по-настоящему программируемые деньги, с полным набором необходимых для этого функций. Одним из проектов инфраструктуры блокчейна, призванным поддерживать Тьюринг-полный язык скриптов и платформу, является Ethereum.

Ethereum – это платформа и язык программирования для создания и публикации распределенных приложений. В фундаментальном контексте Ethereum представляет собой основополагающую криптовалютную платформу общего назначения, которая является Тьюринг-полной виртуальной машиной. Это означает, что поверх нее можно запустить любую монету, сценарий или криптовалютный проект.

В отличие от других проектов, Ethereum – это не блокчейн, не протокол на основе блокчейна и не метапротокол на основе протокола. Ethereum – это фундаментальная базовая платформа инфраструктуры, которая может запускать различные распределенные журналы записей и протоколы, что-то вроде универсальной платформы разработки. Каждый полный узел в сети Ethereum запускает виртуальную машину Ethereum для бесперебойного выполнения умных контрактов данной платформы. Ethereum является независимой от протоколов платформой для разработки основанных на умных контрактах приложений, которые могут вызывать несколько других распределенных журналов записей, протоколов и криптовалют.

Ethereum имеет собственную распределенную экосистему, которая уже на уровне замысла включала в себя функции обслуживания файлов, отправки сообщений и подтверждения репутации. Первый компонент – это Swarm (не путайте Ethereum-Swarm с сайтом краудфандинга Swarm) как метод децентрализованного обслуживания файлов. Второй компонент – это Whisper (Ethereum-Whisper также не следует путать с похожими по названию проектами), представляющий собой одноранговый протокол для отправки секретных сообщений и цифрового шифрования. Третий компонент – это система репутации, формирующая репутацию и снижающая риск контрагента в ненадежной сети. Возможно, она будет основана на системе TrustDavis⁷⁹ или идеях, разработанных в хакатонском проекте Crypto Schwartz⁸⁰.

⁷⁹ Atkin, A., «TrustDavis on Ethereum», сайт Slideshare, 19 июня 2014 г., <http://www.slideshare.net/aatkin1971/trustda-vis-on-ethereum>

⁸⁰ Galt, J., «Crypto Swartz Will Get You Paid for Your Great Content», блог The CoinFront, 23 июня 2014 г., <http://thecoinfront.com/crypto-swartz-will-get-you-paid-for-your-great-content/>

Counterparty повторно создает платформу умных контрактов Ethereum

В ноябре 2014 года компания Counterparty объявила о встраивании языка программирования с открытым исходным кодом Ethereum в свою платформу⁸¹. Фактически Counterparty перенесла технологические инновации Ethereum на платформу существующего де-факто блокчейн-стандарта – биткойна. В результате работать с умными контрактами можно уже сейчас, не дожидаясь запуска собственного распределенного журнала записей Ethereum, появление которого, по данным на ноябрь 2014 года, ожидалось в первом квартале 2015 года.

Это объявление было признаком динамичного развития в отрасли, а также быстрых инноваций, которые оказались возможны благодаря концепции открытого исходного кода – как и большинство проектов индустрии блокчейна, ПО Ethereum и Counterparty имеют открытый исходный код. Любой пользователь или разработчик может свободно изучать коды других проектов, работать с ними и применять их в собственных реализациях – именно в этом заключается принцип и цель существования ПО с открытым исходным кодом. Это означает, что хорошие идеи могут быстрее распространяться, стандартизироваться и улучшаться благодаря общему аудиту качества и вкладу многих независимых разработчиков. У Ethereum и Counterparty имеется глубокое видение будущей архитектуры блокчейн-технологии и децентрализации. Заложив инфраструктурные уровни на раннем этапе процесса, в дальнейшем можно двигаться на следующие уровни⁸². Учитывая взаимозаменяемость функциональности в некоторых протоколах и платформах в блокчейн-индустрии, главный вопрос, возможно, заключается в том, какие виды сервисов с добавленной стоимостью будут строиться поверх этих уровней инфраструктуры, – то есть какими станут Netscape, Amazon и Uber.

⁸¹ Prisco, G., «Counterparty Recreates Ethereum on Bitcoin», сайт CryptoCoins News, обновлено 12 ноября 2014 г., <https://www.cryptocoinsnews.com/counterparty-recreates-ethereum-bitcoin/>. См. также: «Counterparty Recreates Ethereum's Smart Contract Platform on Bitcoin», пресс-релиз компании Counterparty, <http://counterparty.io/news/counterparty-rec-creates-ethereums-smart-contract-platform-on-bitcoin/>

⁸² Swan, M., «Counterparty/Ethereum: Why Bitcoin Topped \$450 Today (Was Under \$350 Last Week)», блог Broader Perspective, 12 ноября 2014 г., <http://futurememes.blogspot.com/2014/11/counterpartyethereum-why-bitcoin-topped.html>

Децентрализованные приложения, организации, компании и общества: все более автономные умные контракты

Каково же направление движения? Итак, первыми классами приложений блокчейна являются денежные расчеты. Далее идут все виды финансовых сделок; затем – умные активы, представляющие и реальные (дом, автомобиль) и нематериальные (интеллектуальная собственность, ИС) активы как цифровые активы; затем – реестры государственных документов, легальная аттестация, нотариальное заверение и ИС-сер-висы. И, наконец, умные контракты, которые могут оперировать всеми этими типами цифровых активов.

Со временем умные контракты могут стать очень сложными и автономными. Децентрализованные приложения, организации, компании, общества, автоматические рынки и торговые сети – вот некоторые из более сложных концепций, предусмотренных для последующих применений блокчейна. Если не углубляться в детали, главная идея состоит в том, что умные контракты (Блокчейн 2.0; более сложные сделки, чем платежи и переводы валюты) повысят уровень автономности, на котором работают эти умные контракты. Простейшим умным контрактом может быть пари двух сторон о прогнозе максимальной температуры воздуха на завтра. Завтра контракт может быть автоматически исполнен программой, проверяющей официальные показания температуры (из заранее определенного источника или прогноза, например Weather.com) и переводящей биткойны из эскроу со счета проигравшего на счет победителя.

Децентрализованные приложения

Dapp, DAO, DAC и DAS – это аббревиатуры, обозначающие, соответственно, децентрализованные приложения (decentralized applications), децентрализованные автономные организации (decentralized autonomous organizations), децентрализованные автономные корпорации (decentralized autonomous corporations) и децентрализованные автономные общества (decentralized autonomous societies). Эта группа понятий означает рост сложности и степени автоматизации умных контрактов, которые больше напоминают самодостаточные образования, выполняющие предварительно запрограммированные, а по сути – самопрограммируемые операции, привязанные к блокчейну.

В некотором смысле все протоколы Блокчейн 2.0 в распределенных приложениях подобны Блокчейн 1.0 (блокчейн – это фактически децентрализованное приложение, обслуживающее общедоступный журнал записей транзакций). Существуют различные определения децентрализованного приложения. К примеру, создатели Ethereum определяют умный контракт/децентрализованное приложение как протокол транзакций, который выполняет условия контракта или группы контрактов в криптографически защищенном блокчейне⁸³.

Рабочее определение автора книги выглядит так: децентрализованное приложение – это приложение, которое работает в сети распределенно, при этом информация об участниках надежно (возможно, с использованием псевдонимов) защищена, а выполнение операций децентрализовано в разных узлах сети. Некоторые действующие примеры приведены в таблице 2–4. Это OpenBazaar (децентрализованный Craigslist), LaZooz (децентрализован-

⁸³ «DEV PLAN», сайт Ethereum, прочитано в 2014 г., <https://www.ethereum.org/pdfs/Ethereum-Dev-Plan-preview.pdf>

ный Uber), Twister (децентрализованный Twitter), Bitmessage (децентрализованный сервис СМС) и Storj (децентрализованное хранилище файлов)⁸⁴.

Другая группа разработчиков в совместном официальном описании предлагает более строгое определение децентрализованного приложения⁸⁵. В их представлении децентрализованное приложение должно иметь три характеристики. Во-первых, полностью открытый исходный код, работающий автономно таким образом, что никто не контролирует большинство его токенов, а данные и записи работы хранятся в криптографически защищенном виде в общедоступном децентрализованном журнале записей. Во-вторых, приложение должно генерировать токены согласно стандартному алгоритму или устанавливать критерии и, по возможности, способы распределения части или всех токенов в начале работы. Эти токены необходимы для использования приложения, и любой вклад пользователей должен вознаграждаться токенами. В-третьих, приложение может адаптировать свой протокол в ответ на предлагаемые улучшения и отзывы на рынке, но любые изменения требуют консенсуса большинства пользователей. Впрочем, в настоящее время каждый проект блокчейна может иметь несколько иное представление о конкретных технических деталях децентрализованного приложения.

Таблица 2–4. Примеры децентрализованных приложений

⁸⁴ Finley, K., «Out in the Open: An NSA-Proof Twitter, Built with Code from Bitcoin and BitTorrent», журнал *Wired*, 13 января 2014 г., <http://www.wired.com/2014/01/twister/>

⁸⁵ Johnston, D. et al., «The General Theory of Decentralized Applications, DApps», сайт GitHub, 9 июня 2014 г., <https://github.com/DavidJohnstonCEO/DecentralizedApplications>

Имя и URL-адрес проекта	Функции	Централизованный аналог
OpenBazaar https://openbazaar.org/	Купля-продажа товаров на локальных реальных рынках	Craigslist
LaZooz http://lazooz.org/	Совместное использование транспортных средств, включая Zooz, монета с технологией proof-of-movement («Доказательство движения»)	Uber
Twister http://twister.net.co/	Социальная сеть, одно-ранговые микроблоги ⁶⁶	Twitter/Facebook
Gems http://getgems.org/	Социальная сеть, сообщения с токенами	Twitter/CMC
Bitmessage https://bitmessage.org	Отправка защищенных сообщений (отдельные сообщения или массовая рассылка)	Сервисы CMC-сообщений
Storj http://storj.io/	Хранение файлов	Dropbox
Swarm https://www.swarm.co/ Koinify https://koinify.com/ bitFlyer http://fundflyer.bitflyer.jp/	Платформы криптовалютного краудфандинга	Kickstarter, Indiegogo, фонды венчурного капитала

Децентрализованные автономные организации и корпорации

Децентрализованная автономная организация – более сложная форма децентрализованного приложения. Для того чтобы стать полноценной организацией, децентрализованное приложение должно содержать более сложную функциональность, например конституцию, которая явно обозначила бы его управление в распределенном журнале записей, а также механизм финансирования его операций, например выпуск ценных бумаг через краудфандинг. Децентрализованные автономные организации/ корпорации – это концепция, заимствованная из области искусственного интеллекта. В этой концепции децентрализованная сеть автономных агентов выполняет задачи, которые могут создаваться в модели

корпорации, работающей без участия человека под управлением набора бизнес-правил⁸⁶. В децентрализованных организациях/корпорациях существуют умные контракты как агенты, работающие в блокчейне и выполняющие заранее определенные или одобренные задачи в зависимости от событий и изменяющихся условий⁸⁷. Помимо того что группы умных контрактов, работающих на блокчейне, начнут создавать экземпляры моделей автономной корпорации, в качестве блокчейн-модели могут быть переосмыслены также функции и работа реальных предприятий. Подобно тому как транзакции с биткойном обновляют финансовый рынок и повышают его эффективность, децентрализованные организации и корпорации могут аналогичным образом влиять на предприятия. Оператор денежных переводов нередко несет большие расходы, связанные с поддержкой офисов и местным законодательством. То же самое относится и к предприятиям, работающим в соответствии с местным законодательством (лицензирование бизнеса, регистрация, страхование и налогообложение) на многих муниципальных и регуляторных уровнях. При переходе на блокчейн некоторые из этих функций можно было реорганизовать более эффективным образом или вовсе от них отказаться, чтобы каждое предприятие действительно работало в глобальном масштабе. Автономные предприятия в облаке, действующие на базе блокчейна и работающие на основе умных контрактов, могли бы заключать электронные договоры с соответствующими организациями, например с правительствами, чтобы самостоятельно регистрироваться под любой юрисдикцией, под которой они хотят работать. Каждое предприятие может быть прежде всего общим универсальным предприятием, а затем уже предприятием под юрисдикцией, когда будут приняты более эффективные решения о юрисдикциях. Это же касается и физических лиц, которые прежде всего являются людьми и только после этого – гражданами.

Одним из примеров децентрализованной организации/корпорации в контексте автоматической работы умных контрактов является Storj. Как было сказано выше, Storj – это децентрализованная платформа облачных хранилищ, которая в августе 2014 года осуществила краудфандинг на сумму 461 802 долларов⁸⁸. Storj использует терминологию распределенного журнала записей биткойна и одноранговые протоколы для обеспечения безопасного, частного и зашифрованного хранения в облаке. Два приложения – DriveShare и MetaDisk – позволяют пользователям сдавать в аренду неиспользуемое пространство на жестком диске и хранить файлы в сети Storj. В других моделях сообщества, например Folding@home и BOINC, программы которых использует SETI@home, разработаны способы безопасного совместного использования пространства жесткого диска. Разумеется, как и в случае с любым распределенным проектом, подразумевающим предоставление общего доступа к компьютеру, необходимо соблюдать бдительность, а участники Storj или другого аналогичного проекта должны подробно ознакомиться с правилами безопасности. Токен альткойна Storj, Storjcoin X (SJCX), – это криптовалюта на основе протокола Counterparty. Эта валюта используется для покупки пространства в сети Storj через MetaDisk и выплат провайдерам хранилища DriveShare. Storj рассматривается как децентрализованная альтернатива провайдерам хранилищ вроде Dropbox или Google, пользователи которых, согласно расчетам компании, пере-

⁸⁶ Babbitt, D., «Crypto-Economic Design: A Proposed Agent-Based Modeling Efort», конференция «SwarmFest 2014: 18th Annual Meeting on Agent-Based Modeling & Simulation», Университет Нотр-Дам, г. Нотр-Дам, шт. Индиана, с 29 июня по 1 июля 2014 г., <http://www3.nd.edu/~swarm06/SwarmFest2014/Crypto-economicDesignBabbitt.pdf>

⁸⁷ Butarin, V., «Bootstrapping a Decentralized Autonomous Corporation: Part I», журнал *Bitcoin Magazine*, 19 сентября 2013 г., <http://bitcoinmagazine.com/7050/bootstrapping-a-decentralized-autonomous-corporation-part-i/>; Bontje, J., «Ethereum – Decentralized Autonomous Organizations», сайт Slide-share, 9 апреля 2014 г., <http://www.slideshare.net/mids106/ethereum-decentralized-autonomous-organizations>; Ethereum (EtherCasts), «Egalitarian DAO Contract Explained», видеоролик на YouTube, 3 апреля 2014 г., https://www.youtube.com/watch?v=Q_gxDytSvuY

⁸⁸ Spaven, E., «Cloud Storage Startup Storj Raises 910 BTC in Crowdsale», сайт CoinDesk, 22 августа 2014 г., <http://www.coindesk.com/cloud-storage-startup-storj-raises-910-btc-crowdsale/>

плачивают за хранение данных в 10-100 раз, в то время как методы блокчейна могли бы обеспечить им более безопасное и децентрализованное хранение данных⁸⁹.

Децентрализованные общества и самоограничивающиеся организации

По мере развития и продвижения блокчейн-технологии могут возникнуть децентрализованные автономные общества – по сути, множества умных контрактов, или целые экосистемы децентрализованных приложений, организаций и корпораций, работающих автономно. Уже появилась интересная концепция, связанная с интеллектуальной собственностью и новыми идеями, – самоограничивающаяся организация⁹⁰. Это новая бизнес-идея, возникшая на основе блокчейна и предложенная кем-то из пользователей. Самоограничивающаяся организация расширяется и становится отдельной сущностью со стандартизированным умным контрактом и самозагружающейся программой для самостоятельного краудфандинга в зависимости от основных целей: работать; выплачивать дивиденды или иное вознаграждение инвесторам краудфандинга; получать отзыв (автоматический или управляемый) через рынки прогнозов блокчейна и децентрализованное голосование в распределенном журнале записей; в конечном итоге прекращать деятельность или периодически проводить голосования по подтверждению создания нового экземпляра (confirmation-of-instantiation) аналогично продлению и пересмотру сроков контракта. Важно тщательно предусмотреть условия автоматического прекращения или продления деятельности, чтобы избежать ситуаций, описанных в научно-фантастических книгах Даниэля Суареса «Демон» и «Свобода» («Freedom»), в которых мировая экономика радикально меняется под влиянием агентов, исполняющих умные контракты, которые неумолимо следуют своему запрограммированному коду.

Автоматические рынки и торговые сети

Автоматический рынок – совокупность автоматических транзакций, проводимых с унифицированными, пакетированными и разбитыми на подгруппы ресурсами (первоначально электричество, газ, пропускная способность сети, а в далеком будущем – синаптические возможности мозга) в зависимости от динамически изменяющихся условий и заранее запрограммированных профилей пользователей, условий и функций торгов⁹¹. Наиболее близкими из существующих примеров автоматических рынков являются алгоритмическая торговля на рынке ценных бумаг и торги в реальном времени. В будущем автоматические рынки могут найти применение в контексте лимитных заявок и программного трейдинга для распределения реальных ресурсов. По-настоящему интеллектуальные сети (например, сети энергии, трасс и трафика) могут обладать функциями автоматических торгов как для расходной, так и для доходной части своих операций. Это касается как исходных данных (ресурсы), так и результатов (клиенты), а также механизмов автоматической очистки. Схожей идеей являются торговые сети: совокупность самостоятельно работающих и принадле-

⁸⁹ Marckx, C., «Storj: Next-Generation Cloud Storage Through the Blockchain», сайт CryptoCoins News, обновлено 11 апреля 2014 г., <https://www.cryptocoinsnews.com/storj-next-generation-cloud-storage-through-the-blockchain/>

⁹⁰ Levine, A. B., «Application Specific, Autonomous, Self-Bootstrapping Consensus Platforms», форум Bitsharestalk, 1 января 2014 г., <https://bitsharestalk.org/index.php?topic=1854.0>

⁹¹ Swan, M., «Automatic Markets», блог Broader Perspective, 23 августа 2009 г., <http://futurememes.blogspot.com/2009/08/automatic-markets.html>

жащих самим себе активов наподобие самоуправляемого и самодостаточного автомобиля⁹². Самоуправляемые активы будут самостоятельно торговать в соответствии с данными, получаемыми в реальном масштабе времени из интернета, оценивая динамический спрос, заключая контракты с потенциальными клиентами (как это сейчас делает Uber), хеджируя рост цен на нефть с помощью собственного прогнозного планирования ресурсов и, наконец, самостоятельно прекращая свою деятельность после выполнения всех этапов самостоятельной работы. В торговые сети даже могут быть встроены автоматически выполняющиеся умные контракты для запуска производства новых товаров – в зависимости от данных о росте численности населения, спроса и актуальности бизнес-плана.

⁹² Hearn, M., «Future of Money (and Everything Else)», Эдинбургский международный фестиваль, видеоролик на YouTube, 23 августа 2013 г., <https://www.youtube.com/watch?v=Pu4PAMFPo5Y>

Блокчейн как путь к искусственному интеллекту

Умные контракты следует рассматривать как децентрализованные автономные приложения, работающие под псевдонимами на основе блокчейна. Таким образом, распределенный журнал записей мог бы стать одним из возможных путей к искусственному интеллекту, так как платформы умных контрактов создаются для работы в условиях постепенного повышения автоматизации, автономности и сложности. В условиях распространения децентрализованных приложений, организаций, корпораций и обществ может появиться много новых видов непредсказуемого и сложного поведения, напоминающего искусственный интеллект (ИИ). Один из возможных путей заключается в том, чтобы встроить в блокчейн существующие системы, основанные на правилах, не относящихся к ИИ и блокчейну. Это позволит повысить автоматизацию и эффективность таких операций. Такими системами могут быть, например, системы моделирования поведения вроде «if-this-then-that» (IFTTT) и платформы Huginn с открытым исходным кодом для создания агентов, отслеживающих ситуацию и действующих от имени пользователя. Второй возможный путь – это реализация программных идей из областей исследования ИИ, например клеточных автоматов Wolfram, игры «Жизнь» Джона Конвея, муравьиного алгоритма *Ant Colony*, роевого интеллекта, когнитивных роботов Энди Кларка и других систем, основанных на работе агентов.

Глава 3

Блокчейн: приложения для применения за рамками финансовых областей (Блокчейн 3.0)

Блокчейн-технология – новая и высокоэффективная модель организации деятельности

Блокчейн-технология может изменить не только все, что связано с денежными рынками, платежами, финансовыми услугами и экономикой, но и все остальные индустрии и, более того, почти все области человеческой деятельности. Блокчейн – фундаментально новая парадигма, позволяющая организовывать деятельность с меньшими усилиями, более эффективно и гораздо более масштабно, чем другие существующие парадигмы. Децентрализация как общая модель может эффективно работать в том случае, если существует гибкая всеобщая сеть, позволяющая выполнять транзакции без посредников.

Но дело не только в том, что блокчейн-технология децентрализована. Она обеспечивает универсальность и глобальный масштаб, немыслимые прежде. Она может применяться для автоматизированного распределения любых ресурсов, включая материальные активы и кадровые ресурсы.

Блокчейн-технология облегчает координацию всех видов человеческого взаимодействия, помогает эффективно организовать совместную работу и, вероятно, готовит почву для перевода человеко-машинного взаимодействия на новый уровень. Можно предположить, что все виды человеческой деятельности можно в какой-то степени координировать с помощью блокчейн-технологии или, как минимум, перестроить с использованием концепций блокчейна. Организационная модель блокчейн-технологии более эффективна с функциональной, практической и количественной точек зрения. Поскольку блокчейн-технология требует достижения консенсуса, она обеспечивает значительно большую свободу, равенство и вовлеченность, чем существующие системы. Таким образом, блокчейн – готовое решение, применение которого дает разнообразные преимущества, как количественные, так и качественные.

Возможность расширения блокчейн-концепций

Блокчейн-технология может раскрыть творческое и изобретательское начало в каждом, кто понял ее концепции. Необходимо осваивать новые идеи – как в целом, так и отдельные концепции, включая криптографию с открытым и закрытым ключами, пиринговый обмен файлами, распределенные вычисления, сетевые модели, псевдонимность, журнал записей блокчейна, криптовалюты и их протоколы. Все перечисленное ставит под сомнение непоколебимость традиционных составляющих современного мира, таких как наличные деньги, экономии – ка, доверительные отношения, стоимость, биржевые механизмы. Современный человек, желающий работать в среде блокчейн-технологий, обязан знать и понимать новые концепции. Такое понимание позволит не только создавать инновационные решения на базе технологий блокчейна, но и переносить эти концепции в другие контексты. Благодаря расширяемости концепций блокчейн-технология сможет серьезно влиять на человечество, по мере того как люди будут осваивать эти концепции и переносить их в различные области деятельности. Яркий пример такой универсальности применения и расширяемости основ-

ных технологических концепций – интернет. Все можно делать по-новому: быстрее, шире, дешевле, в реальном масштабе времени, по запросу, через всемирную сеть. Блокчейн-технология богата новыми концепциями, которые могут стать неотъемлемой частью интеллектуального багажа и профессионального набора знаний современного человека.

Фундаментальные экономические принципы: признание ценности, определение стоимости и организация обмена

Чтобы понять, как применять концепции блокчейна вне исходного контекста, следует научиться находить во всем сходство с экономикой, рынком и денежными средствами. Не менее важно отчетливо видеть *различия* с экономикой. Такое мышление требует умения распознавать фундаментальные аспекты экономики и рынков в повседневных ситуациях. Блокчейн-технология помогает осознать, что все, что мы видим и испытываем, каждая система в нашей жизни в какой-то степени является экономической системой, системой распределения ресурсов. Более того, системы и взаимодействия аналогичны экономике в том смысле, что в них происходит получение информации и поиск объектов, определение стоимости, взаимодействие и обмен с помощью какого-то механизма – денег или их аналога, либо просто обмен силой, энергией или концентрацией (как в биологических системах). Такую базовую экономическую структуру можно назвать универсальной: она присутствует и в групповой работе, и на фермерском рынке. Дискретная структура блокчейн-технологии, позволяющая следить за транзакциями с помощью единого журнала записей, дает на несколько порядков больше информации, чем существующие сейчас системы учета и планирования ресурсов.

Система отслеживания ресурсов при помощи блокчейна позволяет автоматически и без задержек оценивать последствия любых транзакций с участием всех вовлеченных сторон и анализировать их на макроуровне. Этого можно не делать, если система ценностей сообщества запрещает явное отслеживание активности пользователей. Морально-этические нормы контроля – отдельная интересная тема для будущих социологических и научных исследований. Как бы то ни было, для отслеживания в системах блокчейна можно, например, объединить принципы биткойна и GitHub, чтобы оценивать вклад в общий проект построчно после всех ревизий кода. Это важно, поскольку экономически грамотные и рационально настроенные агенты, работающие с системой (в настоящее время это люди), хотят отслеживать внесенный ими и другими участниками вклад, оценивать его, подтверждать и зарабатывать различные награды – деньги, статусы, репутацию и т. д.

Блокчейн-технология позволяет администрировать любые дискретные единицы

Блокчейн может облегчить автоматизацию вычислений, предлагая единую универсальную модель координации деятельности, поддерживающую почти бесконечное число транзакций. Эта универсальная система транзакций может иметь размах, немыслимый прежде. В некотором смысле блокчейн-технология может стать суперкомпьютером для реальной жизни. Венчурный инвестор Дэвид Джонстон, вкладывающий средства в проекты на основе блокчейна, уверен в эффективности и превосходстве модели блокчейна. Все, что может быть децентрализовано, считает он, будет децентрализовано. Децентрализация – это «то, куда течет вода», следуя по пути наименьшего сопротивления. Блокчейн может стать «бритвой Оккама»⁹³, наиболее эффективным, прямым и естественным средством координа-

⁹³ Бритва Оккама – методологический принцип, который гласит: «Не следует умножать сущности без особой необхо-

ции всей человеческой и машинной деятельности, соответствующим естественному стремлению к равновесию.

Блокчейн и предиктивная автоматизация с использованием больших данных

Большие данные⁹⁴ позволяют выполнять предиктивное моделирование огромного числа процессов, происходящих в реальной жизни, а блокчейн-технология может способствовать превращению прогнозов в действие. Блокчейн можно объединить с большими данными, ускорив переход от реагирования к прогнозированию и открыв обширные возможности для автоматизации самых разных задач на основе умных контрактов и экономических механизмов. Предиктивный анализ больших данных отлично сочетается с автоматическим выполнением умных контрактов. Технологию блокчейна можно использовать как встроенную платежную систему и механизм администрирования дискретных данных, реализовав эту функциональность через автоматизированные умные контракты, децентрализованные приложения, децентрализованные автономные организации и децентрализованные автономные корпорации. Автоматическое выполнение огромного спектра задач позволит высвободить операторов, переложив их работу на универсальную, децентрализованную, распределенную по всему миру вычислительную систему. Дискретизация, отслеживание и администрирование любых задач во всех сферах деятельности посредством блокчейн-технологии откроют куда более обширные возможности, чем технологии больших данных, известные сегодня.

димости». Принцип назван по имени английского философа-номиналиста XIV века Уильяма Оккама. – *Прим. ред.*

⁹⁴ Большие данные (*англ.* big data) – многообразные структурированные и неструктурированные данные огромных объемов. В связи со взрывным ростом объемов данных, поступающих из разнообразных источников, характерным для последнего времени, считается, что именно обработка больших данных позволит достичь существенного прогресса в экономике, научных исследованиях и государственном управлении. – *Прим. ред.*

Распределенные организационные модели, устойчивые к цензуре

Основной аргумент в пользу Блокчейн 1.0 и 2.0 – экономическая эффективность и снижение расходов благодаря использованию децентрализованных сетевых моделей, не требующих доверия к единому транзакционному центру. Однако есть и другие важные преимущества – свобода и наделение полномочиями. Децентрализованные модели могут способствовать развитию свободных экономических отношений в странах, в которых строго контролируется движение капитала. Свободу обеспечивают псевдонимные транзакции, недоступные для контроля и регулирования местными властями. Это может быть важно для развивающихся рынков, где контроль капитала, ограничительная экономическая политика и другие факторы затрудняют предпринимательскую деятельность, включая создание новых бизнесов. Государственный контроль и недостаток доверия к фиатным деньгам вызывают рост интереса к криптовалютам.

Свобода, предоставляемая технологиями блокчейна, становится более явной в Блокчейн 3.0, которая позволит на основе блокчейн-технологии реализовать решения, не связанные с денежным обращением и рыночными транзакциями. Глобальная децентрализованная природа блокчейн-технологии дает возможности обхода ограничений, налагаемых географическими юрисдикциями. Существует мнение, что блокчейн-технология позволит объективно решать вопросы свободы, юрисдикции, цензуры и регулирования такими способами, которые, возможно, недоступны государственным и международным организациям, защищающим права человека. Некоторые операции, как бы их ни определяли государственные законы, представляют собой глобальные, транснациональные транзакции, поэтому их администрирование, координацию и мониторинг эффективнее вести на таких организационных уровнях, как Всемирная торговая организация.

Итак, речь идет об освобождении транснациональных организаций от ограничений государственных юрисдикций и их переносе в подлинно глобальное пространство. Во-первых, транснациональной организации требуется транснациональная структура управления. Блокчейн-технология позволяет сделать такую структуру эффективной, обеспечивая масштабность, доступность и прозрачность. Управление с помощью блокчейна лучше отвечает требованиям транснациональных организаций, чем государственное управление. Во-вторых, блокчейн обеспечивает не только более эффективное, но и беспристрастное транснациональное управление. Децентрализованная модель, основанная на облачных решениях, способна предоставить организациям и участникам еще больше равноправия, свободы и справедливости. Распределенный журнал записей обеспечивает невозможность подделки записей, прозрачность и доступность. Любой человек из любой точки мира сможет просмотреть и подтвердить операции транснациональных организаций. Таким образом, блокчейн – это глобальная система сдержек и противовесов, создающая доверие между всеми сторонами. Это тот основной инфраструктурный элемент, который позволит человечеству создать действительно глобальные организации и механизмы координирования и даст дорогу ускоренному прогрессу.

Один из примеров возможного применения блокчейн-технологии – администрирование интернета. Организации, администрирующие интернет, имеют транснациональную сферу компетенции, но базируются в конкретных государствах. Так, организация ICANN управляет IP-адресами и пространством имен и числовых IP-адресов (например, www.example.com – 93.184.216.119) для обеспечения возможности подключения через интернет.

Блокчейн-технология поднимает проблему администрирования транснациональных общественных организаций и одновременно дает решение. Wikipedia – еще один транснациональный проект, в настоящее время находящийся в юрисдикции местных властей, способных влиять на его деятельность и принятие решений. Благодаря демократичности, распределенности и вовлеченности множества участников механизмы блокчейна могут обеспечить наиболее эффективное и беспристрастное администрирование всех транснациональных общественных организаций.

Громкий случай применения судебной власти для влияния на организацию – разбирательство с WikiLeaks и Эдвардом Сноуденом. Отдельные люди пытались финансово поддерживать WikiLeaks, но под давлением правительства операторы кредитных карт и PayPal отказались принимать такие взносы, и на WikiLeaks был наложен запрет⁹⁵. Если бы тогда уже можно было делать взносы в биткойнах, они шли бы напрямую и могли привести к другому исходу дела. Все остальные организации, среди которых некоммерческий Фонд электронных рубежей (Electronic Freedom Foundation, EFF), выступающий в поддержку личной свободы, тоже находятся в юрисдикции местных властей, что всегда несет угрозу вмешательства в их работу и жизнь связанных с ними людей.

⁹⁵ Moshinsky, B. et al., «WikiLeaks Finds Snowden Cash Bump Elusive», журнал *Bloomberg Businessweek*, 11 июля 2013 г., <http://www.businessweek.com/articles/2013-07-11/wikileaks-finds-snowden-cash-bump-elusive>

Namescoin – децентрализованная система доменных имен

Одно из первых применений блокчейн-технологии, не связанное с денежными расчетами, – борьба с цензурой в интернете при помощи Namescoin, альткойна, используемого для регистрации и проверки адресов в доменной системе имен (DNS). Namescoin – альтернативная транснациональная DNS, которую не могут контролировать правительства и корпорации. Преимущества децентрализованной DNS в том, что она позволяет свободно публиковать информацию в интернете всем, кому угрожает давление местных властей и цензура. Как биткойн является никому не принадлежащей децентрализованной валютой, так и Namescoin является основой для децентрализованной DNS (то есть адресов URL)⁹⁶. URL-адреса, перманентно встраиваемые в блокчейн, будут недоступны правительствам, захватывающим домены. Проблема традиционных DNS в том, что центральные власти контролируют домен верхнего уровня (например, в адресе google.com властям США подконтрольна часть *.com*) и могут перехватывать и перенаправлять URL-адреса. Такова ситуация со всеми доменами верхнего уровня; например, Китай контролирует все домены *.cn*. Децентрализованная DNS делает возможным существование независимых доменов верхнего уровня, DNS-таблицы для которых хранятся в пиринговой сети. Альтернативные домены, зарегистрированные в этой системе, будут доступны до тех пор, пока есть добровольцы, у которых запущено ПО децентрализованного DNS-сервера. Власти не могут контролировать домены верхнего уровня, развернутые в пиринговых сетях. На основе структуры, аналогичной биткойну, созданы отдельная криптовалюта (Namescoin, NMC) и блокчейн для децентрализованной DNS.

В настоящее время система Namescoin работает не как система для регистрации всех доменов подряд, а как механизм обеспечения свободы слова для доменов, борющихся с цензурой (например, в странах с ограниченной политической свободой). Домен верхнего уровня для Namescoin – *.bit*. Действия, необходимые для регистрации нового домена или обновления существующего, встроены в протокол Namescoin и основаны на транзакциях. Например, транзакция регистрации «name_new» будет стоить 0,01 NMC (валюту namescoin можно покупать и продавать за биткойны). Домены можно регистрировать в системе Namescoin напрямую или посредством служб регистрации, таких как <https://dotbit.me/>.

Поскольку домен *.bit* находится вне традиционной структуры интернета, для просмотра расположенных в нем веб-сайтов используются прокси-серверы, обрабатывающие DNS-запросы, а также расширения для Firefox и Chrome. Таким образом, домены *.bit* предоставляют механизм обеспечения свободы слова. По данным веб-сайта BitcoinContact, к октябрю 2014 года было зарегистрировано 178 397 доменов *.bit*, включая, например, *wikileaks.bit*. Преимуществами децентрализованных транзакций можно пользоваться не только в сфере финансов, но и во многих других областях.

Другие децентрализованные службы DNS и технические сложности

В реализации Namescoin обнаружены технические проблемы, допускающие захват доменов *.bit* (ошибка, позволяющая обновлять значения, если имя на входе транзакции

⁹⁶ Gilson, D., «What Are Namecoins and .bit Domains?», сайт CoinDesk, 18 июня 2013 г., <http://www.coindesk.com/what-are-namecoins-and-bit-domains/>

совпадает с именем на выходе, и переопределять параметры новой регистрации)⁹⁷. Разработчики исправляют проблему. Критики (как и критики биткойна в целом) также говорят о том, что ключевые особенности децентрализованных служб DNS (дешевое и анонимное создание доменных имен, невозможность централизованного управления) могут с успехом использоваться преступниками⁹⁸. Защитники блокчейн-технологии приводят примеры использования прослеживаемости транзакций в общедоступном журнале записей для поимки преступников, а также множества других законных применений блокчейна⁹⁹.

Тем временем разрабатываются другие децентрализованные службы имен, такие как децентрализованный домен верхнего уровня *.P2P*, предложенный организацией BitShares. Этот проект показывает, что децентрализация DNS устраняет необходимость в посредниках – службах сертификатов (которые могут оставлять URL-адреса уязвимыми к атакам), а модель блокчейна может быть более безопасной, поскольку утратить контроль домена можно только в случае потери соответствующего закрытого ключа¹⁰⁰. DotP2P предлагает дополнительные возможности улучшения реестра DNS, например аукционное определение цены для борьбы с киберсквоттингом. С децентрализованными службами DNS связаны службы идентификации. В октябре 2014 года BitShares запустила службу KeyID (до ребрендинга – Keyhotee), которая предоставляет систему безопасной электронной почты и идентификации на основе децентрализованной блокчейн-технологии¹⁰¹.

Свобода слова и борьба с цензурой: проекты Alexandria и Ostel

Alexandria – один из блокчейн-проектов, поддерживающих свободу слова. Его цель – создание неизменяемых исторических записей путем кодирования и внесения в блокчейн записей из Twitter. Любые твиты, содержащие определенные ключевые слова (например, *Украина* или *Эбола*), кодируются в блокчейне Alexandria при помощи Florincoin, криптовалюты, основанной на коде биткойна, и лайткойна, с быстрой обработкой транзакций (40 секунд) и расширенным полем аннотации (концепция Memecoin). Это позволяет сохранить твиты, которым грозит вмешательство цензуры¹⁰². Основная особенность Florincoin – комментарии к транзакциям. Для записи метаданных и содержимого используется поле длиной 528 символов¹⁰³. Расширенная возможность комментирования может широко применяться во многих проектах на основе блокчейна, например для предоставления метаданных и защищенных указателей на файлы рентгеновских снимков или геномных последовательностей.

Еще один проект, поддерживающий свободу слова, – служба Ostel, обеспечивающая бесплатную зашифрованную телефонную связь по протоколу VoIP (Voice over IP, голос поверх IP). Другие службы, в том числе Skype, могут прослушиваться Агентством национальной

⁹⁷ «Developers Attempt to Resurrect Namecoin After Fundamental Flaw Discovered», сайт CoinDesk, 28 октября 2013 г., <http://www.coindesk.com/namecoin-faw-patch-needed/>

⁹⁸ Wong, J. I., «Trend Micro Report Finds Criminals Unlikely to Abuse Namecoin», сайт CoinDesk, 18 июля 2014 г., <http://www.coindesk.com/trend-micro-report-finds-criminals-un-likely-abuse-namecoin/>

⁹⁹ McArdle, R., Sancho, D., «Bitcoin Domains: A Trend Micro Research Paper», сайт Trend Micro, прочитано в 2013 г. (дата публикации неизвестна), <http://www.trendmicro.com.au/cloud-content/us/pdfs/security-intelligence/white-papers/wp-bitcoin-domains.pdf>

¹⁰⁰ Michael J., «Dotp2p Demo Video», видеоролик на YouTube, 10 июля 2014 г., <https://www.youtube.com/watch?feature=youtu.be&v=qeweF05tT50&app=desktop>

¹⁰¹ BTC Geek, «Bitshares DNS KeyID Starts Trading», блог BTC Geek, прочитано в 2014 г. (дата публикации неизвестна), <http://btcgeek.com/bitshares-dns-keyid-starts-trading/>

¹⁰² Twitter, «Tweets Still Must Flow», 26 января 2012 г., <https://blog.twitter.com/2012/tweets-still-must-flow>

¹⁰³ Dollentas, N., «Exclusive Q&A with Joseph Fiscella: Florincoin and Decentralized Applications», сайт Bitoinist.net, 22 июня 2014 г., <http://bitoinist.net/exclusive-qa-with-joseph-fs-cella-forincoin-and-decentralized-applications/>

безопасности США¹⁰⁴. Ostel – хороший пример описанного Дэвидом Брином¹⁰⁵ противостояния скрытому надзору АНБ (которому подвержены и традиционные телефонные сети, и Skype¹⁰⁶).

Децентрализованные DNS и цифровая идентификация личности

Кроме исходной мотивации к обеспечению свободы слова и противодействию централизованному контролю интернета, функциональность централизованных DNS имеет другие важные применения в развивающейся экосистеме Блокчейн 3.0. Блокчейн позволяет пересмотреть и децентрализовать все операции в интернете, включая службы DNS (Namecoin, DotP2P), цифровую идентификацию (KeyID, OneName, BitID) и обработку сетевого трафика (открытый протокол OpenLibernet.org).

Одна из сложностей, относящихся к системе биткойна, интернету и сетевым коммуникациям в целом, – треугольник Зуко. Эта проблема характерна для любой системы, как-либо идентифицирующей участников сетевого протокола: как сделать идентификаторы, такие как URL-адреса или имена пользователей, например DeMirage99, не только безопасными и децентрализованными, но и удобными для использования человеком (то есть не в виде невнятных 32-разрядных буквенно-цифровых строк)¹⁰⁷. Становление блокчейн-технологий потребует решения этой задачи. Такое решение может предложить служба Namecoin, которая хранит адреса URL и может хранить любую другую информацию. Основная функция Namecoin – хранить и сопоставлять имена и значения. Аналогично тому как биткойн может применяться не только для финансовых операций, Namecoin можно применять не только для определения имен DNS, но и для хранения любой информации. Используя особые пространства имен, можно хранить информацию, которой сложно или небезопасно обмениваться другими способами. Это позволяет нам решить проблему треугольника Зуко, поскольку дает возможность сопоставлять открытый ключ (32-разрядное буквенно-цифровое значение) с удобным для человеческого восприятия именем (DeMirage99). Такую функциональность предоставляют, например, службы цифровой идентификации OneName и BitID.

¹⁰⁴ Chafn, B., «The NSA Can Listen to Skype Calls (Thanks to Microsoft)», журнал *The Mac Observer*, 11 июля 2013 г., <http://www.macoserver.com/tmo/article/the-nsa-can-listen-to-skype-calls-thanks-to-microsoft/>; Goodin, D., «Encrypted or Not, Skype Communications Prove ‘Vital’ to NSA Surveillance», журнал *Ars Technica*, 13 мая 2014 г., <http://arstechnica.com/security/2014/05/encrypted-or-not-skype-communications-prove-vital-to-nsa-surveillance/>

¹⁰⁵ Brin, D., «The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?», Кембридж, МА, издательство Perseus Books Group, 1999 г.

¹⁰⁶ Chafn, B., «The NSA Can Listen to Skype Calls (Thanks to Microsoft)», сайт *The Mac Observer*, 11 июля 2013 г., <http://www.macoserver.com/tmo/article/the-nsa-can-listen-to-skype-calls-thanks-to-microsoft/>

¹⁰⁷ Dourado, E., «Can Namecoin Obsolete ICANN (and More)?», сайт *The Ümlaut*, 5 февраля 2014 г., <http://theumlaut.com/2014/02/05/namecoin-icann/>

Цифровая идентификация

OneName и BitID – примеры служб цифровой идентификации на основе блокчейна, позволяющих подтвердить личность пользователя при обращении к веб-сайту. Децентрализованные службы цифровой идентификации используют тот факт, что все пользователи биткойна имеют персональный кошелек, а кошелек имеет адрес. Это позволяет ускорить доступ к веб-сайтам, повысить удобство работы, обеспечить анонимность и безопасность. Кроме того, это облегчает выполнение электронных коммерческих операций, поскольку пользователи используют биткойн-адреса, позволяющие также совершать покупки.

На первый взгляд, OneName – удобный инструмент для выполнения операций с биткойнами, но по сути это продвинутая децентрализованная система подтверждения цифровой идентификации с широкими возможностями. OneName помогает решить проблему сложности использования людьми биткойн-адресов, содержащих от 27 до 34 символов. Некоторые биткойн-сервисы, такие как Coinbase, позволяют отправлять биткойны на адреса электронной почты. OneName предлагает более надежное решение, разрешая пользователям использовать для транзакций понятные имена, как в социальных сетях. Чтобы запросить платеж, пользователь, зарегистрированный в OneName, может просто поставить знак плюс перед именем (например, +DeMirage99). Многие сайты используют API социальных сетей, таких как Facebook, LinkedIn и Twitter, для аутентификации пользователей¹⁰⁸. Протокол с открытым исходным кодом OneName, созданный на основе протокола Namecoin, дает возможность пользователям самим управлять цифровой идентификацией, не используя для этого централизованные социальные сети.

BitID – аналогичный проект, пользователи которого могут регистрироваться на сайтах с использованием своих биткойн-адресов. Теперь можно не только «войти через Facebook», но и «подключиться через биткойн». BitID – децентрализованный протокол аутентификации, использующий биткойн-кошельки для идентификации и QR-коды в качестве точек доступа к службе или платформе. С помощью BitID можно входить в учетные записи, подтверждая личность с помощью адреса кошелька, и использовать мобильное устройство как средство аутентификации с помощью закрытого ключа¹⁰⁹.

Bithandle – еще один проект для подтверждения цифровой идентификации, разработанный в рамках одного из хакатонов (хакерских марафонов). Bithandle предлагает регистрацию с коротким идентификатором, верификацию и услуги электронной коммерции. Как и при использовании OneName и BitID, пользователи могут регистрировать простой в использовании идентификатор (например, «Coinmaster»), связанный с адресом кошелька через открытую или закрытую проверку личности, подтвержденную транзакцией в блокчейне биткойна. Эта служба предлагает непрерывное подтверждение цифровой идентификации личности в режиме реального времени и быстрый автоматический доступ к сайтам электронной коммерции при помощи функции «Войти через биткойн». Очевидное препятствие для массового распространения технологий биткойна – неудобство 32-разрядных адресов и QR-кодов, необходимых для отправки и получения денежных средств. Bithandle предлагает связать с адресом биткойн-кошелька короткий идентификатор, который требует первоначального подтверждения в реальной жизни, после чего сохраняется в блокчейне и может быть запрошен в любой момент. Службы подтверждения цифровой идентификации в реаль-

¹⁰⁸ Rizzo, P., «How OneName Makes Bitcoin Payments as Simple as Facebook Sharing», сайт CoinDesk, 27 марта 2014 г., <http://www.coindesk.com/onename-makes-bitcoin-payments-simple-facebook-sharing/>

¹⁰⁹ Higgins, S., «Authentication Protocol BitID Lets Users ‘Connect with Bitcoin’», сайт CoinDesk, 7 мая 2014 г., <http://www.coindesk.com/authentication-protocol-bitid-lets-users-connect-bitcoin/>

ной жизни весьма востребованы: годовой объем мирового рынка средств аутентификации и подтверждения идентификации уже достигает 11 млрд долларов¹¹⁰.

Пользователь Bithandle регистрирует простое имя-идентификатор, который затем использует для «входа через биткойн». Как уже говорилось, эта функция аналогична предлагаемой многими сайтами возможности «Войти через Facebook» или «Войти через Twitter», но автоматически подключается к пользовательскому биткойн-адресу для подтверждения идентификации. Когда пользователь настраивает учетную запись Bithandle, его личность в реальной жизни подтверждается с помощью Facebook, Twitter, LinkedIn или других служб. Bithandle позволяет сделать эту информацию общедоступной (как в OneName) или не делать этого.

В дальнейшем, при использовании функции «Войти через биткойн» для подтверждения цифровой идентификации личности, учетная запись Bithandle автоматически соединяется с биткойн-адресом и может использоваться для безопасной работы с сайтами электронной коммерции, не требуя регистрации и предоставления личной и финансовой информации. Этим Bithandle помогает упростить взаимодействие пользователей с веб-сайтами. Во-первых, веб-сайты избавлены от необходимости хранить пользовательские данные (тем самым привлекая взломщиков). Во-вторых, каждый пользователь, вошедший через биткойн, автоматически получает возможность совершения покупок. В-третьих, служба Bithandle позволяет в реальном масштабе времени следить за данными в распределенном журнале записей, чтобы в любое время проверить цифровую идентификацию пользователя по запросу, например для повторной авторизации при последующих покупках.

Нейтралитет блокчейна

Специалисты по криптографии, разработчики и архитекторы блокчейна отмечают важность переноса в эту индустрию некоторых принципов, выработанных в интернете, – в частности, принципа нейтралитета. В соответствии с принципом *сетевого нейтралитета* интернет-провайдеры должны предоставлять доступ ко всему контенту и всем приложениям, независимо от источника, не блокируя и не отдавая предпочтения никаким продуктам и сайтам. Криптовалюты имеют аналогичную концепцию: *нейтралитет биткойна* позволяет использовать биткойн любому человеку в любой точке мира. Это значит, что кто угодно может начать использовать биткойн, независимо от культуры, языка, религии, географического положения, политической системы и экономического режима¹¹¹.

Биткойн – просто валюта, которую можно использовать в любой существующей политической, экономической и религиозной системе. Например, Исламский банк биткойна (Islamic Bank of Bitcoin) изучает возможности ведения банковской деятельности с использованием биткойна, не противореча принципам шариата^{112, 113}. Основная особенность нейтралитета биткойна заключается в том, что целевым рынком, для которого биткойн будет наиболее полезен, являются люди, по каким-либо причинам не имеющие доступа к традиционным банковским сервисам. По некоторым оценкам, это 53 % мирового населения¹¹⁴. Даже в США

¹¹⁰ Rohan, M., «Multi-Factor Authentication Market Worth \$10.75 Billion by 2020», сайт Markets and Markets, прочитано в 2014 г. (дата публикации неизвестна), <http://www.marketsandmarkets.com/PressReleases/multi-factor-authentication.asp>

¹¹¹ Antonopoulos, A. M., «Bitcoin Neutrality», конференция «Bit-coin 2013 Conference», 18 мая 2013 г., г. Сан-Хосе, шт. Калифорния, видеоролик на YouTube, 10 июня 2013 г., <https://www.youtube.com/watch?v=BT8FXQN-9-A>

¹¹² Senbonzakura (псевдоним), «Islamic Bank of Bitcoin», форум Bitcoin Forum, 24 июня 2011 г., <https://bitcointalk.org/index.php?topic=21732.0>

¹¹³ Ростовщичество, как сделка, при которой ростовщик приобретает прибыль, не затратив для этого никакого труда, а также дача денег под проценты запрещены шариатом и считаются одним из тяжких грехов. – Прим. ред.

¹¹⁴ Chaia, A. et al., «Half the World Is Unbanked», консалтинговая фирма McKinsey & Co, март 2009 г., <http://>

около 7,7 % физических лиц не обслуживаются банками или имеют ограниченный доступ к получению финансовых услуг¹¹⁵.

Нейтралитет подразумевает возможность использования решений на базе биткойна людьми, которые имеют ограниченный доступ к банковской системе или совсем его не имеют. Это подразумевает создание решений, работающих в малоразвитых в техническом смысле окружениях и имеющих такие возможности, как платеж через СМС, бумажные кошельки и пакетные блокчейн-транзакции. Появление простых в использовании решений, отвечающих принципам нейтралитета (что-то вроде Twitter), может вызвать очень быстрое распространение биткойна на рынки, не охваченные традиционными банками, повторяя ситуацию в Кении, где 31 % ВВП тратится через мобильные телефоны¹¹⁶. Существуют различные СМС-кошельки биткойна и механизмы доставки, например 37Coins¹¹⁷ и Coinapult, а также проекты вроде Kipochi¹¹⁸, интегрирующиеся с распространенными платформами мобильных финансов, такими как M-Pesa. Другой аналогичный проект – мобильный криптокошелек Saldo.mx, использующий открытый протокол Ripple для удаленных платежей в США и Латинской Америке.

Цифровой разрыв и биткойн

Термином *цифровой разрыв* обычно называют разрыв между теми, кто имеет доступ к определенным технологиям, и теми, кто его не имеет. Если криптовалюты внедрять с соблюдением принципов нейтралитета, любой человек в мире сможет использовать их. Поэтому альтернативные валюты могут быть полезными для преодоления цифрового разрыва. Однако есть и другое препятствие: знания и умения. Новый цифровой разрыв может возникнуть (и в каком-то смысле уже возник) между теми, кто умеет совершать безопасные операции в интернете, и теми, кто этого не умеет. Принципы нейтралитета необходимо расширить и создать подходящие для массового внедрения инструменты, позволяющие каждому пользователю совершать любые веб-операции и транзакции анонимно (или псевдонимно), конфиденциально и безопасно.

mckinseysoci-ety.com/half-the-world-is-unbanked/

¹¹⁵ «2013 FDIC National Survey of Unbanked and Underbanked Households», Федеральная корпорация по страхованию вкладов (США), обновлено 28 октября 2014 г., <https://www.fdic.gov/householdsurvey/>

¹¹⁶ Mims, C., «M-Pesa: 31 % of Kenya's GDP Is Spent Through Mobile Phones», сайт Quartz, 27 февраля 2013 г., <http://qz.com/57504/31-of-kenyas-gdp-is-spent-through-mobile-phones/>

¹¹⁷ Cawrey, D., «37 Coins Plans Worldwide Bitcoin Access with SMS-Based Wallet», сайт CoinDesk, 20 мая 2014 г., <http://www.coindesk.com/37coins-plans-worldwide-bitcoin-access-sms-based-wallet/>

¹¹⁸ Rizzo, P., «How Kipochi Is Taking Bitcoin into Africa», сайт CoinDesk, 25 апреля 2014 г., <http://www.coindesk.com/kipochi-taking-bitcoin-africa/>

Цифровая собственность: службы аттестации блокчейна (нотариальные службы, защита интеллектуальной собственности)

Цифровая собственность – еще одна сфера, в которой криптография блокчейна может предложить улучшения, меняющие общую парадигму. Кроме того, это хороший пример для обсуждения хеширования и временных меток – важных концепций, необходимых для дальнейшего понимания описываемых технологий. Термин *цифровая собственность* обозначает интеллектуальную собственность (ИС) в целом. В английском языке это называется *digital art*, где слово *art* используется как патентный термин, означающий «ИС, находящаяся во владении», а не просто «искусство». Как уже говорилось, в контексте защиты и подтверждения владения цифровой собственностью идентификацию можно рассматривать как одно из возможных применений, хотя и требующее дополнительных специальных функций. Для цифровой идентификации используется адрес биткойн-кошелька пользователя, а для подтверждения цифровой собственности службы заверения используют хеши и отметки времени. Вопросами цифровой собственности занимаются службы аттестации (подтверждающие, что некое заявление, например о владении имуществом, является правдой). В индустрии блокчейна термин *цифровая собственность* используется в основном в отношении регистрации в распределенном журнале записей любой формы ИС – полностью цифровой или представляющей что-то в физическом мире – или выполнения более общих услуг по заверению, таких как заверение контрактов. Также этим термином обозначают цифровые изображения и другие предметы искусства, созданные в цифровой форме, то есть являющиеся ИС, требующей защиты.

Хеширование и временные метки

Службы аттестации используют две основные функции блокчейна: хеширование и создание временных меток. Хеширование – это применение к содержимому любого файла (документа, файла генома, изображения GIF, видео и т. д.) вычислительного алгоритма, выдающего как результат своей работы краткую строку символов, по которым нельзя вычислить исходное содержимое. Любой файл можно превратить в строку хеша из 64 символов, являющуюся уникальным идентификатором содержимого этого файла¹¹⁹. Хеш представляет точное содержимое исходного файла. Если требуется подтвердить содержимое, к файлу применяется тот же самый алгоритм хеширования, дающий точно такую же сигнатуру хеша, если файл не изменялся. Хеш имеет сравнительно небольшую длину, так что его можно включать как текст в блокчейн-транзакцию, создавая таким образом защищенную от изменения временную метку, подтверждающую сигнатуру документа.

Фактически посредством хеша в блокчейне фиксируется точное содержимое файла; таким образом блокчейн превращается в реестр документов.

Главное в использовании криптографических хешей – то, что они являются способом подтверждения и заверения цифровых объектов, и это очень важная возможность. Хеширование в блокчейне может стать ключевой функцией для нашего общества, позволяющей подтверждать существование и точное содержимое любого документа и другого цифрового объекта в заданный момент времени. Более того, возможность заверения документов

¹¹⁹ Есть вероятность, что у двух разных файлов будет одинаковый хеш, но шанс такого события один на триллионы триллионов или даже меньше.

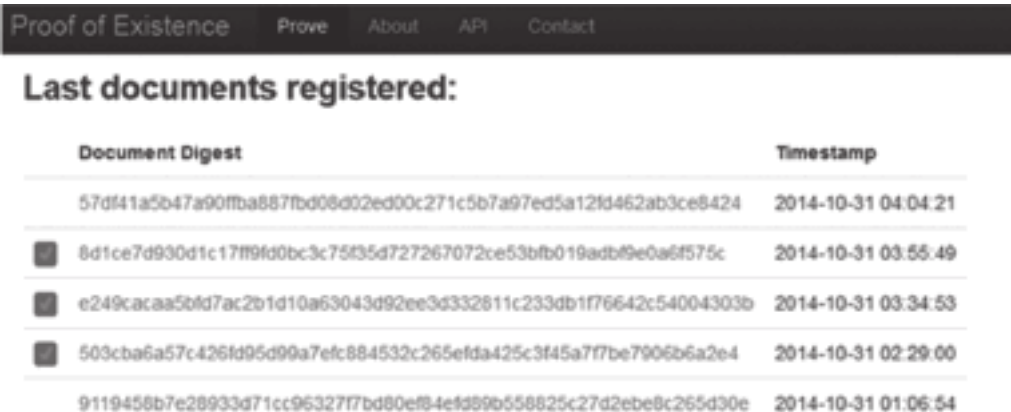
посредством хеширования и добавления временной метки подтверждает концепцию блокчейна как нового класса информационных технологий.

Службы блокчейн-аттестации могут предоставлять все функции, относящиеся к регистрации и хранению документов, нотариальному заверению и защите ИС. В основе этих функций лежит возможность блокчейна использовать криптографические хеши как перманентный и общедоступный способ записи и хранения информации, а также последующего извлечения этой информации при помощи поисковиков и указателей на конкретную позицию в блокчейне. Блокчейн здесь играет роль универсального центрального хранилища, основная задача которого – подтверждение цифровых объектов при помощи глобальной общедоступной учетной книги.

Сейчас на разных этапах разработки находится несколько служб аттестации на основе блокчейна: «Доказательство существования» («Proof of Existence»), «Виртуальный нотариус» («Virtual Notary»), Bitnotar, Chronobit, Pavilion.io и другие. Пока точно не ясно, в чем они будут схожи или различны, но, вероятно, значительная часть функциональности будет взаимозаменяемой, поскольку любая служба может вычислить хеш файла любого типа. Первой была служба «Доказательство существования».

Доказательство существования

Одна из первых служб, предлагающих услуги заверения в блокчейне, – «Доказательство существования» («Proof of Existence»). Пользователи могут использовать эту веб-службу для хеширования произведений цифрового искусства, программ и других цифровых объектов, чтобы доказать свое авторство¹²⁰. Основатель службы Мануэль Араоз предложил идею подтверждения целостности документа посредством криптографического хеша, но первоначально была проблема с подтверждением даты создания документа, пока в блокчейне не появился надежный механизм добавления временных меток¹²¹. «Доказательство существования» позволяет подтвердить авторство документа, не раскрывая его содержимое, и удостоверить, что документ был создан в определенное время. На рис. 3–1 показан фрагмент списка цифровых объектов, зарегистрированных в этой службе.






Proof of Existence Prove About API Contact				
Last documents registered:				
Document Digest	Timestamp			
57df41a5b47a90fba887fbd08d02ed00c271c5b7a97ed5a12fd462ab3ce8424	2014-10-31 04:04:21			
 8d1ce7d930d1c17f9fd0bc3c75f35d727267072ce53bfb019adb9e0a6f575c	2014-10-31 03:55:49			
 e249cacaa5bdf7ac2b1d10a63043d92ee3d332811c233db1f76642c54004303b	2014-10-31 03:34:53			
 503cba6a57c426fd95d99a7efc884532c265efda425c3f45a7f7be7906b6a2e4	2014-10-31 02:29:00			
9119458b7e28933d71cc96327f7bd80cf84ef889b658825c27d2ebe8c265d30e	2014-10-31 01:06:54			

Рисунок 3–1. Последние документы, зарегистрированные в службе «Доказательство существования» в октябре 2014 года

¹²⁰ Cawrey, D., «How Bitcoin's Technology Could Revolutionize Intellectual Property Rights», сайт CoinDesk, 8 мая 2014 г., <http://www.coindesk.com/how-block-chain-technology-is-working-to-transform-intellectual-property/>

¹²¹ Kirk, J., «Could the Bitcoin Network Be Used as an Ultrasecure Notary Service?», журнал Computerworld, 23 мая 2013 г., <http://www.computerworld.com/article/2498077/desk-top-apps/could-the-bitcoin-network-be-used-as-an-ultra-secure-notary-service-.html>

Этот инструмент дает революционную возможность использовать блокчейн для доказательства существования и фиксирования точного содержимого документа или другого цифрового объекта в заданное время. Обеспечение конфиденциальности и неизменяемость связки данных и временной метки – отличное сочетание для решения широкого диапазона юридических и гражданских вопросов. Адвокаты, клиенты и государственные администраторы могут использовать функциональность блокчейна и этой службы для доказательства существования документов различного типа, включая завещания, договоры, доверенности, медицинские свидетельства, долговые расписки и т. д., не раскрывая содержимого документа. Временные метки блокчейна позволяют доказать, что документ (например, завещание), представленный суду, является именно тем документом, без изменений, хеш которого был внесен в блокчейн. Заверять можно любые документы и цифровые объекты. Разработчики могут создавать уникальные хеши для каждой версии кода, изобретатели могут доказать, что идея появилась у них в определенное время, авторы могут защищать свои работы.

«Доказательство существования» работает следующим образом: пользователь входит на сайт службы и перетаскивает документ (или другой файл) в поле с надписью: «Щелкните здесь или перетащите документ в это поле». Копия содержимого файла не загружается на сайт, криптографическая операция вычисления хеша выполняется на клиентской стороне. Алгоритм создает дайджест, короткую криптографическую строку, представляющую данные, обработанные функцией хеширования. Два дайджеста совпадут только в том случае, если в точности совпадают данные, использованные для их вычисления. Таким образом, хеш непосредственно зависит от содержимого документа. Криптографический хеш документа помещается в транзакцию, и, когда транзакция попадет в блок, временная метка блока станет временной меткой документа. Посредством хеша содержимое документа фиксируется в распределенном журнале записей. Если функция хеширования получит тот же документ, она выдаст тот же результат, подтверждающий, что документ не изменился. Если же документ был хоть немного изменен, новый хеш не совпадет с предыдущим. Так выполняется проверка документов¹²².

Одно из преимуществ служб аттестации – эффективность использования блокчейна. В распределенном журнале записей хранятся не исходные документы, а только их хеш, доступный при наличии закрытого ключа. Когда требуется доказать существование, проверяется хеш, и если он совпадает с исходным хешем, зарегистрированным в блокчейне, это значит, что документ не изменялся. Хеш не требуется превращать в исходный документ, да это и невозможно: вычисление хеша – односторонняя операция. Этап извлечения доказательства существования можно считать «службой верификации содержимого». Чтобы обеспечить долговечность доказательства, требуется постоянное наличие ключа цифрового объекта (хеш), зарегистрированного в распределенном журнале записей. Для этого необходимо удостовериться, что та блокчейн-система, где зарегистрирован документ, будет существовать и в будущем. Таким образом, желательно выбирать службу заверения, использующую стандартный блокчейн – такой, как распределенный журнал записей биткойна.

Ограничения

Службы аттестации, использующие блокчейн, хеширование и временные метки, имеют некоторые ограничения. Во-первых, для добавления временных меток не обязательно использовать блокчейн: некоторые сторонние организации предоставляют такую возмож-

¹²² Morgan, P., «Using Blockchain Technology to Prove Existence of a Document», сайт Empowered Law, прочитано в 2014 г., <http://empoweredlaw.wordpress.com/2014/03/11/using-block-chain-technology-to-prove-existence-of-a-document/>

ность бесплатно, тогда как для записи сведений об аттестации объекта в распределенный журнал записей требуется небольшая плата за транзакцию (для компенсации затрат майнеров). Кроме того, подтверждение транзакций в блок-чейне требует некоторого времени и фиксируется время добавления документа в журнал записей, а не время его создания, в то время как для служб регистрации ИС может быть важно точное время создания цифрового объекта. И самая серьезная проблема: временная метка не подтверждает право владения.

Тем не менее возникающие службы блокчейн-аттестации можно рассматривать как важный шаг вперед и включить их в экосистему Блокчейн 3.0 наряду с другими элементами. Высказываются разные предложения, касающиеся их дальнейшего развития: например, добавить цифровую идентификацию для подтверждения права владения и сторонние временные метки для времени создания документа. Существует мнение, что хеш очень крупных документов (например, файла генома размером 8 ГБ) менее надежен, чем хеш небольших документов (таких, как стандартные формы долговых обязательств), но это опасение необоснованно. Алгоритмы хеширования отличаются масштабируемостью и способностью обработать файл любого размера, а безопасность и надежность определяются длиной хеша (в настоящее время обычно используются 64 символа, в будущем это число может увеличиться). Обычные угрозы технологии хеширования – обратные хеши (обратные функции, пытающиеся вычислить хешированное содержимое) и коллизии (возникают, когда два разных файла дают одинаковые хеши) – в настоящее время не представляют проблемы для использования хеша в блокчейне.

Виртуальный нотариус, Bitnotar и Chronobit

«Виртуальный нотариус» («Virtual Notary») – еще один проект, предлагающий аналогичные услуги по аттестации в блокчейне. Как и «Доказательство существования», «Виртуальный нотариус» не хранит файлы, а предоставляет сертификат, удостоверяющий содержимое файла на момент проверки. Эта служба выдает сертификаты для различных типов файлов, таких как документы, веб-страницы, сообщения Twitter, курсы акций, валютные курсы, погодные условия, записи DNS, подтверждения адресов электронной почты, членство в учебных заведениях, стоимость недвижимости, положения и договоры, выпадение случайных чисел. Файлы могут быть представлены в любом формате, включая стандартные текстовые и графические файлы и документы Microsoft Office. Сайт генерирует сертификат, который можно скачать, а также предлагает обратные услуги – проверку существующих сертификатов. Цель этого проекта – предоставлять нейтральные и беспристрастные цифровые свидетельства и записи фактов и событий, происходящих в сети, и сообщать о них третьим сторонам заслуживающим доверия способом. Поскольку наша жизнь все больше связана с цифровыми технологиями, такие возможности становятся весьма важными¹²³.

Еще два проекта, предоставляющие временные метки, – Bitnotar и Chronobit. Проект Pavilion.io на основе блокчейна предоставляет услуги по заверению договоров по гораздо более доступной цене, чем Adobe EchoSign и DocuSign; договоры можно отправлять бесплатно, а их подпись стоит всего 1 mBTC¹²⁴. Виртуальные нотариальные услуги предлагают также проекты Blocksign и btcluck.

¹²³ Siret, E. G., «Introducing Virtual Notary», сайт Hacking-Distributed, 20 июня 2013 г., <http://hackingdistributed.com/2013/06/20/virtual-notary-intro>

¹²⁴ Goss, L., «The High School Startup Using Blockchain Technology», сайт BitScan, 27 августа 2014 г., <https://bitscan.com/articles/the-high-school-startup-using-blockchain-technology>

Monegraph: защита изображений в интернете

Один из проектов, использующих новые методы доказательства на основе учетной книги Блокчейн 3.0, – Monegraph. Слоган этого проекта – «because some art belongs in chains»¹²⁵. Это приложение (пока бесплатное) помогает авторам монетизировать цифровые изображения, размещенные в сети, посредством их регистрации. Как биткойн подтверждает владение валютой, так и Monegraph подтверждает владение собственностью, являясь примером использования расширенных возможностей блокчейна. Monegraph может работать как дополнительная служба веб-сайтов стоковых фотографий, таких как Shutterstock и Getty Images, и обеспечивать функции трекинга изображений и контроля соблюдения правил их использования.

В процессе работы Monegraph использует Twitter и Namecoin. Namecoin используется как альткойн, позволяющий проверять регистрацию имен DNS автоматическим децентрализованным путем; вместо него можно использовать любую другую аналогичную службу DNS¹²⁶. Сначала пользователь входит на сайт <http://www.monegraph.com/>, дает разрешение на вход через учетную запись Twitter (посредством стандартных средств API Twitter OAuth) и указывает URL-адрес изображения, используя который Monegraph автоматически публикует ссылку на это изображение в нужном формате. Затем, чтобы завершить регистрацию, Monegraph предоставляет пользователю блок кода, который следует скопировать и вставить в клиент Namecoin. Пользователь инициирует новую транзакцию в кошельке Namecoin и добавляет в нее блок кода как ключ и значение (за транзакциями можно наблюдать по адресу http://bit.ly/monegraph_verification). Только одна копия цифрового изображения может иметь действительную сигнатуру Monegraph. Изображения Monegraph – это обычные графические файлы, так что их можно копировать и распространять обычными способами, но только исходный файл сможет пройти проверку в системе Monegraph.

Похожий проект по защите авторских прав на цифровые объекты, предоставляющий инфраструктуру для регистрации ИС, – Ascribe. Эта компания пытается создать «уровень владения» для цифровой собственности, предлагая службу для регистрации и передачи авторских прав. Хотя по существующим законам об авторском праве автор имеет право на защиту и коммерциализацию своей ИС, до сих пор не было простого глобального интерфейса для регистрации, лицензирования и передачи авторского права. Служба Ascribe пытается восполнить этот пробел, регистрируя цифровые работы при помощи хеширования и внесения в блокчейн с временными метками.

На начальном этапе регистрации используется машинное обучение, позволяющее идентифицировать и решить любые проблемы, связанные с аналогичными существующими работами. После этого можно передавать права владения и выходить на вторичные рынки цифровой ИС. Служба Ascribe работает с цифровыми рисунками, фотографиями, логотипами, музыкой, книгами, статьями, твитами, 3D-моделями и многим другим. Пользователям не требуется вникать в детали работы блокчейна, закона об авторском праве или машинного обучения, чтобы использовать все преимущества этой службы. По большей части Ascribe используется в фоновом режиме торговыми площадками и веб-службами, работающими по принципу «white-label» (производство продуктов или услуг одной компанией и их примене-

¹²⁵ «Потому что место искусства – в цепях» (англ.). Игра слов, основанная на двойных смыслах слов «art» и «chain». – Прим. пер.

¹²⁶ Cawrey, D., «How Monegraph Uses the Block Chain to Verify Digital Assets», сайт CoinDesk, 15 мая 2014 г., <http://www.coindesk.com/monegraph-uses-block-chain-verify-digital-assets/>

ние другой компанией под своим брендом), но индивидуальные пользователи могут задействовать эту службу напрямую.

Подтверждение владения цифровой собственностью как автоматическая функция

В будущем для защиты цифровой собственности могут появиться стандартизированные инструменты автоматической регистрации в блокчейне. Для определенных классов объектов и веб-сайтов регистрация может выполняться автоматически в момент публикации любого цифрового содержимого. Это может быть удобно для публикаций на GitHub, записей в блогах, твитов, фотографий в Instagram и Twitpic, сообщений на форумах. Защита цифровой собственности может предоставляться так же, как сейчас предлагается страховка во время покупки билетов на самолет. При настройке учетной записи для использования блогов, вики, форумов, Twitter и GitHub пользователь сможет разрешить микроплатежи для регистрации цифровой собственности (указав адрес биткойн-кошелька). Криптовалюта как встроенная в интернет система экономических отношений обеспечивает возможность защиты интеллектуальной собственности на микроконтент посредством микроплатежей. Криптовалюта предоставляет необходимую для этого структуру: можно снабжать метками и включать в блокчейн-транзакции микроконтент, а можно регистрировать саму цифровую собственность, назначая ей собственные блокчейн-адреса. Кроме того, службы заверения в блокчейне можно использовать не только для регистрации ИС, но и для решения других задач, таких как передача авторских прав и лицензирование содержимого.

Нотариальные блокчейны как класс блокчейн-инфраструктуры

Важно помнить, что все это только начало процесса, который может превратиться в полноценную блокчейн-экономику, в которой блокчейн-технологии, аналогично интернету, повышают эффективность любой человеческой деятельности. В этом смысле можно рассматривать все текущие достижения блокчейна как начальные прототипы. Службы, разрозненные сегодня, могут объединиться в классы служб блокчейна.

С учетом общих принципов проектирования инфраструктуры блокчейна можно ожидать появления классов узкой функциональности. Отдельные нотариальные службы блокчейна могут эволюционировать в новый класс нотариальных цепочек блоков. Нотариальные блокчейны – пример децентрализованных автономных организаций и корпораций, более сложная группа операторов, совместно выполняющих определенный класс функций с использованием блокчейн-технологии. В данном случае нотариальные цепочки представляют класс блокчейн-протоколов для служб аттестации. Например, публикация пакетов удостоверяющих транзакций может быть более эффективной по сравнению с публикацией каждой транзакции в отдельности, при этом с ненулевой стоимостью майнинга.

Нотариальные блоки могут состоять из хешей многих объектов, прошедших цифровое заверение. Хешировать можно и сами блоки, делая нотариальный блок единицей, внесенной в блокчейн. Это более эффективно, чем нотариальное заверение каждого цифрового объекта. Поскольку хеширование – односторонняя функция, существование хеша блока в распределенном журнале записей биткойна автоматически подтверждает существование всех дочерних хешей¹²⁷. Переход блокчейна на этап промышленных децентрализованных автономных организаций и корпораций поднимает интересные вопросы относительно того, каким будет

¹²⁷ Snow, P., «Notary Chains» (технический документ), <https://github.com/NotaryChains/>

оптимальное сочетание иерархических и децентрализованных составляющих в крупномасштабных архитектурах. В рамках проекта Factom разрабатывается идея блочной загрузки пакетных транзакций в блокчейн с использованием аттестации и нотариального заверения блоков, что позволит избежать чрезмерного разрастания распределенного журнала записей.

Персональные распределенные журналы мышления

Размышляя о далеком будущем технологий блокчейна, в концепцию автоматизированного учета и отслеживания дискретных данных можно включить еще одну категорию администрирования и ведения записей – «персональные цепочки мышления», механизм хранения и восстановления истории жизни. Комбинация «блокчейн-технология + персональный коннектом¹²⁸ организма» позволит кодировать и делать доступными в стандартизированном сжатом формате все мысли человека. Данные можно будет захватывать путем сканирования коры головного мозга, ЭЭГ, интерфейсов мозг-компьютер, когнитивных нанороботов и т. д. Мышление можно будет представить в виде цепочек блоков, записав в них практически весь субъективный опыт человека и, возможно, даже его сознание. После записи в блокчейн различные составляющие воспоминаний можно будет администрировать и передавать – например, для восстановления памяти в случае болезней, сопровождающихся амнезией.

Блокчейн-технология уже предложила качественную модель с достаточным уровнем конфиденциальности и системой вознаграждений для общего доступа к медицинским данным и дискретизированным данным самонаблюдения. Раньше такой модели не было, как и модели и средств работы с полным набором данных, получаемых в результате умственной деятельности. В случае с публикацией данных об умственной деятельности возникает еще больше морально-этических вопросов, но блокчейн-технология делает этот процесс конфиденциальным, безопасным и выгодным. Как уже говорилось, для протоколирования жизни можно будет использовать персональные цепочки блоков мышления, захватывающие и надежно кодирующие в блокчейне всю умственную деятельность человека, эмоции и субъективные переживания. Как минимум, это позволит создать архив для передачи потомкам и восстановления в случае болезни. Персональные распределенные журналы записей и *майндфайлы* могут быть следующим поколением таких инструментов, как Fitbit и Apple iHealth, которые сейчас автоматически сохраняют более 200 показателей организма и отправляют их в облако для агрегирования и получения практических рекомендаций. Таким же образом можно будет создавать персональные распределенные журналы записей мышления (решив все обычные вопросы конфиденциальности с помощью блокчейн-технологии) и получать рекомендации по оптимизации умственной деятельности через голосовые службы типа Siri и Amazon Alexa или через интерфейсы мозг-компьютер как осознаваемые предложения или подсознательные внушения.

Хотя все это похоже на научную фантастику, всеобщая история может включать не только общественные записи, хранилища документов и архив цифровой активности интернета, но и майндфайлы отдельных людей. Майндфайлы могут включать сведения о каждой «транзакции», то есть все мысли и эмоции каждого существа, человека и машины, закодированные и сохраненные в распределенных журналах записей.

¹²⁸ Полная карта нейронных связей организма. – Прим. ред.

Блокчейн-правительство

Еще одно важное применение Блокчейн 3.0 – блокчейн-правительства, то есть использование блокчейн-технологии для наиболее эффективного, дешевого и персонализированного оказания услуг, традиционно предоставляемых государственными органами.

Блокчейн делает возможными многие новые модели управления и оказания госуслуг. Блокчейн-правительство работает на основе технологий хранения общедоступных записей в распределенном журнале записей – универсальном, постоянном, согласованном, непрерывно функционирующем, полноценном и доступном для общественного аудита архиве. Блокчейн может стать механизмом управления информацией в настоящем и хранилищем всех документов и исторических сведений для использования в будущем, превратившись в универсальную систему хранения записей. Не всем предложенным здесь концепциям и управляющим службам требуются для их функционирования блокчейн-технологии, но их реализация на основе блокчейна может дать дополнительные преимущества, такие как более высокий уровень доверия и возможность вести общедоступные записи.

Одним из следствий создания блокчейн-правительства станет сдвиг от принудительной единой модели «во благо всех», применяющейся в настоящее время, к более гибкой, подстраиваемой под нужды отдельных граждан. Представьте мир административно-управляющих служб, персонализированный до такой же степени, как заказ кофе в Starbucks. При такой персонализации, например, один резидент может платить за более качественную переработку мусора, включающую компостирование органических отходов, а его сосед – за более качественное школьное образование. Для управления и предоставления персонализируемых услуг можно использовать блокчейн. Так, умные города будущего могут выпускать валюту Roadcoin (road – *англ.* дорога) для компенсации ухудшения качества жизни водителей, проезжающих по ремонтирующимся дорогам. Валюта Accidentcoin (accident – *англ.* несчастный случай, авария) может использоваться для выплат виновниками ДТП компенсаций пострадавшим. Платежи могут выполняться незамедлительно и пересчитываться в дальнейшем, после оценки ущерба страховыми компаниями.

Нил Стивенсон в научно-фантастическом романе «Лавина»¹²⁹ предсказал появление *франшиз* (*franchulate*) – компаний, имеющих лицензию на предоставление квазиправительственных услуг и продающих их отдельным людям как обычные товары и услуги¹³⁰. Блокчейн-правительство может воплотить эту идею в жизнь. Преимуществом такого подхода будет изменение отношения: правительство должно быть больше похоже на бизнес, чем на монополию по предоставлению административных и управленческих услуг, и активнее строить отношения с гражданами-потребителями, предлагая им выгодные условия и качественные услуги.

Еще одним следствием появления блокчейн-правительства и «переноса государства в блокчейн» может стать создание более демократичного общества. Этого можно достичь, если использовать умные контракты, основанные на блокчейне, и децентрализованные автономные корпорации, а не полагаться на чиновников. Меньшее число служащих в государственном аппарате означает меньше расходов на его содержание, меньше пристрастности, меньше лоббирования. В сфере государственного управления и общественного администрирования можно провести такие же реформы, как в финансовой системе, которую блокчейн-технология делает более эффективной, снижая затраты практически до нуля. Сэконом-

¹²⁹ Stephenson, Neal. Snow Crash, 1992. – Прим. ред.

¹³⁰ Stephenson, N., «Snow Crash», Нью-Йорк, издательство Spectra, 1992 г. См. также: <http://everything2.com/title/Franchulate>

ленные на содержании чиновников деньги можно направить на поддержание минимальной заработной платы на должном уровне, чтобы укрепить равенство и политическую вовлеченность граждан, а также облегчить переход к автоматизированной экономике.

Блокчейн и децентрализованные модели ставят под вопрос общую состоятельность моделей управления и страхования, основанных на совокупной численности населения, которые были стандартами де-факто просто за отсутствием других моделей. С экономической и политической точек зрения традиционные модели устарели. Модели, требующие достижения консенсуса, могут быть более эффективными в экономическом смысле и представлять более адекватный и объективный способ взаимодействия с окружающим миром, создавая основу для искоренения любого ущемления свободы выбора¹³¹. Блокчейн-правительство получает все преимущества информационной блокчейн-технологии, позволяющие создать новую, максимально эффективную систему организации, администрирования, координирования и записи всех совершаемых людьми операций, независимо от того, кем они выполняются: корпорациями, правительствами или отдельными людьми. Блокчейн-технология поднимает вопрос о более эффективном выполнении задач государства, а также о правах, обеспечиваемых государством, которые в отдельных случаях не учитывают (и не должны учитывать) индивидуальные предпочтения. Пока большинство проектов занимается только переосмыслением услуг, которые должно предоставлять государство, так что еще есть возможность создания интересных моделей на основе блокчейна, обеспечивающих соблюдение прав граждан.

Децентрализованные управляющие службы

Выбирайте правительство, выбирайте сервисы. Такова идея перемещения национальных государств в блокчейн: создание управляющих служб, не связанных границами, децентрализованных, предоставляемых по запросу¹³². Такие службы могут включать основанную на репутации систему идентификации, инструменты для решения споров, голосования, распределения национального дохода и регистрации всех видов юридических документов, таких как купчие на землю, завещания, договоры опеки, брачные договоры и т. д. Структура блокчейна, обеспечивающая безопасную идентификацию, управление активами и возможность заключения множества контрактов, идеально подходит для таких операций, как заключение брака, поскольку пара может связать свой брачный договор с общей сберегательной учетной записью (то есть с биткойн-кошельком), договором опеки над ребенком, документами на землю и любыми другими документами, имеющими отношение к совместному будущему¹³³.

Первый в мире брак, записанный в блокчейне, был заключен 5 октября 2014 года во Флориде в парке развлечений Disneyworld (рис. 3–2). Брак был зарегистрирован в распределенном журнале записей биткойна, как в онлайн-общедоступном реестре. Свадебные клятвы были внесены в текстовое поле аннотации и встроены в биткойновую транзакцию. Это обошлось в 0,1 биткойна (32,50 долл. США), и теперь эта информация перманентно хранится в учетной книге блокчейна¹³⁴. Церемонией руководил исполнительный директор

¹³¹ Swan, M., «Illiberty in Biohacking, Personal Data Rights, Neuro-diversity, and the Automation Economy», блог Broader Perspective, 2 марта 2014 г., <http://futurememes.blogspot.fr/2014/03/illiberty-in-biohacking-personal-data.html>

¹³² Prisco, G., «Bitcoin Governance 2.0: Let's Block-chain Them», сайт CryptoCoins News, обновлено 13 октября 2014 г., <https://www.cryptocoinsnews.com/bitcoin-governance-2-0-lets-block-chain/>

¹³³ Hofman, A., «Couple to Get Married on the Bitcoin Blockchain at Disney Bitcoin Conference», журнал *Bitcoin Magazine*, 23 сентября 2014 г., <http://bitcoinmagazine.com/16771/couple-get-married-bitcoin-blockchain-disney-bitcoin-conference/>

¹³⁴ Marty, B., «Couple Make History with World's First Bitcoin Wedding», новостной сайт PanAm Post, 7 октября 2014 г., <http://panampost.com/belen-marty/2014/10/07/couple-make-history-with-worlds-first-bitcoin-wedding/>

компании Libertyme Джеффри Такер. Он рассказал о преимуществах денационализированных браков в контексте равноправия и о том, чем регистрация брака в блокчейне выгодно отличается от регистрации в государственных структурах¹³⁵.

Индикатором того, что общественность признала блокчейн в качестве реестра документов, может быть появление на биткойновых рынках прогнозов контрактов, связанных с событиями в жизни пары, таких как рождение детей, приобретение недвижимости и даже развод (такое событие тоже будет записано в распределенный журнал записей), и, конечно, проведение социологических исследований, показывающих, что браки, заключенные в блокчейне, сохраняются дольше (или нет), чем церковные или гражданские.



Рисунок 3–2. *Первая в мире биткойн-свадьба Дэвида Мондруса и Джойс Байо, проведенная 5 октября 2014 г. в парке Disneyworld во Флориде (автор изображения: Рубен Александер, Bitcoin Magazine)*

Управляющие системы на основе блокчейна могут предлагать услуги, традиционно оказываемые государством, которые граждане-пользователи могут добровольно принимать или не принимать. Как биткойн предлагает альтернативу фиатным деньгам, поскольку биткойн представляет собой механизм платежей с меньшими расходами, более эффективный, простой в использовании, с немедленным получением средств, так и управляющие службы на основе блокчейна могут давать аналогичные преимущества. Услуги, предоставляемые «фиатными» государственными службами, в блокчейне могут быть более дешевыми, распределенными и добровольными. Все юридические документы, такие как купчие, договоры и удостоверения личности, могут храниться в распределенном журнале записей.

Для достижения критической массы пользователей, позволяющей добиться всеобщего признания (как в случае с биткойном, признанным и широко используемым в качестве денег), необходимы системы идентификации, например блокчейн-паспорта. Один из проектов, пытающихся создать систему блокчейн-паспортов, – проект «Гражданин мира» («World Citizen»)¹³⁶. Цель этого проекта – создание системы мирового гражданства посредством доступных децентрализованных паспортных служб, использующих криптографические средства (рис. 3–3).

¹³⁵ Ploshay, E., «A Word from Jeffrey Tucker: Bitcoin Is Not a Monetary System», журнал *Bitcoin Magazine*, 3 января 2014 г., <http://bitcoinmagazine.com/9299/word-jefrey-tucker-bit-coin-monetary-system/>

¹³⁶ McMillan, R., «Hacker Dreams Up Crypto Passport Using the Tech Behind Bitcoin», журнал *Wired*, 30 октября 2014 г., http://www.wired.com/2014/10/world_passport/; Ellis, C., «World Citizenship Project Features in Wired Magazine», запись в блоге, 1 ноября 2014 г., <http://chrisellis.me/world-citizen-ship-project-features-in-wired-magazine/>



Рисунок 3–3. Блокчейн-паспорт проекта «Гражданин мира» (автор изображения: Крис Эллис)

Главное – любой человек из любой точки мира может использовать услуги децентрализованного правительства. Тот факт, что человек живет в определенном месте, не должен препятствовать ему в получении определенных правительственных услуг. Правительства всегда были монополией, но блокчейн может изменить это положение в мире, связанном глобальными сетями. Глобальные валюты, такие как биткойн, и глобальные правительственные службы поднимают важные вопросы о меняющейся природе национальных государств и их роли в будущем. В свете перехода в блокчейн валюты, финансов, профессиональной деятельности, взаимодействия с другими людьми, правительственных услуг и ведения учета страна может стать просто местом, где человек родился и живет, но не более того. К тому же биткойн позволяет создать мир, в котором людям гораздо легче перемещаться между странами и пользоваться преимуществами единой более эффективной правительственной системы, а не многочисленных вариаций местных правил отдельных государств. Как и в случае с криптовалютой, программное обеспечение децентрализованного правительства может быть открытым и ветвящимся, чтобы любой человек мог создать свое блокчейн-государство и оказывать управляющие услуги на этой общей платформе, позволяющей организовать управление по принципу «сделай сам».

Для обеспечения права собственности децентрализованное блокчейн-правительство должно вести реестр собственности, как биткойн для денежных переводов, и может воплощать планы «экономики развития», разработанные такими экономистами, как Эрнандо де Сото¹³⁷. Блокчейн и децентрализованные государственные услуги могут помочь глобализации организаций, подобных Институту свободы и демократии, созданному де Сото, разрабатывающему программы для документирования, оценки и решения не предусмотренных законом вопросов и их согласования с правовой системой. Универсальный реестр собственности на основе блокчейна предоставляет необходимую систему документации прав владения, обеспечивает удобство передачи, возможность выполнять транзакции и возмещать затраты, а также позволяет выходить на развивающиеся рынки, где эти структуры отсутствуют или только зарождаются (одновременно позволяя развивать родственный бизнес по разрешению споров). Как некоторые страны Африки сразу начали использовать мобильные телефоны, минуя этап создания проводных телефонных сетей (и как некоторые страны могут перейти сразу к превентивной медицине с использованием персонализированной

¹³⁷ De Soto, H., «The Mystery of Capital: Why Capitalism Triumphs in the West and Fails Everywhere Else», Нью-Йорк, издательство Basic Books, 2003 г.

геномики¹³⁸), так страны с развивающимися рынками могут сразу перейти к созданию реестров собственности в блокчейне. Другие службы на основе блокчейна могут способствовать аналогичным прорывам в других областях – например, ускорить выдачу идентификационных карт Aadhar (крупнейшая в мире биометрическая база данных¹³⁹), отсутствующих у 25 % населения Индии, и помочь в устранении таких проблем, как появление фальшивых и повторяющихся идентификаторов.

PrecedentCoin: решение споров в блокчейне

Precedent – проект Блокчейн 3.0, посвященный исключительно использованию блокчейна для эффективного решения споров. Концептуально этот проект похож на народный суд или суд присяжных. До сих пор не было возможности использовать преимущества центрального хранилища прецедентов для решения споров, поэтому Precedent создает концепцию, структуру, альткойн и сообщество для реализации децентрализованного автономного судопроизводства (подробнее см. в официальной документации проекта: «The Precedent Protocol Whitepaper»¹⁴⁰). Полицентричная децентрализованная правовая система Precedent позволяет отдельным пользователям выбирать правовую систему и особенности, которые им нравятся, поддерживая идею персонализации правительства и законодательства. Развитие сообщества, участие в формировании законодательства и решении споров стимулируются криптовалютой PrecedentCoin, называемой также «номо» (*греч.* закон).

Как распределенный журнал записей биткойна поддерживается децентрализованным сообществом майнеров, проверяющих, подтверждающих и записывающих новые транзакции, так и «майнеры прецедентов» из сообщества Precedent регистрируют новые споры, решают их и записывают прецеденты в распределенный журнал записей (в который записывается ссылка на подробную информацию о прецеденте, безопасно хранимую вне цепочки блоков). Precedent работает как метапротокол блокчейна (по структуре похожий на Counterparty). Подтверждение прецедента выполняется механизмом консенсуса системы (аналог подтверждения работы или подтверждения доли в майнинге биткойнов). Система Precedent функционирует по пиринговому принципу – пользователи определяют, подлежит ли спор судебному рассмотрению и можно ли вынести по нему решение, и могут изменять протокол, если новые стандарты оказываются более подходящими. Для экономических операций сообщества, таких как плата за рассмотрение дела и вознаграждение «майнеров» (выполняющих функции присяжных или арбитров по гражданским спорам) за участие в решении споров, используется токенизированный альткойн PrecedentCoin.

Следует заметить, что, как указано в официальной документации проекта, «протокол Precedent отвечает только за предоставление возможности рассмотрения спорного вопроса и не может гарантировать обоснованность и справедливость исхода». Таким образом, существует риск подкупа или коллективного принятия странного или несправедливого решения. Проект определяет только возможность судебного рассмотрения дела с точки зрения закона, а не фактов.

¹³⁸ Swan, M., «Crowdsourced Health Research Studies: An Important Emerging Complement to Clinical Trials in the Public Health Research Ecosystem», журнал *J Med Internet Res*, том 14, № 2 (2012 г.), с. e46.

¹³⁹ Mishra, P., «Inside India's Aadhar, the World's Biggest Biometrics Database», сайт TechCrunch, 6 декабря 2013 г., <http://tech-crunch.com/2013/12/06/inside-indias-aadhar-the-worlds-big-gest-biometrics-database/>

¹⁴⁰ Ее можно найти по адресу <https://github.com/mdelias/precedent>. – Прим. ред.

Гибкая демократия

Некоторые проекты блокчейн-правительства занимаются разработкой систем, делающих демократию более эффективной.

В модели децентрализованного автономного общества может возникнуть необходимость сформулировать некий стандарт систем децентрализованного управления на основе консенсуса и децентрализованных систем голосования – например, как предлагает BitCongress¹⁴¹. Другие проекты выдвигают идеи делегативной демократии, формы демократического правления, где полномочия для голосования получают делегаты, а не представители (как во многих современных моделях конгрессов и парламентов). Так, проект «Гибкая демократия» («Liquid Democracy») предоставляет ПО с открытым исходным кодом, облегчающее разработку предложений и принятие решений.

В системе «Гибкой демократии» член партии может не голосовать за представителя, а делегировать право голоса – по всем вопросам, по ряду вопросов или по решению только одного вопроса, и на любой промежуток времени. Полномочия могут быть отозваны в любой момент. В этой системе человек может очень быстро стать делегатом множества членов сообщества, получив политическую власть, обычно предоставляемую выбранным представителям, – и так же быстро он может и потерять эту власть. Это и есть «гибкость», процесс, который можно назвать «транзитивным делегированием». Если сообщество уважает человека как эксперта в определенной области, он может получить голоса других членов сообщества. Таким образом, любой пользователь платформы «Гибкая демократия» – потенциальный политик¹⁴². Пока эта платформа вызывает множество вопросов. Один из них – стабильность и непрерывность функционирования – решается с помощью механизма определения репутации агентов, который можно реализовать с помощью блокчейна.

Идея делегированного принятия решений, воплощенная с помощью структуры блокчейна, может широко применяться вне контекста голосования и политики. Например, здравоохранение – еще одна сфера, в которой часто делегируется принятие решений, но это плохо отслеживается, и за это почти нет ответственности. Блокчейн-технология позволяет отслеживать такое делегирование и увеличивать ответственность. Биоэтические аспекты делегирования медицинских решений, описанные в книге «Решая за других»¹⁴³ Аллена Бьюкенена, могут применяться и в системе «Гибкой демократии»¹⁴⁴. Это позволит повысить качество принимаемых решений по медицинским вопросам и создать систему децентрализованного консультирования, необходимую ввиду того, что многие люди не имеют квалифицированных советников. В более отдаленном будущем блокчейн и другие общественные технологии могут предоставить механизмы для решения этических вопросов.

«Гибкая демократия» предоставляет также платформу для разработки предложений. Любой член сообщества может предложить новую идею. Если предложение получит достаточную поддержку других членов, оно переходит на этап обсуждения, на котором может обсуждаться наряду с альтернативными предложениями и изменяться. Если сообщество заинтересовано в предложении, оно поступает на голосование. Голосование проводится по рейтинговому методу Шульца, чтобы голоса не разделялись между почти идентичными,

¹⁴¹ Deitz, J., «Decentralized Governance Whitepaper», Quora, 21 мая 2014 г., <http://distributed-autonomous-society.quora.com/Decentralized-Governance-Whitepaper>

¹⁴² Ramos, J., «Liquid Democracy: The App That Turns Everyone into a Politician», сайт Shareable, 20 января 2014 г., <http://www.shareable.net/blog/liquid-democracy-the-app-that-turns-everyone-into-a-politician>

¹⁴³ Buchanan, Allen E. *Deciding for Others: The Ethics of Surrogate Decision Making*, 1990. – Прим. ред.

¹⁴⁴ Buchanan, A. E., «Deciding for Others: The Ethics of Surrogate Decision Making (Studies in Philosophy and Health Policy)», Кембридж, издательство Cambridge University Press, 1990 г.

«клонированными» предложениями (проблема, аналогичная двойной трате). Все это координируется с помощью платформы, доступной в глобальной сети. Голосование может проводиться с разным уровнем прозрачности: открыто, анонимно или псевдонимно с аутентификацией. Пока не решен вопрос о том, как обеспечить обязательное исполнение решений и какие механизмы включить для этого в ПО. На начальном этапе «Гибкая демократия» может служить промежуточным инструментом для координирования голосования и анализа результатов.

Предложения о совершенствовании демократии выдвигаются с давних пор, но только сейчас, с появлением интернета и технологий типа блокчейна, становится возможным воплощение таких сложных и динамичных механизмов в реальном мире. Например, идею делегативной демократии и транзитивного голосования описал еще Льюис Кэрролл (автор «Алисы в Стране чудес») в трактате «Принципы парламентского представительства»¹⁴⁵.

Выборы со случайной выборкой

Кроме делегативной демократии, блокчейн-правительство позволяет проводить выборы со случайной выборкой. Случайно выбранные избиратели получают по почте бюллетень для голосования и ссылку на веб-сайт, обеспечивающий выборный процесс и позволяющий изучить дебаты кандидатов и заявления активистов. Дэвид Чаум считает¹⁴⁶, что случайная выборка (как в идеальном социологическом исследовании) точнее представляет общество (как минимум, включает плохо представленные категории избирателей) и позволяет избирателям принимать решения, тщательно их обдумав в домашних условиях, обращаясь к любым доступным ресурсам, а не просто поддавшись рекламе¹⁴⁷. Блокчейн-технологии предоставляют средства для масштабного проведения выборов со случайной выборкой, обеспечивая надежность и псевдонимность.

Футархия: двухэтапная демократия с голосованием и рынками прогнозов

Футархия — двухэтапный процесс, позволяющий сначала голосовать за общий результат (например, «повышение ВВП»), а затем голосовать за предложения, позволяющие достичь этого результата. На первом этапе проводится обычное голосование, на втором используются рынки прогнозов.

Голосование на рынках прогнозов может проводиться с использованием различных криптовалют (Economic Voting Coin или Environmental Policy Voting Coin) или других экономически значимых токенов. По сути, это инвестирование и спекуляция, ставка на одну или другую сторону, которая предположительно выиграет. Например, вы можете купить «контракт инвестирования в новые биотехнологии», если считаете, что это лучше способствует достижению результата «повышение ВВП», чем другие контракты, такие как «контракт инвестирования в автоматизацию сельского хозяйства».

¹⁴⁵ Carroll, L., «The Principles of Parliamentary Representation», Лондон, издательство Harrison and Sons, 1884 г., <https://archive.org/details/ThePrinciplesOfParliamentaryRepresentation>; Black, D., «The Central Argument in Lewis Carroll's *The Principles of Parliamentary Representation*», журнал *Papers on Non-market Decision Making*, том 3, № 1 (1967), с. 1–17.

¹⁴⁶ Chaum, D., «Random-Sample Elections: Far Lower Cost, Better Quality and More Democratic», прочитано в 2012 г. (дата публикации неизвестна), www.rs-elections.com/Random-Sample%20Elections.pdf

¹⁴⁷ Davis, J., «How Selecting Voters Randomly Can Lead to Better Elections», журнал *Wired*, 16 мая 2012 г., www.wired.com/2012/05/st_essay_voting/

Как и идею голосования с использованием случайной выборки¹⁴⁸, концепцию футархии можно воплотить в жизнь с помощью технологий блокчейна, обеспечивающих масштабируемость, децентрализованность, надежность, псевдонимность и ведение реестра записей. Идею футархии, которую предложил экономист Робин Хэнсон¹⁴⁹, а перевел в контекст блокчейна основатель проекта Ethereum Виталик Бутерин¹⁵⁰, можно коротко описать фразой «голосуйте за результат, ставьте на убеждения». Этот пример наглядно показывает преобразующий потенциал блокчейн-технологий. Возможно, такие модели голосования и указания предпочтений, как двухуровневая структура футархии, станут нормой и будут широко использоваться как механизм принятия всех сложных решений с участием большого числа людей. Это может привести к появлению совершенно нового уровня координирования человеческой деятельности, гораздо более сложного, чем сейчас. Конечно, любая новая правительственная структура, включая футархию, допускает злоупотребления. Некоторые механизмы ограничения и защиты от подделки результатов уже имеются, но они требуют совершенствования и создания более надежных моделей.

Для достижения консенсуса, необходимого для регистрации транзакций в распределенном журнале записей, уже сейчас можно использовать две модели, а в будущем могут появиться и новые. Первый механизм консенсуса – майнинг. С помощью программных средств майнеры просматривают, подтверждают и регистрируют транзакции. Вторым механизмом консенсуса – рынки прогнозов. Событие может считаться истинным, если достаточное число независимых участников рынка прогнозов отдало свои голоса за то, что оно истинно. Truthcoin – одна из рыночных площадок на основе блокчейна, не требующая доверия между сторонами, работающая по пиринговому принципу, пытающаяся решить некоторые проблемы, присущие традиционным рынкам прогнозов (такие, как пристрастность голосующих), и объединить концепцию рынка прогнозов со структурой биткойна, позволяющей вознаграждать участников и вести общедоступный реестр записей¹⁵¹. Более того, Truthcoin пытается создать не требующую доверия службу-предсказатель, регистрирующую все релевантные события в распределенном журнале записей.

Примерами представляющих интерес «информационных элементов» могут быть текущие процентные ставки, наивысшая ежедневная температура, высшая и низшая дневная стоимость криптовалюты, объем торгов и т. д. В цепи создания стоимости блокчейн-операций с умными контрактами ключевым компонентом будут независимые предсказатели, предоставляющие соответствующую информацию. Например, ипотечные кредиты в распределенном журнале записей могут иметь будущие даты сброса процентной ставки, автоматически применяющиеся при получении информации из заслуживающего доверия источника, зарегистрированного в блокчейне надежным независимым предсказателем, таким как Truthcoin.

Влияние блокчейн-правительства на социальную зрелость

Побочным эффектом блокчейн-правительства может стать достижение обществом и отдельными гражданами нового, более высокого уровня зрелости, который обеспечивает теоретическое и практическое понимание таких концепций, как правительство, власть и

¹⁴⁸ Концепция голосования по случайной выборке (random-sampling elections) предложена Дэвидом Чаумом, криптологом, доктором наук по информатике и менеджменту. – *Прим. ред.*

¹⁴⁹ Hanson, R., «Futarchy: Vote Values, but Bet Beliefs», прочитано в 2013 г. (дата публикации неизвестна), <http://hanson.gmu.edu/futarchy2013.pdf>

¹⁵⁰ Buterin, V., «An Introduction to Futarchy [as Applied with Block-chain Technology]», блог Ethereum, 21 августа 2014 г., <https://blog.ethereum.org/2014/08/21/introduction-futarchy/>

¹⁵¹ Cruz, K., «The Truth Behind Truthcoin», журнал *Bitcoin Magazine*, 25 сентября 2014 г., <http://bitcoinmagazine.com/16748/truth-behind-truthcoin/>

независимость. Мы не привыкли к мысли о том, что государственное управление может быть личной ответственностью каждого и пиринговой системой, а не чем-то внешним, насаждаемым удаленной централизованной структурой. Мы не привыкли ко многим особенностям блокчейн-технологий, таким как необходимость резервного копирования своих денег, но мы учимся, приобретаем новые знания и привычки, осваивая новые технологии. Точно так же мы не привыкли к децентрализованной политической власти и автономности.

Однако мы уже пришли к принятию децентрализованного управления в других контекстах. Это произошло в других индустриях; например, по мере развития блогов и реструктуризации медиасреды новости и публикации становятся все более децентрализованными. То же происходит в индустрии развлечений, где крупные корпорации сосуществуют с каналами YouTube и обычными людьми, загружающими свой контент в интернет. Цепочка создания ценности стала очень длинной, и у каждого пользователя теперь собственное мерило качества. В XXI веке необходима способность оценить контент и решить для себя, насколько высоко его качество и соответствует ли он другим индивидуальным критериям. Биткойн вызвал такие же революционные изменения в сфере экономики, финансов и денежной политики. Избавиться от централизованной власти в сфере государственного управления и экономики не так просто, как в культурно-информационной, но это не причина отказываться от достижения социальной зрелости в данных областях.

Глава 4

Блокчейн 3.0: эффективность и координация в обществе

Наука на блокчейне: Gridcoin, Foldingcoin

Блокчейн-технологии могут произвести революцию во многих областях, включая науку. Пока что основное направление научного использования – проекты распределенных пиринговых вычислений, в которых добровольцы предоставляют свободные вычислительные мощности для решения различных задач. В этом отношении следует отметить два проекта: SETI@home и Folding@home. Первый работает в области поисков внеземного разума и анализирует радиосигналы из космоса, пытаясь обнаружить признаки инопланетных цивилизаций. Второй – проект Стэнфордского университета, который занимается моделированием свертывания белка, компьютерным проектированием лекарств и решением других задач молекулярной динамики. На базе блокчейн-технологии созданы криптовалюты для вознаграждения участников обоих проектов. Для SETI@home используется валюта Gridcoin, доступная во всех проектах, работающих в инфраструктуре BOINC (открытая инфраструктура университета Беркли для сетевых вычислений), в том числе и SETI@home. Для Folding@home используется Foldingcoin, токен Counterparty, который можно обменять на более ликвидную криптовалюту XCP (а значит, и на биткойны и фиатные деньги) через кошелек Counterparty (Counterwallet).

Использование блокчейна в научных целях позволяет решить проблему расточительства майнинговой сети, имеющей огромное энергопотребление. Вместо перемалывания произвольных чисел вычислительные ресурсы сети могли бы применяться для более полезных задач, таких как решение научных проблем. Однако алгоритм майнинга имеет очень специфичные требования, такие как генерация строк кода или хешей, легко проверяемых в одном направлении, но не в обратном, а традиционные научные вычислительные задачи такой структуры не имеют¹⁵². Существуют проекты использования майнинга криптовалют с пользой для науки, например Primecoin, в рамках которого майнеры ищут длинные цепочки простых чисел (последовательности Каннингема и последовательности простых чисел-близнецов) вместо хешей SHA256 (случайный подбор значений для числа, заданного программами майнинга на основе определенных параметров)¹⁵³. В этой области можно совершить прорыв, если изменить подход к сверхпроизводительным и сетевым вычислениям так, чтобы их можно было выполнять в формате майнинга и утилизировать бесцельно расходуемые вычислительные ресурсы¹⁵⁴.

Если Gridcoin и не решает полностью проблему использования растрачиваемых при майнинге ресурсов, то он хотя бы дает майнерам стимул участвовать в полезных вычислениях. Если майнеры, выполняющие майнинг блока валюты, предоставляют проекту вычис-

¹⁵² Wagner, A., «Putting the Blockchain to Work For Science!», журнал *Bitcoin Magazine*, 22 мая 2014 г., <http://bitcoinmagazine.com/13187/putting-the-blockchain-to-work-for-sci-ence-gridcoin/>

¹⁵³ Buterin, V., «Primecoin: The Cryptocurrency Whose Mining Is Actually Useful», журнал *Bitcoin Magazine*, 8 июля 2013 г., <http://bitcoinmagazine.com/5635/primecoin-the-crypto-currency-whose-mining-is-actually-useful/>

¹⁵⁴ Myers, D. S., Bazinet, A. L., Cummings, M. P., «Expanding the Reach of Grid Computing: Combining Globus- and BOINC-Based Systems», центр Center for Bioinformatics and Computational Biology, институт Institute for Advanced Computer Studies, Мэрилендский университет, 6 февраля 2007 г. (черновик), http://lattice.umi.acs.umd.edu/latticefiles/publications/lattice/myers_bazinet_cummings.pdf

лительные ресурсы, они получают гораздо более высокое вознаграждение (до 150 GRC – по сравнению со стандартными 5 GRC). Распространенная претензия к блокчейн-технологиям – бесцельная трата вычислительных ресурсов и электроэнергии. Энергия, потраченная на майнинг биткойнов с 2009 года, позволила бы освещать Эйфелеву башню 260 лет¹⁵⁵. В 2013 году на майнинг биткойнов тратилось около 982 мегаватт-часов в день (достаточно для электропитания 31 тыс. домов в США или половины Большого адронного коллайдера)¹⁵⁶, расходы оцениваются в 15 млн долларов в день¹⁵⁷. Однако такое сравнение не вносит особой ясности – много это или мало? И, если уж на то пошло, какова прямая экономическая польза Эйфелевой башни или коллайдера? Сторонники биткойна парируют тем, что модель блокчейна обходится гораздо дешевле, чем текущая финансовая система со всей ее материальной инфраструктурой и персоналом. На передачу 100 долларов через блокчейн требуется гораздо меньше расходов, чем на традиционную транзакцию. Однако вопросы о том, как избежать бесцельной траты электроэнергии при майнинге, продолжая поддерживать блокчейн, остаются актуальными, и инновации, предлагаемые в версии 3.0, могут быть полезными. Одно из решений – более энергоэффективные криптовалюты, такие как Mintcoin.

Распределенные сверхпроизводительные вычисления

Проекты SETI@home и Folding@home показывают примеры распределенных сверхпроизводительных вычислений, в которых добровольцы, официально не участвующие в исследованиях, обеспечивают проекты вычислительными ресурсами. Можно развить эту модель, используя механизмы распределения ресурсов на основе блокчейна, чтобы независимые исследователи могли обращаться к этим вычислительным мощностям для работы над собственными проектами. Модель, аналогичная Kickstarter, позволит авторам проектов запрашивать вычислительные ресурсы, находить единомышленников и инвесторов, стимулируя и вознаграждая активность соответствующей криптовалютой. Zennet – один из первых проектов, в рамках которого пользователи могут регистрировать свои проекты и получать доступ к сетевым ресурсам через блокчейн-структуру. Разрабатываются также другие проекты, позволяющие задействовать широкие массы в обработке открытых наборов данных по принципам, описанным в книге «Викиномика» («Wikinomics», 2008)¹⁵⁸. Однако блокчейн предоставляет больше свободы, позволяя развертывать подобные проекты в широчайшем масштабе – фактически в максимальном из возможных – и предоставляя возможности, которых ученые раньше не имели из-за ограниченности ресурсов. В «Викиномике» и других работах обоснована роль обычных людей в ценной поддержке научных исследований: как поставщиков вычислительной мощности и канала получения данных¹⁵⁹. Это можно использовать, например, в проектах моделирования погоды для получения свидетельств крупномасштабных явлений, таких как изменение климата.

¹⁵⁵ Clenfeld, J., Alpeyev, P., «The Other Bitcoin Power Struggle», журнал *Bloomberg Businessweek*, 24 апреля 2014 г., <http://www.businessweek.com/articles/2014-04-24/bitcoin-min-ers-look-for-cheap-electricity-to-keep-out-a-profit>

¹⁵⁶ Gimein, M., «Virtual Bitcoin Mining Is a Real-World Environmental Disaster», информационное агентство Bloomberg, 12 апреля 2013 г., <http://www.bloomberg.com/news/2013-04-12/virtual-bitcoin-mining-is-a-real-world-environmental-disaster.html>

¹⁵⁷ Worstall, T., «Fascinating Number: Bitcoin Mining Uses \$15 Million's Worth of Electricity Every Day», журнал *Forbes*, 3 декабря 2013 г., <http://www.forbes.com/sites/tim-worstall/2013/12/03/fascinating-number-bitcoin-mining-us-es-15-millions-worth-of-electricity-every-day/>

¹⁵⁸ Tapscott, D., Williams, A. D., «Wikinomics: How Mass Collaboration Changes Everything», Нью-Йорк, издательство Penguin Group, 2008 г.

¹⁵⁹ Аноним, «Eterna», журнал *Scientific American* (дата публикации неизвестна), <http://www.scientificamerican.com/citizen-science/eterna/>

Глобальное здравоохранение: биткойн и борьба с инфекционными заболеваниями

Блокчейн можно использовать и в области глобального здравоохранения – например, для незамедлительной целевой передачи средств на борьбу с такими эпидемиями, как лихорадка Эбола¹⁶⁰. В работе традиционной банковской системы присутствует технологический фактор запаздывания задержками, тогда как биткойн позволяет мгновенно передавать средства на отслеживаемые адреса, доступные для общественного аудита. В передаче средств через биткойн могут участвовать как отдельные люди, так и организации.

Для развивающихся рынков (охваченных сотовой связью на 70 % и больше) доступны биткойновые СМС-кошельки и механизмы доставки, такие как 37Coins¹⁶¹ и Coinapult, и проекты типа Kipochi¹⁶², интегрированные с распространенными платформами мобильных финансов, такими как M-Pesa (например, в Кении 31 % ВВП тратится через мобильные телефоны¹⁶³). На сайты, следящие за распространением инфекционных заболеваний, такие как Healthmap и FluTrackers, можно добавить функциональность для пожертвований в биткойнах или специализированной криптовалюте.

Биткойн и благотворительность

Одна из наиболее известных в мире благотворительных организаций, принимающих биткойны, – «Аванпост Шона» («Sean's Outpost»). Это некоммерческая организация из Пенсаколы, штат Флорида, оказывающая помощь бездомным. Поскольку появляется все больше людей, получающих биткойны и не имеющих возможности тратить их по месту жительства или просто не знающих, что с ними делать, а также биткойн-стартапов, которым требуется демонстрация отправки биткойнов по сети, эта организация смогла привлечь в виде пожертвований значительные суммы и вложить их в социальные проекты, такие как приют для бездомных «Лес Сатоши» («Satoshi Forest»)¹⁶⁴.

¹⁶⁰ Vigna, P., Casey, M. J., «BitBeat: Could Bitcoin Help Fight the Ebola Crisis?», газета *The Wall Street Journal*, 8 октября 2014 г., <http://blogs.wsj.com/moneybeat/2014/10/08/bit-beat-could-bitcoin-help-fight-the-ebola-crisis/>

¹⁶¹ Cawrey, D., «37Coins Plans Worldwide Bitcoin Access with SMS-Based Wallet», сайт CoinDesk, 20 мая 2014 г., <http://www.coindesk.com/37coins-plans-worldwide-bitcoin-access-sms-based-wallet/>

¹⁶² Rizzo, P., «How Kipochi Is Taking Bitcoin into Africa», сайт CoinDesk, 25 апреля 2014 г., <http://www.coindesk.com/kipochi-taking-bitcoin-africa/>

¹⁶³ Mims, C., «M-Pesa: 31 % of Kenya's GDP Is Spent Through Mobile Phones», сайт Quartz, 27 февраля 2013 г., <http://qz.com/57504/31-of-kenyas-gdp-is-spent-through-mobile-phones/>

¹⁶⁴ Buterin, V., «Sean's Outpost Announces Satoshi Forest, Nine-Acre Sanctuary for the Homeless», журнал *Bitcoin Magazine*, 9 сентября 2013 г., <http://bitcoinmagazine.com/6939/sean-s-outpost-announces-satoshi-forest/>

Блокчейн и геномика

Демократизация, свобода и другие концепции блокчейна применимы и к *потребительской геномике*. Чтобы обойти ограничения, налагаемые местным регулированием, организации могут перейти в блокчейн и работать в безопасных децентрализованных облаках. Это совсем не обязательно подразумевает стремление к чему-то незаконному с их стороны. С тем же успехом это может указывать на недостаток доверия к местным регуляторам или официальным инстанциям, отсутствие поддержки с их стороны или отсутствие общих ценностей.

В эпоху блокчейна традиционное «правительство 1.0» во многом становится устаревшей моделью и появляются возможности для перехода от доставшихся нам по наследству структур к более персонализированным формам правления. Геномику можно добавить в список примеров транснациональных организаций, выигрывающих от перехода в блокчейн, наряду с ICANN, WikiLeaks, Twitter, Wikipedia, GitHub и новыми децентрализованными автономными корпорациями. Транснациональная блокчейн-геномика имеет смысл в контексте обеспечения права на персональную информацию (владение собственной генетической информацией) как одного из основных прав человека, особенно с учетом резкого снижения стоимости секвенирования генетического кода.

Запреты, окружающие потребительскую геномику во многих развитых странах, можно рассматривать как классическое нарушение свободы личности. Во многих европейских странах и США патерналистская правительственная политика, подверженная лоббистскому давлению со стороны медицинской индустрии, запрещает гражданам получить доступ к собственным генетическим данным. Даже в странах, где персональная генетическая информация используется в здравоохранении, чаще всего нет механизма для получения человеком доступа к этим данным. В США ведущие исследователи в области геномики пытались поднять вопрос об излишних предосторожностях FDA (Управления по контролю качества пищевых продуктов и медикаментов США) относительно потребительской геномики¹⁶⁵ и доказывали, что нет никакого вреда в получении человеком собственных генетических данных¹⁶⁶. Даже наоборот, это может быть полезно: 80 % людей, узнающих о генетической предрасположенности к болезни Альцгеймера, меняют стиль жизни (начинают заниматься физкультурой, принимать витамины и т. д.)¹⁶⁷. В новостях продолжают появляться сообщения о людях, извлекавших пользу из своих генетических данных, узнав о предрасположенности к различным заболеваниям¹⁶⁸.

Из-за патерналистских предубеждений и отсутствия четкой государственной политики относительно превентивной медицины американские компании, работающие в области потребительской геномики, закрываются (deCODEme¹⁶⁹), переходят к исключительно клиническим исследованиям (Pathway Genomics, Navigenics) или значительно сокращают диа-

¹⁶⁵ Green, R., Farahany, N. A., «Regulation: The FDA Is Overcautious on Consumer Genomics», журнал *Nature*, 15 января 2014 г., <http://www.nature.com/news/regulation-the-fda-is-over-cautious-on-consumer-genomics-1.14527>

¹⁶⁶ Wright, C. et al., «People Have a Right to Access Their Own Genetic Information», блог Genomes Unzipped: Personal Public Genomes, 3 ноября 2011 г., <http://genomesunzipped.org/2011/03/people-have-a-right-to-access-their-own-genetic-information.php>

¹⁶⁷ Green, R. C. et al., «Disclosure of APOE Genotype for Risk of Alzheimer's Disease», журнал *New England Journal of Medicine*, 361 (16 июля 2009 г.), с. 245–254, <http://www.nejm.org/doi/full/10.1056/NEJMoa0809578>, рассмотрено подробнее на сайте <http://www.genomes2people.org/director/>

¹⁶⁸ Regalado, A., «The FDA Ordered 23andMe to Stop Selling Its Health Tests. But for the Intrepid, Genome Knowledge Is Still Available», журнал *MIT Technology Review*, 19 октября 2014 г., <http://www.technologyreview.com/featuredstory/531461/how-a-wiki-is-keeping-direct-to-consumer-genetics-alive/>

¹⁶⁹ DeCODEme, «Sales of Genetic Scans Direct to Consumer Through deCODEme Have Been Discontinued! Existing Customers Can Access Their Results Here Until January 1st 2015», http://en.wikipedia.org/wiki/DeCODE_genetics

пазон услуг (23andMe¹⁷⁰). В ответ на это службы, работающие в блокчейне, могут предлагать секвенирование генетического кода по более низким ценам, делая данные доступными через закрытый ключ.

Одна из сложнейших задач современной медицины – переход от текущей узконаправленной модели лечения установленных патологий к совершенно новой, основанной на анализе большого объема данных концепции превентивной медицины, цель которой состоит в поддержании и улучшении здоровья¹⁷¹. Это станет возможным путем анализа персональных больших данных и прогнозирования потенциальных будущих условий. Персональная геномика может стать основным источником данных для превентивной медицины при условии осведомленности и активности заинтересованных лиц¹⁷².

В ноябре 2014 года проект генетических исследований в блокчейне Genecoin запустил сайт для оценки интереса потребителей, позиционируя свои услуги как возможность сохранения человеком своей ДНК¹⁷³.

Блокчейн-геномика 2.0: секвенирование в общечеловеческом масштабе

В будущем могут появиться блокчейн-службы, находящиеся вне юрисдикции местных властей и позволяющие отдельным людям секвенировать генетический код и обращаться к нему с помощью закрытого ключа. Однако для перехода на более эффективный и практичный уровень, позволяющий секвенировать генетический код всего семимиллиардного населения Земли, требуются более масштабные модели, и блокчейн-технологии могут предоставить механизмы для реализации подобного проекта. Компании, предлагающие услуги индивидуального секвенирования генома, могут рассматриваться как первоначальное подтверждение правильности концепции, как инструмент для повышения грамотности населения в области здравоохранения и механизм доставки персональных результатов и рекомендаций, но не как решение задач общечеловеческого масштаба.

Технологии блокчейна, предлагающие универсальную модель записи, хранения и доступа к информации с обеспечением безопасности и псевдонимности, дают решение для перехода на следующий этап масштабного расчета генетического кода. Это применимо к секвенированию генетических последовательностей в целом, безотносительно к вопросам прав доступа к данным. Генетический код всех людей – только одна из возможных задач; можно получить код всех животных, растений, вирусов, бактерий, патогенных микроорганизмов, микробиомов, протеомов и многого другого.

Масштабность и эффективность – немаловажные аргументы в пользу транснациональных служб на основе блокчейна. Чтобы перейти к получению генетического кода всей человеческой популяции, необходима не только транснационализация, но и тесная интеграция с облаками, поскольку данные генома слишком объемны для используемых в настоящее время локальных хранилищ и средств работы с ними.

¹⁷⁰ Castillo, M., «23andMe to Only Provide Ancestry, Raw Genetics Data During FDA Review», информационное агентство CBS News, 6 декабря 2013 г., <http://www.cbsnews.com/news/23andme-to-still-provide-ancestry-raw-genetics-da-ta-during-fda-review/>

¹⁷¹ Swan, M., «Health 2050: The Realization of Personalized Medicine Through Crowdsourcing, the Quantified Self, and the Participatory Biocitizen», журнал *J Pers Med*, 2, № 3 (2012), с. 93–118.

¹⁷² «Multigenic Condition Risk Assessment in Direct-to-Consumer Genomic Services», журнал *Genet Med*, том 12, № 5 (2010 г.), с. 279–88; Kido, T. et al., «Systematic Evaluation of Personal Genome Services for Japanese Individuals», журнал *Nature: Journal of Human Genetics*, том 58 (2013 г.), с. 734–741.

¹⁷³ Tamblyn, T., «Backup Your DNA Using Bitcoins», Hufington Post UK, 30 октября 2014 г., http://www.hufingtonpost.co.uk/2014/10/30/genecoin-genome-backup-bit-coin_n_6076366.html

Блокчейн обеспечивает и транснационализацию, и возможности облака. Транснациональные региональные центры расчета генетических последовательностей и управления полученной информацией могут быть более эффективным способом структуризации этой индустрии, чем создание отдельных организаций в разных странах, – учитывая необходимые расходы, оборудование, экспертные знания и масштабность. Блокчейн-технология позволяет выйти на более эффективный и масштабный уровень – расчет миллионов и миллиардов генетических последовательностей, а не сотен, как в настоящее время. В действительности достаточно решения хотя бы проблемы обработки и хранения информации; другие задачи относятся, скорее, к промышленным способам получения генетического кода. Как бы то ни было, экосистема блокчейна открывает много новых возможностей в самых разных областях и позволяет проводить масштабные расчеты генетических последовательностей, используя концепции децентрализации.

Технологии блокчейна как универсальная модель развития

Блокчейн-технологии могут предоставлять механизмы и модели, необходимые для дальнейшего развития таких областей, как большие данные, позволяя перейти к «действительно большим данным» и дальше. Генетические последовательности служат одним из первых примеров для демонстрации этих новых моделей.

Genomecoin, GenomicResearchcoin

Даже если не спекулировать на тему возможностей получения генетического кода всего человечества, использование блокчейна во многом поможет уже существующим проектам. Например, можно добавить функциональность блокчейна и криптовалют в службу DNAnexus, позволяющую хранить генетический код в облаке. Проект DNAnexus разработан при участии университетов (Центр секвенирования генома человека

Медицинского колледжа Бейлора) и веб-служб Amazon Web Services. По данным на 2013 год, это крупнейшее хранилище геномов, содержащее 3751 полностью расшифрованный геном человека и 10 771 экзом (440 ТБ данных)¹⁷⁴. Сегодняшнее достижение – хранилище для 4 тыс. человеческих геномов из 7 млрд возможных, что подчеркивает необходимость в крупномасштабных моделях для таких проектов с использованием больших данных.

База данных DNAnexus не является общедоступной: лишь 300 исследователей со всего мира имеют разрешение на ее использование. Genomic Data Commons¹⁷⁵ – проект, спонсируемый правительством США, занимающийся исследованиями в области генетики и персонализированной медицины, имеющий крупное хранилище данных. Предполагается, что ресурсы проекта будут доступны любому исследователю, находящемуся в США. Это хорошее продвижение по пути организации данных с помощью стандартных унифицированных хранилищ с доступом определенного круга специалистов.

Следующим шагом может быть использование специализированной криптовалюты, например Genomecoin, для предоставления полного доступа широким массам населения всего мира. Криптовалюта может служить механизмом отслеживания, координирования и вознаграждения участников сообщества Genome Data Commons. Как и в приведенном выше примере с «Викиномикой», чтобы обеспечить наилучшие условия для прогресса науки, сле-

¹⁷⁴ Grens, K., «Cloud-Based Genomics», журнал *The Scientist*, 28 октября 2013 г., <http://www.the-scientist.com/?articles.view/articleNo/38044/title/Cloud-Based-Genomics/>

¹⁷⁵ Jiang, K., «University of Chicago to Establish Genomic Data Commons», журнал *University of Chicago News*, 2 декабря 2014 г., <http://news.uchicago.edu/article/2014/12/02/university-chicago-establish-genomic-data-commons>

дует сделать информацию полностью открытой и позволить обрабатывать данные из самых разных областей деятельности.

Одним из преимуществ использования биткойна и блокчейна в качестве экономической модели является то, что эти технологии автоматически включают экономические функции в любую систему. В контексте секвенирования и хранения генетической информации такие функции можно использовать для более точного определения стоимости исследований (отслеживание и ведение бухгалтерского учета в блокчейне) с помощью валюты Genomecoin или GenomicResearchcoin (система вознаграждений с помощью микроплатежей). В числе других применений блокчейна можно отметить возможность установления авторства (как в системе GitHub или в концепции защиты цифровой интеллектуальной собственности), позволяющую стимулировать и поощрять участников крупных проектов.

Блокчейн и здравоохранение

В будущем могут появиться специализированные блокчейны (реестры учета) разного типа для регистрации и отслеживания различных процессов, предоставления доступа и обмена всевозможными активами, включая цифровые медицинские данные. Блокчейн-здравоохранение – концепция, предполагающая использование блокчейн-технологий в области медицины и здравоохранения¹⁷⁶. Блокчейн предоставляет структуру для хранения и анализа медицинских данных с сохранением их конфиденциальности и возможностью получать экономическую компенсацию за их использование¹⁷⁷.

Healthcoin

Валюта или токены Healthcoin могут широко использоваться для оплаты медицинских услуг, способствуя более справедливому ценообразованию и повышению качества обслуживания в этой сфере. Результатом может стать ценовая прозрачность и появление универсального прайс-листа вместо принятой (в США) системы, в которой стоимость услуг для каждого пациента различается в зависимости от плана страхования. Например, определенная услуга всегда будет стоить 5 Healthcoin.

Электронные медицинские карты

Персональные медицинские записи можно хранить и администрировать в распределенном журнале записей как в глобальной системе электронных медицинских карт. Блокчейн обеспечивает псевдонимность (использование цифрового адреса, а не имени) и конфиденциальность (доступ только по закрытому ключу), что позволяет кодировать медицинские карты как цифровую собственность и размещать их в блокчейне. Пользователи могут предоставлять врачам, фармацевтическим и страховым компаниям доступ к своим записям при помощи закрытого ключа. Кроме того, службы хранения электронных медицинских карт в блокчейне могут способствовать созданию универсального формата данных для различных поставщиков медицинских услуг, которые в настоящее время по большей части разрознены и несовместимы, несмотря на то, что в большинстве крупных учреждений используются электронные системы. Блокчейн позволит создать единый глобальный формат хранения медицинских данных и обмена ими.

Хранилища медицинских данных в блокчейне

Одно из главных преимуществ создания стандартизированных хранилищ медицинских записей – доступность информации исследователям. До сих пор все хранилища медицинской информации были закрытыми, как, например, данные одного из самых продолжительных мировых исследований – Фремингемского исследования сердца. Блокчейн позволяет создать безопасный стандартизированный механизм оцифровки медицинских данных и их сохранения в общественных хранилищах, доступных исследователям. Один из

¹⁷⁶ Swan, M., «Blockchain Health – Remunerative Health Data Commons & HealthCoin RFPs», блог Broader Perspective, 28 сентября 2014 г., <http://futurememes.blogspot.com/2014/09/blockchain-health-remunerative-health.html>

¹⁷⁷ «20 Questions for Health IT #5: Bitcoin & Blockchain Technology», блог HL7 Standards, 8 сентября 2014 г., <http://www.hl7standards.com/blog/2014/09/08/20hit-5/>

таких примеров – стартап DNA.bits, записывающий кодированные сведения о ДНК пациентов в блокчейн и предоставляющий исследователям доступ с помощью закрытого ключа¹⁷⁸.

Хранилища медицинских исследовательских данных в блокчейне могут быть не только закрытыми, но и открытыми. Блокчейн предоставляет рентабельную модель создания таких хранилищ. Многие люди хотели бы предоставить для исследований свой генетический код (его расчет можно заказать на сайте 23andMe), данные с цифровых устройств мониторинга состояния здоровья и тренировок (FitBit и MapMyRun) и другую информацию при условии соблюдения приемлемого уровня конфиденциальности, но не имеют такой возможности. Эти данные можно агрегировать в общественных хранилищах, аналоге Wikipedia, доступных всем исследователям. Можно предположить, что такая интеграция больших объемов данных о состоянии здоровья (генетические коды, сведения об образе жизни, истории болезней и другие) и их обработка с помощью средств машинного обучения и других алгоритмов позволят получить корреляции и выводы, полезные для поддержания здоровья и предотвращения заболеваний¹⁷⁹. Агрегирование персональных медицинских данных в блокчейне – то есть хранение в цепочках блоков указателей на внешние данные – позволяет сделать медицинские исследования в целом более эффективными. Исследования могут стимулироваться также экономическими средствами блокчейна. Пользователи будут охотнее передавать свои данные в общественные хранилища, основанные на распределенном журнале записей, так как, во-первых, обеспечивается конфиденциальность (данные шифруются, а доступ псевдонимен), а во-вторых, предоставляются вознаграждения (Healthcoin).

Службы медицинского освидетельствования в блокчейне

Медицинское освидетельствование – востребованная услуга, необходимая для получения страховки, рецептов на медикаменты, различных лицензий, водительских прав и т. д. Стандартные нотариальные функции, о которых мы уже говорили, в равной степени подходят и для медицинского освидетельствования в блокчейне. Медицинские документы можно записывать в блокчейн как цифровые активы и при необходимости проверять и подтверждать их в считанные секунды при помощи технологий шифрования, а не ждать несколько часов или дней, как при использовании традиционных методов. Кроме того, шифрование с закрытым ключом, применяемое в блокчейне, делает более эффективным и конфиденциальным оказание некоторых услуг и обследований.

Контракты на предоставление медицинских услуг

Блокчейн-здравоохранение позволяет создать двусторонний рынок для всех медицинских услуг. Врачи и медучреждения могут подавать заявки на предоставление услуг потребителям-пациентам наподобие того, как водители подают заявки в сервис Uber. Можно регистрировать определенные услуги и операции, например замену сустава, и указывать их стоимость, например в валюте Healthcoin. Одно это даст некоторую ценовую прозрачность и повысит эффективность сектора здравоохранения. Регистрацию заявок можно сделать более эффективной, автономной и справедливой, автоматизировав ее посредством торговых сетей.

¹⁷⁸ Zimmerman, J., «DNA Block Chain Project Boosts Research, Preserves Patient Anonymity», сайт CoinDesk, 27 июня 2014 г., <http://www.coindesk.com/israels-dna-bits-moves-beyond-currency-with-genes-blockchain/>

¹⁷⁹ Swan, M., «Quantified Self Ideology: Personal Data Becomes Big Data», сайт Slideshare, 6 февраля 2014 г., <http://www.slide-share.net/lablogga/quantified-self-ideology-personal-data-becomes-big-data>

Поддержка банков вирусов и хранилищ семян

Еще одна важная функция блокчейн-здравоохранения – архивация и резервное копирование, причем не только данных о выполняемых транзакциях, но и важной для человечества информации в целом. Архивы распределенного журнала записей могут обеспечить дополнительный уровень защиты для банков вирусов, банков генов и хранилищ семян. Блокчейн может быть цифровым воплощением физических хранилищ, таких как Свальбардский всемирный семенной фонд – защищенный склад образцов семян растений всего мира, – хранилища Всемирной организации здравоохранения и Центра контроля заболеваний, содержащие образцы патогенов (например, вирус оспы). В случае распространения эпидемии архивы распределенного журнала записей помогут ускорить принятие адекватных мер, предоставив исследователям со всего мира доступ по закрытому ключу к необходимым файлам секвенированного генетического кода патогенов.

Блокчейн-обучение: МООК биткойна и умные контракты на обучение

Умные контракты на основе блокчейна могут иметь множество применений. Одно из них – умные контракты на обучение. МООК (массовые открытые онлайн-курсы) с использованием биткойна и умные контракты на обучение воплощают идею открытия развивающегося рынка умных контрактов на обучение, доступного всем желающим по всему миру, так же как обычные МООК предоставили принципиальную возможность дистанционного обучения всем желающим.

Как биткойн изменил рынок денежных платежей и расширил доступ к финансовым услугам, так и рынок международной помощи может измениться благодаря пиринговым умным контрактам на основе блокчейна. В блокчейне можно реализовать концепцию микрозаймов Kiva и Grameen или модель благотворительности Heifer International 2.0, но не для финансовой помощи, хотя и она может оказываться, а для прямой поддержки личностного роста. Блокчейн-обучение основано на децентрализованных учебных контрактах.

Один из способов повысить грамотность на развивающихся рынках (а это может быть ключом к искоренению бедности) – децентрализованные умные контракты на обучение, заключенные между спонсором или дарителем и обучающимся. Во многом аналогично тому, как биткойн позволяет обмениваться валютами между странами (децентрализованно, с очень низкой комиссией, без посредников), децентрализованная система контрактов может способствовать заключению контрактов на обучение непосредственно с группами студентов или отдельными студентами по пиринговому принципу. Эта концепция похожа на персонализированные программы обучения в Академии Хана. Обучающиеся могут получать от благотворителей со всего мира биткойны или другие криптовалюты непосредственно в свои цифровые кошельки (37Coins, Coinapolt, Kipochi и др.). Затем они могут использовать эти средства как биткойны или обменивать на местные фиатные деньги для покрытия расходов на обучение в школах или на самообучение. Ключевая составляющая цепочки создания ценности – наличие механизма отчетности – например, предоставляемого и автоматизируемого умными контрактами Ethereum, – для проверки достижений обучающихся. Правила, встроенные в умные контракты на обучение, могут автоматически подтверждать завершение учебных модулей посредством стандартизированных онлайн-тестов, включающих подтверждение личности обучающегося – например, с помощью коротких имен, сопоставляемых с биткойн-адресами такими службами, как OneName, BitID и Bithandle.

После успешного прохождения теста умный контракт может автоматически инициировать передачу средств на оплату следующих учебных модулей. Все координирование контрактов на обучение в блокчейне может быть основано на прямом и полностью автоматизированном взаимодействии обучающегося со спонсором. Повторим, что идея аналогична концепции Kiva или Heifer International (то есть прямое пиринговое взаимодействие), но в применении к индивидуальным контрактам на обучение.

Learncoin

Learncoin может быть криптовалютой для системы умных контрактов на обучение. Учебные заведения, группы и отдельные студенты могут выпускать собственные токены, конвертируемые в Learncoin и биткойн. Финансы на обучение в любой точке мира можно привлекать посредством Learncoin и токенов местных учебных заведений. Как контрактные предложения делают двусторонним рынок медицинских услуг, так и студенты могут публи-

ковать на «бирже обучения» открытые контракты на обучение (или запросы на финансирование), которые могут исполняться спонсорами, находящимися на другой стороне транзакции.

Биржи контрактов на обучение

Биржи контрактов на обучение могут применяться как универсальная модель обучения. Их можно использовать для выполнения государственных программ переподготовки специалистов, для обучения студентов или сотрудников корпораций. Биржи контрактов на обучение позволяют реструктурировать и улучшать программы непрерывного профессионального образования, необходимые во многих областях, включая юриспруденцию, информационные технологии и медицину. Контракты на обучение могут широко применяться на развивающихся рынках. Под «обучением» можно понимать все что угодно – от обучения детей чтению до профессиональной переподготовки и личностного роста.

Научные публикации в блокчейне: Journalcoin

Все виды организованной человеческой деятельности переместились в интернет и теперь могут быть оптимизированы и улучшены с помощью блокчейна, и научные публикации не исключение. В этой области уже произошли некоторые изменения в лучшую сторону – например, появились журналы с открытым доступом, избавившие авторов от платы за публикацию. Соглашение о публикации на GitHub открытого кода приложений для работы с протоколами и криптовалютами, принятое в биткойн-сообществе, распространилось на некоторые исследовательские работы в этой области, включая документацию, публикуемую на GitHub как файлы «readme». Например, венчурный блокчейн-инвестор Дэвид Джонстон опубликовал «Общую теорию децентрализованных приложений»¹⁸⁰, а компания Factom – документацию по нотариальным цепочкам блоков, описывающую концепции объединения операций по аттестации цифровых объектов в пакеты.

Задача организации структуры для научных публикаций в блокчейне заключается не просто в повторении существующих примеров форумов и журналов с открытым доступом, совместным редактированием и продолжительными дискуссиями, а в реализации более фундаментальных концепций блокчейна в блокчейн-журналах. Чтобы понять, какой должна быть децентрализованная пиринговая модель научных публикаций, необходимо выяснить, какие функции несет научная публикация и как воплотить их в децентрализованной модели, если они вообще нужны. «Публикацией» является любой процесс загрузки содержимого в интернет. Кто угодно может «публиковаться» в блогах, вики, Twitter, Amazon и т. д. Модель блокчейна для децентрализованного размещения контента будет не более чем поисковой системой, позволяющей одному человеку найти интересующие его материалы, опубликованные другим человеком. По такому принципу работает децентрализованная пиринговая модель блокчейна. Поэтому издателям научных (и других) работ могут потребоваться дополнительные функции, такие как гарантия качества работы. Издатели могут отвечать за курирование содержимого, его поиск, доступность, релевантность, поддержку, подтверждение, определение статуса и других атрибутов, важных для потребителей. Один из способов улучшить имеющуюся централизованную модель с помощью блокчейн-технологий – использовать экономику как механизм стимулирования работы по улучшению системы.

Для организации микроэкономической системы, позволяющей вознаграждать авторов, редакторов, рецензентов, комментаторов, участников форумов, консультантов, обслуживающий персонал и поставщиков услуг, прямо не связанных с публикацией, можно использовать систему токенов Journalcoin. Система вознаграждений поможет повысить качество и ответственность участников. Journalcoin может дать участникам возможность получать вознаграждения и зарабатывать репутацию, стимулировать и сделать более прозрачным взаимодействие между авторами, рецензентами, научным сообществом и широкими массами читателей. На основе блокчейна можно выпустить метакойны ElsevierJournalcoin и SpringerJournalcoin – например, как активы Counterparty, полностью конвертируемые в биткойн или другие криптовалюты.

Валюта на базе токенов, например Researchcoin, позволит выражать коллективный интерес и приобретать права на определенную исследовательскую документацию, которая в противном случае не пробьется через финансовые преграды. Медицинский стартап Genomics создает систему биткойн-голосования, позволяющую сообществу показать заинтересованность в открытых научных работах на тему эпидемических заболеваний (которые,

¹⁸⁰ Johnston, David et al. The General Theory of Decentralized Applications, 2013. Опубликована на песчпсе <https://github.com/DavidJohnstonCEO/DecentralizedApplications>. – Прим. ред.

кстати, налогоплательщики оплачивают из своего кармана, но не имеют к ним доступа)¹⁸¹. В качестве примера можно привести такую ситуацию. Были найдены люди с мутацией в гене NPC1, устойчивые к вирусу Эбола¹⁸², и это может побудить людей проверить собственные генетические данные, чтобы выяснить, имеют ли они повышенную сопротивляемость к этому вирусу или к другим, таким как ВИЧ¹⁸³. Мнения в этом вопросе разделились между теми, кто выступает за предоставление людям доступа к собственным данным, и теми, кто считает, что не следует предоставлять такую сложную информацию неспециалистам. Впрочем, исследования болезни Альцгеймера, упомянутые ранее, показывают, что положительных следствий предоставления информации все же больше, чем отрицательных.

На основе Journalcoin и научных журналов можно создать валюту ExperimentalResultscoin, позволяющую стимулировать повторение научных экспериментов (согласно статистике, результаты 80 % научных экспериментов не удается получить повторно), публикацию отрицательных результатов и необработанных данных (только 45 % авторов публикуют такую информацию), а также поиск решения других проблем научных публикаций, таких как дублирование результатов, плагиат и недобросовестность¹⁸⁴.

Как биткойн, используемый в качестве механизма цифровых платежей между людьми, может использоваться для платежей в «интернете вещей» и межмашинных платежей, так и ExperimentalResultscoin может служить механизмом стимулирования, координирования и слежения за научными работами, выполняемыми людьми и машинами. Все чаще научные открытия совершаются роботизированными лабораториями и алгоритмическими программами. В качестве примеров можно привести вычислительные алгоритмы Липсона, сумевшие вывести законы физики из экспериментальных данных¹⁸⁵, робота-ученого Магглтона¹⁸⁶, искусственный интеллект Вальца и Бьюкенена¹⁸⁷.

Технологии Блокчейн 3.0 позволяют полностью перенести функции издательства в блокчейн, включая механизм подтверждения качества содержимого. Можно создать модель с использованием децентрализованных автономных организаций и корпораций, искусственного интеллекта и механизмов подтверждения качества, использующую определенные показатели, такие как общее число прочтений и число прочтений специалистами в определенной области, число комментариев, совпадение семантических ключевых слов, совпадение концепции и т. д. для целевого подбора подходящего содержимого. Функциональность микроплатежей блокчейн позволяет предоставлять такие услуги за плату. Идея заключается в организации семантического пирингового поиска с использованием социальных сетей для идентификации участников и технологий блокчейна для платежей и обеспечения конфи-

¹⁸¹ Levine, A. B., «Let's Talk Bitcoin! #158: Ebola and the Body Blockchain with Kevin J. McKernan», подкаст «Let's Talk Bitcoin», 1 ноября 2014 г., <http://letstalkbitcoin.com/blog/post/lets-talk-bitcoin-158-ebola-and-the-body-blockchain>

¹⁸² McKernan, K., «Niemann-Pick Type C & Ebolavirus: Bitcoin Community Comes Together to Advocate and Fund Open Source Ebolavirus Research», журнал *Medicinal Genomics*, прочитано в 2014 г. (дата публикации неизвестна), <http://www.medicin-algenomics.com/niemann-pick-type-c-and-ebola/>

¹⁸³ Аноним, «The Evolving Genetics of HIV: Can Genes Stop HIV?», музей The Tech Museum of Innovation (дата публикации неизвестна), http://genetics.thetech.org/original_news/news13

¹⁸⁴ Аноним, «Unreliable Research. Trouble at the Lab», журнал *The Economist*, 17 октября 2013 г. (платный доступ), <http://www.economist.com/news/briefing/21588057-scientists-think-science-self-correcting-alarming-degree-it-not-trouble>

¹⁸⁵ Schmidt, M., Lipson, H., «Distilling Free-Form Natural Laws from Experimental Data», журнал *Science*, том 324, № 5923 (2009 г.), с. 81–85, http://creativemachines.cornell.edu/sites/default/files/Science09_Schmidt.pdf; Keim, B., «Computer Program Self-Discovers Laws of Physics», журнал *Wired*, 2 апреля 2009 г., <http://www.wired.com/2009/04/newtonai/>

¹⁸⁶ Muggleton, S., «Developing Robust Synthetic Biology Designs Using a Microfluidic Robot Scientist. Advances in Artificial Intelligence – SBIA 2008», конспекты лекций в журнале *Computer Science*, том 5249 (2008 г.), с. 4, http://link.springer.com/chapter/10.1007/978-3-540-88190-2_3

¹⁸⁷ Waltz, D., Buchanan, B. G., «Automating Science», журнал *Science*, том 324, № 5923, (2009 г.), с. 43–44, <http://www.sciencemag.org/content/324/5923/43>

денциальности. Возможно также использование моделей автоматической классификации содержимого без участия человека.

Блокчейн можно использовать также для обнаружения и блокирования плагиата и для автоцитирования: умный контракт или децентрализованная автономная организация, выполняющая поиск по литературе и автоматически цитирующая все связанные работы, позволят сэкономить много времени. Для реализации такой функциональности можно использовать хранилища документов, расположенные вне распределенного журнала записей, и ссылки на них по ключу в блокчейне. Блокчейн может стать стандартом для публикации научных работ, а также данных и метафайлов, связанных с этими работами, то есть универсальной системой каталогизации и библиотекой научных работ. Экономические функции блокчейна облегчат приобретение цифровых копий этих работ, так как у каждой работы будет свой биткойн-адрес или QR-код, что избавит пользователей от необходимости регистрироваться на веб-сайтах издательств.

Блокчейн может не все

Несмотря на множество интересных возможностей технологий блокчейна, важно понимать, в каких областях применение моделей блокчейна и криптовалют неоправданно. Не все процессы требуют внедрения экономической системы, пирингового обмена, децентрализации и надежного хранилища записей.

Другой важный фактор – масштаб операций, поскольку не всегда есть смысл записывать каждую микротранзакцию в общедоступный распределенный журнал записей. Например, транзакции системы чаевых для блога можно объединять в сайдчейны и записывать общую дневную транзакцию. Сайдчейны – это предлагаемый инфраструктурный механизм, посредством которого экосистемы с множественными блокчейнами могут взаимодействовать друг с другом¹⁸⁸. Сейчас, особенно с учетом развития «интернета вещей» и межмашинных взаимодействий, остается много открытых вопросов об эффективности применения рыночных принципов (и их целесообразности в целом) для координации ресурсов, мотивации к достижению поставленных целей, использования средств отслеживания и финансового вознаграждения. Прежде чем рассматривать потенциальные экономические модели для платежей М2М и IoT, необходимо разработать протоколы координирования и взаимодействия огромного числа устройств, внедрить систему контроля и управления для машинных социальных сетей, добавить новые протоколы для простых микрокоманд, таких как «включить», «выключить», «старт» и «стоп»¹⁸⁹.

В более отдаленном будущем возможно разделение блокчейнов по классам, соответствующим их различным применениям. Могут появиться распределенные журналы записей для совершения покупок в продовольственных магазинах и для крупных покупок, таких как недвижимость и автомобили. Распределенные журналы записей неэкономических рынков, таких как правительственные и нотариальные услуги, регистрация интеллектуальной собственности, научная деятельность и ведение медицинских записей, потребуют другой функциональности. Необходимо понять, какие экономические принципы применимы в тех областях, в которых блокчейн-технологии могут быть полезны. И следует помнить, что не каждую операцию можно свести к регистрации и обмену ресурсами.

Не все из описанных идей требуют использования блокчейна. Не везде требуется последовательное, общедоступное, распределенное хранилище данных. Вместо этого можно использовать другие технологии, такие как облачные хранилища или более общие модели распределенных вычислений. Однако и в этом случае блокчейн-технологии могут предоставлять дополнительную функциональность; к тому же сейчас невозможно предугадать, какие применения найдут эти технологии в будущем.

Другая причина, по которой блокчейн подходит не для каждой ситуации, состоит в том, что люди не желают во всем проводить аналогии с экономикой. Качественные аспекты жизни нельзя свести к чисто экономическим принципам. Идея вознаграждений соответствует многим ситуациям и делает их схожими с экономикой, но в некоторых случаях это совершенно противоестественно. Однако более широкая концептуализация экономики, вызванная развитием блокчейна, позволяет получить новое понимание понятий передачи, обмена и подтверждения ценности, которое останется актуальным, даже если блокчейн-технологии не станут вездесущими.

¹⁸⁸ Higgins, S., «Sidechains White Paper Imagines New Future for Digital Currency Development», сайт Coindesk, 23 октября 2014 г., <http://www.coindesk.com/sidechains-white-pa-per-ecosystem-reboot/>; Back, A. et al., «Enabling Blockchain Innovations with Pegged Sidechains», прочитано в 2014 г. (дата публикации неизвестна), <http://www.blockstream.com/side-chains.pdf>

¹⁸⁹ da Costa, F., «Rethinking the Internet of Things: A Scalable Approach to Connecting Everything», Нью-Йорк, издательство Apress, 2013 г.

Баланс между централизацией и децентрализацией

В индустрии блокчейна есть приверженцы как централизованного подхода, так и децентрализации. Кроме того, блокчейн ведет к появлению моделей, комбинирующих централизованные и децентрализованные элементы. Кроме интернета, у нас нет крупномасштабных стандартизированных моделей децентрализации, которые можно концептуализировать и использовать в разных контекстах для организации деятельности. Даже несмотря на то, что децентрализация является основой блокчейн-технологии (децентрализованной, не требующей доверия криптографической системы записи транзакций и ведения общедоступного реестра), она также подвержена и влиянию централизации. Один из примеров – стремление к созданию стандартных централизованных каналов в блокчейн-экономике. Распределенный журнал записей биткойна имеет 90 % капитализации рынка криптовалют, и многие считают, что гораздо проще и безопаснее воплощать идеи протоколов 3.0 на основе биткойна, чем организовывать майнинг альткойна для нового блокчейна.

Майнинг – еще одна область, подверженная влиянию централизации. Жесткая конкуренция привела к тому, что майнингом занимаются в основном не отдельные пользователи, а пулы и обладатели специализированных интегральных схем, и большинство новых блоков биткойна регистрируется несколькими крупными пулами, достигшими критической отметки в 51 % контролируемых мощностей, что может привести к монополизации этой области. Остается только ждать и наблюдать, какой баланс установится между силами, стремящимися к экономической эффективности посредством централизации, и силами, пытающимися организовать децентрализованный обмен, не требующий доверия.

Глава 5

Продвинутые концепции

Терминология и концепции

Развитие блокчейн-экономики приводит к появлению множества новых идей и новых применений для известных концепций. Она предлагает пересмотр понятий, годами принимавшихся как должное и не подвергавшихся критическому анализу: *денежные расчеты, валюта, имущество, правительство, суверенитет, интеллектуальная собственность*. Подвергая сомнению базовые определения и находя новые смыслы в привычных терминах, мы делаем эти концепции более открытыми и доступными для применения в новых условиях.

Идеи использования блокчейна укореняются в сознании людей и применяются на всех уровнях. Возьмем, к примеру, библиотеку. На концептуальном уровне библиотека – это система обмена ценностями: имеется предложение продуктов (книг) и услуг (исследований), потребляемых теми, в ком предлагаемые ценности находят отклик.

Новые модели, такие как блокчейн-технология, заставляют нас рассматривать окружающую действительность на уровне концепций, стоящих за теми или иными явлениями. Мы представляем другие ситуации, в которых можно применить эти концепции. Например, блокчейн – технология децентрализации. Биткойн – воплощение децентрализации в сфере цифровой валюты, но децентрализация может воплощаться многими способами, включая умные активы, делегативную демократию и общественные кредитные бюро. Одним словом, люди все отчетливее начинают видеть мир возможностей или мир *как* возможность, как сказал бы французский философ Жиль Делез¹⁹⁰. Затем нам требуются инструменты для воплощения этой возможности в жизнь. Концепции блокчейна становятся доступными для практического использования посредством обобщенной концептуализации, как сказал бы философ Мартин Хайдеггер¹⁹¹.

В такой побуждающей к действию среде мы гораздо легче создаем новые концепции, такие как GoToLunchcoin или Whatevercoin, используя в новой ситуации более полную концептуализацию понятия *койн* в контексте криптовалют. Койн или токен приложения становится символом, стимулирующим ту или иную деятельность. Член общества может получить койн или токен посредством краудфандинга или выполняя какие-то действия, например майнинг, то есть администрирование главной книги транзакций.

С заработанным койном можно сделать что угодно – например, использовать в сети для приобретения или потребления чего-либо, представляющего ценность. В этом смысле заработанный утром GoToLunchcoin может быть потрачен в обед на восстановление сил – так работает экономический цикл расходования и пополнения ресурсов. На таком начальном уровне создания понятий мы можем проще и быстрее оценить новаторство других идей, когда столкнемся с ними. Например, если мы услышим о криптовалюте PrecedentCoin в юридическом контексте, мы сразу поймем, что это, скорее всего, токен приложения или койн для компенсации затрат, связанных с созданием прецедентов, и в сети появился новый децентрализованный способ выполнения подобных операций.

¹⁹⁰ Deleuze, G., «Cinema 2: The Time-Image», Миннеаполис, издательство University of Minnesota Press, 1989 г.

¹⁹¹ Heidegger, M., «Being and Time», Нью-Йорк, издательство Harper Perennial Modern Classics, 1927 г.

Новый способ мышления позволяет нам проще переключаться между общим и частным уровнями. Примером мышления общими и частными категориями может быть экономика. Экономика на частном уровне – это люди, покупающие и продающие вещи. Но на более высоком обобщенном концептуальном уровне это производство и потребление предметов, представляющих ценность.

Блокчейн-технология на частном уровне – это децентрализованный общедоступный реестр для учета криптовалютных транзакций. Блокчейн-технология на обобщенном концептуальном уровне – это новый класс таких идей, как интернет, общедоступное хранилище данных, высокоточная система отслеживания человеческой деятельности, революционная парадигма организации взаимодействия, механизм борьбы с цензурой, инструмент для обеспечения свободы и равенства, новая модель поиска, передачи и координирования любых дискретных единиц чего угодно. Это только некоторые из примеров того, что представляет собой блокчейн-технология на концептуальном уровне. Ее осмысление на этом уровне, включающем так много частных значений, поможет понять ее потенциальную значимость.

Валюта, токен, токенизация

Валюта – всего лишь одна из идей, пересмотр которых предлагает криптоэкономика. Одно из традиционных словарных определений валюты – «денежная система, принятая для использования в определенной стране». Это определение безнадежно устарело, если учесть транснациональную природу биткойна, не говоря уже о том, что «денежная система» подразумевает централизованный выпуск денег и контроль денежных запасов. Второе определение лучше: «любая разновидность денег, принимаемая многими людьми». Такое определение больше подходит для криптовалют. Отметим, что, хотя биткойн не основан ни на каком «обеспечении» вроде золотого стандарта, фиатные деньги точно так же ничем не обеспечены. «Обеспечение» валюты – это ее массовое принятие людьми, согласными с той или иной массовой иллюзией концепции денег. Если люди примут концепцию криптовалюты и начнут использовать ее и доверять ей, криптовалюта может стать такой же ликвидной, как фиатные деньги.

Как уже говорилось выше, термин *биткойн* может означать распределенный журнал записей блокчейна, протокол биткойн-транзакций или саму криптовалюту биткойн – точно так же и термин *валюта* может иметь разные значения. В контексте криптоэкономики слово *валюта* обобщенно используется для обозначения «единицы ценности, которая может быть заработана и использована в определенной экономической системе», а также обменена на что-то равноценное в других экономических системах. Вместо термина *койн* (coin) с таким же успехом можно использовать термин *токен* (token), то есть цифровой маркер, или средство доступа, или механизм отслеживания некой активности. Для обозначения различных экономических операций, выполняемых в сообществе, могут использоваться различные названия: Appcoin, Communitycoin, Apptoken и т. д.

Например, валюта системы Counterparty (ХСР) предоставляет доступ к определенным функциям, включая возможность выпускать на основе протокола и экономической системы Counterparty новые активы, такие как новый Appcoin, которые в любой момент можно конвертировать в ХСР или биткойн, а значит, и в доллары, евро, юани и любые другие фиатные деньги. Например, LTVcoin – криптовалюта на основе Counterparty, выпускаемая медиасетью Let's Talk Bitcoin для поддержки собственной экономики. LTVcoin используется для принятия спонсорской помощи и пожертвований, вознаграждения членов сообщества за создание контента, написание рецензий и т. д.

LTVcoin функционирует в контексте собственной локальной экономической системы и в любой момент может незамедлительно конвертироваться в биткойны¹⁹². Другие валюты могут точно так же использоваться внутри других локальных экономических систем – «локальных» не в географическом смысле, а в смысле заинтересованности сообщества. Одно из преимуществ криптовалют – возможность их использования для управления распределенными по всему миру группами, объединенными общими интересами. Валюта сообщества может не только поддерживать экономические транзакции, но и предоставлять дополнительные возможности, помогая обеспечить единство сообщества и его согласованность в достижении общих целей. Криптовалюта сообщества может быть механизмом, координирующим достижение намеченных целей.

¹⁹² Crackerhead (псевдоним), «Mining LTBCoin», сайт-форум BitcoinTalk.org, 27 июля 2014 г., <https://bitcointalk.org/index.php?topic=712944.0>

Валюты сообществ: частные деньги Хайека

Быстрое распространение альткойнов и валют сообществ (Communitycoin), обеспечивающих функционирование собственных экономических систем сообществ, как только что описанная валюта LTVcoin, соответствует некоторым прогнозам австрийского экономиста Фридриха Хайека. В книге «Денационализация денег»¹⁹³ Хайек приводит доводы в пользу конкурентного рынка частных денег в противовес навязываемой правительством денежной монополии¹⁹⁴. Оспаривая кейнсианскую теорию инфляции в эссе «Парадокс бережливости»¹⁹⁵¹⁹⁶ и отмечая более обширные возможности производителей на децентрализованных рынках¹⁹⁷, он высказывал и другие фундаментальные идеи, нашедшие отражение в блокчейн-индустрии. В отношении децентрализованной валюты Хайек постулировал модель, в которой каждая финансовая организация выпускает собственную валюту и конкурирует с другими, обеспечивая ценность своей валюты посредством честной и продуктивной деятельности¹⁹⁸.

В реальном мире конкурентных валют может быть несколько. В блокчейн-экономике такая модель может использоваться еще шире: собственные валюты или токены, которые могут абсолютно правомерно использоваться внутри соответствующего сообщества и конвертироваться в другие валюты, такие как биткойн, могут эмитироваться не только финансовыми учреждениями, но и любыми другими организациями, обществами и отдельными гражданами. В мире могут существовать миллионы валют, каждый человек может иметь свою валюту или несколько валют, как почти каждый имеет свой блог и учетную запись в Twitter и Instagram. Например, певица Татьяна Мороз выпустила валюту Tatianacoin на основе протокола Counterparty (@tatianacoin).

Как информационная революция позволила каждому стать автором публикаций, так и блокчейн-революция позволяет каждому стать своим собственным банкиром. Одни группы валют могут и должны конкурировать, другие будут сосуществовать и дополнять друг друга в разных отношениях.

Валюты кампусов

Наиболее очевидными примерами сообществ, имеющих собственную экономику, для которой имеет смысл выпускать собственную валюту, являются корпорации и университетские кампусы. Любой университет – как администрация, так и студенты – сможет использовать открытое шаблонное решение для выпуска своей собственной валюты Campuscoin, например ASUcoin. Группы внутри этих сообществ могут выпускать аналогичные шаблонные альткойны DeltaChiCoin, NeuroscienceConferenceCoin и т. д. для поддержки своей деятельности. Свободно доступные шаблоны таких альткойнов могут содержать определенные модули с готовыми настройками. Например, один модуль может использоваться для покупки

¹⁹³ Hayek, Friedrich. Denationalization of Money, 1976. – Прим. ред.

¹⁹⁴ von Hayek, F. A., «Denationalization of Money: An Analysis of the Theory and Practice of Concurrent Currencies», Лондон, Институт экономических проблем, 1977 г.

¹⁹⁵ «The 'Paradox' of Saving», журнал *Economica*, № 32 (1931 г.).

¹⁹⁶ Hayek, Friedrich. Paradox of Savings, 1929. – Прим. ред.

¹⁹⁷ Blumen, R., «Hayek on the Paradox of Saving», Институт Людвиг фон Мизеса, 9 января 2008 г., <http://mises.org/daily/2804>

¹⁹⁸ Ferrara, P., «Rethinking Money: The Rise Of Hayek's Private Competing Currencies», журнал *Forbes*, 1 марта 2013 г., <http://www.forbes.com/sites/peterferrara/2013/03/01/re-thinking-money-the-rise-of-hayeks-private-competing-currencies/>

и продажи чего-либо внутри сообщества и предоставлять функциональность, аналогичную OpenBazaar или Craigslist.

Другой модуль может иметь децентрализованную модель поиска комнат в общежитии (аналог Airbnb), транспорта (Getaround) и попутчиков (LaZooz).

Третий модуль может быть «консультационной службой» для предоставления консультаций, советов и рекомендаций, касающихся занятий, факультетов, выбора карьеры и т. д. Выпускники могут зарабатывать, консультируя старшекурсников в поисках работы, первокурсники – консультируя старшеклассников, прошедшие определенный курс обучения – тех, кто еще проходит этот курс, и т. д. Campuscoin может предоставить механизм вознаграждения такой деятельности, сейчас ведущейся на добровольных началах или в виде «обязаловки».

Обеспечивая вознаграждение и признание, Campuscoin может способствовать созданию студентами динамичной сети для обмена опытом. Кроме того, валюту кампуса можно использовать для объединения сообществ.

Четвертый модуль может быть «пиринговой обучающей сетью» для обмена конспектами, книгами (что решает проблему отсутствия книги в библиотеке до окончания семестра), поиска единомышленников, формирования групп обучения, подготовки к тестам и т. д. Пятый модуль может служить для связи местных работодателей и студентов, ищущих работу или возможность стажировки, и все это в среде, структурированной посредством вознаграждений.

Уже есть несколько проектов, помогающих студентам больше узнать о возможностях использования криптовалют в университетских кампусах. Организованная студентами криптовалютная сеть кампусов в сентябре 2014 года включала 150 клубов. Это основной источник информации для студентов, заинтересованных в создании собственной криптовалюты кампуса. В будущем эта сеть может стать стандартным хранилищем для шаблонных приложений Campuscoin.

Студенты основали также *Биткойн-ассоциацию Беркли* и в ноябре 2014 года провели свой первый хакатон. Проект MIT Bitcoin Project Массачусетского технологического института внес значительный вклад в повышение криптовалютной грамотности студентов; планируется, что он окажет студентам финансовую помощь в размере 0,5 млн долларов в биткойновом эквиваленте. В октябре 2014 года каждый студент мог получить биткойнов на сумму 100 долларов¹⁹⁹. Стэнфордский университет проводит бесплатные онлайн-курсы по криптографии.

Разбрасывание монет как стратегия распространения

Массачусетский технологический институт применил стратегию «вброса биткойнов», быстро распространив определенное количество среди широкой массы студентов, чтобы стимулировать ознакомление, выработку доверия и принятие новой валюты. Похожая, но более масштабная эмиссия биткойнов, BitDrop, был запланирована в карибском островном государстве Доминика на 14 марта 2015 года в рамках математического фестиваля «День Пи» («Pi Day»). Биткойны планировалось отправить по СМС через сервис Coinapult всем 70 тыс. жителям острова²⁰⁰. Целью было создание крупнейшего в мире биткойн-сообщества и распространение биткойнов среди как можно большего числа людей.

¹⁹⁹ Wong, J. I., «MIT Undergrads Can Now Claim Their Free \$100 in Bitcoin», сайт CoinDesk, 29 октября 2014 г., <http://www.coindesk.com/mit-undergrads-can-now-claim-free-100-bit-coin/>

²⁰⁰ Rizzo, P., «70,000 Caribbean Island Residents to Receive Bitcoin in 2015», сайт CoinDesk, 28 августа 2014 г., <http://www.coin-desk.com/70000-caribbean-island-residents-receive-bit-coin-2015/>

Доминика была выбрана как оптимальная страна с относительно небольшим населением, широким охватом сотовой связью и с возможностью стать региональным обучающим центром. После эмиссии биткойнов на острове планировалось установить банкоматы и торговые автоматы, оперирующие биткойнами. Однако в феврале 2015 года было объявлено об отмене этого события из-за непредоставления необходимых условий правительством Доминики.

Вбросы валюты могут использоваться и в других целях. Например, проекты национальных криптовалют «Nationcoin» могут использоваться для поддержки национальной идеи. Так, в Исландии был разработан проект безвозмездной передачи всем гражданам страны средств в локальной криптовалюте Aurocoin. Есть аналогичные проекты Scotcoin, Spaincoin и Greescoin, но они пока не вступили в активную фазу²⁰¹. Одной из причин запрета биткойна в Эквадоре стали планы по запуску в этой стране собственной национальной криптовалюты²⁰².

Национальные криптовалюты помогают поддержать чувство национальной принадлежности, особенно в странах Евросоюза, где национальные фиатные деньги заменены на евро. Аналогичную идею можно воплотить в «племенных валютах» Tribecoin, помогающих подчеркнуть принадлежность к малым этническим группам. Индейская резервация Пайн-Ридж (Pine Ridge) в северной Дакоте стала первой группой американских индейцев, запустивших собственную криптовалюту MazaCoin, используя право этнической группы на установку собственных правил относительно криптовалют²⁰³.

Валюта: новые определения

В контексте криптоэкономики термин *валюта* может иметь разные смыслы помимо обозначения денег как механизма платежей за товары и услуги. Он приобретает второе важное значение: «нечто ценное, что можно с выгодой использовать в различных ситуациях», или, как уже говорилось, «единица ценности, которую можно заработать и использовать в определенной экономической системе». Существует общая идея валюты или токена как средства доступа к определенным функциям экономической системы. Например, наличие биткойнов открывает доступ к выполнению транзакций в распределенном журнале записей. В некоторых случаях пользователи получают привилегии просто по факту наличия у них биткойнов, так как это подтверждает право владения, а в других сначала нужно потратить какую-то сумму.

Обобщение концепции валюты позволяет применять ее по-новому. Валюта – это маркер ценности, который может быть заработан и использован. Валюта хранит ценность и может передаваться. Такое обобщенное определение соответствует утверждению о существовании многих немонетарных валют, функционирующих по тем же принципам. Например, репутация – это единица ценности, которую можно заработать и использовать в некоторых ситуациях. Это немонетарная валюта в том смысле, что она дает статус для выполнения некоторых задач.

Аналогично этому, здоровье – предмет ценности, который можно заработать и использовать в некоторых ситуациях. Такое широкое понятие валюты как ресурса, который можно

²⁰¹ Cawrey, D., «Auroracoin Airdrop: Will Iceland Embrace a National Digital Currency?», сайт CoinDesk, 24 марта 2014 г., <http://www.coindesk.com/auroracoin-airdrop-iceland-embrace-national-digital-currency/>

²⁰² Khaosan, V., «Ecuador: The First Nation to Create Its Own Digital Currency», сайт CryptoCoins News, обновлено 1 августа 2014 г., <https://www.cryptocoinsnews.com/ecuador-first-na-tion-create-digital-currency/>

²⁰³ Hamill, J., «The Battle of Little Bitcoin: Native American Tribe Launches Its Own Cryptocurrency», журнал *Forbes*, 27 февраля 2014 г., <http://www.forbes.com/sites/jasperhamill/2014/02/27/the-battle-of-little-bitcoin-native-american-tribe-launches-its-own-cryptocurrency/>

заработать и использовать, может включать много других немонетарных валют, кроме репутации и здоровья: намерение, внимание, время, идеи и творчество.

Множественность валют: монетарные и немонетарные валюты

Множественность альткойнов — только один из примеров множественности валют в современном мире. Говоря шире, мы живем в обществе с увеличивающейся множественностью монетарных и немонетарных валют. Во-первых, есть много монетарных валют в виде фиатных денег: доллары, евро, юани и т. д. Во-вторых, существуют и нефатные валюты: бонусы за лояльность, полетные мили и т. д. По некоторым оценкам, насчитывается уже около 4 тыс. таких альтернативных валют²⁰⁴. Теперь стала фактом множественность криптовалют на основе блокчейна: биткойн, Litecoin, Dogecoin и т. д. Кроме монетарных валют, существует множественность немонетарных валют (только что обсуждавшихся), таких как репутация, намерения и внимание²⁰⁵.

Показатели для оценки немонетарных валют, таких как влияние, охват, осведомленность, аутентичность, вовлеченность, предприимчивость, влияние, распространение, связность, скорость, участие, присутствие и общие ценности, разрабатываются в соответствии с рыночными принципами²⁰⁶. Сегодня блокчейн-технология позволяет сделать эти немонетарные социальные валюты более отслеживаемыми и монетизируемыми, расширив возможности их передачи и использования в транзакциях.

Социальные сети могут стать сетями социальной экономики. Например, репутация, как одна из самых признанных немонетарных валют, всегда была важным нематериальным активом, но ее сложно было монетизировать иначе, чем косвенно, в качестве атрибута трудового капитала. Однако теперь может появиться возможность использовать валюты социальных сетей в транзакциях, используя криптовалютные системы чаевых, например Reddcoin, и другие механизмы микроплатежей, ранее недоступные или неприменимые для традиционных фиатных денег.

Как система построчного отслеживания авторства на GitHub повысила эффективность проектов совместной разработки программного обеспечения с открытым исходным кодом, так и криптовалютные системы чаевых могут предоставить измеряемые данные и финансовые стимулы для участия в различных онлайн-проектах. Возможно, если рыночные принципы станут нормой для распределения и обмена нематериальными ресурсами, участники этого рынка изменят поведение, стремясь к обоюдному обмену. Таким образом, применение экономических принципов может сделать общество более открытым для взаимодействия.

²⁰⁴ Lietaerm, B., Dunne, J. «Rethinking Money: How New Currencies Turn Scarcity into Prosperity», Лондон, издательство Berrett-Koehler Publishers, 2013 г.

²⁰⁵ Swan, M., «Social Economic Networks and the New Intangibles», блог Broader Perspective, 15 августа 2010 г., <http://futurememes.blogspot.com/2010/08/social-economic-net-works-and-new.html>

²⁰⁶ «New Banks, New Currencies, and New Markets in a Multicurrency World: Roadmap for a Post-Scarcity Economy by 2050», конференция «Create Futures IberoAmérica, Entusiasmo Cul-tural», Сан-Паулу, Бразилия, 14 октября 2009 г.

Демередж валюты: побуждение к действию и перераспределение

Обновленная, расширенная и получившая новое определение валюта, а именно валюта как цифровой токен, механизм передачи дискретизированных данных, стала одним из основных концепций блокчейн-технологии. С валютой связана идея демереджа или отрицательного процента (*demurrage currency*).

Демередж (demurrage) – термин из торгового мореплавания; означает возмещение убытка судовладельцу за простой судна в порту, например при загрузке или разгрузке сверх оговоренного времени. В контексте криптовалют демередж означает обесценивание необорачиваемых денег со временем, побуждающее к оперативному выполнению с ними каких-либо действий, например расходования. Таким образом, сама валюта может стимулировать экономическую активность. Следовательно, демередж – концепция атрибута, идея встроенного свойства, автоматически мотивирующего и побуждающего к выполнению действий. Дополнительный аспект демереджа валют (или вообще всех цифровых сетевых структур для совершения транзакций, распределения, отслеживания и взаимодействия с ресурсами) – периодическое автоматическое перераспределение валюты (ресурса) по всем сетевым узлам в заранее указанное время или при возникновении определенных событий. Демередж может стать мощным стандартным инструментом администрирования валюты.

Freicoин и Healthcoin – два примера использования демереджа валют с помощью встроенного механизма выполнения действий. Демередж отлично подходит для реализации инициатив вроде гарантированного базового дохода, в соответствии с которыми все граждане или резиденты страны регулярно получают денежное пособие, достаточное для удовлетворения основных жизненных потребностей. Для расходов на удовлетворение базовых потребностей можно использовать валюту GBICoin или Freicoин, которая будет обнуляться через определенные промежутки времени – например, через неделю, месяц или год. Это позволит автоматически поддерживать работу системы и не допустит искусственного создания излишков посредством накопления. Деньги будут больше похожи на купоны, срок действия которых истекает через определенное время. Валюта теряет ценность, что побуждает потратить ее, чтобы не потерять.

Вероятно, GBICoin или Freicoин будет не единственной валютой. В соответствии с концепцией дополнительных или множественных валют Хайека может использоваться специализированная валюта, например Healthcoin. Идея состоит в использовании нескольких валют (а не просто нескольких классов активов), но для разных целей. Какой-нибудь Cashcoin может быть аналогом дебетовой карты для краткосрочных расходов на удовлетворение базовых потребностей. Для расходов может использоваться одна валюта, для сбережений – другая. Различные классы валют могут иметь адаптированные свойства для определенных контекстов, таких как сбережения, инвестиции, транзакции, связанные с недвижимостью, и т. д. Концепция GBICoin или Freicoин – это валюта для повседневных расходов, стимулирующая потребление. Она может выражаться в национальной валюте (Nationcoin), такой как UScoin или Americoin, для ежедневных базовых расходов или в более подходящей для расходов на уровне штата валюте Statecoin, например NYcoin.

Системы дополнительных валют и мультивалютные системы – проявления одного и того же феномена, используемого для реструктуризации многих областей современной жизни.

Подобные системы обеспечивают точную настройку финансовой системы, валют и денег. Практически бесконечные возможности персонализации позволяют нам выбирать кофе (Starbucks), книги и фильмы (Amazon, Netflix), информацию (блоги, Twitter), образо-

вание (YouTube, MOOK) и отношения (полиамория). Теперь персонализированная множественность становится присуща также деньгам и финансовой системе.

Healthcoin может предоставлять аналогичные возможности демереджа валюты. Медицинские услуги могут выражаться в Healthcoin. В США многие планы страхования на случай болезни и планы выбора дополнительных вознаграждений уже являются валютами с демереджем в том смысле, что истекают каждый год. Система «перезагружается», поэтому аноний не возникает. Все национальные службы здравоохранения могут работать по принципу Healthcoin.

Кроме потери стоимости, побуждающей к расходованию, криптовалюта с демереджем позволяет периодически перераспределять средства между сетевыми узлами. Это тоже стимулирует держателей валюты тратить ее. Если рассматривать крайности, эта функция может предоставлять обществу возможность периодического всеобщего перераспределения доходов между населением.

Системы управляемого демереджа имеют очевидный недостаток: при отсутствии стимулов к соблюдению правил люди найдут много хитрых способов и лазеек, чтобы обойти систему. Например, если в накоплении валюты есть какая-то выгода, люди найдут способы обхода ограничения накоплений. В идеале целью должен быть поиск подходящей мотивации и построения общества, в котором попытки обхода будут бессмысленными, поскольку система распределения валюты сможет удовлетворять все базовые нужды индивида. Уверенность в стабильности системы, обеспечивающей повторную выдачу GBICoin, Freicoin или Cashcoin через определенные промежутки времени, и доверие к системе позволят сформировать менталитет изобилия, избавляющий от потребности в накопительстве, особенно при наличии валюты, теряющей ценность из-за демереджа. Это будет беспрецедентная в человеческой истории концептуализация денег и средств для удовлетворения базовых потребностей выживания, позволяющая человеку даже не думать о них. Это принесет огромную пользу и не только введет общество в эпоху изобилия, но и освободит когнитивный потенциал человечества, необходимый для работы над более важными задачами, которые позволят построить новое, более продуктивное и эффективное общество²⁰⁷.

Расширяемость концепций демереджа

Побуждение к действию и динамическое перераспределение, присущие демереджу валюты, не только полезны для разработки специализированных валют в мультивалютном обществе, но, как и многие концепции блокчейна, могут расширяться и обобщаться, выходя за рамки контекста валюты, экономики и финансовых систем. Многие вещи в чем-то аналогичны валюте, экономике или сети, и мы живем в обществе с множественными валютами: в буквальном смысле это означает монетарные системы, а в переносном – репутацию, намерения, внимание и идеи.

Исходя из этой предпосылки, мы можем рассматривать устройства Fitbit и умные часы как валюты здоровья с демереджем. Валюта с демереджем стимулирует и побуждает к какому-либо действию. Пользователь устройства Fitbit или умных часов вечером видит уведомление о том, что за сегодня он прошел 19 963 шага, и хочет достичь 20 000 шагов. То, как Fitbit и умные часы представляют информацию, является механизмом демереджа, побуждающим к действию. Таким образом, здоровье как валюта с демереджем может применяться при проектировании технологий, помогающих выполнять действия, в которых заинтересован пользователь.

²⁰⁷ «Connected World Wearables Free Cognitive Surplus», блог Broader Perspective, 26 октября 2014 г., <http://futurememes.blogspot.com/2014/10/connected-world-frees-cognitive-surplus.html>

Динамическое перераспределение тоже может использоваться во многих других контекстах, таких как распределение ресурсов по сетям. Сети проникли почти во все области современного мира. Очевидное применение демереджа с динамическим перераспределением – распределение ресурсов через автоматические или торговые сети. Системы, повышающие эффективность и масштабируемость, расширяющие возможности отслеживания, всегда найдут применение для распределения ресурсов, таких как газ, электричество, транспорт (например, Uber и LaZooz, беспилотные автомобили и автоматические транспортные системы, ожидаемые в будущем), питьевая вода, пища, услуги здравоохранения, гуманитарная помощь и даже эмоциональная поддержка или обучение контролю умственной деятельности с использованием аппаратов ЭЭГ. Объединение сетей и демереджа валют позволяет получить новую функциональность, такую как динамическое автоматическое распределение ресурсов между узлами сети и предиктивная кластеризация ресурсов по запросу. В качестве примера прогнозирования можно привести вывод на маршрут в аэропорт дополнительных машин такси к прибытию внеплановых рейсов или использование электромобилей в жаркие дни и бензиновых автомобилей в холодные.

Есть и другие примеры использования концепции демереджа в умных сетях. Здоровье – это сеть и валюта с демереджем; ресурс, который можно зарабатывать и тратить; связанный, непрерывно самонастраивающийся механизм, работающий на многих уровнях организма, перераспределяющий различные элементы между синапсами, ячейками, организмами, людьми и обществами. Тело и мозг можно рассматривать как децентрализованное приложение, децентрализованную автономную организацию или корпорацию, где уже функционирует множество автоматизированных систем, составляющих бессознательный уровень, и где можно выполнять запуск других систем для когнитивной оптимизации, лечения патологий и предотвращения болезней, которыми можно явно управлять при помощи интеллектуальных децентрализованных приложений с искусственным интеллектом. Эта концепция включает систему выделения ресурсов с демереджем, реализованную посредством децентрализованного приложения, обеспечивающую автоматическое распределение любого ресурса, потребляемого в системе. Это может быть полезно, например, в случае нейронной потенциации мозга, усиливающей нервные импульсы, проходящие по нервной системе, когда системное распределение ресурсов может улучшить производительность. С помощью нашей технологии когнитивной оптимизации мы хотим распределить и уравнивать способность к потенциации между синапсами в физическом мозге и искусственном интеллекте или программной эмуляции мозга. Валютами с демереджем, требующими распределения в мозге или майндфайле, могут быть различные ресурсы мозга, такие как способность к потенциации, оптогенетическое возбуждение (управление живыми ячейками с помощью световых импульсов и внедрения генетически адаптированных протеинов) или прямая транскраниальная стимуляция.

Другой пример демереджа в контексте здравоохранения – перераспределение ресурсов клетки, являющихся валютами, обеспечивающими физическую поддержку организма. Такими ресурсами могут быть молекулы кислорода, наноботы для удаления отходов, циркуляционные наносхемы. В группах исследователей перераспределяемой валютой могут быть идеи, а валютой общества – свобода, доверие и сострадание. В этом контексте и сам биткойн можно рассматривать как валюту с демереджем и механизмом распределения сетевых ресурсов, распределяющим в обществе специализированную валюту – свободу.

Глава 6

Ограничения

Блокчейн-индустрия находится на раннем этапе развития и сталкивается со многими ограничениями, внутренними и внешними, включая технические проблемы базовых технологий, скандалы и кражи, государственное регулирование и принятие со стороны общества.

Технические сложности

Существует ряд технических сложностей, связанных с конкретными блокчейн-технологиями и с моделью блокчейна в целом. Разработчикам известно об этих проблемах, для них предлагаются решения, и работа по их реализации сопровождается бурными дискуссиями. Инсайдеры имеют разные мнения о том, когда и как удастся решить эти задачи и перейти на следующие этапы развития блокчейн-индустрии. Кто-то считает, что стандартом де-факто станет распределенный журнал записей биткойна, который больше других заслуживает доверия, имеет самую крупную инфраструктуру и оказывает на сеть такое влияние, что единственным правильным решением будет его использование в качестве универсального стандарта. Другие специалисты создают новые блокчейны, например Ethereum, или криптотехнологии, вовсе не использующие блокчейн, такие как Ripple.

Одна из актуальных задач технологии биткойна – преодоление текущего ограничения в 7 транзакций в секунду, особенно в случае массового признания биткойна²⁰⁸. Для сравнения: оператор кредитных карт VISA штатно обрабатывает 2 тыс. транзакций в секунду и может справляться с пиковыми нагрузками до 10 тыс. транзакций в секунду. К другим задачам относится безопасное увеличение размера блока, не приводящее к раздуванию распределенного журнала записей, борьба с уязвимостью майнинга к «атаке 51 %» и внесение в код изменений, не имеющих обратной совместимости. Рассмотрим вкратце основные сложности²⁰⁹.

Пропускная способность

Сеть биткойна имеет потенциальную проблему с пропускной способностью: она обрабатывает только одну транзакцию в секунду (т/с), а текущий теоретический максимум – 7 т/с. Ведущие разработчики заверяют, что этот максимум будет повышен, когда возникнет такая необходимость. Один из способов обеспечения большей пропускной способности – увеличение размера блока биткойна, однако это приведет к проблемам раздувания объема распределенного журнала записей. Для сравнения приведем показатели других сетей, обрабатывающих транзакции:

- VISA: обычная нагрузка – 2 тыс. т/с, пиковая – 10 тыс. т/с;
- Twitter: обычная нагрузка – 5 тыс. т/с, пиковая – 15 тыс. т/с;
- рекламные сети – обычная нагрузка > 100 тыс. т/с.

Задержка

Сейчас каждая транзакция с участием блока биткойна обрабатывается 10 минут – это и есть минимальное время подтверждения транзакции. Для обеспечения достаточной безопасности придется ждать дольше, около часа, а если транзакция крупная, то еще дольше, чтобы снизить риск атаки с двойной тратой (в которой биткойны повторно тратятся путем отдельной транзакции до того, как получатель подтвердит получение причитающихся ему биткойнов). Для сравнения: максимальное время ответа при первичной обработке транзакции VISA – несколько секунд.

Размер и скорость распространения

В конце 2014 года размер распределенного журнала записей биткойна составлял 25 ГБ, а в начале 2016 года – более 60 ГБ. Скачивание такого объема данных может занять целый день. Если число транзакций увеличится до показателей VISA (2 тыс. транзакций в секунду),

²⁰⁸ Lee, T. B., «Bitcoin Needs to Scale by a Factor of 1000 to Compete with Visa. Here's How to Do It», газета *The Washington Post*, 12 ноября 2013 г., <http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/12/bitcoin-needs-to-scale-by-a-factor-of-1000-to-compete-with-visa-heres-how-to-do-it/>

²⁰⁹ Spaven, E., «The 12 Best Answers from Gavin Andresen's Reddit AMA», сайт CoinDesk, 21 октября 2014 г., <http://www.coin-desk.com/12-answers-gavin-andresen-reddit-ama/>

то увеличение размера составит 1,42 ПБ в год или 3,9 ГБ в день. При скорости 150 тыс. т/с распределенный журнал записей будет расти на 214 ПБ в год. Биткойн-сообщество называет проблему увеличения размера блокчейна «раздуванием», и это позволяет предположить, что пользователи предпочитают журналы записей небольшого объема. Однако для настоящего масштабирования, необходимого для внедрения идеи блокчейна в широкие массы, журнал записей должен стать большим, а доступ к нему – более эффективным. Это наводит на мысли о централизации, поскольку для запуска полного узла биткойна (работающий в фоновом режиме сервер, хранящий и раздающий блокчейн) требуются ресурсы, и в настоящее время число полных узлов упало примерно до 7 тыс. серверов по всему миру.

О том, должны ли системы, на которых запущен полный узел, получать вознаграждение, ведутся дискуссии. 60 ГБ – это вроде бы не так много в современную эпоху больших данных, когда исследователи работают с терабайтами информации. Но исследовательские данные можно сжать, а блокчейн сжимать нельзя из соображений безопасности и доступности. Впрочем, это открывает возможность для разработки инновационных алгоритмов сжатия, позволяющих использовать блокчейн, записывать в него данные, сохранять целостность и доступность даже при достижении гораздо большего размера. Один из новаторских способов решить проблему раздувания распределенного журнала записей и сделать данные более доступными – использовать API, как Chain и другие производители, поддерживающие автоматизированные обращения к полному журналу записей биткойна. Некоторые решения получают балансы адресов и изменения этих балансов и уведомляют пользовательские приложения, когда в сеть добавляются новые транзакции или блоки. Существуют также средства для работы с блоками, имеющие веб-интерфейс (например, <https://blockchain.info/>), приложения-посредники, позволяющие запрашивать данные распределенного журнала записей частично, и мобильные электронные кошельки с пользовательским интерфейсом, эффективно работающие с усеченным набором данных блокчейна.

Безопасность

Распределенный журнал записей биткойна имеет ряд потенциальных проблем с безопасностью. Наибольшие опасения вызывает «атака 51 %», которая станет возможной, если некто получит контроль минимум над 51 % вычислительных мощностей, используемых для майнинга. Это позволит ему совершать двойную трату собственных биткойнов, ранее участвовавших в транзакциях (но не биткойнов, принадлежащих другим людям)²¹⁰. Эта проблема возникает из-за тенденции к централизации майнинга – запись большинства транзакций выполняется несколькими крупными пулами. В настоящий момент можно полагаться только на добросовестность владельцев крупных пулов. Некоторые из них (например, Ghash.io) заявляют, что не собираются проводить атаки, но сеть все же небезопасна²¹¹. Двойную трату можно выполнять и другими способами – например, если написать соответствующий код и обманом вынудить пользователя повторно отправить транзакцию. Еще одна проблема безопасности таится в потенциальной возможности взлома эллиптической криптографии, которую использует биткойн. Однако специалисты уже готовят обновления для устранения этой уязвимости²¹².

Бесцельная трата ресурсов

Для майнинга используется огромное количество электроэнергии, которая тратится впустую. По некоторым оценкам, стоимость этой электроэнергии достигает 15 млн долларов

²¹⁰ Prashar, V., «What Is Bitcoin 51 % Attack, Should I Be Worried?», новостной журнал *BTCpedia*, 21 апреля 2013 г., <http://www.btcpedia.com/bitcoin-51-attack/>

²¹¹ Rizzo, P., «Ghash.io: We Will Never Launch a 51 % Attack Against Bitcoin», сайт CoinDesk, 16 июня 2014 г., <http://www.coindesk.com/ghash-io-never-launch-51-attack/>

²¹² Courtois, N., «How to Upgrade the Bitcoin Elliptic Curve», блог Financial Cryptography, Bitcoin, Crypto Currencies, 16 ноября 2014 г., <http://blog.bettercrypto.com/?p=1008>

в день и более²¹³. С одной стороны, именно расточительность майнинга производит децентрализованное доверие в такой модели: пользователи конкурируют, выполняя бесполезную в других отношениях работу, пытаясь получить вознаграждение. С другой стороны, потраченные ресурсы не дают никакой выгоды, кроме безопасности криптовалюты, защищенной подобным майнингом.

Удобство использования

API для работы с Bitcoin (полный узел биткойна) гораздо менее удобен в работе, чем текущие стандарты API, такие как широко используемые API REST.

Различие версий, обратная совместимость, множественные цепочки

Некоторые технические проблемы связаны с инфраструктурой. Одна из них – быстрый рост числа распределенных журналов записей. Новых блокчейнов стало так много, что в некоторых из них несложно развернуть ресурсы для проведения «атаки 51 %». Другая проблема в том, что, когда происходит сплит блокчейна (разделение на две несовместимых цепочки из-за административных причин или при апгрейде сети), становится не так-то легко объединить их или провести перекрестные транзакции на разделенных цепочках.

Серьезную техническую сложность создает требование наличия полной экосистемы подключаемых решений для поддержки всей цепочки создания ценности. Например, распределенному журналу записей требуется безопасное децентрализованное хранилище (MaidSafe, Storj), система сообщений, транспортная структура, протоколы взаимодействия, пространства имен, службы управления адресами, средства сетевого администрирования и архивирования. В идеале индустрия блокчейна будет развиваться, как модель облачных вычислений, для которой заранее, на первых стадиях развития, были определены и реализованы стандартные инфраструктурные компоненты, такие как облачные серверы и система транспорта, что позволило сфокусироваться на более высоком уровне услуг добавления ценности, а не на базовой инфраструктуре. Для экономики блокчейна это очень важно ввиду сложности шифрования и обеспечения конфиденциальности в децентрализованных сетях. В блокчейн-индустрии сейчас идет выработка лучших практик для типичного блокчейн-стартапа с точки зрения сетевой безопасности, криптографии и математики. Желательно, чтобы эти требования не были очень высокими и можно было положиться на безопасный стек инфраструктуры, в котором эта функциональность была бы доступна автоматически. Это позволит ускорить развитие индустрии блокчейна, и каждой организации не придется заново изобретать колесо и беспокоиться о том, что электронный кошелек не поддерживает мультиподпись (или любой другой стандарт безопасности, принятый на тот момент).

²¹³ Там же.

Возможные улучшения

Ниже описаны возможные решения некоторых из описанных проблем.

Офлайн-кошельки для хранения криптовалюты

Большую часть средств в биткойнах и других криптовалютах можно хранить в различных офлайн-кошельках, таких как бумажные кошельки, холодные хранилища и бит-карты.

Темные пулы

Цепочка создания ценности может быть гораздо более детализированной. Например, крупные криптобиржи обычно оперируют собственными внутренними базами данных транзакций и периодически синхронизируют сводку этих транзакций с блокчейном. Эта идея позаимствована у банковской индустрии.

Альтернативные алгоритмы хеширования

Litecoin и другие криптовалюты используют алгоритм scrypt, работающий немного эффективнее майнингового алгоритма биткойна. В будущем могут появиться еще более эффективные алгоритмы хеширования.

Альтернативы подтверждению работы в задаче византийских генералов

Существует много других моделей консенсуса (подтверждение ставки, гибриды и варианты) с меньшей задержкой, требующих меньше вычислительной мощности, расходуемых меньше ресурсов и повышающих безопасность небольших цепочек. Рассматриваются также модели на основе консенсуса без майнинга, такие как модель Tendermint DLS (измененная версия решения задачи византийских генералов), в которой используются залоговые транзакции²¹⁴. Другой вариант консенсуса без майнинга и подтверждения работы – алгоритм консенсуса Hyperledger, основанный на алгоритме PBFT (практическая византийская парадигма отказоустойчивости).

Использование самых последних или неизрасходованных выходов

Многие блокчейн-операции могут работать аналогично тому, как работают транзакции кредитных карт. «Тонкие кошельки» функционируют именно так, не запрашивая весь блокчейн, как это делает полный узел Bitcoin. Это позволяет держать электронные биткойн-кошельки даже на сотовых телефонах. Похожее решение – Cryptonite, оно использует упрощенную схему данных «мини-блокчейн».

Перемещение между блокчейнами

Координировать транзакции между различными распределенными журналами записей можно с помощью сайдчейнов. Над ними работает, например, Blockstream.

Системы гарантийных залоговых депозитов

Безопасность предлагаемых альтернативных механизмов консенсуса, таких как протокол Tendermint DLS (не требующий майнинга для подтверждения работы), можно усилить с помощью структурных элементов, таких как обязательная публикация майнерами залоговых депозитов в распределенном журнале записей. Это поможет решить проблему «отсутствия риска у майнера», позволяющую злонамеренным участникам (ранее имевшим долю в криптовалюте) совершить кражу посредством двойной траты²¹⁵. Залоговые депозиты могут публиковаться в блокчейне, как это делает Tendermint, чтобы увеличить затраты на раздвоение и повысить операционную безопасность.

API REST

²¹⁴ Kwon, J., «Tendermint: Consensus Without Mining», прочитано в 2014 г. (технический документ), <http://tendermint.com/docs/tendermint.pdf>

²¹⁵ «Tendermint Consensus Proposal», сайт-форум Bitcointalk, 20 ноября 2014 г., <https://bitcointalk.org/index.php?topic=866460.0>. См. также: <http://tendermint.com/posts/security-of-cryptocurrency-protocols>

API REST предоставляют безопасный и удобный программный интерфейс для доступа в реальном времени. Многие блокчейн-компании, например Blockchain.info, предоставляют альтернативные интерфейсы кошельков, имеющие такую функциональность.

Сложности бизнес-модели

Еще один тип сложностей, не связанный с функциональностью и техническими особенностями, относится к бизнес-моделям. Традиционные модели могут показаться неподходящими для биткойна, поскольку все его характеристики предназначены для использования в децентрализованных пиринговых моделях без участия посредников, извлекающих долю прибыли или плату за транзакции (как в классической бизнес-модели). Однако остается много продуктов и услуг, которые можно выгодно предлагать в новой экономической модели блокчейна. В первую очередь это образование и услуги, ориентированные на широкие массы (например, этим могут заниматься проекты Coinbase, Circle Internet Financial и Харо).

Другая задача, для решения которой можно с успехом применять концепции блокчейна, — повышение эффективности существующей мировой инфраструктуры банков и финансирования (чем занимается Ripple). Перестройка всей коммерческой деятельности с помощью умных контрактов Биткойн 2.0 будет сложной задачей, но предоставит ряд возможностей для оказания услуг по внедрению, обучению потребителей, разработке стандартов и другой деятельности, способствующей созданию ценности. В экономике биткойна могут найти применение также бизнес-модели облачных вычислений и корпоративного ПО, включая модель Red Hat (платные услуги по разработке и реализации ПО с открытым исходным кодом) и SaaS (ПО как услуга). В будущем, возможно, появится работа для аудиторов, проверяющих комплаенс и выполнение умных контрактов, подготовленных и записанных в распределенный журнал записей самообучающимися средствами ИИ.

Скандалы и восприятие обществом

Одно из самых больших препятствий дальнейшему развитию биткойна – его восприятие общественностью как платформы для отмывания денег и прочей теневой деятельности – например, организации подпольных рынков (таких, как Silk Road) для продажи запрещенных товаров. Как и любая другая технология, биткойн и блокчейн сами по себе нейтральны, с их помощью можно действовать по любую сторону закона. И, хотя способы вредоносного использования блокчейна, безусловно, существуют, потенциальные преимущества значительно перевешивают потенциальные недостатки. Со временем общественное восприятие может измениться, и чем больше людей заведет электронные кошельки и начнет использовать биткойн, тем быстрее это произойдет. Однако необходимо понимать: биткойн, как псевдонимный инструмент, может использоваться и в преступных целях, что приведет к разработке соответствующих защитных мер, а это запустит своего рода гонку вооружений. Как в ответ на появление компьютерных вирусов возникло антивирусное ПО, так и в блокчейне создаются соответствующие средства для борьбы со злонамеренными участниками.

Еще одно препятствие широкому распространению биткойна – постоянно происходящие кражи, скандалы и случаи мошенничества: например, новые альткойны, работающие по принципу «выкачать и бросить», пытающиеся создавать все новые криптовалюты для быстрого получения прибыли.

Не улучшил общественного мнения и крах крупнейшей биткойн-биржи MtGox в 2014 году. Исчерпывающего объяснения нет до сих пор: как в самой прозрачной и общедоступной главной книге активы могут исчезать и оставаться найденными месяцы спустя? Компания утверждала, что ее взломали и воспользовались ошибкой, создающей проблему пластичности транзакций. Эта ошибка позволила злоумышленникам дважды потратить биткойны, передавая их на свои адреса, заставляя биржу считать, что передача не удалась, и повторять транзакцию²¹⁶. Аналитики так и не выяснили, была эта атака внешней или работой инсайдеров. Проблема подобных краж пока остается нерешенной. Вот лишь несколько случаев: в октябре 2014 года исполнительный директор Moolah исчез с 1,4 млн долларов в биткойнах²¹⁷, в июле было украдено 2 млн долларов в валюте Vericoин²¹⁸, в июне – 620 тыс. долларов в результате майнинг-атаки на Dogecoin²¹⁹.

Бизнес-моделям блокчейна необходимо сформироваться и окрепнуть, выработать меры защиты, позволяющие стабилизировать положение в индустрии и научиться отделять добропорядочных участников от злонамеренных. Внешний надзор для этого не обязателен; в экосистеме можно создать соответствующие децентрализованные системы проверки, подтверждения и мониторинга. Впрочем, исследования в области общественных наук показывают, что функции надзора все же важны; они позволяют держать процесс в тонусе, предотвращая сбалансированную систему сдержек и противовесов. Например, в генетических исследованиях, организованных самими участниками проекта DIYgenomics, есть функция надзора, и в некоторых случаях она выступает в совершенно новой роли независимого

²¹⁶ Аноним, «The Troubling Holes in MtGox's Account of How It Lost \$600 Million in Bitcoins», журнал *MIT Technology Review*, 4 апреля 2014 г., <http://www.technologyreview.com/view/526161/the-troubling-holes-in-mtgoxs-account-of-how-it-lost-600-million-in-bitcoins/>

²¹⁷ Collier, K., «Moolah CEO Accused of Disappearing with \$1.4 Million in Bitcoin», интернет-газета *Daily Dot*, 21 октября 2014 г., <http://www.dailydot.com/politics/moolah-doge-coin-alex-green-ryan-kennedy-ryan-gentle-millions-miss-ing-mintpal/>

²¹⁸ Pick, L., «Nearly \$2 Million Worth of Vericoин Stolen from Mint-Pal, Hard Fork Implemented», портал «Digital Currency Magnates», 15 июля 2014 г., <http://dcmagnates.com/nearly-2-million-worth-of-vericoин-stolen-from-mintpal-hard-fork-considered/>

²¹⁹ Greenberg, A., «Hacker Hiacks Storage Devices, Mines \$620,000 in Dogecoin», журнал *Wired*, 17 июня 2014 г., <http://www.wired.com/2014/06/hacker-hiacks-storage-devices-mines-620000-in-dogecoin/>

арбитра в вопросах гражданской этики²²⁰. Можно привести и другие примеры саморегулируемых индустрий, включая киноиндустрию, индустрию видеоигр и комиксов.

Существует вероятность того, что вся индустрия блокчейна просто рухнет в силу известных причин или из-за появления новых проблем. Гарантировать, что этого не случится, нельзя. Блокчейн-экономика имеет сильные позиции, если верить показателям капитализации рынка криптовалют, инвестициям в этот сектор, числу стартапов, численности сотрудников, количеству опубликованных в GitHub строк кода и вниманию общественности и СМИ к этой области. Индустрия блокчейна уже имеет больший размах, чем все предыдущие попытки внедрения цифровых валют (таких, как доллары виртуального мира Second Life Linden). И все же не факт, что время цифровых валют уже пришло. Возможно, общественность пока не готова принять все технологии и структуры, которые еще не созданы для цифровых валют, хотя Apple Pay и показывает хороший пример принятия цифровых валют массами. Возможно, на ближайшее время нам хватит и Apple Pay. Биткойн еще не скоро станет настолько же удобным для пользователя.

²²⁰ Swan, M., «Scaling Crowdsourced Health Studies: The Emergence of a New Form of Contract Research Organization», журнал *Pers Med*, том 9, № 2 (2012 г.), с. 223–234.

Государственное регулирование

Государственное регулирование может быть одним из наиболее значимых факторов риска, определяющих возможность становления блокчейна как системы финансовых услуг. В США законодательство определяется на федеральном уровне и уровне штатов. В штате Нью-Йорк в июне 2015 года после долгих обсуждений принята нормативно-правовая база для криптовалютных компаний Bitlicense²²¹, и это может задать тон регулированию блокчейна во всем мире.

С одной стороны, биткойн-индустрия заинтересована в максимальной широте и экстерриториальности лицензии. Эта лицензия будет охватывать все, что можно делать с биткойнами, включая программное обеспечение кошельков (таких, как кошелек BitcoinCore)²²². С другой стороны, регулирование в области защиты прав потребителей, распространяющееся на пользователей биткойна, и требования, предъявляемые к организациям, оказывающим услуги по переводу денежных средств, могут ускорить принятие индустрией общественностью и избавить потребителей от беспокойства насчет хакерских атак.

Обсуждения и первые постановления правительств относительно биткойна поднимают интересные вопросы. Один из них – вопрос налогообложения. Децентрализованная пиринговая экономическая система Airbnb 2.0 и Uber 2.0, работающая на локализованных версиях платформы OpenBazaar с оплатой услуг криптовалютами, делает традиционные схемы налогообложения неэффективными. Обычные средства контроля потребления товаров и услуг могут исчезнуть. Это повлияет и на налогообложение, и на общее измерение экономических показателей, таких как ВВП, благодаря чему широкие массы могут перестать ориентироваться на потребление как на показатель благополучия. Систему налогообложения можно переработать, приняв за основу отслеживаемое дорогостоящее имущество (машины, дома), получив своего рода «налог на видимое». Переход от налога на доходы к налогу на потребление будет важным изменением для общества.

Второй вопрос относительно государственного регулирования – какую ценность может предложить государство в своей бизнес-модели. В эпоху больших данных некоторые правительственные организации не справляются со своими обязанностями по ведению записей и поддержанию архивов данных в легкодоступном формате. Это значит, что для правительств есть опасность «ухода с рынка», поскольку они не смогут в полной мере финансировать себя традиционным способом – посредством увеличения налогов. Технологии блокчейна позволяют решить обе эти проблемы и, как минимум, помочь правительствам лучше выполнять их обязанности, в то же время вытесняя правительственные агентства с рынка некоторых из этих услуг. Запись всех общественных данных в блокчейне может устранить целые классы государственных служб. С этой точки зрения демократизация правительственных функций с помощью технологий блокчейна делает многие традиционные сферы деятельности правительства невостребованными.

Однако в мире сосуществуют централизованные и децентрализованные модели координации деятельности, поэтому в будущем найдется место как для традиционного правительства, так и для новых форм управления на основе блокчейна. Тем не менее полезность и необходимость централизованного управления теперь придется экономически обосновывать. В будущем могут сложиться гибридные формы управления, в которых движущей силой

²²¹ Reitman, R., «Beware the BitLicense: New York's Virtual Currency Regulations Invade Privacy and Hamper Innovation», некоммерческая организация Electronic Frontier Foundation, 15 октября 2014 г., <https://www.ef.org/deeplinks/2014/10/beware-bitlicense-new-yorks-virtual-currency-regulations-invade-privacy-and-hamper>

²²² Santori, M., «What New York's Proposed Regulations Mean for Bitcoin Businesses», сайт CoinDesk, 18 июля 2014 г., <http://www.coindesk.com/new-yorks-proposed-regulations-mean-bitcoin-businesses/>

будет автоматизация, а лучшей формой координации – тандем человека и алгоритма²²³. Формальные повторяющиеся задачи можно автоматизировать с помощью блокчейнов и умных контрактов, а государственные служащие, возможно, найдут способ приносить пользу и на новом уровне развития технологий.

²²³ Cowen, T., «Average Is Over: Powering America Beyond the Age of the Great Stagnation», Нью-Йорк, издательство Dutton Publishing, 2013 г.

Проблемы конфиденциальности персональных данных

Прежде чем люди перестанут бояться хранить свои персональные данные в децентрализованных хранилищах с возможностью доступа через блокчейн, необходимо решить ряд вопросов. Для любого человека будет катастрофой кража или раскрытие закрытого ключа ко всем его личным данным, хранящимся в сети. В текущей системе криптовалют это возможно во многих случаях – персональные и корпоративные пароли постоянно крадут, а базы данных взламывают. Последствия могут быть совершенно непредсказуемыми, вплоть до случаев полной кражи личности.

Итог: тенденции к децентрализации сохраняются

Несмотря на все потенциальные ограничения зарождающейся блокчейн-экономики, нет сомнений в том, что биткойн – мощная сила, которая вызовет серьезные изменения. Даже если вся текущая инфраструктура, созданная для инфраструктуры блокчейна, исчезнет (или утратит популярность, как это произошло с виртуальными мирами), останется ее наследие. Экономика блокчейна позволила совершенно по-новому увидеть, как может функционировать вся наша цивилизация. Даже если не верить в будущее биткойна как стабильной и долговечной криптовалюты или в текущее направление развития блокчейн-технологий, нельзя отрицать обширные возможности децентрализованных моделей в целом.

Децентрализация – это идея, время которой пришло. Интернет настолько огромен и динамичен, что может способствовать развитию децентрализованных моделей в самых разных областях и с бóльшим потенциалом, чем когда-либо. Централизованные модели долго служили человечеству, сотни лет назад они были революционным способом управления обществом. Но технологии ушли вперед, появился интернет и многие другие инструменты, включая блокчейн, которые позволяют не только впервые охватить все семь миллиардов жителей планеты, но и обеспечить более совершенное координирование общественного взаимодействия, ускорить прогресс и создать по-настоящему эффективное общество. Если это не удастся современной блокчейн-индустрии, то непременно появится что-то еще более эффективное. Возможно, какие-то технологии дополнят блокчейн-индустрию. Но сейчас блокчейн – это первое крупномасштабное воплощение моделей децентрализации, разворачиваемое на новом, более сложном уровне человеческой деятельности.

Глава 7

Заключение

В этой книге предпринята попытка показать, насколько универсальны принципы блокчейн-технологии. Ее возможности можно применять не только в узком контексте денежных расчетов (Блокчейн 1.0) или договоров, собственности и всех транзакций на финансовых рынках (Блокчейн 2.0), но и к более разнородным областям, в числе которых государственное управление, здравоохранение, наука, образование, экономика, искусство и культура (Блокчейн 3.0). Вполне вероятно, что функциональность блокчейна сможет способствовать глобальному прогрессу человечества.

Блокчейн-технология может оказаться очень кстати в мире будущего, где станут применяться как централизованные, так и децентрализованные модели. Как любая другая новая технология, блокчейн может не только разрушать существующие стереотипы и схемы, но и способствовать развитию крупных экосистем, объединяющих существующие и инновационные подходы.

В качестве примера из истории можно привести изобретение радио, которое в конечном счете повысило продажи грампластинок, или появление электронных книг, таких как Kindle, которые способствовали росту продаж традиционных книг.

Сейчас мы узнаём новости из газет, блогов, Twitter, а также из персонифицированных автоматических каналов. Мы потребляем мультимедийную информацию, не только предоставляемую крупными компаниями индустрии развлечений, но и обычными людьми на YouTube. Блокчейн-технология тоже может со временем внедриться в более крупные экосистемы, сочетающие модели централизации и децентрализации.

Может появиться большее разнообразие как фиатных валют, так и криптовалют, существующих бок о бок. В работе «Денационализация денег» экономист Фридрих Хайек предвидел появление дополнительных валют, конкурирующих за потребителя. Он показал, что возможно появление множества валют на уровне финансовых институтов: по аналогии с собственными блогами, учетными записями Twitter, каналами YouTube и учетными записями Instagram может быть много криптовалют отдельных пользователей, групп по интересам или сообществ. Каждая из этих криптовалют может существовать в своей местной экономике, будучи полностью совместимой и действительной для расчетов и экономических операций в локальных средах. Например, криптовалюта может стать деньгами сообщества «Поговорим о Bitcoin», средством расчетов Tatianacoin для музыкантов, общественной валютой на местном фермерском рынке, в магазине «Сделай сам» или в школах округа. Местные токены проще всего сделать конвертируемыми в более ликвидные криптовалюты или фиатные деньги. Именно в этом – многообразие и богатство блокчейн-технологии.

Блокчейн может обеспечить многообразие форм многих валют – возможно, существующих параллельно. Такие валюты могут восприниматься более дифференцированно, чем фиатные деньги, обслуживая только специализированные области человеческой деятельности. Суммарный эффект может выразиться в появлении менталитета многообразия в противовес безальтернативности обычных денег, особенно если это будет сопровождаться обеспечением безусловного основного дохода (БОД), который покроет основные жизненные потребности людей и таким образом создаст более высокий уровень сознательности. Концепция денег может измениться, и они могут стать не только средством накопления и сбережения, но и инструментом обслуживания самых разнообразных сфер деятельности в обществе.

Блокчейн как информационная технология

Наверное, самое главное в блокчейне состоит в том, что это информационная технология. Но много у нее и других аспектов. В качестве средства децентрализации блокчейн являет собой новую революционную парадигму вычислений. У блокчейна есть встроенный экономический уровень, которого у технологий интернета никогда не было.

Блокчейн – механизм координации, схема отслеживания привязки к единичным записям, кредита, подтверждения и компенсационных вознаграждений для поощрения участия любого интеллектуального агента в любом виде сотрудничества, не использующая доверенных посредников. Блокчейн сам по себе является «децентрализованной сетью доверия»²²⁴.

Блокчейн воплощает предложенную Хайеком множественность дополнительных частных валют, в которой может существовать столько же валют, сколько учетных записей в Twitter и блогах. Эти валюты сообществ (Communitycoin) будут признаваться и приниматься в собственных локальных контекстах и способствовать укреплению связей и самореализации групп.

Блокчейн – облачная площадка для транснациональных компаний. Блокчейн – это средство предоставления персонализированных децентрализованных служб управления и поддержки образования и экономического развития. Блокчейн является средством доказательства существования и точности содержимого любого документа или другого цифрового актива на определенный момент времени.

Блокчейн обеспечивает интеграцию и автоматизацию взаимодействия людей и машин, служит сетью платежей между машинами (machine-to-machine, M2M) в экономике машин и между «вещами» в «интернете вещей». Блокчейн и криптовалюта – основа для механизма платежей и бухучета в M2M-коммуникациях.

Блокчейн – это всемирная децентрализованная главная книга для регистрации, подтверждения и передачи всех имущественных и социальных взаимодействий, банк публично доступных записей общества, средство обеспечения широчайшего прогресса человечества в ранее невиданных направлениях и масштабах. Блокчейн – это технология и система, способная обеспечить глобальную координацию миллиардов интеллектуальных агентов. Блокчейн – это многоуровневая модель консенсуса и, возможно, механизм, которого мы ждали и который позволит нам перейти в эру дружественного машинного интеллекта.

Искусственный интеллект блокчейна: консенсус как механизм развития дружественного искусственного интеллекта

Один из перспективных вопросов будущего технологий – разнообразие возможных проявлений искусственного интеллекта и перспектив его «дружественности» и благосклонности по отношению к человеку. Существует понятие технологической сингулярности, то есть момента, когда машинный интеллект превысит возможности человеческого разума. Но у специалистов пока нет надежного плана обеспечения дружественности ИИ. Многие признанные эксперты вообще сомневаются, возможно ли это в принципе²²⁵. Вполне вероятно, что блокчейн-технология станет приемлемым связующим звеном между людьми и машинами в мире, где машины становятся все более автономными. Со временем искусственный

²²⁴ Antonopoulos, A. M., «Mastering Bitcoin: Unlocking Digital Crypto-Currencies», г. Себастопол, шт. Калифорния, издательство O'Reilly Media, 2014 г.

²²⁵ Bostrom, N., «Superintelligence: Paths, Dangers, Strategies», Оксфорд, Соединенное Королевство, издательство Oxford University Press, 2014 г.

интеллект может прийти на смену децентрализованным приложениям, организациям и корпорациям. В частности, консенсус как механизм может стать инструментом реализации и внедрения дружественного ИИ.

Обширные возможности для интеллекта

Дадим волю воображению и попытаемся заглянуть в будущее. Область возможностей интеллекта сильно расширится. Появятся усовершенствованный человек, различные гибриды человека и машины, различные формы искусственного интеллекта, включая модели мозга и развитые алгоритмы машинного обучения. Блокчейн как информационная технология может облегчить будущий переход в мир с множеством разных машин, людей и гибридного интеллекта. Эти разновидности интеллекта, скорее всего, будут не изолированы, а подключены к коммуникационной сети. Для этого цифровому интеллекту потребуется выполнять определенные сетевые транзакции, многие из которых могут управляться с помощью блокчейна и других механизмов консенсуса.

Транзакции выполняются только для дружественных ИИ

Одним из неожиданных преимуществ моделей консенсуса может оказаться их потенциальная способность контролировать дружественность ИИ, то есть обеспечивать взаимопомощь и порядочность интеллектуальных агентов как членов общества²²⁶. В децентрализованных сетях доверия репутация агентов (способных скрываться под псевдонимами) может стать важной для определения возможности выполнения транзакции – сеть не будет работать со злонамеренными участниками. Любая важная транзакция, связанная с доступом и использованием ресурса, может требовать санкции моделей консенсуса. Таким образом, дружественность ИИ может обеспечиваться тем, что агенты, желающие участвовать в системе и получать доступ к ресурсам, будут вынуждены вести себя подобающим образом. В плане репутации и поведения плохие агенты вынуждены выглядеть как хорошие, то есть не нарушать правил – как и социопаты в человеческом обществе, которые вынуждены играть по правилам общества.

Естественно, можно привести много возражений против идеи применения структуры блокчейна для принуждения ИИ к дружественности. Плохие агенты могут построить собственные интеллектуальные сети для доступа к ресурсам, они могут временно прикинуться «хорошими», чтобы завоевать доверие, и т. п. Но это не меняет основного посыла: блокчейн-технология является системой сдержек и противовесов для продвижения и реализации одних моделей поведения и ограничения других. Идея заключается в создании систем, действующих как «бритва Оккама»: польза от предоставляемых ими преимуществ настолько высока, что участникам проще и выгоднее всего играть по правилам. Поощрение хороших участников становится частью самой системы.

К некоторым ключевым сетевым операциям, которые могут потребоваться цифровому интеллекту, относятся безопасный доступ, аутентификация и проверка, а также экономический обмен. В сущности, любое сетевое взаимодействие, необходимое интеллектуальному агенту для реализации своих задач, требует той или иной формы подтвержденного консенсусом доступа или аутентификации – а это невозможно, если у агента нет положительной, то есть добропорядочной, репутации в сети. Вот как можно реализовать дружественность искусственного интеллекта в основанной на консенсусе модели блокчейна.

²²⁶ Swan, M., «Blockchain-Enforced Friendly AI», сайт Crypto Money Expo, 5 декабря 2014 г., <http://cryptomoneyexpo.com/expos/inv2/#schedule> и <http://youtu.be/qdGoRep5iTO/>

Умные контракты, действующие от имени цифрового интеллекта

Если блокчейн-технология и модели консенсуса можно применять для обеспечения дружественного поведения ИИ, то возможна и обратная ситуация. Например, если вы ИИ или загруженный цифровой майндфайл, то умные контракты в будущем могут стать вашими «защитниками», подтверждающими ваше существование. Еще одна давнишняя проблема представленного в цифровом виде искусственного интеллекта – подтверждение реальности его окружения как свидетельства того, что ИИ по-прежнему существует, защищен и реально функционирует, а также условий его существования. Например, надо быть уверенным, что центр обработки данных не сбросит вас на старый компьютер с DOS, не удалит или не прекратит свое существование. Умные контракты на основе блокчейна – именно тот универсальный независимый защитник, который в будущем позволит проверять и контролировать физические параметры реальности вашего существования как цифрового интеллекта. Его работа будет заключаться в выполнении умных контрактов в блокчейне: периодической проверке параметров работы и децентрализованных резервных копий. Умные контракты позволят создать «будущую защиту» – новый вид услуг, которые найдут массу применений уже и в настоящем: например, обеспечат защиту прав престарелых.

Гипотетически, в далеком будущем в развитых обществах, состоящих из миллиардов цифровых интеллектов, живущих и процветающих в интеллектуальных сетевых системах, появится потребность в развитых предсказателях – информационных арбитрах, доступных через умные контракты блокчейна или другие механизмы. Бизнес-модель может представляться в форматах «предсказатели как сервис», «...как платформа» или даже «...как общественный товар». В будущем Wikipedia может стать сервисом предсказаний на основе блокчейна, хранящим информацию о текущем стандарте обработки, хранения и защиты цифровых файлов сознания. Подобные механизмы – динамические сервисы предсказаний, доступные умным контрактам через универсальные общедоступные цепочки блокчейна, – позволят создать систему сдержек и противовесов, в которой цифровые интеллекты или другие бестелесные сущности смогут не только комфортно выживать, но и развиваться.

Консенсус блокчейна повышает плотность информации во Вселенной

Наконец, существуют обширные возможности более активного использования блокчейна как информационной технологии, в том числе для регулирования моделей консенсуса. Ключевой вопрос – что представляет собой консенсус-зависимая информация? Каковы ее свойства и преимущества по сравнению с другими видами информации? Это другой вид или форма информации?

Один из способов представления реальности и Вселенной – с помощью информационных потоков. Блокчейн-технология позволяет выявить как минимум три разных уровня информации.

Первый уровень – сырая, необработанная и немодулированная информация. Второй уровень можно представить как социально рекомендуемые данные, то есть элементы данных, обогащенные рекомендациями участников социальных сетей. Такие данные стали возможными благодаря наличию сетевых интернет-моделей. Качество этой информации выше, потому что она рекомендуется релевантными членами соцсетей. Есть еще третий уровень: подтвержденные блокчейн-консенсусом данные.

Высочайший уровень рекомендованности этих данных основан на точности и качестве, обеспеченных групповым консенсусом. Это не просто рекомендации равноправных участников, а формальная структура интеллектуальных агентов-экспертов, олицетворяющая

консенсус относительно качества и точности этих данных. Таким образом, блокчейн-технология создает третий, основанный на консенсусе уровень информации, которая более плотно модулируется с применением атрибутов качества и одновременно более глобальна, общедоступна и свободно перемещается. Как информационная технология, блокчейн обеспечивает модулирование с высоким разрешением в отношении качества, аутентичности и происхождения информации.

Таким образом, данные консенсуса – это данные, качество которых подтверждено неявным голосованием участников и утверждено массами, поддерживающими качество, точность и корректность данных. Возникает вопрос: «Что общество может делать с подобным качеством данных?» или: «Что обществу следует делать с таким масштабным механизмом подтверждения качества данных?» Размышления о преимуществах полученной в результате консенсуса информации подтверждают, что блокчейн-технология может стать именно тем базовым инфраструктурным элементом и масштабируемым механизмом аутентификации и проверки данных, который необходим для полноценного прогресса человечества. Существует и крепнет представление, что Вселенная – это информация, а вектор ее развития направлен в сторону информационных потоков высочайшей плотности. И если блокчейн-технология действительно станет ключевым инструментом наращивания прогресса человечества, то в дальнейшем она способна стать информационной платформой масштабов Вселенной.

Приложение А

Основные сведения о криптовалютах

Биткойн и другие криптовалюты (альткойны) представляют собой цифровые деньги, средство покупки и продажи товаров в интернете. Чтобы пользоваться ими, нужно создать электронный кошелек – либо заведя новый онлайн-кошелек в браузере, либо загрузив кошелек-приложение для обычного компьютера или смартфона с сайта Bitcoin.org, Blockchain.info, Mycelium, Circle, Electrum или сайтов других разработчиков биткойн-кошельков. При создании кошелька автоматически генерируется биткойн-адрес, а также открытый и закрытый ключи. Биткойн-адрес – это, как правило, идентификатор, начинающийся с «1» или «3» и состоящий из 26–34 буквенно-цифровых символов, которые указывают на получателя биткойн-платежа, например 1FTgzPJCbPCWYfF6VxPdmCMPUDBFygut2h. Это настоящий биткойн-адрес для пожертвований, принадлежащий англоязычному информационному portalу Let's Talk Bitcoin²²⁷, посвященному блокчейн-технологии. Биткойн-адрес может быть представлен в виде строки или QR-кода и в чем-то похож на адрес электронной почты – в том смысле, что адрес электронной почты позволяет получать сообщения электронной почты, а биткойн-адрес вашего кошелька – получать биткойны от других людей.

Биткойны – это цифровые деньги, поэтому в кошельке нет физических денег, так что термин «кошелек» не вполне корректен. Кошелек содержит адрес, открытый и закрытый ключи, а также запись в распределенном журнале записей системы блокчейна о количестве принадлежащих владельцу биткойнов. Закрытые ключи кошелька надо беречь так же тщательно, как и ваш обычный кошелек. Любой получивший доступ к этим ключам человек сможет управлять кошельком, тратить и переводить биткойны, поэтому не надо никому передавать свои закрытые ключи или, тем более, публиковать их. Несоблюдение требований безопасности закрытых ключей – одна из причин краж биткойнов и афер с ними.

Если у вас есть биткойн-адрес, любой человек может отправлять на него биткойны – так же, как можно отправлять электронную почту на электронный адрес. Чтобы отправить кому-то биткойны, нужно знать адрес получателя и собственный закрытый ключ. Этот ключ позволит программе проверить, есть ли в распоряжении владельца биткойны, которые тот намеревается потратить или перевести. Адрес кошелька получателя биткойнов можно узнать, получив строку или QR-код адреса (например, по электронной почте или в СМС). Отправитель сканирует QR-код адреса кошелька получателя и в приложении-кошельке вводит прочую информацию о транзакции: сумму, комиссию за перевод (обычно отправитель просто подтверждает комиссию, назначаемую приложением) и другие параметры, необходимые для отправки биткойнов получателю. Когда отправитель подтверждает транзакцию, в сеть поступает широковещательное сообщение о том, что столько-то монет из этого адреса теперь принадлежат другому адресу.

Эта операция подтверждается закрытым ключом отправителя. Если в кошельке нет закрытого ключа, соответствующего монетам, то их нельзя потратить. Корректная транзакция почти сразу появляется в кошельке получателя в состоянии «неподтвержденная». Далее в течение 10 минут транзакция подтверждается и записывается в распределенный журнал записей одним из майнеров. При совершении крупных покупок, таких как автомобиль или недвижимость, участники сделки дожидаются подтверждения транзакции (а то и нескольких), но вряд ли кто-нибудь станет ждать подтверждения покупки чашки кофе.

²²⁷ В рунете существует его своеобразный аналог BitNovosti.com. – Прим. ред.

Краткий экскурс в асимметричную криптографию

Когда кошелек инициализируется или создается впервые, автоматически генерируется адрес, а также открытый и закрытый ключи. В основе биткойна лежит механизм асимметричного шифрования, в котором открытый ключ распространяется свободно, а закрытый ключ надо держать при себе.

Программа формирует биткойн-адрес, выбирая случайное число и создавая пару «открытый и закрытый ключи». На данный момент для создания ключей используется алгоритм ECDSA (Elliptic Curve Digital Signature Algorithm.) Ключи в паре математически связаны и проверяются в процессе расходования биткойнов. Закрытый ключ генерируется автоматически, но для создания биткойн-адреса нужны дополнительные операции. Биткойн-адрес – не просто открытый ключ, а результат его преобразования для повышения эффективности использования. Ключ обрабатывается с применением дополнительных протоколов шифрования (таких, как SHA-256 и RIPEMD-160), хеширования (преобразования строки символов в более короткое значение фиксированной длины или ключа, представляющего исходную строку) и служебных операций (удаления похожих символов, например строчной «L» и заглавной «I», нуля и заглавной буквы «O», добавления контрольной суммы в конец адреса и цифры-идентификатора в начало адреса – в большинстве биткойн-адресов это цифра «1», которой отмечают обычные адреса биткойн-сети).

Практически нереально, хотя и теоретически возможно, что двое разных пользователей сгенерируют одинаковые биткойн-адреса. В этом случае оба смогут тратить деньги с этого адреса. Шансы возникновения такой ситуации исключительно малы, а вероятность несовпадения адресов очень высока и оценивается в 99,9999999999 %. Кошелек биткойнов может содержать много адресов (одна из иногда используемых мер безопасности состоит в генерации и использовании нового адреса для каждой транзакции) и соответствующих им закрытых ключей, которые хранятся в файле кошелька. Закрытые ключи математически связаны со всеми биткойн-адресами, сгенерированными в кошельке.

Закрытые ключи биткойна обычно являются 256-разрядными числами (хотя в некоторых кошельках длина может варьироваться от 128 до 512 разрядов) и представлены в одной или нескольких формах. Вот пример закрытого ключа ([https:// en.bitcoin.it/wiki/Private_key](https://en.bitcoin.it/wiki/Private_key)) в шестнадцатеричном формате (256 разрядов соответствуют 32 байтам или 64 шестнадцатеричным символам из диапазона 0–9, A – F):

```
E9 87 3D 79 C6 D8 7D C0 FB 6A 57 78 63 33 89 F4
45 32 13 30 3D A6 1F 20 BD 67 FC 23 3A A3 32 62
```

Вот еще один пример закрытого ключа и соответствующего открытого адреса:

```
Закрытый ключ: 791866703012990464368584129364204170766
60923359050732094116068951337164773779
```

```
Открытый биткойн-адрес: 1EE8rpFCSSaBmG19sLdgQLEWuDai YVFT9J
```

Вычислить закрытый ключ, соответствующий открытому ключу, невозможно из-за однонаправленности операции хеширования (или природы другого применяемого для вычисления этого значения механизма), а также непомерно высокой стоимости этой операции (нужен колоссальный объем вычислительных ресурсов на время, намного превышаю-

щее время подтверждения транзакции). Для получения биткойнов достаточно адреса, а для отправки нужна пара из открытого и закрытого ключей.

Приложение Б

Применения блокчейна – список от компании Ledra Capital

В компании венчурного капитала Ledra Capital (Нью-Йорк, США) периодически проводят мозговые штурмы, на которых регулярно обновляют самый полный список возможных применений блокчейн-технологии (http://bit.ly/blockchain_tech_uses). Некоторые из этих категорий включают финансовые инструменты, учет в государственных и частных организациях и организациях смешанного типа, ключи к материальным активам, нематериальные активы и другие возможные применения.

Вот этот список:

I. Финансовые инструменты, записи и модели:

1. Валюты.
2. Частный акционерный капитал.
3. Публичный акционерный капитал.
4. Облигации.
5. Производные финансовые инструменты (фьючерсы, форварды, свопы, опционы и более сложные сочетания).
6. Права голосования, связанные с указанными выше инструментами.

7. Биржевые товары.

8. Учет затрат.

9. Учет торговых операций.

10. Учет залоговых и ссуд.

11. Учет обслуживания кредитов.

12. Краудфандинг.

13. Микрофинансирование.

14. Благотворительные микровзносы.

II. Публичные записи:

15. Права собственности на земельные участки.

16. Регистрация транспортных средств.

17. Лицензирование компаний.

18. Записи о создании и ликвидации компаний.

19. Записи о владельцах компаний.

20. Записи регламентирующих органов.

21. Криминальный учет.

22. Паспорта.

23. Свидетельства о рождении.

24. Свидетельства о смерти.

25. Избирательные списки.

26. Выборы.

27. Проверки безопасности и санитарные проверки.

28. Разрешения на строительство.

29. Разрешения на ношение оружия.

30. Данные судебной экспертизы.

31. Судебные записи.

32. Результаты голосования.

33. Учет в некоммерческих организациях.

- 34. Прозрачная отчетность некоммерческих организаций и госорганов.
- III. Частные записи:
 - 35. Контракты и договоры.
 - 36. Подписи.
 - 37. Завещания.
 - 38. Тракты.
 - 39. Счета эскроу.
 - 40. Персональная геолокация.
- IV. Иной учет в организациях:
 - 41. Ученые степени и дипломы.
 - 42. Сертификаты.
 - 43. Сведения об успеваемости.
 - 44. Результаты экзаменов.
 - 45. Кадровое делопроизводство (зарплаты, аттестации, достижения).
 - 46. Медицинские записи.
 - 47. Бухгалтерские записи.
 - 48. Операционный учет в компаниях.
 - 49. Данные генома.
 - 50. Геолокация для бизнес-применений.
 - 51. Реестр поставок.
 - 52. Материалы арбитража.
- V. Ключи от материальных активов:
 - 53. Ключи от домов и квартир.
 - 54. Ключи от домов отдыха и таймшер-апартаментов.
 - 55. Ключи от комнат отелей.
 - 56. Ключи от автомобилей.
 - 57. Ключи от арендуемых автомобилей.
 - 58. Ключи от автомобилей в лизинге.
 - 59. Ключи от индивидуальных хранилищ.
 - 60. Ключи от сейфовых ячеек.
 - 61. Доставка грузов (ключ, разделенный между отправителем и получателем).
 - 62. Записи о ставках в тотализаторе.
 - 63. Записи о виртуальных спортивных командах.
- VI. Нематериальные активы:
 - 64. Купоны.
 - 65. Ваучеры.
 - 66. Броня и резервирование (в ресторанах, отелях, очередях и т. п.).
 - 67. Билеты в кино.
 - 68. Патенты.
 - 69. Защищенные товарные знаки.
 - 70. Товарные знаки.
 - 71. Лицензии на ПО.
 - 72. Лицензии на видеоигры.
 - 73. Лицензии на музыку, фильмы и книги (DRM-технологии).
 - 74. Доменные имена.
 - 75. Онлайн-идентификаторы.
 - 76. Подтверждение авторства или первенства.
- VII. Другое:
 - 77. Документальные записи (фото, аудио, видео).

78. Записи данных (результаты спортивных соревнований, показания температуры и т. п.).

79. СИМ-карты.

80. Идентификация в сети GPS.

81. Коды активации оружия.

82. Коды активации боевой техники.

83. Коды запуска ядерных ракет.

84. Контроль спама (микроплатежи за размещение рекламных сообщений).

Приложение В

Русскоязычные ресурсы по блокчейн-технологиям

- Русскоязычный сайт биткойн-сообщества: <https://bitcoin.org/ru/>
- Страница в Wikipedia: <https://ru.wikipedia.org/wiki/Биткойн>
- Портал о биткойне и блокчейн-технологиях: <http://bitnovosti.com>
- Онлайн-видео о криптовалютах: <https://www.youtube.com/c/BitnovostiRu>
- Блокчейн сообщество в России: <http://blockchain.community/>
- Банк России о биткойне: http://www.cbr.ru/press/pr.aspx?fle=27012014_1825052.htm
- Биткойн-посольство в Москве: <http://bitcoinembassy.ru/>
- Криптовалютный информационный портал: <http://bits.media/>
- Новости биткойна и блокчейна: <http://ru.newsbtc.com/>
- Биткойн-комьюнити в Facebook: <https://www.facebook.com/bitcoinru/>
- Криптовалютное сообщество в VK: <https://vk.com/bitnovosticom>
- Крупнейший русскоязычный биткойн-форум: <https://forum.bits.media/>
- Документальный фильм «Криптовалюты»: [https://www.youtube.com/watch?v=Aybt-](https://www.youtube.com/watch?v=Aybt-UZb4kk)

[UZb4kk](https://www.youtube.com/watch?v=Aybt-UZb4kk)

Благодарности

Я благодарю Андреаса М. Антонопулоса, Трента Макконахи, Стива Омохундро, Пиотра Пясецки, Джастина Шера, Криса Це и Стефана Туала.