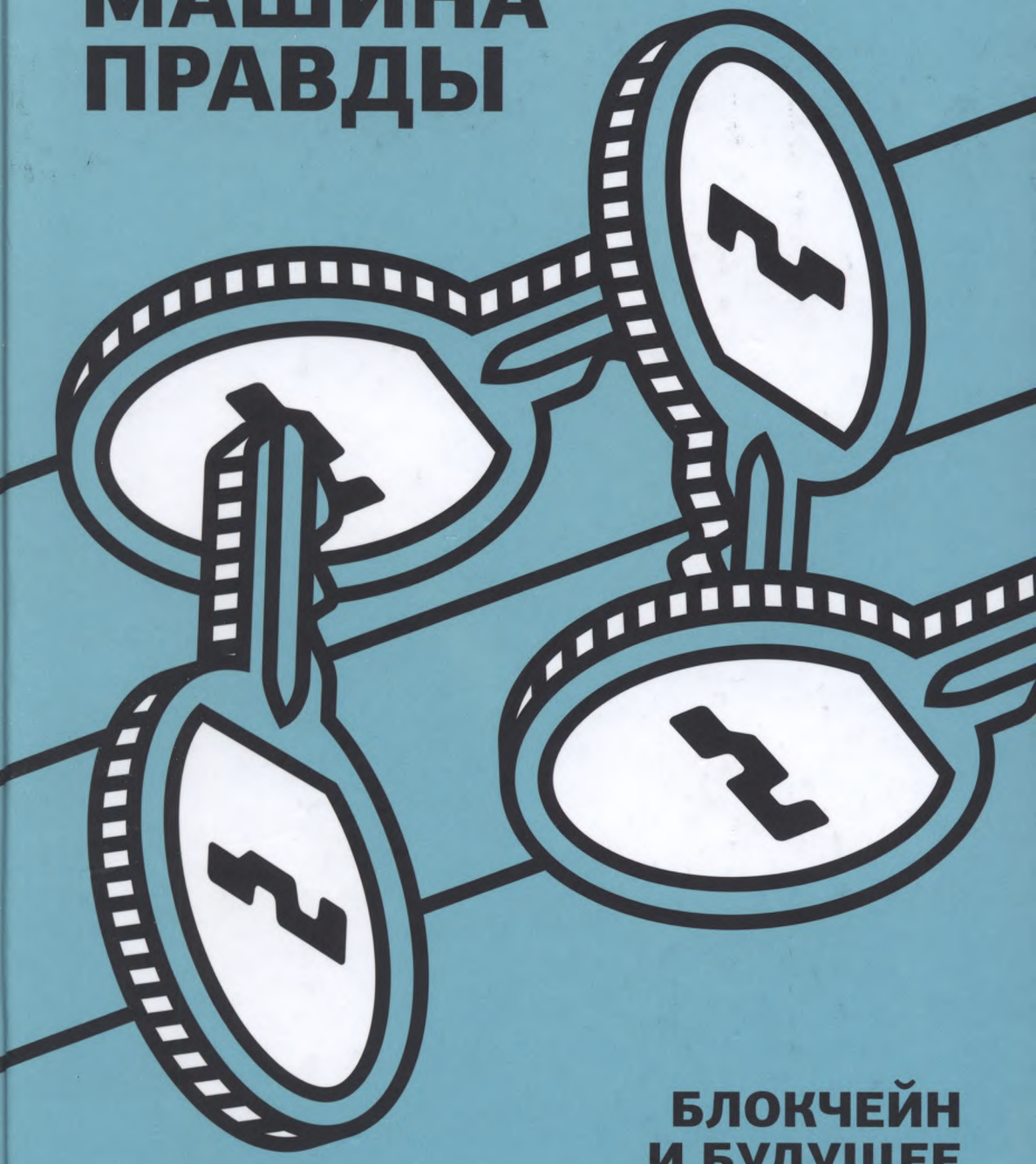
Пол Винья
Майкл Кейси

МАШИНА ПРАВДЫ



БЛОКЧЕЙН И БУДУЩЕЕ ЧЕЛОВЕЧЕСТВА

Эта книга принадлежит

_____

Контакты владельца

_____

Эту книгу хорошо дополняют:

Эпоха криптовалют
Пол Винья, Майкл Кейси

Неизбежно
Кевин Келли

Сдвиг
Джой Ито, Джефф Хоуи

Верховный алгоритм
Педро Домингос

Paul Vigna, Michael J. Casey

The Truth Machine:

The Blockchain and the Future of Everything

ST. MARTIN'S PRESS NEW YORK

Пол Винья, Майкл Кейси

Машина правды

Блокчейн и будущее человечества

Перевод с английского
Марии Сухотиной

Москва
«МАНН, ИВАНОВ И ФЕРБЕР»
2018

УДК 336.74:007
ББК 65.050.253
В50

Научный редактор Кейт Щеглова

Издано с разрешения Michael Casey & Paul Vigna
и литературного агентства The Marsh Agency Ltd.
in conjunction with Gillian MacKenzie LLC

На русском языке публикуется впервые

Книга рекомендована к изданию Ильей Саламатиным

В50 **Винья, Пол**
Машина правды. Блокчейн и будущее человечества / Пол Винья, Майкл Кейси ; пер. с англ. М. Сухотиной ; [науч. ред. К. Щеглова]. — М. : Манн, Иванов и Фербер, 2018. — 320 с.

ISBN 978-5-00117-660-2

Новая книга Майкла Кейси и Пола Винья о потенциале технологии блокчейн и расширении сфер ее применения читается на одном дыхании. Не навязывая своего мнения, авторы представляют факты, аргументы и рассуждения о четвертой промышленной революции и мире будущего, основанном на «интернете вещей».

Эта книга для тех, кто интересуется технологией блокчейн, проблемами децентрализации и цифровым будущим человечества.

УДК 336.74:007
ББК 65.050.253

ISBN 978-5-00117-660-2

Оглавление

Предисловие партнера издания

О блокчейне, биткоине и криптовалютах последние пару лет слышится отовсюду. Новости о безудержном росте капитализации биткоина и в целом рынка цифровых валют будоражат умы миллионов. А жесткие регулятивные меры в разных странах и откровенное мошенничество привели к массовому разочарованию частных инвесторов. Так в представлении большинства блокчейн стал ассоциироваться с риском, легкими деньгами и биржевыми спекуляциями.

Десятилетиями информационные технологии заставляли финансовые институты меняться, однако в последние годы банковский сектор стал реагировать на вызовы гораздо оперативнее и эффективнее. Роботизация, биометрия, облачные технологии, искусственный интеллект, анализ больших данных эффективно работают на финансистов и банкиров уже сегодня. Но блокчейн как новый главный тренд остается для них пока темной лошадкой. Одни усматривают в распространении технологии распределенных сетей угрозу собственному существованию из-за ослабления контроля, другие — необходимые инструменты развития.

Что касается сухих цифр, то банкам с их устаревшими системами денежных переводов есть о чем подумать. Пропускная способность сети SWIFT — 50 тысяч транзакций в секунду. Visa заявляла о способности одномоментно обрабатывать 65 тысяч транзакций. Эти показатели действительно впечатляют, пока не начинаешь их сравнивать со скоростью блокчейнов. Виталик Бутерин, основатель платформы Эфириум, анонсировал 1 миллион транзакций в секунду после масштабирования сети! Новый проект Harmony, собравший на стадии посевной инвестиции 18 миллионов долларов, обещает 10 миллионов транзакций

в секунду. При этом денежные переводы, основанные на технологии блокчейн, еще и существенно дешевле, так как избавляют от участия посредников.

Несмотря на избалованный вниманием общества рынок криптовалют, технология блокчейн несет в себе гораздо больше фундаментальных новшеств, чем перемены в финансовом секторе. Распределенные сети и смарт-контракты до неузнаваемости изменят все виды деятельности, связанные с хранением и передачей данных и сферой, где гарантом доверительных отношений и сертификации подлинности чего-либо традиционно выступал человек. Уверен: в ближайшие годы блокчейн прочно займет свое законное место в юриспруденции, нотариальных услугах, авторском праве, венчурном инвестировании, медицине, работе архивов, избирательном процессе, социальных сетях и даже в развитии инфраструктуры самого интернета.

Авторы книги «Машина правды: блокчейн и будущее человечества» ставят появление систем распределенных сетей в один ряд с такими значимыми событиями, как изобретение точных измерительных приборов, электричества и интернета. Книга изобилует примерами нетривиальных решений социальных и экономических проблем с помощью технологии блокчейн. После ее прочтения у вас не останется сомнений, что мы живем в интереснейшее время и стоим на пороге глобальных перемен.

Кирилл Семенихин,
директор Университета Иннополис

Предисловие научного редактора

Децентрализация как элемент будущего процветания

Появление Биткоина — доказательство запроса общества на децентрализацию, а также подтверждение возможности существования новой парадигмы финансовой системы. Так, если раньше имели место лишь примеры централизованных систем во главе с регулятором и целой закрытой и полностью контролируемой инфраструктурой, то сегодня мы наблюдаем становление совершенно новой парадигмы. Она демонстрирует, что наличие никем не контролируемой, полностью открытой и при этом безопасной системы возможно. И за этим будущее.

На сегодняшний день у сети Биткоина есть как ряд преимуществ, так и недостатков. К последним можно отнести длительность прохождения транзакций, высокие комиссии, слабую анонимность, высокие риски получения злоумышленниками доступа к аккаунтам, невозможность отмены транзакции и некоторые другие. Многие пока что обусловлены технологическими особенностями сети и уже находятся в процессе устранения. В то же время ряд проблем, равно как и повышенный интерес к самому биткоину, вызваны его растущей стоимостью и вниманием, проявляемым массовым инвестором к первой криптовалюте мира.

По мере роста интереса и спроса в сети Биткоина растет и количество запросов и транзакций, с чем сеть попросту не справляется. Это

некая «болезнь роста», которая, с одной стороны, позволит усовершенствовать всю систему, а с другой — приведет к появлению новых криптовалют (что уже происходит), которые более успешно в технологическом плане смогут решить ту или иную проблему, к примеру анонимности.

Можно смело говорить о том, что сеть Биткоина как первая в мире криптовалютная площадка является неким полигоном для отладки совершенно новой финансовой системы децентрализованного обмена активами. Проблемы в сети провоцируют дискуссии в криптосообществе, способствуя появлению новых технологических решений, увеличивая спектр криптовалют в мире и еще больше распространяя «вирус децентрализации» на уровне массового потребителя.

Столкновение традиционной и инновационной (децентрализованной) парадигм увеличивает количество сторонников и противников каждого из подходов. Сегодня у Биткоина есть и те и другие, предсказывающие криптовалюте совершенно противоположное будущее, равно как и децентрализованному мироустройству. Единства мнений нет ни в оценках перспектив, ни в оценках стоимости биткоина. Меняется и поведение самих сторонников и противников, что обусловлено начавшейся в этом году «войной систем, или войной миров» — централизованного и децентрализованного.

Книга Майкла Кейси и Пола Винья «Машина правды. Блокчейн и будущее человечества» предлагает беспристрастный взгляд на зарождающийся децентрализованный мир. Не навязывая определенное мнение, она предоставляет читателю исключительно факты, аргументы и рассуждения на эту тему. Стиль книги напоминает журналистское расследование, основанное на взвешенном фактаже и глубокой исследовательской базе.

Книгу можно назвать визионерской. В ней много рассуждений на тему четвертой промышленной революции и мира будущего, построенного на «интернете вещей». Раскрывая глубину технологии блокчейн, этот труд также дает много ориентиров по долгосрочному инвестированию. Становится очевидным, что будущее — за проектами, которые позволят масштабировать децентрализованное мироустройство и объединить различные индустрии, например «интернет вещей» и блокчейн.

Кейт Щеглова,
член сообщества Global Blockchain Ladies,
издатель Future magazine

Посвящается Лиз,
Дженни, Саре и Ди
М. К.

Посвящаю моим родителям
П. В.

Предисловие

В книге The Age of Cryptocurrency* мы рассматривали цифровую валюту биткоин и возможность создания новой, более справедливой глобальной платежной системы, независимой от банков и прочих посредников. К тому времени, когда книга увидела свет, стало очевидно, что истинный потенциал биткоина** и стоящих за ним технологий намного мощнее: электронная денежная единица способна разрешить проблемы доверия между частными лицами и организациями при товарообмене, заключении контрактов, приобретении собственности и обмене конфиденциальными данными. В результате (естественно, не без помощи информационной шумихи) компании, правительственные структуры и СМИ начали проявлять активный интерес к *технологии блокчейн*, которая позволяла обойти привычные централизованные механизмы, до сих пор регулировавшие обмен ценностями в обществе. К примеру, сообщества «производящих потребителей» — хозяйств, которые не только потребляют электроэнергию, но и производят ее с помощью солнечных панелей, — могли бы сформировать собственный энергетический рынок и устанавливать цены без оглядки на коммунальные компании и службы. Точно так же домовладельцы, покупатели недвижимости и ипотечные заимодатели

* Издана на русском языке: *Винья П., Кейси М.* Эпоха криптовалют. Как биткоин и блокчейн меняют мировой экономический порядок. М. : Манн, Иванов и Фербер, 2018. *Прим. ред.*

** В книге употребляются два варианта написания термина «биткоин» — с прописной и строчной буквы, что объясняется разницей в значении. Слово «биткоин» в значении валюта, денежная единица, пишется со строчной буквы; если же речь идет о платежной системе и одноименном протоколе передачи данных, лежащем в основе технологии блокчейн, — то с прописной.

получили бы альтернативу не всегда надежным государственным реестрам и смогли бы создать независимую базу данных с меньшим риском взлома, кражи или простой ошибки, управляемую децентрализированной сетью. И это лишь часть перспектив, которые привлекли широкое внимание к технологии блокчейн.

Возросшая популярность биткоина уже привела к двум важным переменам в нашей жизни. Во-первых, один из авторов книги — Майкл Кейси — так увлекся новой технологией и открывающимися горизонтами, что решил оставить журналистику и полностью посвятить себя исследованиям. Всего через полгода после выхода нашей предыдущей книги он уволился из редакции The Wall Street Journal и перешел в медиалабораторию Массачусетского технологического института, неистовый директор которой Дзёити Ито, более известный как Джой, быстро подметил параллели между становлением биткоина и взрывным развитием цифровых технологий при появлении интернета. Осознав, что существует запрос на новую децентрализированную структуру, Ито решил направить самые мощные интеллектуальные и финансовые ресурсы на развитие зарождающейся технологии. Результатом стала программа исследования криптовалют: научная инициатива, объединившая студентов и профессоров, инженеров и специалистов в области криптографии, а также финансистов, начинающих предпринимателей и бизнес-стратегов из списка Fortune 500, благотворителей и правительственных чиновников в целях разработки цифровой архитектуры принципиально нового «интернета ценностей». Когда Майкл получил предложение влиться в ряды исследователей, он, разумеется, не мог отказаться. Не каждому выпадает шанс приложить руку к экономической революции!

Второй важный результат — книга, которую вы читаете. В «Эпохе криптовалют» мы сосредоточились на применении биткоина как платежной системы, способной повлиять на все валюты мира. Однако с тех пор мы осознали, что технология — рискованный предмет для писателя: она постоянно развивается, а слова на странице остаются прежними. За прошедшие три года столько всего изменилось, что нам пришлось написать еще одну книгу. В ней мы не только продолжим начатый в 2015 году разговор, но и выведем его на следующий, более высокий уровень. Нам предстоит рассмотреть, как биткоин-технология

и ее различные ответвления могут реорганизовать общественные институты и найти новые сферы применения.

В условиях современной экономики миром правит тот, кто контролирует потоки информации. Это хорошо видно на примере таких информационно-технологических гигантов, как Google и Facebook: они постоянно накапливают данные о нас и нашем взаимодействии. В XXI веке само понятие власти определяется наличием полномочий собирать, хранить и публиковать данные. Сейчас эти полномочия носят централизованный характер и разделены между несколькими крупными корпорациями. Если вы не видите здесь проблемы, вспомните о том, как тайный алгоритм сети Facebook (нацеленный прежде всего на продвижение интересов компании) повлиял на политическую ситуацию в США. Поощряя создание и распространение нередко весьма сомнительной информации, чтобы вызвать коллективные всплески эмоций в группах единомышленников, этот алгоритм сыграл немалую роль в ошеломляющем исходе президентских выборов 2016 года.

Концепция блокчейна* может положить конец нынешней иерархии власти в информационном поле. В результате способность накапливать и обрабатывать данные перейдет к децентрализованной, *никому* не принадлежащей структуре. Теперь мы можем представить мир, неподвластный мегакорпорациям вроде Google и Facebook или даже силовым ведомствам вроде Агентства национальной безопасности. Мы, люди — граждане мирового сообщества, — сами будем решать, что делать с имеющейся информацией.

Вот, пожалуй, самое важное, что нужно знать о технологии блокчейн. «Машина правды» — наша попытка донести до вас эту мысль.

* Термин «блокчейн» в последнее время употребляется широко, но не всегда корректно. Мы будем использовать его в трех основных значениях. Первое — «Блокчейн» с прописной буквы как изначальный распределенный реестр биткоина. Второе — «блокчейн» со строчной буквы (имеет форму множественного числа «блокчейны») как любой распределенный реестр, имеющий вид непрерывной цепочки блоков. Наконец, третье — «технология блокчейн», включающая в себя всю совокупность методов, принципов, технологий и их применения. Кроме того, говоря о технологии «распределенных реестров», мы имеем в виду не только блокчейны, но и любые распределенные реестры вообще. Нам не хотелось бы использовать слово «блокчейн» как неизменяемое и неисчислимое абстрактное существительное. С нашей точки зрения, блокчейн (как и любой реестр) — вполне конкретный объект, а не процесс и не метод. В названии книги мы пишем слово «Блокчейн» с прописной буквы, чтобы подчеркнуть ту роль, которую изначальный Блокчейн — реестр биткоина — сыграл в становлении новой технологической сферы.

Введение

Инструмент общественного строительства

В шестидесяти милях к востоку от Аммана на небольшом участке сухой каменистой почвы, очищенной от песков Иорданской пустыни, расположен лагерь сирийских беженцев Азрак, открытый Управлением верховного комиссара ООН. В нем во временных домах — белых металлических постройках, расположенных в строгом линейном порядке, будто армейские казармы, — проживают 32 тысячи лишившихся крова сирийцев. В сущности, Азрак — это небольшой город со всеми типичными городскими проблемами. Однако Управление Верховного комиссара ООН по делам беженцев (УВКБ ООН) и другие гуманитарные миссии могут предоставить беженцам только кров и пищу. В их распоряжении нет структур и инстанций, обеспечивающих порядок, безопасность и жизнедеятельность городов.

Любому лагерю беженцев по определению не хватает того, что политологи называют «социальным капиталом»: налаженных связей и отношений, которые позволяют сообществу нормально функционировать и вступать во взаимодействие с другими группами. В Азраке эта проблема стоит особенно остро. В лагере есть отряд полиции, но служат в нем только иорданцы. Они не принадлежат к числу беженцев и воспринимаются как чужаки. Конечно, уровень преступности в Азраке ниже, чем в соседнем лагере Заатари, где 130 тысяч сирийцев проживают в условиях, которые представители ООН определили как «хаос и беззаконие». Тем не менее этот выжженный клочок земли трудно назвать гостеприимным. Когда в 2014 году Азрак был создан в качестве

альтернативы переполненному Заатари, беженцы жаловались на его неприспособленность к бытовым нуждам. Электричество поступало с большими перебоями, что усложняло процесс зарядки телефонов — единственного средства связи с родными и близкими. Кроме того, отсутствие доверительных отношений внутри сообщества делало лагерь более уязвимым для боевиков Исламского государства — по крайней мере, в глазах самих беженцев. Поначалу многие отказывались переселяться в Азрак. И хотя в последнее время желающих стало больше, рассчитанный на 130 тысяч человек лагерь по-прежнему заполнен лишь на треть.

Неудивительно, что этот свежеиспеченный город, почти лишенный социального капитала, стал площадкой для радикального эксперимента — поиска новых моделей управления, благоустройства, самоорганизации, общественного строительства и распределения ресурсов. В основу проекта легла технология блокчейн — децентрализованная система хранения данных, которая обслуживает цифровую валюту биткоин и обеспечивает надежный, немедленный способ отслеживать совершенные транзакции. Всемирная продовольственная программа (ВПП) ООН, обеспечивающая питанием около 80 миллионов человек во всем мире, пригласила 10 тысяч беженцев к участию в пилотном проекте, в рамках которого технология блокчейн используется для более эффективного распределения запасов продовольствия. ВПП взяла на себя очень сложную административную миссию: проследить, чтобы каждый беженец в лагере, где процветает воровство и почти ни у кого нет удостоверяющих личность документов, получал причитающийся ему паек.

Среди участников проекта оказалась сорокатрехлетняя Наджа Салех аль-Меймед — одна из более чем пяти миллионов сирийцев, оставивших свой дом из-за тягот гражданской войны. В начале июня 2015 года на фоне перебоев с продовольствием и слухов о похищении молодых девушек боевиками в соседних селениях Наджа с мужем решились покинуть родной городок Хасака, где их семьи жили с незапамятных времен. «Не приведи Господи никому испытать то, через что прошли мы», — сказала Наджа в интервью, проведенном по нашей просьбе представителями ООН в лагере Азрак [1].

Оставив дом, имущество, привычный круг соседей и друзей и почти все связи с некогда единым сирийским народом, Наджа утратила нечто

весьма ценное и значимое, что в обычных обстоятельствах мы воспринимаем как должное: доверительные отношения, чувство идентичности и принадлежности, личную и коллективную историю, которая связывает наше прошлое с настоящим и позволяет участвовать в жизни сообщества. Объем данных, подтверждающих нашу гражданскую сознательность, обычно накапливается различными учреждениями в виде официальных документов: свидетельства о рождении, домовой книги, выписки с банковского счета, диплома, водительских прав и т. п. Теряя все это — как происходит с беженцами, которые поневоле приобретают «внегосударственный» статус, — человек попадает в крайне уязвимое положение и становится легкой добычей для преступников и террористов. Если ты не способен подтвердить собственную личность, твоя судьба оказывается в руках посторонних людей. Вот почему одна из главных задач Управления по делам беженцев ООН и Всемирной продовольственной программы — создание хотя бы временных социальных структур и институтов. И она не менее важна, чем раздача продуктов. В пыльных палаточных городках, заселенных беженцами из разных стран мира, гуманитарные миссии должны выполнять сложнейшую задачу — восстанавливать систему социального доверия. Фактически им приходится выстраивать общество с нуля. И, как недавно выяснилось, технология блокчейн может служить инструментом такого строительства.

[22]

Именно в той сфере, где человеку отчаянно нужны надежные структуры, чтобы отслеживать социальное взаимодействие и подтверждать репутацию, технология блокчейн раскрывает свой потенциал. Благодаря ей мы можем обойтись без официальных инстанций, доказывающих нашу гражданскую полноценность. Программы на основе блокчейна содержат сложный набор функций, которые дают беспрецедентный результат: запись транзакции доступна всем пользователям и может быть подтверждена в любой момент, но не контролируется ни одной властной структурой. Это обеспечивает две крайне важные вещи: невозможность изменить или удалить запись в своих интересах и больший контроль над своими данными. Едва ли нужно пояснять их ценность для тысяч сирийцев, живущих в лагере на выжженной земле.

При операциях с биткоином использование распределенного реестра исключает «двойное расходование» средств — то есть

предотвращает мошенничество и не позволяет потратить одну и ту же единицу на несколько разных покупок. Точно так же в лагере Азрак технология блокчейн исключает двойную выдачу пайка одному и тому же лицу. Это крайне важно, когда запасы продовольствия ограниченны, ведь криминальные элементы нередко крадут или незаконно получают пайки, а затем продают их на черном рынке. Теперь же беженцы в любой момент смогут подтвердить законность получения провианта. Это положит конец сбоям при использовании продовольственных карточек. Любое несоответствие сразу же привлечет внимание администраторов, которые приостановят выдачу пайка подозрительному лицу до выяснения ситуации.

В рамках пилотного проекта все, что нужно для заключения договора о выдаче продовольствия, — сканировать радужную оболочку глаза беженца и предоставить скан раздатчикам продуктов. В сущности, глаз становится чем-то вроде цифрового кошелька, избавляющего от необходимости наличных денег, чеков, банковских карт или смартфонов, что снижает вероятность кражи. (Безусловно, вы можете расценить сканирование радужки как вторжение в частную жизнь, но об этом мы поговорим чуть позже.) Всемирной продовольственной программе уже удалось сэкономить миллионы долларов за счет проведения таких электронных транзакций, ведь они не предусматривают посредников (например, банков и платежных систем), которым нужно платить процент с каждой операции.

Итак, всякий раз, когда беженец тратит какую-то часть своего цифрового «капитала» на покупку муки, эта операция автоматически регистрируется в общедоступном реестре, который невозможно подделать. Такая предельно прозрачная, моментально обновляющаяся, очень надежная система учета позволяет администраторам ВПП в любое время отслеживать поток транзакций, даже не ведя централизованных записей. Подобная организация может поддерживать платежную систему во всем лагере без необходимости брать на себя роль банка или платежной платформы.

Однако программа идентификации УВКБ ООН, встроенная в блокчейн-проект лагеря Азрак, по-прежнему имеет вид централизованной базы данных, что вызывает тревогу у многих критиков проекта. Такие базы данных восприимчивы к взлому, поскольку содержат огромный массив информации, что автоматически превращает их в так

называемый вектор атаки. Подобные риски ставят под удар и без того одну из самых уязвимых категорий населения. А представьте, что будет, если эти биометрические данные попадут в руки любителей этнических чисток — вроде боевиков ИГИЛ. Разработчики блокчейна, которые вообще очень трепетно относятся к вопросам конфиденциальности, громче всех заявляют об этой проблеме. Некоторые из них ищут способ распределить контроль над личной информацией так, чтобы избавиться от больших «залежей данных». Вероятно, технология блокчейн поможет справиться и с этой проблемой, но пока она не решена, ВПП и УВКБ ООН сошлись во мнении, что на данный момент плюсы единой безналичной системы расчетов перевешивают возможный риск.

По словам официального представителя ВПП Алекса Слоана, пилотный проект уже увенчался значительным успехом: он сэкономил средства и предоставил весьма эффективный способ борьбы с несоответствиями в счетах беженцев [2]. В свете полученных результатов организация намерена включить в проект до 100 тысяч беженцев. В недалеком будущем, полагает Слоан, воспользоваться аналогичными программами смогут около 20 миллионов малоимущих, которые получают дотации от ВПП. Перед лицом худшего гуманитарного кризиса в истории — результата алчности, беспощадной борьбы за власть и провальной политики западных держав, не сумевших вовремя обуздать хаос, — мы обязаны помочь пострадавшим, привнеся в их жизнь утраченное доверие и обеспечив им безопасность. Возможно, технология блокчейн даст нам шанс на успех.

Эксперимент в лагере Азрак — лишь один пример того, как международные структуры пытаются поставить технологию блокчейн на службу обездоленным. В начале 2017 года группа энтузиастов при штабе ООН в Нью-Йорке запустила сайт и призвала к совместной работе других сотрудников организации. Вскоре группа насчитывала уже 85 участников из разных стран мира. Сейчас коллектив в партнерстве с правительствами ряда европейских стран, например Норвегии, ведет несколько пилотных проектов по внедрению блокчейна в сфере градостроительства. При Всемирном банке открыта новая лаборатория, чья задача — применить технологию блокчейн для борьбы с нищетой путем создания неуязвимых реестров собственности

и надежных цифровых идентификаторов личности. Межамериканский банк развития* США и медиалаборатория Массачусетского технологического института работают над программой, которая поможет беднейшим латиноамериканским фермерам получать кредит на основе записей о покупках инвентаря и сельхозтехники, подтвержденных блокчейн-реестрами. Неправительственные и благотворительные организации — такие как Всемирный экономический форум и Фонд Рокфеллера — также изучают потенциал технологии блокчейн.

Что же находят эти почтенные и далеко не новые организации в малопонятной цифровой технологии, изобретенной криптолибертарианцами и киберпанками — создателями биткоина? Надежду, что децентрализованная система хранения данных решит проблему дефицита социального капитала, которую мы обсуждали на примере лагеря Азрак. Пилотный проект ООН, в рамках которого возник единый каталог транзакций внутри сообщества, помог беженцам обрести взаимное доверие и создал платформу для обмена ценностями. Проблема недоверия и подозрительности стара как мир, однако теперь, имея новый, беспрецедентно мощный инструмент, который можно направить на ее решение, сообществам станет легче накапливать социальный капитал. Для развивающихся стран такая возможность особенно важна, поскольку позволит их экономикам приблизиться к модели первого мира. Например, домовладельцы с невысоким доходом смогут брать кредит на улучшение жилищных условий; мелкие уличные торговцы получат доступ к страховым программам. Миллиарды граждан сделают первый шаг к обретению экономических возможностей, которые нам даны чуть ли не от рождения.

Однако потенциал блокчейна заметен не только при применении в развивающихся странах или гуманитарных миссиях. В штаб-квартирах компаний из списка Fortune 500 тоже ищут способ стимулировать экономический рост. Вероятно, блокчейн способен вытеснить устаревшую централизованную модель доверительного управления, которая сейчас влияет на все аспекты экономической и социальной жизни.

До сих пор экономическое взаимодействие между субъектами осуществлялось посредством вовлечения банков, регистрационных

* Международная финансовая организация, созданная в 1959 году в целях финансовой поддержки экономики стран Латинской Америки и Карибского бассейна.

служб и прочих учреждений. Эти «доверенные третьи стороны» фиксируют проведенные операции, что позволяет нам доверять экономической системе, обмениваться материальными и нематериальными ценностями и в идеале выстраивать полноценное общество. Проблема, однако, в том, что все эти институты часто действуют как привратники, решая, кого впускать или не впускать в поле финансового взаимодействия (причем берут за это комиссию). К тому же они не всегда надежны — вспомните кризис 2008 года, когда банки откровенно нарушили обязательство вести прозрачный учет. Кроме того, они часто пользуются властной позицией, чтобы установить непомерно высокие комиссии или проценты по кредитам. Неэффективность и нерентабельность посредников нередко приводит к отказу от сделок и транзакций. Отыскав способ обходиться без посредничества, мы не только сэкономим средства, но и создадим принципиально новые модели предпринимательской деятельности.

Появление интернета уже избавило нас от части назойливых посредников, теперь блокчейн продолжает эту тенденцию. Однако стоит отметить, что за успехом каждого нового приложения стоит некий механизм, который помогает разрешить вечную проблему доверия. Кто десять лет назад мог себе представить, что будет комфортно себя чувствовать в машине незнакомца, с которым только что познакомился через смартфон? Однако сервисы вроде Uber и Lyft помогли нам преодолеть барьер недоверия благодаря встроенной системе рейтинга водителей и пассажиров, что стало возможным лишь с развитием социальных сетей и цифровых коммуникаций. Этот пример показывает, что, если технология помогает решить проблему доверия и обеспечить чувство безопасности, человек вполне готов и способен к прямому взаимодействию с совершенно незнакомыми людьми. Все это открывает перед нами путь к экономической модели *peer-to-peer* (P2P).

Технология блокчейн ставит перед нами логичный вопрос: зачем останавливаться на Uber? Зачем нам вообще именно эта компания, если она забирает себе 25 процентов с каждой поездки и нередко злоупотребляет безграничным доступом к информации о пассажирах? [3] Как насчет полностью децентрализованной системы вроде израильской платформы Commuterz на основе блокчейна? В этом случае у платформы нет конкретных владельцев; она, как и биткоин,

использует ПО с открытым исходным кодом, которое может скачать каждый. За ней не стоит корпорация, которая забирает себе 25 процентов выручки. Вместо этого пользователи ведут расчеты в цифровой валюте; система поощряет совместные поездки, чтобы разгрузить дороги и снизить стоимость перемещения.

В широком смысле, возложив управление социальным капиталом на децентрализованную сеть с открытым протоколом вместо ряда уполномоченных посредников и создав новые цифровые валюты, токены и активы, мы сможем изменить саму природу общественной организации. Возникнут новые, прежде невозможные подходы к сотрудничеству и взаимодействию, что преобразит многие отрасли и организации. Потенциал блокчейна вполне под стать широте открывающихся горизонтов. Вот выборка результатов, которые мы можем получить в обозримом будущем; и это далеко не исчерпывающий перечень.

— *Неуязвимые реестры собственности*, с помощью которых можно доказать право на владение домом, автомобилем и другими активами.
— *Мгновенные, прямые, защищенные межбанковские операции*, что позволит высвободить триллионы долларов на межбанковском рынке, которые сейчас тратятся на проведение транзакций через десятки специализированных учреждений в течение двух–семи рабочих дней.
— *Цифровые удостоверения личности*, которые можно получить без участия государственных структур и бюрократических инстанций.
— *Децентрализованные вычислительные системы и хранилища данных*, которые вытеснят корпоративные облачные вычисления и веб-хостинг. Для их поддержания хватит мощностей обыкновенного персонального компьютера.
— *Децентрализованный «интернет вещей»*, где любые устройства смогут обмениваться информацией без посредников. Вероятно, это приведет к большим переменам в сфере логистики, а также к созданию децентрализованных энергосетей.
— *Цепи поставок на основе блокчейна*: использование поставщиками общей информационной платформы значительно

повысит прозрачность и эффективность всех операций по производству товара.

[28]

— *Децентрализация СМИ и контента*, что позволит музыкантам, художникам и в идеале всем производителям уникального контента распоряжаться и управлять своим «цифровым активом».

Технология блокчейн открывает нам путь к тому, что ряд экспертов уже называют «интернетом 3.0», — реструктуризации Всемирной сети в целях придания ей демократического характера, о котором мечтали создатели интернета 1.0 [4]. Выяснилось, что просто объединить компьютеры в сеть, чтобы избавиться от информационной власти мегакорпораций, недостаточно. Вольнолюбивые программисты Кремниевой долины не учли склонность общества возлагать проверку благонадежности на централизованные институты. Их промах стал очевиден на стадии интернета 2.0, когда мощь социальных сетей не только открыла перед пользователями новые возможности, но и превратила наиболее расторопные компании в гигантские монополии. Вспомним о Facebook и Twitter, выросших в мегакорпорации, а также о суперуспешных детищах «шеринговой экономики»* вроде Uber и Airbnb. Технология блокчейн, как и прочие находки «интернета 3.0», обещает покончить с любыми посредниками, чтобы люди могли сами выстраивать социальные сети и заключать торговые сделки на собственных условиях.

Однако свержение нынешних колоссов — отнюдь не единственная надежда, которую дает блокчейн. Многие крупные корпорации тоже видят в новой технологии возможность высвободить потоки капитала и направить их в более выгодное русло. Одни усматривают в ней потрясающие перспективы, другие — серьезную угрозу. В любом случае многие отрасли и предприятия считают нужным хотя бы поэкспериментировать с технологией блокчейн, чтобы понять, к чему приведет ее развитие.

* Также известна как экономика совместного потребления. Концепцию предложили экономисты Рэйчел Ботсман и Ру Роджерс исходя из идеи, что потребителю часто выгоднее платить за временный доступ к продукту, чем владеть им. Данная экономическая модель набирает популярность и, по версии журнала Time, относится к явлениям, которые изменят мир в ближайшем будущем. *Прим. ред.*

В банковской сфере — отрасли, которую биткоин угрожает свести на нет, — начинают осознавать, что блокчейн-протоколы могут значительно упростить громоздкие процессы перевода и зачисления средств, а также одобрения и подтверждения операций. Используя надежный общедоступный реестр, который можно обновлять одновременно в режиме реального времени, банки существенно понизили бы стоимость транзакций и высвободили капитал для новых вложений. Это прекрасная новость для инвестиционных банков, таких как Goldman Sachs, но потенциальная угроза для депозитарных банков вроде State Street или клиринговых компаний вроде Deposit Trust и Clearing Corporation, чья бизнес-модель основана на выполнении посреднических функций. Тем не менее все виды финансовых организаций сейчас испытывают потребность исследовать новую технологию.

К примеру, нью-йоркская научно-техническая лаборатория R3 CEV получила 107 миллионов долларов от более чем ста крупнейших финансовых компаний мира на разработку технологии распределенного реестра [5]. Предложенная командой R3 платформа Corda построена по базе блокчейна, хоть это и не отображено в названии. Она должна соответствовать моделям и правилам банковского дела, при этом удешевляя защищенные межбанковские операции на триллионы долларов.

Предприятия, не связанные с финансовым сектором, тоже понемногу включаются в процесс. Консорциум Hyperledger разрабатывает стандартизированные открытые версии блокчейна для сферы логистики — например, управления цепями поставок. Под руководством Linux Foundation консорциум объединяет гигантов вроде IBM, Cisco и Intel, а также стартап Digital Asset Holdings во главе с бывшим топ-менеджером банка J.P. Morgan Блайт Мастерс.

Один из показателей растущего энтузиазма можно найти в анналах CoinDesk. Эта медиаплатформа проводит ежегодную конференцию, посвященную технологии блокчейн. Первая конференция прошла в 2015 году и собрала 600 участников. Вторую посетили 1500 человек. В 2017 году в мероприятии уже участвовало 2800 человек и еще 10 500 интернет-пользователей подписались на онлайн-трансляцию. Участники прибыли из 96 стран мира, а состав спонсоров оказался столь разнородным, что включал исследовательский центр компании Toyota, консалтинговое агентство Deloitte, торговую палату

правительства Австралии и Cryptonomos — молодой онлайн-магазин цифровых токенов [6].

[30] Впрочем, не нужно думать, что новая сфера уже целиком захвачена международными корпорациями. Когда мы работали над этой книгой, в мире разразилась очередная эпидемия золотой лихорадки, даже затмившая взлет цен на биткоин в 2013 году. На сей раз любителей скорого богатства прельстила новая форма привлечения инвестиций — ICO, или первичное предложение монет (токенов), — суть которой заключается в продаже инвесторам фиксированного количества единиц криптовалюты, полученных путем разовой или ускоренной эмиссии. Этот инструмент краудфандинга основан на технологии блокчейн. Возникший вокруг него ажиотаж очень напоминал «пузырь доткомов» конца 1990-х: те же отчаянные попытки сделать деньги из воздуха путем рискованных спекуляций и то же чувство, что за общим безумием все-таки проглядывает новаторская технология, которая завтра в корне изменит деловой мир.

Стартапы, возникшие на волне интереса к ICO, продвигают новые децентрализованные приложения, которые могут произвести революцию в любой сфере — от рекламы до медицины. В их основе лежат специальные токены, которые служат как для привлечения инвестиций, так и для создания сети пользователей. Механизм отчасти напоминает работу краудфандинговых сайтов (например, Kickstarter), однако в данном случае покупатель токена имеет шанс быстро заработать на вторичном рынке. На момент написания этих строк рекордная сумма, вырученная от предварительной продажи токенов в ходе проведения ICO, составляет 257 миллионов долларов. Именно столько заработала сеть лабораторий Protocol Labs, выпустив токен под названием Filecoin для продвижения нового протокола децентрализованной сети IPFS. Идея проекта сводится к установке пользователями специального ПО, которое позволяет хранить данные на жестких дисках их компьютеров. За предоставленное пространство на диске они получают токены, которые затем можно обменять на биткоины или другие криптовалютные единицы.

Вполне вероятно, что многие ICO нарушают протоколы безопасности и рано или поздно мыльный пузырь лопнет, причем пострадают ни в чем не повинные инвесторы. Однако в новом цифровом буме есть и нечто освежающее, демократическое. Целые когорты мелких

инвесторов получили доступ к первым стадиям капиталовложений — привилегии, как правило, венчурных инвесторов и других профессионалов финансовой сферы.

Прародитель всей мировой криптовалюты, биткоин, тоже не сходит с дистанции, что отражается в его цене. Несмотря на ожесточенную борьбу между разработчиками и майнерами, которые подтверждают транзакции в сети Биткоин — а она уже привела к модификации исходного кода и форку биткоина, — курс биткоина в ноябре 2017 года достиг рекордной отметки в 7601 доллар США. В результате его рыночная капитализация составила более 126 миллиардов долларов. Таким образом, с момента публикации нашей предыдущей книги (январь 2015 года) стоимость биткоина увеличилась на 2823 процента, а с момента первых продаж на полуликвидном рынке в июле 2010 года он вырос в цене на 12,7 миллиона процентов. Вложив 8000 долларов в биткоин при старте продаж, вы сейчас стали бы миллиардером. Такие результаты вполне убедительно подтверждают оценку криптоаналитиков Криса Берниска и Джека Татара, назвавших биткоин «самым заманчивым из альтернативных капиталовложений XXI века» [7].

В сущности, блокчейн — это цифровой реестр (или проще — учетная книга), распределенный по децентрализованной сети автономных компьютеров, которые обновляют и поддерживают его таким образом, чтобы любой пользователь мог доказать достоверность и подлинность записи. Это достигается за счет особого алгоритма, встроенного в ПО, которое установлено на всех компьютерах сети. Алгоритм постоянно поддерживает между компьютерами консенсус относительно того, какие данные добавлять в реестр, включая и обрабатывая все виды финансовых транзакций, претензии на право собственности и другую ценную информацию. Каждый компьютер самостоятельно обновляет свою версию реестра, следуя при этом общему алгоритму консенсуса. Как только в реестр добавляется новая запись, специальная криптографическая защита делает возврат к прежнему состоянию системы практически невозможным. Владельцы компьютеров либо получают плату в цифровой валюте, что мотивирует их повышать уровень безопасности системы, либо работают в рамках соглашения о консорциуме. Результат уникален: группа независимых субъектов, действующих

в сугубо личных интересах, объединившись, производит нечто для общего блага — неуязвимый для подделки архив, которому может доверять каждый пользователь, без централизованных владельцев или посредников.

[32]

Группа компьютеров, обрабатывающих данные с помощью сложных математических алгоритмов, кажется не таким уж важным явлением. Но, как мы объясним в следующей главе, системы хранения записей, а в особенности учетные книги необходимы для функционирования любого сообщества. Без них мы не набрали бы нужный капитал доверия, чтобы заключать сделки, строить торговые отношения, создавать организации и союзы. Потому улучшение этого ключевого общественного механизма и его выход из-под контроля централизованных инстанций, несомненно, скажется на всех сферах нашего взаимодействия.

Такой принцип работы с информацией сделает возможной коммерцию в формате P2P, устранив посредников из всех видов деловых операций. Благодаря встроенным протоколам защиты данных блокчейн позволит организациям и частным лицам вступать в деловые отношения без страха быть обманутыми и, вероятно, ознаменует начало новой эпохи открытой и прозрачной информации. Это означает, что мы сможем делиться ею более активно. Как правило, открытый обмен положительно влияет на сферы экономической деятельности, что, в свою очередь, создаст больше возможностей для бизнеса.

Технология блокчейн подводит всю цифровую экономику к так называемому интернету ценностей [8]. В то время как нынешняя версия интернета позволяет напрямую передавать друг другу информацию, «интернет ценностей», как следует из названия, позволит напрямую обмениваться ценностями — будь то деньги, активы или конфиденциальные сведения, которые прежде никто не рискнул бы передать с помощью сети. Если интернет первого поколения создал новые бизнес-модели и головокружительные возможности заработка, помогая перешагнуть через многие барьеры и вступить в игру, то следующая фаза обещает устранить барьеры вообще. Теоретически это означает, что каждый владелец цифрового устройства с доступом в интернет сможет участвовать в глобальной экономике. Грядет расширение сферы открытых технологий, которое даст толчок новым идеям, концепциям и механизмам.

Вспомните, как избавление от посредников уже преобразило мировую экономику на заре интернет-технологий, и сможете представить, насколько масштабные перемены обещает нам следующий этап. Подумайте, например, о том, как аутсорсинг в сфере техподдержки, вебдизайна и даже бухгалтерских услуг сократил рабочие места в странах Запада, но способствовал экономическому росту в таких местах, как Бангалор в Индии. Можно вспомнить и о виртуальных досках объявлений на сайтах с глобальным охватом, где каждый может разместить бесплатно информацию, которые нанесли огромный ущерб индустрии частных объявлений и привели к банкротству многих региональных газет. Если технология блокчейн не обманет наших ожиданий и обусловит полную децентрализацию экономики, все прежние потрясения померкнут перед этим тектоническим сдвигом.

Однако нам еще многое предстоит сделать, прежде чем эта технология полностью раскроет свой потенциал. Возможно, она никогда и не выйдет на уровень, который необходим для поистине масштабных перемен. Тем не менее почти в каждой отрасли уже осознали заложенные в ней перспективы. Например, решение проблемы доверия позволило бы нам эффективнее применять свои активы, идеи, творческие способности, вкладывая их в любое продуктивное начинание по собственному выбору. Ведь если я могу доверять человеку — его документам об образовании, финансовой отчетности, профессиональной репутации, — потому что все это объективно подтверждено децентрализованной системой, то мне ничто не помешает установить с ним деловые отношения. Я могу взять его на работу. Могу основать с ним совместное предприятие. Могу поделиться с ним конфиденциальной деловой информацией. И мне не нужно полагаться на посредников вроде юристов или регистраторов, которые добавляют стоимости нашим операциям, понижая при этом их эффективность. Подобные соглашения — катализатор экономического роста. Они дают толчок инновациям и процветанию. Любая технология, которая избавляет от трений и облегчает сотрудничество, служит на благо обществу.

Безусловно, нет никаких гарантий, что технология будет развиваться по самому благоприятному сценарию. Мы уже наблюдали за поглощением интернета мегакорпорациями и знаем, к чему привела такая централизация власти — от создания огромных массивов конфиденциальных данных, привлекающих хакеров, до активных вбросов

дезинформации, порождающих хаос в политической жизни. Поэтому крайне важно не допустить, чтобы влиятельные группы поставили новую технологию на службу своим интересам. Как и при зарождении интернета, придется проделать немалый путь, чтобы сделать технологию блокчейн достаточно безопасной, доступной и обеспечивающей должный уровень конфиденциальности.

Блокчейн — в первую очередь социальная технология, новый алгоритм и принцип управления сообществами, от напуганных беженцев в иорданской пустыне до межбанковского рынка, где крупнейшие финансовые структуры мира ежедневно обмениваются триллионами долларов. По определению, в работу над технологией блокчейн должны включиться все слои общества. Наша книга — не только справочник, но и призыв к активному действию.

Глава

1

Протокол Господа Бога

Наверное, вас это удивит, но мечта самого пылкого либертарианца — обитателя даркнета, самая провокационная, спорная, самая бунтарская концепция в современном мире финансов, концепция настолько мощная, что все правительства планеты сейчас решают, взять ее под свою опеку или полностью запретить, — это обычная бухгалтерская книга.

Да-да, тот самый гроссбух, или учетный реестр.

Первым плодом этой крамольной идеи стал, конечно же, биткоин, основной принцип которого сводится к ведению цифрового учетного реестра, где отображаются все транзакции. Что же делает эту незамысловатую идею столь новаторской? Способ ведения записей, который мы называем «блокчейн», то есть цепочка блоков. Биткоин, выпущенный в 2009 году человеком или группой людей под псевдонимом Сатоши Накамото, разрабатывался как средство обойти банки и правительства, которые на протяжении веков стояли на страже нашей финансовой системы. Его реестр, или блокчейн, сулил новый подход к процессам, которые в лучшем случае выполнялись посредниками за определенное вознаграждение за каждую операцию, а в худшем — приводили к рукотворным экономическим катастрофам.

Вы, наверное, купили эту книгу, рассчитывая найти в ней безумные вдохновенные картины нашего цифрового будущего... а мы подсунули вам старый добрый гроссбух. Но ведь конторские и бухгалтерские книги на протяжении тысячелетий были неотъемлемой частью

развития цивилизации. Письменность, деньги и учетные реестры — вот святая троица изобретений, которые позволили нашим предкам вести дела вне узких родовых групп и в результате основывать более крупные поселения. Все понимают роль письменности и денег в истории человечества, а вот о роли всевозможных реестров знают обычно лишь те, кто изучал скучное бухгалтерское дело.

Первые деловые реестры появились в третьем тысячелетии до нашей эры в Месопотамии, или Междуречье (современный Ирак). Из десятков тысяч дошедших до наших дней месопотамских глиняных табличек большинство представляет собой именно «бухгалтерские книги»: в них ведется учет податей, сделок, личных трат, выплат мастерам. Знаменитый Кодекс Хаммурапи — свод законов Вавилонии — тоже своего рода реестр, только высеченный на камне. Впрочем, свои законы устанавливали и записывали многие правители. Появление сводов и реестров совпало с возникновением первых крупных цивилизаций [1].

Почему же учетные записи так важны для человечества? Обмен товарами и услугами — ключевой фактор развития общества, но он возможен лишь при условии отслеживания сделок. Это несложно сделать в маленьком стойбище, где было нетрудно запомнить, кто ел мясо, когда кто-то из охотников убивал кабана, и проследить, чтобы позже эти люди заплатили за еду (например, принесли охотнику новые наконечники для стрел или еще что-то ценное). В такой ситуации вполне можно положиться на доверительные отношения внутри рода. Куда сложнее добиться соблюдения обязательств, когда речь идет о большой группе незнакомых друг с другом людей — при том что к чужакам вообще относятся подозрительно. Учетная книга гарантирует выполнение обязательств и помогает при дефиците доверия. Она позволяет отследить все операции, лежащие в основе общественной жизни. Без учетных книг и реестров гигантские сообщества XXI века просто не смогли бы существовать. Конечно, реестр нельзя назвать воплощением истины в строгом смысле слова — ведь когда речь заходит о ценностях, всегда возникает элемент субъективного суждения. Скорее, его можно рассматривать как инструмент, позволяющий приблизиться к истине, выработать картину действительности, которая устроит всех участников. Проблемы возникают в случае, когда сообщество слепо доверяет реестрам, особенно если их контролирует группа, которая

может злоупотреблять доверием в своих интересах. Именно это произошло в 2008 году, когда недостаточно пристальное внимание к действиям Lehman Brothers и прочих банков погрузило общество в пучину финансового кризиса.

Деньги как явление неразрывно связаны с идеей реестра. Материальные денежные единицы — монеты и купюры — тоже, в сущности, представляют собой учетные записи и несут в себе память сообщества. Просто в данном случае вместо конторской книги роль свидетельства транзакции исполняет материальный объект (токен): золотая монета, долларовая купюра и т. п. По согласию всего сообщества подобный объект подтверждает, что его владелец заслужил право на товары и услуги, выполнив некую работу.

Когда люди начали обмениваться товарами и деньгами на большом расстоянии, материальные объекты уже не могли успешно выполнять свою роль. Покупатель не имел физической возможности доставить деньги продавцу без помощи курьера, который вполне мог их и украсть. И тогда возникло новое решение: принцип двойной записи в бухгалтерских книгах, впервые опробованный итальянскими банкирами эпохи Возрождения. Именно эти записи заложили основы современного бухгалтерского дела и значительно расширили возможности человеческого взаимодействия. Не будет преувеличением сказать, что эта революция в системе учета помогла выстроить современный мир. Но она же заново поставила извечный вопрос: может ли общество доверять тем, кто ведет его реестры?

Биткоин предложил решение проблемы: изменить саму идею реестра. Ведь риск того, что банкир окажется недобросовестным и присвоит ваши средства с помощью скрытых комиссий и непрозрачных платежей, есть всегда. Впервые ответственность за подтверждение и запись транзакций возлагалась на группу пользователей, которые проверяют работу друг друга и совместно создают реестр, где показано общепризнанное представление об истинных фактах. Децентрализованная компьютерная сеть без единого контролера должна была вытеснить банки и прочие авторитетные инстанции, которые Накомото назвал «доверенными третьими сторонами». Реестр, созданный первыми участниками проекта, получил название *блокчейн.*

С сетью независимых компьютеров, проверяющих любое совершённое действие, можно производить транзакции в пиринговом

режиме (P2P), — то есть напрямую от человека к человеку. Это совсем не похоже на сложную систему платежей по дебетовым и кредитным картам, где любой перевод проходит через длинную цепь посредников — как минимум два банка, одну или две платежные платформы, платежную систему вроде Visa или Master Card и еще несколько инстанций в зависимости от того, где осуществляется транзакция. Каждое звено в этой цепочке ведет собственный учет, который затем нужно синхронизировать с реестрами других посредников, — несущий новые риски процесс, требующий времени и дополнительных затрат. Возможно, вы думали, что деньги незамедлительно приходят продавцу, как только вы оплатили картой покупку в магазине. Ничего подобного. На самом деле нужно несколько дней, чтобы средства проделали весь этот путь и осели на счетах магазина. Разумеется, это порождает издержки и повышает риск сбоев. В системе Биткоин вся транзакция должна занимать от десяти до шестидесяти минут (если не считать проблем с пропускной способностью сети, которые сейчас решают разработчики) и нет надобности полагаться на посредников, чтобы они провели операцию от вашего лица.

Главная особенность архитектуры биткоина и других криптовалютных систем, за счет которой возможно проведение транзакций в режиме P2P, — *распределенный* характер реестра. Эта децентрализованная структура возникает благодаря уникальному ПО с мощной криптографической защитой и инновационной системой, которая синхронизирует данные между всеми компьютерами в сети. Она работает таким образом, что изменить однажды внесенную и принятую запись практически невозможно.

В результате возникает беспрецедентное явление — учетный метод, который дает нам общепризнанное представление об истине, причем более надежное, чем все, что предлагалось до сих пор. Мы называем блокчейн «машиной правды», и ее применение отнюдь не сводится исключительно к сфере финансов.

Чтобы понять важность «божественного ока» блокчейна, давайте отвлечемся от биткоина и вернемся к традиционной банковской системе. Именно здесь кроется множество проблем, для решения которых и создавалась технология блокчейн.

Мыльный пузырь

[40]

Один из ведущих инвестиционных банков США Lehman Brothers опубликовал 29 января 2008 года финансовый отчет за 2007 фискальный год. Этот период оказался вполне успешным для банка, несмотря на колебания рынка ценных бумаг и спад на рынке недвижимости, который был раскален в течение многих лет и стал главным источником дохода для инвестиционных и коммерческих банков. Lehman Brothers, основанный 167 лет назад в Алабаме и прочно закрепившийся на Уолл-стрит, заявил о рекордной выручке в 59 миллиардов долларов и чистой прибыли в 4,2 миллиарда [2]. Суммы более чем вдвое превышали выручку и доход четырехлетней давности. На бумаге дела банка выглядели как нельзя лучше.

А девять месяцев спустя банк разорился...

История Lehman Brothers уже стала хрестоматийным примером обманутого доверия. Гигант с Уолл-стрит оказался банкротом с чудовищными долгами. Видимость успеха долгое время поддерживала лишь теневая бухгалтерия — иными словами, банк подделывал отчетность. Иногда долги попросту исчезали из ведомостей к отчетному сезону. В других случаях «трудно оцениваемым» активам приписывалась многократно завышенная ценность — когда же пришло время их продавать, открылась страшная правда: они не имели никакой цены.

Крах 2008 года помог нам многое узнать о закулисье Уолл-стрит и масштабах поддельной отчетности. Стоимость активов (включая те злополучные кредитно-дефолтные свопы), которую должны были фиксировать бухгалтерские документы, оказалась фикцией. И самое поразительное в деле Lehman Brothers — даже не факт мошенничества, а то, что большинство финансовых экспертов безоговорочно доверяли поддельной отчетности, пока не стало слишком поздно.

Правительства и центробанки всего мира потратили триллионы на выход из кризиса, но, по сути, всего лишь вернулись на исходные позиции из-за того, что неверно диагностировали проблему. Согласно общепринятому мнению, произошел кризис ликвидности и рынок рухнул из-за нехватки краткосрочного финансирования. Если вам когда-либо не хватало пары сотен долларов, чтобы заплатить по ежемесячным счетам, вы знаете, как это бывает. На самом деле банки

буквально «сидели» на триллионах якобы ценных активов, которые на поверку оказались пустышкой. Они просто назначали им произвольную, ничем не обоснованную стоимость и вносили завышенные цифры в документы. А мы верили липовым бумагам, потому что привыкли доверять репутации крупных банков. Истинная проблема заключалась не в ликвидности и не в падении рынка, а в обманутом доверии. Когда обман вскрылся, его воздействие на общество — включая политический раскол — оказалось разрушительным.

После кризиса власти клялись, что взяли ситуацию под контроль: приняли новые законы, чтобы ограничить полномочия банков и оградить вкладчиков от спекуляций. Однако с точки зрения рядовых граждан правительство всего лишь вытащило банки и корпорации из долговой ямы. Накопившееся недовольство вылилось в виде протестного «Движения чаепития» и «Захвати Уолл-стрит». За прошедшие с тех пор годы общественное доверие к правящим кругам так и не восстановилось. За доказательствами далеко ходить не надо: вполне достаточно избрания звезды телешоу в президенты США. Возможно, протестная галочка напротив фамилии Трампа и позволяла избирателю выйти из кабинки с приятным осознанием, что он утер нос элитам. Однако уже сейчас вполне очевидно (по крайней мере, нам), что вся программа Трампа — не более чем те же древние экономические идеи, только чуть-чуть подогретые и поданные под острым соусом. Мы никуда не сдвинулись по сравнению с 2008 годом.

В большинстве сфер американская экономика восстановилась — на данный момент безработица достигла рекордно низкого уровня, а индекс Доу–Джонса взлетел до небывалых высот. Но развитие происходит крайне неравномерно: рост заработной платы в богатейших кругах шестикратно превышает рост доходов среднего класса; с беднейшими слоями населения разрыв еще больше. Такая динамика сохраняется десятилетиями, но ее усугубил финансовый кризис и политическая стратегия, направленная на поддержку финансовых рынков, где держат активы богатейшие слои населения. Вот почему многие американцы (да и граждане других стран) чувствуют, что обмануты теми же структурами, которые в XX столетии обеспечивали прогресс и процветание. Это отчетливо видно по результатам масштабного социологического исследования, проведенного Исследовательским центром

Pew Research, согласно которым уровень доверия американцев к правительству достиг исторического минимума (около 20 процентов в мае
[42] 2017 года) [3]. Другой опрос, проведенный Международным исследовательским центром Гэллапа, показал, что лишь 12 процентов граждан США доверяли Конгрессу в 2017 году, что значительно ниже 40 процентов, зафиксированных в 1979-м. Прессе доверяют 27 процентов американцев, тогда как 38 лет назад ей доверял 51 процент. Доверие к крупным компаниям испытывает 21 процент граждан по сравнению с 32 процентами в 1979 году [4].

Сейчас, когда мы пишем эту книгу, даже вполне лояльные республиканцы задаются вопросом, как Дональд Трамп вообще мог стать президентом и почему столько людей попалось на удочку откровенной дезинформации и теории заговора. Трамп — отъявленный лжец; он лжет даже тогда, когда все факты, опровергающие его слова, налицо. Но есть проблемы и посерьезнее: в мире, где скомпрометировано само понятие доверия, где уже не работают правительственные структуры, а компании, которые раньше гарантировали пожизненное трудоустройство, теперь переносят рабочие места за рубеж или отдают их роботам, ложь Трампа кажется пустяком по сравнению с систематическим обманом избирателей. Некогда надежные информационные агентства теперь вынуждены конкурировать с сомнительными интернет-источниками, причем и тех и других регулярно обвиняют в распространении «фейковых новостей». Запасы общественного доверия к официальным инстанциям истощаются, и без урегулирования этой ситуации наша демократия падет жертвой политиков и СМИ, которые говорят им ровно то, что те хотят услышать.

Доверие — в особенности к общественным институтам — ценнейший социальный ресурс, настоящая смазка человеческого взаимодействия. Когда этот механизм работает, мы принимаем его как должное — терпеливо ждем в очереди, соблюдаем правила дорожного движения, полагая, что и остальные делают то же самое. Доверие, которое стоит за нашим контактом с окружающими, даже не фиксируется в нашем сознании. Но когда доверия нет, мир в буквальном смысле начинает рушиться. Сегодня это особенно заметно на примере таких стран, как Венесуэла, где население утратило веру в правительство и выпускаемые им деньги, что привело к гиперинфляции, дефициту товаров, голоду, насилию, вооруженным протестам и полному социальному хаосу.

Но похожие тенденции, хоть и завуалированные, можно наблюдать и в западном мире. В то время как правительства и центробанки пытаются привлечь инвестиции и создать рабочие места, печатая деньги или наделяя новыми привилегиями смежные структуры, граждане начинают выражать недоверие государству. В результате этих процессов США получили Дональда Трампа, а Великобритания — Brexit. Еще одним последствием стала экономическая дисфункция. Когда люди не доверяют экономической системе, они предпочитают не рисковать — то есть не тратить деньги. От этого страдает экономический рост и развитие.

Проблема доверия неразрывно связана с реестрами и ведением учетных записей. Чтобы понять эту связь, обратимся к малоизвестной истории одного монаха-францисканца. Будучи страстным любителем математики, он разработал систему, которая помогла Европе выйти из тьмы Средневековья в гораздо большей степени, чем банкиры Медичи, финансировавшие рост европейских держав. От этой истории можно протянуть нить к Lehman Brothers и рассмотреть, как более эффективные системы учета — такие как блокчейн — помогают обществу в кризисной ситуации.

Истина, доверие и реестры

Как так получилось, что компания заработала 4,2 миллиарда долларов в один год и обанкротилась на следующий? Дело не только в подтасовке отчетности, которой занимался банк Lehman Brothers, но и в злоупотреблении доверием акционеров, регуляторов и широкой общественности. Если говорить об отчетности, то руководство банка прибегло к бесчисленным уловкам, чтобы «навести красоту» в книгах и ведомостях — ключевых финансовых документах, на которые полагаются инвесторы и прочие заинтересованные лица, чтобы оценить возможные риски. Например, в конце квартала бухгалтеры Lehman Brothers убирали миллиарды долларов долга из балансового отчета и прятали их на временных счетах для сделок РЕПО (предназначенных для краткосрочных займов, а вовсе не для сокрытия долгов) [5]. В результате отчеты показывали более низкий уровень финансовой зависимости,

чем на самом деле. По окончании отчетного периода долги снова вписывали в книги. В сущности, банк вел два вида документации: одну для
[44] публики, а вторую — для внутреннего пользования. Большинство принимало публичную бухгалтерию (банковскую версию «правды») на веру. Мошенничество обнаружилось в сентябре 2008 года. Однако корень проблемы — в слепом доверии общественности к банку. И это проблема *веры* — в буквальном смысле слова, — насчитывающая уже много веков.

Двойная бухгалтерия распространилась в Европе к концу XV столетия [6]. Большинство историков сходятся во мнении, что она подготовила почву для расцвета Ренессанса и зарождения современного капитализма. Что менее понятно, так это *почему* так получилось. Как нечто столь обыденное и скучное, как бухгалтерская книга, могло произвести культурную революцию в Европе?

За прошедшие почти семь столетий мы стали отождествлять (в коллективном бессознательном) финансовые отчеты с самой истиной. Например, если мы сомневаемся в благонадежности соискателя, то первым делом заглядываем в выписку с его счета — в персональный баланс. Когда компания хочет привлечь капитал из широких источников, она должна предоставить потенциальным инвесторам доступ к своей отчетности. Чтобы удержаться на рынке, ей нужны бухгалтеры, которые будут регулярно заверять эту отчетность. Прозрачная, тщательно заполненная документация — это святыня бизнеса.

Восхождение конторской книги до статуса носителя истины заняло несколько веков и началось с откровенной враждебности, высказываемой европейскими христианами ростовщикам до появления системы двойной записи. В древних цивилизациях к займам относились вполне уважительно. Общий тон задали вавилоняне: в Кодексе Хаммурапи прописаны правила выдачи и возврата ссуд, а также меры, которые полагалось применять к должникам. Однако в иудеохристианской традиции ростовщичество объявлялось грехом. «Не отдавай в рост брату твоему ни серебра, ни хлеба, ни чего-либо другого, что можно отдавать в рост» (Второзаконие 23:19-20), — гласит Священное Писание. «Взятки берут у тебя, чтобы проливать кровь; ты берешь рост и лихву и насилием вымогаешь корысть у ближнего твоего, а Меня забыл, говорит Господь Бог», — сказано в книге Иезекииля. Благодаря распространению христианской религии неприятие

ростовщичества вплелось в ткань европейской культуры на добрую тысячу лет, что совпало с «Темными веками» — периодом, когда Европа утратила не только величие Древней Греции и Рима, но и растеряла почти все познания в математике. Наукой счисления в те времена пользовались разве что монахи, которым нужно было как-то определять точную дату Пасхи. [45]

Только в XII веке, с началом Крестовых походов и торговли со странами Востока, европейцы познакомились с математическими системами, разработанными в арабском мире и Азии [7]. В XIII столетии итальянский купец по прозвищу Фибоначчи посетил Египет, Сирию, Грецию и Сицилию, где собрал множество трудов по математике. Его Liber Abaci («Книга абака») — полный сборник арифметических и алгебраических сведений того времени — содержит и задачи на коммерческую арифметику [8]. Фибоначчи показал, как применить новую науку, например, к обмену валют и подсчету прибыли. До Фибоначчи европейские купцы просто не умели высчитывать то, что нам кажется элементарным; он научил их составлять пропорции, объяснил, как, скажем, разделить тюк сена на равные доли и назначить за каждую справедливую цену. Фибоначчи научил их делить прибыль от сделки. Математика дала купцам точный инструмент для ведения дел, каким они не располагали ранее.

Новая счетная система Фибоначчи произвела фурор в купеческом сословии и на протяжении веков оставалась главным источником математических знаний в Европе. Примерно в то же время европейцы сделали еще одно очень важное открытие: познакомились с двойной системой записи в учетном реестре, которой арабские купцы пользовались с VII века. Купцы из Флоренции и других итальянских городов стали применять этот принцип учета в повседневных сделках. Фибоначчи подарил им новые методы счисления, а двойная система позволила записывать полученные результаты. Наконец наступил исторически важный момент: в 1494 году, спустя два года после того, как Колумб впервые ступил на землю Америки, монах-францисканец по имени Лука Пачоли написал первое руководство по ведению бухгалтерских книг.

Его труд под названием Summa de arithmetica, geometria, proportioni et proportionalita («Сумма арифметики, геометрии, отношений и пропорций»), написанный не на латыни, а по-итальянски, чтобы быть

более доступным общественности, стал первой научно-популярной книгой по математике и бухучету [9]. Раздел, посвященный бухгалтерскому делу, оказался настолько востребованным, что издатель в итоге напечатал его отдельным томом. Пачоли познакомил публику с точнейшими математическими инструментами. «Без системы двойной записи торговый человек не смог бы спать спокойно по ночам», — писал он, объединяя практику с теорией [10]. Его книга надолго стала самоучителем ремесла для европейских торговцев.

Очень важно, что системой бухгалтерского учета заинтересовался священнослужитель. Труды Пачоли помогли преодолеть давнее отвращение христиан к ростовщичеству. Торговцам нужно было доказать церкви, что их ремесло не греховно, а служит на благо роду человеческому. По словам историка Джеймса Ахо, «в Средние века сама мысль о том, что можно жаждать прибыли и при этом быть христианином, казалась возмутительной» [11]. Система двойной записи совершенно непреднамеренно помогла обойти этот культурный запрет. Как? Ответ можно найти в Откровении св. Иоанна — христианской версии конца света и Страшного суда, — где сказано:

> И увидел я мертвых, малых и великих, стоящих перед Богом, и книги раскрыты были, и иная книга раскрыта, которая есть книга жизни; и судимы были мертвые по написанному в книгах, сообразно с делами своими (Откр. 20:12).

Что это означает? Мертвые встают перед Богом и открывают свои книги. Затем Господь открывает *свою* книгу — «иную книгу», вторую. Что это, как не система двойной записи? «И кто не был записан в книге жизни, тот был брошен в озеро огненное». Благодаря простому методу учета торговцам наконец удалось то, что было невозможно почти тысячу лет: сделать кредитование приемлемым и почтенным ремеслом. Как пишет Джеймс Ахо, «система двойной записи способствовала появлению новой "видимой фигуры" — христианского торговца и банкира» [12].

В трудах Пачоли проводится осознанная, намеренная параллель между Священным Писанием и конторской книгой. Первый же пункт руководства по применению нового метода гласит: «Торговцу должно при каждой записи ставить дату с годом от Рождества Христова, дабы

она напоминала ему о чистоте помыслов и любую сделку он совершал бы со святым именем Господним на устах» [13].

Едва банковское дело избавилось от стигмы безбожия, нашлось немало желающих им заняться. Первыми знаменитыми банкирами стали члены флорентийского семейства Медичи: им удалось занять нишу посредников, через которых проходили почти все денежные потоки в Европе. Столь ошеломительный успех стал возможен благодаря скрупулезному ведению двойной записи. Если торговец из Рима желал что-то продать покупателю в Венеции, новый тип конторских книг решал проблему доверия между людьми, живущими далеко друг от друга. Занося одни и те же суммы в дебет плательщика и в кредит получателя, — то есть ведя двойную запись, — банкиры могли переводить средства без отправки наличных денег. В результате они в корне изменили систему платежей, подготовив почву для зарождения капитализма. Что не менее важно, банкиры создали для себя авторитетную роль — поручителей, носителей капитала доверия в обществе — и занимают эту позицию уже около 500 лет.

Таким образом, ценность двойной записи не только в сухой эффективности. Конторская книга со временем начала восприниматься как моральный ориентир, обращение к которому наделяло всех участников сделки праведной силой. Торговец становился благочестивым, а банкиру приписывалась святость — в конце концов, три папы римских в XVI и XVII веках происходили из рода Медичи. Перекупщик славил Господа своими трудами. Негоцианты, прежде вызывавшие подозрение, превращались в моральные авторитеты, столпы общества. Джеймс Ахо отмечает: «Основатель методистской церкви Джон Уэсли, баптисты Даниель Дефо и Сэмюэл Пепис, деист Бенджамин Франклин, многие нынешние сообщества экуменистов и адвентистов — все настаивают на том, что скрупулезный учет финансов есть проявление высших добродетелей: честности, ответственности, порядочности и трудолюбия».

Благодаря математическим концепциям, завезенным со Среднего Востока в ходе Крестовых походов, система двойной записи создала моральные предпосылки для зарождения капитализма в Европе, а банковские «крючкотворы» фактически стали жрецами новой религии. Мало кто в наши дни воспринимает текст Библии как буквальную, дословную истину (хотя, конечно, есть и такие),

тем не менее это не помешало уверовать в истинность отчетов Lehman Brothers — пока не обнаружился разрыв между видимостью
[48] и реальностью.

Величайшая ирония кризиса 2008 года состояла в том, что вера в систему финансовой отчетности (так глубоко укорененная в коллективном бессознательном, что мы ее даже не замечаем) сделала нас легкой добычей для мошенников. Даже вполне добросовестно составленная отчетность иногда базируется на более или менее обоснованных догадках. Современная бухгалтерия, особенно в больших международных банках, превратилась в настолько сложный и запутанный процесс, что стала практически бесполезна. В 2014 году колумнист Bloomberg Мэтт Левин весьма наглядно показал, что балансовая ведомость любого банка почти абсолютно непрозрачна. По замечанию Левина, «ценность» большинства отображенных в ней активов определяется на основе ожидаемой возвратности ссуд или рыночной стоимости облигаций, которыми владеет банк. На другой чаше весов оказываются столь же приблизительно оцененные пассивы и обязательства. Если разница между предположительной оценкой и реальной стоимостью составит хотя бы один процент, квартальная прибыль может превратиться в убыток. Угадывать, приносит ли банк прибыль, — все равно что решать школьный тест «методом тыка». «В этом тесте вообще нет правильных ответов, — пишет Левин. — Никто не может знать, заработал ли Банк Америки что-то в текущем квартале или потерял. Банковская отчетность, по сути, серия более или менее разумных предположений» [14]. Не угадаешь — вылетишь из бизнеса, что и произошло с Lehman и другими проблемными банками.

Мы отнюдь не стремимся опорочить нынешнюю систему учета или сами банки, поскольку на поверку система двойной записи принесла больше пользы, чем вреда. Наша истинная цель — вскрыть глубокие культурно-исторические корни общественного доверия к такой форме учета. Сейчас, после катастрофы, перед нами стоит вопрос: поможет ли технология, которая позволяет вести учет на других основаниях, вернуть доверие к экономической системе? Может ли блокчейн, который постоянно открыт для публичной проверки и подтверждается не одним банком, а серией математически защищенных операций, производимых множеством компьютеров, возродить наш утраченный социальный капитал?

Божий протокол

В 2008 году, когда мир утопал в пучине финансового кризиса, мало кто заметил статью за подписью некоего Сатоши Накамото, опубликованную 31 октября. В ней описывалось нечто под названием «биткоин» — система электронной наличности, не требующая государственного обеспечения [15], в основе которой лежал открытый реестр, доступный любому для просмотра, но не для изменений. Фактически он представлял собой объективную цифровую запись реального положения дел. Несколько лет спустя этот реестр назовут блокчейном.

Накамото объединил в концепции биткоина несколько элементов, но, как Фибоначчи и Пачоли в свое время, был не единственным, кто стремился оптимизировать систему учета с помощью новых знаний и технологий. В 2005 году Йен Григг, компьютерный эксперт из компании Systemics, представил пробную версию системы под названием «тройная запись» [16]. Григг работал в области криптографии — науки, восходящей к тем давним временам, когда впервые появились шифрованные послания, или тайнопись. С тех пор как вычислительная машина Алана Тьюринга взломала код немецкого шифратора «Энигма», криптография во многом определяет ход нашей цифровой революции. Без криптографии мы не смогли бы обмениваться конфиденциальной информацией через интернет — например, совершая платежи и покупки онлайн, — не опасаясь, что она попадет в чужие руки. При взрывном росте вычислительных мощностей соответственно усилилась и роль криптографии в нашей жизни. Йен Григг, со своей стороны, полагал, что следующей ступенью станет программируемая система ведения учета, которая сделает мошенничество технически невозможным. В сущности, он предлагал добавить к традиционной системе двойной записи третий компонент — независимый общедоступный реестр, криптографически защищенный от любых изменений. По мнению Григга, это позволяло полностью исключить вероятность подтасовки.

Предполагалось, что в новой системе пользователь будет вести обычную двойную запись, но к цифровому реестру добавится еще одна функция, своего рода штамп времени: криптографически защищенное, подписанное подтверждение каждой транзакции.

[50]

(«Подпись» в криптографии — гораздо более сложное и наукоемкое понятие, чем в повседневной жизни. Оно предполагает совмещение двух цифровых последовательностей, или «ключей», — общедоступного и известного лишь владельцу. Их полное совпадение математически доказывает, что поставившее подпись лицо обладает на нее эксклюзивным правом.) Григг представлял себе систему тройной записи как специальную компьютерную программу, включенную в ПО компании или организации. Однако третий реестр, содержащий последовательность всех подписанных операций, будет открыт для верификации в режиме реального времени. Любое расхождение с подтвержденными записями укажет на подделку. Представьте себе мошенника вроде Берни Мэдоффа, который просто выдумывал транзакции и отображал их в фиктивных ведомостях, — и поймете ценность системы, позволяющей проверять счета в режиме реального времени.

Еще раньше, в 1990-х, другой изобретатель также подметил богатый потенциал цифрового реестра. Это был Ник Сабо — один из первых шифропанков* и автор ряда концептов, которые впоследствии легли в основу архитектуры биткоина, что стало причиной появления версии, будто за псевдонимом Сатоши Накамото скрывается именно он. Его протокол по сути представляет собой таблицу, которая запускается на «виртуальной машине» — то есть сети объединенных компьютеров, доступной множеству пользователей. Сабо разработал сложную систему открытых и зашифрованных данных, которая должна защищать конфиденциальность пользователей, но в то же время предоставлять достаточно информации, чтобы создать верифицируемую историю операций. Хотя системе Сабо — он назвал ее «божьим протоколом» — уже более двадцати лет [17], она на удивление близка к платформам и протоколам блокчейна, о которых пойдет речь в следующих главах. Сабо, Григг и другие разработчики первыми опробовали метод, который, возможно, приведет к появлению неизменяемых записей, исключающих вмешательство мошенников вроде Мэдоффа или недобросовестных банкиров. Хочется надеяться, что новый метод поможет восстановить общественное доверие к системам, используемым нами для взаимодействия.

* О культуре шифропанка и ее роли в становлении криптовалют подробно рассказывается в книге «Эпоха криптовалют».

«Большая математика», открытость и новый инструмент консенсуса

Если отдельные группы хотят производить между собой обмен и создавать эффективно функционирующие общества, они должны прийти к общеприемлемому представлению о реальности. В цифровом мире XXI столетия, когда многие сообщества формируются виртуально, вне государственных границ и местных юрисдикций, старые институты и критерии, которыми мы пользовались для установления истины, уже не выполняют своих функций. По мнению сторонников блокчейна, процесс выяснения истины лучше всего организовать на основе распределенной записи, без централизованного контроля, что сделает данные неуязвимыми для взлома, подкупа, ошибки или стихийного бедствия.

Кроме того, результаты записи должны синхронизироваться с помощью сложных криптографических операций, которые предотвратят их перезапись в дальнейшем. Вот каким образом криптография выполняет свои задачи: она использует защитные коды, сгенерированные из настолько большого набора возможных чисел, что это выходит за рамки человеческого воображения. Само количество вариантов исключает взлом кода методом угадывания, то есть подбора цифр, из-за чрезмерной трудоемкости процесса. На данный момент биткоин — самая мощная вычислительная сеть в мире: общая «мощность хеширования» к августу 2017 года позволила ее компьютерам коллективно осуществлять более семи миллионов триллионов операций по подбору номера в секунду. Однако и ей понадобится около 4500 триллионов триллионов триллионов лет на обработку всех последовательностей, которые может сгенерировать криптографическая хеш-функция SHA-256; именно она защищает данные биткоина. Для сравнения: это в 36 264 триллиона триллиона раз больше, чем известный нам возраст Вселенной. Иными словами, криптография биткоина вполне надежна*.

* Важное примечание: если ученые сумеют создать полноценный квантовый компьютер, то и защиту такого уровня можно будет взломать. Однако квантовые машины — пока еще дело далекого будущего. Кроме того, их появление сделает неработоспособными все системы кибербезопасности, а не только протокол биткоина. Тем не менее разработчики криптовалют уже занимаются системами нового поколения, которые теоретически смогут отражать и квантовые атаки.

И все же для работы такой системы честного учета нужно нечто большее, чем криптография. Записанная последовательность транзакций должна быть полностью прозрачной и открытой для публичного контроля. Это означает, что, во-первых, учетный реестр нужно сделать общедоступным, а, во-вторых, управляющий им алгоритм должен работать по принципу *open-source*, чтобы любой клиент мог посмотреть и проверить его исходный код.

В то же время система должна гарантировать защиту конфиденциальных данных, иначе никто не станет доверять ей личную информацию или важные коммерческие тайны, если к ним любой сможет получить доступ. Биткоин пока решает эту проблему, отображая лишь одноразовые буквенно-цифровые «адреса», которые в произвольном порядке назначаются пользователям при получении криптовалюты и ничего не говорят об идентичности своих владельцев. Но все же это не полностью анонимная система — ее лучше описать как «псевдонимную». В ней заложена возможность проследить цепочку транзакций между адресами и отыскать точку, в которой пользователь может быть идентифицирован, — например, при обналичивании средств и переводе их в доллары через обменный сервис или биржу криптовалют. Там ведется запись имен, адресов и прочих данных каждого клиента. Для отдельных криптографов, слишком серьезно относящихся к вопросам конфиденциальности, подобная система недостаточно надежна, поэтому они разрабатывают альтернативные криптовалюты, такие как Zcash, Monero, Dash, имеющие уровень защиты выше, чем у биткоина. Эти системы хранят в реестрах достаточно информации, чтобы компьютеры-валидаторы могли убедиться, что со счетами не производилось незаконных действий, но при этом идентичность пользователей скрывается еще тщательнее.

Можно спорить о необходимости столь радикальных мер по защите конфиденциальности, но в целом вышеописанная модель нового реестра — распределенного, защищенного криптографически, публичного и в то же время приватного — способна решить проблему утраченного доверия к официальным системам записи и снова побудить граждан к экономическому обмену и предпринимательской деятельности.

«Для функционирования общества нужен консенсус относительно фактов», — утверждает Томика Тилльман, директор

вашингтонского фонда «Новая Америка» и председатель Глобального совета предпринимателей по блокчейн-технологиям. «Нам необходима общая реальность, которую признает каждый. Как и во всех развитых странах, у нас есть институты, которые отвечают за установление и подтверждение фактов, но сейчас эти институты находятся под угрозой исчезновения. ...Блокчейн дает нам шанс остановить их распад и создать новое поле взаимодействия, где все мы сможем выверить и подтвердить ключевой набор фактов, обеспечив при этом конфиденциальность сведений, которые не должны быть общедоступны» [18].

Биткоин показал, как эта идея работает в одном особенно важном контексте — финансовом. Новый инструмент подтверждения «фактов» взаимодействия позволил совершенно незнакомым людям использовать независимую валюту для оплаты через интернет и при этом твердо знать, что мошенничество невозможно — даже в отсутствие контролирующей структуры вроде Федерального резерва.

Впрочем, куда важнее само сознание того, что некая группа людей может достичь консенсуса по поводу фактов без помощи централизованных посредников. По утверждению израильского историка Юваль Ноя Харари, власть и сила социальных институтов коренится в человеческой способности творить особо значимые истории о религии, нации, общей валюте и т. п., в которые верят все [19]. В свете этого знания консенсус относительно фактов обретает повышенную важность. История человеческой цивилизации основана не на безусловной истине, поскольку все, даже научное знание, подлежит пересмотру, а на еще более мощном понятии правды: *консенсусе*, общем представлении об истине, социальном договоре, который позволяет нам преодолеть подозрения, добиться взаимного доверия и вступить во взаимодействие. Поэтому разумнее воспринимать блокчейн не как «заменитель» доверия (систему, где оно просто не требуется, по утверждению наиболее фанатичных сторонников криптовалюты), а как инструмент для создания общих историй, необходимых для выхода на новый уровень доверия, накопления социального капитала и построения лучшего мира.

Столь вдохновляющая перспектива помогает объяснить бурный энтузиазм — иногда чрезмерный или неоправданный — относительно блокчейна как решения для... практически всего. По мере того как

специалисты из самых разных сфер исследуют его потенциал для децентрализации своих отраслей и высвобождения капитала, им становится ясно, что блокчейн — не просто «кузница денег». Если он способен порождать консенсус, как показывает пример с биткоином, то уместнее будет рассматривать его как машину правды.

Глава

2

«Управление» цифровой экономикой

Однажды сентябрьским вечером 2011 года предприниматель по имени Питер Симс получил сообщение от своей приятельницы Джулии Эллисон, которая спрашивала, не находится ли он случайно в джипе компании Uber на углу 33-й улицы и Пятой авеню в Нью-Йорке. Симс действительно был там, поэтому решил, что знакомая увидела его из окна другой машины [1].

На самом деле Эллисон была даже не в штате Нью-Йорк, а на корпоративной вечеринке в Чикаго в честь прихода компании Uber в «город ветров». Команда Uber показывала гостям один из своих самых популярных трюков: интерактивную карту «Всевидящее око», где отображалось местонахождение всех машин вместе с именем каждого пассажира. Компания отслеживала не только перемещение автомобилей, но и передвижение их пассажиров. Когда Эллисон объяснила, откуда ей известно местонахождение приятеля, Симс возмутился и написал об этом у себя в блоге гневный пост.

Затем Uber стала объектом секс-скандала: сотрудницы массово заявляли о домогательствах на рабочем месте, из-за чего для спасения репутации пришлось принимать весьма радикальные меры — вплоть до вынужденной отставки соучредителя Uber Трэвиса Каланика. Однако вопрос конфиденциальности оказался не менее важен. Компания не просто владела информацией о частных поездках, но ее топ-менеджеры — по крайней мере, в первые годы работы — охотно этим злоупотребляли. В ноябре 2014 года компания Uber начала расследование

действий генерального менеджера нью-йоркского офиса Джоша Морера [2] в связи с утверждением журналистки BuzzFeed Джоаны Буйан, что он использовал «Всевидящее око» для отслеживания ее передвижений. Этот скандал и другие жалобы на нарушение конфиденциальности в итоге вынудили Uber подписать соглашение с генеральным прокурором Нью-Йорка Эриком Шнайдером об обязательном кодировании имен пассажиров и геолокационных данных [3].

Безусловно, то, что перевозчики вроде Uber и его главного конкурента Lyft сегодня стали частью нашей повседневной жизни, — неоспоримый факт. Когда название вашей компании становится именем нарицательным, начинает склоняться и образовывать однокоренные слова («пользоваться ксероксом», «спросить у гугла», «ехать на убере»), — знайте, что вы преуспели. Но, несмотря на устойчивую ассоциацию бренда с демократичными тарифами, вольным союзом водителей и пассажиров, которые просто «выручают друг друга», Uber — централизованная структура, вовсе не стремящаяся избавить нас от посредничества. Компания отслеживает и контролирует каждую сделку, заключенную между водителем и пассажиром, и берет себе 25 процентов. И она далеко не единственная зарабатывает подобным образом. То, как Uber, Facebook, Google и прочие техногиганты XXI века обращаются с нашими данными, уже пора признать насущной проблемой.

У интернета, если вы не в курсе, есть хозяева — группа ведущих компаний, а именно Google, Amazon, Facebook и Apple (их часто обозначают аббревиатурой GAFA), которые фактически контролируют все. Мы доверили им роль посредников при переписке и общении в соцсетях, поиске и хранении информации и т. п. В общем они неплохо справляются с работой, однако их посредничество обходится нам весьма недешево, ведь мы даем им в руки почти неограниченную власть. Мы — широкая публика — в буквальном смысле создаем стоимость этих компаний, производя для них контент и предоставляя ценную информацию. (Заметьте, бесплатно!) Да, взамен мы получаем услуги, но неравенство в наших отношениях бросается в глаза. Особенно это очевидно в политической сфере.

Как выяснилось после президентских выборов в США 2016 года, Facebook и Google контролируют нашу новостную ленту. Вспомним тайный алгоритм Facebook, который подбирает топ новостей исходя из ваших политических взглядов, создавая целый «хор»

из возмущенных или обрадованных единомышленников, готовых потреблять и делиться сомнительной информацией, которая вписывается в уже сложившуюся у них картину мира. Вот почему во время предвыборной кампании, например, группа подростков из Македонии умудрилась опубликовать фейковые статьи, где говорилось, что Трампа поддерживает папа римский [4]. Эти «новости» собрали больше лайков, репостов и рекламных денег, чем настоящие аналитические материалы, опубликованные солидными, коммерчески успешными изданиями.

И дело даже не в том, что Facebook и Google стали гигантскими социальными платформами. Эти исполины цифровой эпохи обладают беспрецедентной полнотой власти над потоками социально значимой информации, проходящей через интернет. «Бесплатный контент», который они нам якобы предоставляют, — не более чем миф. Конечно, мы не платим за сервисы Google и Facebook, но при этом вручаем им неимоверно ценную валюту — наши персональные данные, обладание которыми превратило эти корпорации в монополии и сделало властелинами цифровой вселенной. Безусловно, это уже не новость; мы просто хотим проиллюстрировать, как безграничная власть над информацией в интернете обостряет проблему его централизованной архитектуры и связанного с ней дефицита доверия [5].

Мечта хакера

Помимо всего прочего, 2016 год запомнился судебными баталиями между Apple и ФБР [6], которое требовало от производителей смартфонов предоставить правоохранительным органам доступ к зашифрованным данным покупателей. В итоге мы, потребители, оказались между молотом и наковальней. Если мы хотим жить в условиях цифровой экономики, то нам придется либо предоставить свои данные частным компаниям и смириться с риском правонарушений, либо позволить властям контролировать эти компании и подвергнуться злоупотреблениям вроде вскрытых Эдвардом Сноуденом в АНБ. На самом деле необязательно выбирать между двумя крайностями — есть и третье решение, но оно предполагает изменение самого принципа размещения данных в сети.

Идеи, положенные в основу биткоина и технологии блокчейн, предлагают новый подход к решению этой проблемы. Ведь вопрос о том, кто контролирует наши данные, должен проистекать из другого фундаментального вопроса: каким лицам или организациям следует *доверять*, чтобы заниматься торговлей, получать услуги или участвовать в жизни общества? Налицо весомые аргументы в пользу полной реорганизации мировой системы информационной безопасности. И для начала необходимо понять, при каких условиях интернет-пользователи могут непосредственно доверять друг другу, чтобы избежать вливания целых потоков информации в централизованные хранилища, без которых сейчас не обходится взаимодействие в сети. Решение проблем безопасности данных, вероятно, потребует сознательного перехода от так называемой *централизованной модели доверия* к *децентрализованной модели.*

В эпоху, когда цифровые технологии вроде бы должны снижать стоимость входа в экономическую систему, устаревшая модель централизованного доверительного управления становится барьером в силу своей дороговизны (подумайте о двух миллиардах человек, которым недоступны банковские услуги). К тому же она чудовищно неэффективна. Так, по оценкам консалтинговой компании Gartner, в 2015 году на кибербезопасность в мире было потрачено около 75 миллиардов долларов [7]. Невзирая на это, как утверждает Инга Бил, CEO* британской страховой компании Lloyd's, общие убытки от интернет-мошенничества за год составили порядка 400 миллиардов долларов [8]. Если вас — вполне оправданно — пугает эта цифра, вот вам еще одна: 2,1 триллиона долларов. Таков предполагаемый убыток от мошенничества в 2019 году, подсчитанный исследовательской группой Juniper Research на основе нынешних тенденций [9]. Для наглядности: это более чем 2,5 процента мирового ВВП в 2019 году (при нынешних темпах роста экономики) [10]. Впрочем, приведенные цифры отражают не только суммы, украденные хакерами, но и издержки на судебные процессы, обновление систем безопасности и т. п. — общие убытки, которые предприятия несут из-за многочисленных атак и взломов. Но даже с этой оговоркой данные свидетельствуют о том, что хакеры — едва ли не самые финансово успешные инноваторы цифровой эпохи.

* Здесь и далее генеральный директор компании. *Прим. ред.*

Очевидный провал наших попыток защитить мировую коммерцию — прямое следствие нестыковки между централизованными методами хранения и обработки данных и требованиями глобальной экономики совместного потребления, которая поощряет децентрализацию — взаимодействие субъектов и устройств в режиме P2P. Все больше и больше пользователей объединяются в пиринговые социальные сети; все больше устройств — например, «умных» термостатов и холодильников — подключаются к так называемому интернету вещей. Однако это означает и рост числа точек доступа, используемых хакерами для взлома *централизованных* хранилищ данных и кражи их содержимого.

Риски, кроющиеся в расхождении двух тенденций, привели в октябре 2016 года к кибератаке на компанию Dyn — крупного провайдера сетевых услуг, в частности DNS (системы доменного имени) [11]. Атака произошла после того, как один хакер обнаружил, что пользователи небольших устройств, таких как игровые консоли и ноутбуки, нерегулярно загружают патчи безопасности. Следовательно, заразив эти устройства определенным вирусом, их затем можно было использовать как стартовую площадку для атак на интернет-узлы. Когда хакер опубликовал пошаговое руководство, разумеется, нашлись желающие применить его на практике. Завладев множеством устройств с помощью ботнета, злоумышленники провели мощную DDOS-атаку (распределенная атака типа «отказ в обслуживании») на серверы Dyn. Их стратегия заключалась в отправке огромного количества запросов к системе, в результате чего пользователи лишились доступа ко многим страницам и сервисам, включая Twitter, Spotify, Reddit и другие сайты с большим трафиком. Эта DDOS-атака — прямое следствие обсуждаемого нами парадокса. Системами доменных имен управляют все более крупные, централизованные провайдеры-посредники, тогда как небольшие устройства «интернета вещей» попадают в руки неподготовленной широкой публики. Такое сочетание — мечта любого хакера.

А какой объем данных мы с вами приготовили для ненасытных хакеров! По оценкам компании IBM, в 2014 году пользователи интернета ежедневно генерировали 2,5 эксабайта — то есть 2,5 квинтиллиона байтов — информации [12]. Бóльшая ее часть теперь хранится в облаке — облачные технологии сделали хранение настолько

дешевым, что «чистить» ящики и диски уже нет никакого смысла. Давайте напишем эту цифру полностью, со всеми семнадцатью нулями: 2 500 000 000 000 000 000. (Для наглядности можно сказать еще так: это примерно 2,5 триллиона PDF-версий нашей книги.) По словам экспертов IBM, это число означает, что человечество собрало 90 процентов всех данных, накопленных за нашу историю, всего за два года — и большая их часть хранится на серверах у провайдеров облачных сервисов (таких как IBM). [61]

Пожалуй, единственный способ защитить эти данные и понизить интенсивность атак — убрать информацию с централизованных серверов и сформировать распределенную систему хранения. Контроль нужно вернуть владельцам данных, то есть потребителям и конечным пользователям интернет-услуг. Если хакерам понадобится эта информация, им придется красть ее у каждого из нас, что гораздо дороже взлома гигантской базы данных, где все удобно сложено в одном месте. Но чтобы создать новую систему, нужно перейти к децентрализованной модели доверия.

Прежде чем анализировать это решение, давайте определим, почему оно важно для человечества. Дело ведь отнюдь не в долларах и центах. Существует глубинная связь между неприкосновенностью личного пространства, необходимого для полноценной жизни общества, и защитой конфиденциальных данных. Когда защитные механизмы дают сбой (что, увы, не редкость), благополучие граждан оказывается под угрозой. Они могут лишиться сбережений, подвергнуться вымогательству и шантажу; их имя и репутацию может присвоить злоумышленник; интимные моменты, которыми они делились с ближайшим кругом, становятся достоянием общественности. Кража личных данных нередко приводит к депрессии и даже самоубийству потерпевшего [13]. Хуже того, многие эксперты полагают, что вскоре мы столкнемся с киберубийствами. Подключенные к интернету автомобили и другие потенциально опасные устройства могут стать орудием в руках преступников. Возможно, такие убийства уже совершаются; есть предположение, что загадочное исчезновение рейса MH370 Malaysia Airlines — результат хакерской атаки на системы навигации [14]. И это уже не плод больной фантазии конспирологов: технически подобное вмешательство вполне возможно, поэтому, чтобы исключить такие преступления, проблему нужно устранять в зародыше.

Централизованная модель доверия ставит под угрозу не только отдельных граждан, но и крупные организации. В последние го-
[62] ды от кибератак пострадали даже гиганты из списка S&P 500 — J.P. Morgan, Home Depot, Target, Sony, Wendy's. Всем им пришлось потратиться на судебные процессы, компенсации клиентам и серьезное обновление систем безопасности. Страдают как деловые, так и политические структуры. Вспомним утечку данных из Управления кадровой службы США в 2015 году, когда в руки хакеров попали около 18 миллионов записей о персонале [15]. И конечно же, не будем забывать о кибератаке на Национальный комитет Демократической партии США в 2016 году — предполагаемом «русском» взломе, приведшем к тяжелому политическому кризису в первый год правления Дональда Трампа.

Хакерские атаки — серьезная угроза для корпоративного бюджета и вечная головная боль для IT-отдела любой компании. Каждый новый прием, изобретенный кибервзломщиками, требует новых патчей в системе безопасности, которую все равно со временем сумеют обойти. Это означает огромные капиталовложения в программное обеспечение, которое неизбежно потребует обновления и дальнейших затрат. Образно говоря, компания строит все более и более высокую стену (брандмауэр), прекрасно зная, что грабители уже надстраивают лестницы.

Понятно, что нужна новая архитектура безопасности, и принципы, лежащие в основе технологии блокчейн, могут помочь. В распределенной структуре блокчейна участники не зависят от централизованных организаций, которые выстраивают защитную инфраструктуру с помощью брандмауэров. Вместо этого безопасность становится делом каждого. Индивид, а не уполномоченный посредник отвечает за хранение собственных конфиденциальных данных. При этом любая информация, выложенная в открытый доступ, становится объектом консенсуса и проходит коллективную верификацию.

Потенциал такой схемы хорошо виден на примере биткоина. Даже если этот конкретный блокчейн биткоина оказался не идеальным решением для своих задач, стоит отметить, что, несмотря на отсутствие классических, централизованных средств киберзащиты вроде брандмауэра и наличие весьма заманчивой «кубышки» (более 120 миллиардов долларов рыночной капитализации на момент написания книги),

коллективный реестр биткоина пока неуязвим для взломщиков. Исходя из внутренних стандартов целостности реестра, можно сказать, что девятилетний опыт существования биткоина убедительно доказывает жизнеспособность такой модели распределенного доверия между пользователями. По всей вероятности, одной из самых важных нефинансовых областей применения блокчейна может стать сама сфера компьютерной безопасности.

Встроенная безопасность

Одна из причин жизнеспособности биткоина — отсутствие у хакеров цели взлома: им попросту нечего взламывать в этой системе. Общий реестр не содержит информации о пользователях системы. Что еще важнее, у него нет владельцев и контролеров. Нет у него и одной «главной» версии; с каждой подтвержденной транзакцией к блокчейну добавляется очередной блок, в результате чего реестр полностью обновляется и актуальная версия передается всем подключенным устройствам. Поэтому у хакеров нет основного вектора атаки. Если пострадает один из узлов системы и кто-то попытается стереть или переписать транзакции в локальной версии реестра, то остальные устройства — хранители сотен одобренных версий — откажутся принимать обновления от взломанного узла. Несоответствие между множеством «чистых» реестров и одним поддельным автоматически маркирует взломанный блок как фальшивку. Как мы увидим в дальнейшем, существуют блокчейны с разной степенью защиты — включая «частные», или «закрытые», с ограниченным уровнем допуска. В отличие от них биткоин опирается на децентрализованную модель, которая не требует одобрения или поручительства, а делает ставку на заинтересованность участников в сохранности средств на счетах. В любом случае сама природа блокчейн-реестра — общей, взаимно подтвержденной записи, которая хранится на множестве устройств, — подводит нас к идее распределенной безопасности: риск ошибки или взлома исключается за счет многочисленных «подстраховок».

Однако у крупных компаний несколько иная концепция безопасности. В марте 2016 года в ходе симпозиума, проводимого

расчетно-клиринговым агентством Depository Trust & Clearing Corp., или DTCC, аудиторию, состоявшую в основном из банкиров и дру-
[64] гих представителей сферы финансов, попросили ответить, в какой IT-сектор они вложили бы деньги, будь у них 10 миллионов долларов на инвестиции. Опрос проходил в форме голосования с выбором из нескольких вариантов ответа. Большинство проголосовало за «кибербезопасность»; на втором месте оказалась технология блокчейн. На трибуне в это время находился Адам Лудвин, CEO компании Chain, которая специализируется на услугах по ведению распределенных реестров [16]. Увидев результаты опроса, он незамедлительно упрекнул корпорации с Уолл-стрит в недальновидности и недооценке перспектив, открываемых новой технологией. По словам Лудвина (а среди его клиентов числятся такие гиганты, как Visa и Nasdaq), нетрудно понять, почему участники симпозиума сочли вопросы кибербезопасности приоритетными, ведь в зале сидели люди, чья главная обязанность — постоянно беспокоиться о возможном взломе и утечке данных. Однако, судя по итогам голосования, они пока не осознали, что блокчейн предлагает решение этой проблемы. «В отличие от других видов программного обеспечения, для которых кибербезопасность — внешняя надстройка, блокчейн-системы обеспечивают безопасность в силу собственной архитектуры», — сказал он.

Для приватных блокчейнов, которыми обычно интересуются крупные корпорации — распределенных реестров, где все компьютеры должны пройти авторизацию, чтобы подключиться к сети, — понятие «встроенной безопасности» означает лишь распределение базы данных между несколькими хранилищами вместо одного. Преимущество такой структуры — в создании множества запасных копий, или бекапов, благодаря которым сеть будет работать, даже если один узел подвергнется атаке. Более радикальное решение — открытые, общедоступные реестры, как у биткоина или эфириума, где нет регулирующего органа, отслеживающего, кто пользуется системой. В этом случае суть самого понятия «безопасности» полностью меняется. Оно уже не предполагает наличия стены — брандмауэра — вокруг единого хранилища ценной информации, управляемой доверенной третьей стороной. Скорее, акцент делается на передаче контроля «на окраины», то есть самим пользователям, и ограничении объема

идентифицирующей информации в открытом доступе. И наконец, взлом подобной сети нужно сделать настолько дорогим, чтобы у злоумышленников отпало желание даже пытаться.

На первый взгляд удивительно, что сеть анонимных пользователей оказалась неуязвимой для взлома. Но факт есть факт: система вознаграждений и затрат, встроенная в ПО для генерации криптовалюты, действительно надежна. Основной реестр биткоина не удалось взломать еще никому. Безусловно, будет нелегко убедить организации, которые до сих пор занимались защитой наших данных, передать эстафету децентрализованной сети, где нет единого правления (и не с кем судиться в случае провала). Но именно это, возможно, станет главным шагом к улучшению защитных систем. Безопасность должна зависеть не от сложного кодирования и прочих внешних механизмов, а от экономических факторов, то есть кибератаки должны утратить целесообразность из-за непомерной цены.

Давайте сравним нынешнюю модель защиты данных — назовем ее «общим секретом» — и новую модель «идентичности устройств», предлагаемую блокчейном [17]. Сегодня провайдер услуг и клиент договариваются о секретном пароле и каком-нибудь проверочном вопросе («Назовите девичью фамилию матери»). После этого жизненно важная информация, которая иногда стоит миллионы долларов, отправляется в хранилище данных на сервере провайдера, где ее могут добыть взломщики. В открытом блокчейне клиент сохраняет контроль над данными, а это значит, что точка уязвимости находится на его устройстве. Вместо серверов Visa, содержащих информацию, которая необходима миллионам держателей карт для доступа к платежной системе, правом доступа к сети управляете вы сами — с телефона или компьютера. Теоретически хакер может нацелиться на отдельное устройство и попробовать взломать личный «ключ», используемый для совершения транзакций в децентрализованной сети, и, если повезет, даже украсть несколько тысяч долларов в криптовалюте. Но это гораздо менее прибыльно и более трудозатратно, чем взлом центрального сервера.

Слабым звеном — а такое всегда найдется, это аксиома кибербезопасности — теперь становится само устройство. Ответственность за его защиту ложится на плечи пользователя. Очевидно, широкой публике нужно будет освоить азы криптографии, а также работу

с персональными ключами. Оптимизация криптовалюты потребует от нас взять защиту данных в собственные руки.

[66] Тем не менее, несмотря на новые задачи в плане защиты устройств, мы надеемся на резкое сокращение количества кибератак. Ведь потенциальная выгода от каждой атаки станет гораздо меньше. Вместо получения доступа к миллионам счетов сразу хакеры будут вынуждены взламывать каждое устройство по отдельности ради относительно небольшой добычи. В данном случае безопасность обеспечивается за счет нерентабельности взлома. Защита встроена в саму систему, а не прилагается к ней в качестве «заплатки».

Нам кажется, что от перехода к модели распределенного доверия цифровая экономика существенно выиграет — будь то просто новая система бекапов или более радикальная концепция открытого блокчейна, защищенного нецелесообразностью атак. Стоит освоить общие принципы, и на ум сразу приходят новые модели управления информацией, которые возвращают контроль создателям данных и обеспечивают им гораздо более высокий уровень защиты.

Здравоохранение — одна из сфер, где такое решение придется весьма кстати. В наши дни конфиденциальные истории болезни хранятся в разрозненных (и уязвимых) базах клиник, лабораторий и страховых компаний. Все эти учреждения связаны строгими законами о врачебной тайне, которые, безусловно, прописывались с благими намерениями, однако в рамках полученной системы медики несут суровое наказание при любой утечке данных. Разумеется, они бы с радостью сбросили с себя бремя такой ответственности.

В последнее время кибератаки в медицинской сфере участились. В 2016 году хакеры взломали базу данных страховой компании Anthem Health и обнародовали 78 миллионов историй болезни [18]. При массовом заражении компьютеров «вирусом-вымогателем» WannaCry электронные карты пациентов во многих клиниках оказались закодированы, и хакеры потребовали выкуп в биткоинах за их разблокировку [19]. Разумеется, больницы неслучайно стали мишенью взломщиков, ведь их данные жизненно важны в самом буквальном смысле слова.

Больше всего от недостатков системы страдают пациенты. Нынешняя структура часто обрекает их на лишние расходы и опасные проволочки. Все мы слышали жуткие истории о том, как пациенты умирают в реанимации из-за невозможности бригадой скорой помощи

оперативно добыть их историю болезни у лечащего врача. Отказы в допуске к данным часто замедляют разработку новых лекарств. В американской системе хранения медицинских данных разладилось практически все.

Вот почему у таких инициатив, как проект MedRec — программа с открытым исходным кодом, основанная на блокчейне криптовалюты эфириум, разработанная студентами Массачусетского технологического института Ариэлем Экблау, Асафом Азариа и Тинго Йейра [20], — мощный потенциал. Главная идея проекта состоит в том, что пациент сам решает, кому предоставлять доступ к его истории болезни. Над аналогичными решениями работают и некоторые медицинские стартапы, например компания Gem в Лос-Анджелесе и Blockchain Health в Сан-Франциско. Данные по-прежнему будут храниться на сервере провайдера, но пациент будет использовать личные криптографические ключи (такие как при авторизации платежей в системе биткоина), благодаря чему сможет сам установить параметры доступа к необходимой информации.

Децентрализованная экономика с централизованным доверием

Увидим ли мы когда-нибудь мир «распределенного доверия», где можно смело и практически без затрат совершать сделки и операции в режиме онлайн? Что для этого нужно сделать? Чтобы ответить на этот вопрос, давайте вспомним, как мы дошли от мечты о демократичном интернете равных возможностей (ведь колумнист New York Times Томас Фридман даже писал, что «мир стал плоским», то есть лишился иерархий) до нынешней сети, почти полностью контролируемой несколькими финансовыми гигантами [21].

Начнем с экономики доцифровых времен, с моделей, унаследованных от XX века, когда централизованная модель доверия была единственно возможной. В этой системе, которая доминирует и в наши дни, ответственность за проведение и запись транзакций возлагается на банки, государственные и социальные службы, нотариальные конторы и прочие централизованные учреждения. Они уполномочены

отслеживать нашу деятельность: переводы средств, потребление электричества, всевозможные ежемесячные платежи — от подписки на газеты до телефонных разговоров — и обязуются достоверно отражать эту информацию в учетных реестрах, которые ведут и контролируют только они. Благодаря эксклюзивной осведомленности эти организации приобрели уникальное право решать, кто из нас может заключать сделки и пользоваться услугами. Это они позволяют (или не позволяют) нам получить овердрафт, воспользоваться энергосетью, сделать телефонный звонок. И выставляют нам счет за эту привилегию.

Такая система абсолютно несовместима со структурой интернет-пространства, где нет «одного главного» и полномочия разделены между пользователями. Изначально сеть создавалась для того, чтобы любой мог опубликовать или переслать информацию практически даром. Это открыло для экономики поистине головокружительные возможности, но и обусловило беспрецедентные проблемы в области доверительного управления. У человека, с которым вы ведете дела, может быть фотография собаки на аватаре и ник вроде Voldemort2017. Как определить, что он благонадежен и выполнит условия сделки, которую вы собрались заключить? Многие сервисы, например Yelp и eBay, ввели систему рейтингов-звездочек; однако рейтинг легко поднять с помощью фейковых отзывов и аккаунтов — так же как публикацию в Facebook можно продвинуть в топ за счет заказных лайков. Нельзя полагаться на такие поручительства, если речь идет о крупных сделках. Когда интернет-компании поняли, что не могут разрешить проблему доверия, они прибегли к услугам централизованных посредников. Вероятно, это был вынужденный шаг, но мера оказалась далеко не идеальной и повлекла за собой многочисленные осложнения в сфере безопасности и конфиденциальности.

Система распределенного доверия позволила аферистам с легкостью менять маски и псевдонимы. Кроме того, они получили возможность подделывать и копировать ценную информацию. Поэтому в середине 1990-х годов, когда предприниматели начали осваивать электронный бизнес, им пришлось бросить все силы на разработку платежных систем, которые бы защитили клиентов от мошенничества. Будучи не в состоянии гарантировать клиентам полную сохранность банковских счетов и средств на кредитных картах, они сначала задумались о новых анонимных формах электронной валюты — то есть

поставили именно ту задачу, которую решил Сатоши Накамото, создав биткоин. Ведь при наличии общей цифровой валюты покупатели могли бы расплачиваться ею, не раскрывая личных данных, как при оплате банкнотами. В поисках решения уже упомянутые нами шифропанки (ярые защитники сетевой анонимности, одержимые криптографией) и другие энтузиасты пытались создать частные криптовалюты, в то время как банки и правительства тайно экспериментировали с электронными денежными единицами на базе национальной валюты [22]. (В книге «Эпоха криптовалют» мы рассказывали о малоизвестном пилотном проекте Казначейства США, проведенном при участии Citibank.)

Проклятием первых цифровых валют стала проблема двойной траты: злоумышленники неизменно находили способ копировать свои активы. Исключить такую возможность было крайне важно, ведь одно дело — скопировать и послать кому-нибудь документ Word и совсем другое — расплатиться одними и теми же деньгами по нескольким разным счетам. Такой вид цифрового мошенничества очень скоро обесценил бы любую валюту. Многие технологи пытались разработать систему, которая бы предотвращала двойное расходование, но это оказалось сложнее, чем они думали.

В конце концов, до появления биткоина в сфере интернет-коммерции прижился своего рода «обходной» метод. Компании вроде Verisign разработали модель SSL-сертификатов (SSL, или уровень защищенных сокетов — криптографический протокол повышенной безопасности), подтверждающих надежность шифрования сайтов. Со своей стороны, эмитенты банковских карт ужесточили контроль за транзакциями. К сложной системе международного обмена ценностями вновь добавилась «доверенная третья сторона». Банковская система — та самая, что решала проблему двойного расходования последние пятьсот лет, — довольно-таки неуклюже встроилась в децентрализованный интернет и взяла на себя роль ключевой инфраструктуры доверия.

Когда покупатели обрели уверенность в том, что их не обманут, интернет-коммерция начала развиваться бурными темпами. Однако наличие посредников увеличило стоимость транзакций и понизило общую эффективность системы. Высокие комиссии сделали невозможной поддержку микроплатежей — переводов на очень незначительные суммы, иногда в несколько центов, — которые поначалу

обещали подарить нам новые модели онлайн-бизнеса. Так погибла мечта первых интернет-энтузиастов: глобальный рынок, где про-
[70] граммное обеспечение, медиаконтент и вычислительные мощности продаются и покупаются в малых долях для максимальной эффективности [23]. Компромиссное решение привело еще и к тому, что кредитные карты — прежде финансовый инструмент элит — стали неотъемлемой частью онлайн-инфраструктуры. В результате банки окончательно «прописались» в наших платежных системах. При ныне существующей модели банки берут за защиту от мошенников примерно 3 процента с каждой продажи — добавление в цифровой экономике скрытого налога, который закладывается в цену товара.

Централизованные структуры взяли на себя и другие аспекты управления интернет-средой: например, распределение доменных имен и хостинг — размещение и хранение файлов, из которых состоят клиентские сайты. Любой, кто создает себе сайт, вынужден пользоваться услугами DNS-провайдеров и хостов. Разумеется, за обслуживание нужно платить. Чем больше файлов и страниц вы разместите, тем выше будут тарифы.

Все эти решения приемлемы для тех, кто может себе их позволить. Однако дополнительные комиссии и сборы неизбежно превратились в барьеры, которые помогают крупным игрокам вытеснить конкурентов, ограничить инновацию и лишить миллиарды небогатых людей шанса в полной мере использовать возможности интернета для роста и развития. Вот так мы оказались во власти интернет-монополий. Те, кому удалось первыми захватить рынок, не просто пожинают плоды сетевого эффекта; их позиции косвенно защищены высокими ценами на услуги, с которыми сталкиваются конкуренты при попытке выйти на тот же уровень. Итак, доверительное управление весьма недешево. Из-за его дороговизны и сложились экономические условия, позволяющие корпорациям вроде Amazon, Netflix, Google и Facebook нещадно расправляться с конкурентами. Не менее важно и то, что эти несокрушимые гиганты получили всю полноту власти над растущими массивами наших личных, иногда строго конфиденциальных данных.

Интернет: последняя деталь пазла

Совсем не такой была мечта, изложенная в «Манифесте криптоанархиста» Тима Мэя и прочих сторонников криптографической защиты, анонимности и цифрового мира личных свобод. Технобунтари 1990-х хотели видеть интернет свободным от правительственного и корпоративного контроля как децентрализованное, избавленное от цензуры пространство, где кто угодно может вступить во взаимодействие с кем угодно под любым выбранным именем. Вспомним проекты вроде злополучного Xanadu Теда Нельсона, которому так и не удалось создать обещанную «альтернативную сеть» независимых, полностью автономных, самообновляющихся серверов [24]. В основе подобных идей лежало представление о структуре, в которой контроль над вычислительными мощностями и данными в значительной степени возложен на пользователей. Эти проекты намного опередили свое время и возникли в период, когда технологические, политические и экономические реалии были с ними попросту несовместимы.

И вот, в 2008 году, когда сообщество шифропанков уже совсем опустило руки, появился биткоин. Сама идея криптовалюты как будто сошла со страниц их записных книжек (хотя поначалу мало кто верил, что она заработает). Теперь вопрос о том, кто контролирует данные, утратил всякий смысл. Сохранность информации отныне обеспечивала децентрализованная сеть, которая постоянно самостоятельно обновлялась благодаря встроенным механизмам консенсуса. Как только принципы биткоина стали очевидны, многие создатели первоначальной архитектуры интернета испытали настоящее озарение, в том числе инвестор и предприниматель Марк Андриссен — один из разработчиков первого коммерческого интернет-браузера Netscape. В интервью журналистам Дону и Алекс Тапскотт он заявил, что видит в новой криптовалюте «ту самую сеть распределенного доверия, которой всегда так не хватало интернету» [25].

Когда Андриссен и другие крупные инвесторы Кремниевой долины начали вкладывать средства в разработку биткоина и его клонов, стал очевиден весь масштаб того, чего могла бы достичь технология блокчейн. На сегодняшний день разработчики ищут способы встроить принципы блокчейна во многие инновационные продукты и идеи.

— Для работы «интернета вещей» потребуется децентрализованная система транзакций от устройства к устройству.
— В ходе разработки контента для виртуальной реальности, при которой новые виртуальные миры будут совместно создаваться писателями и программистами, можно будет задействовать систему блокчейн для распределения гонораров по смарт-контрактам.
— Системам искусственного интеллекта и больших данных понадобятся гарантии того, что данные, полученные из многочисленных неизвестных источников, не сфальсифицированы.
— Системы Industry 4.0 для «умного» производства и 3D-печати, а также новые коллективные цепи поставок нуждаются в децентрализованной системе для отслеживания рабочих процессов и затрат каждого поставщика.

Иными словами, блокчейн может подарить нам архитектуру, на базе которой произойдет так называемая *четвертая промышленная революция*, которая соединит «биты и атомы» и будет развиваться за счет массивов глобальной информации. Это наконец сделает возможным «интернет открытых данных». Вся информация мира окажется в свободном доступе, и с ней сможет работать любой желающий. Неограниченный доступ к данным должен помочь человечеству найти коллективные решения многочисленных проблем, повысить качество производства и эффективность труда. Перед нами открываются весьма заманчивые перспективы.

Код не есть закон

Как мы уже говорили, нет ни малейших гарантий, что мечта об эффективной платформе для глобальной цифровой экономики когда-нибудь станет явью. Помимо сложных технологических и управленческих задач, которые мы обсудим в следующих главах, существуют и внешние препятствия для перехода на новую модель. Прежде чем технология блокчейн или любая другая система децентрализованного доверия ляжет в основу финансового и информационного обмена во всем мире, нам придется ответить на ряд весьма сложных вопросов.

В первую очередь они возникают у финансовых регуляторов, которым приходится менять привычные категории из-за появления криптовалют. Управлению финансовых служб Нью-Йорка понадобилось два года на разработку специализированных лицензий BitLicense и выпуск нового списка норм и правил, необходимых для расчета в биткоинах. К 2015 году, когда нормативные акты вступили в силу, в цифровом мире уже появились эфириум и смарт-контракты; теперь на очереди токены, первичные предложения монет и децентрализованные автономные организации, появление которых не могли предвидеть авторы нового уклада. Велик риск того, что регуляторы, сбитые с толку этим потоком инноваций, слишком бурно отреагируют на какой-нибудь скандал — например, если лопнет «мыльный пузырь» ICO и инвесторы понесут крупные убытки. Многие опасаются, что при таком развитии событий будут применены драконовские меры, которые положат конец инновациям в этой сфере или загонят их в подполье (и офшоры). Отдадим должное вашингтонской организации Coin Center, а также Палате электронной торговли, которые постоянно работают с правительственными чиновниками и стараются объяснить важность сохранения конкурентоспособности в мировой гонке финансовых технологий. Однако мы живем во времена политической нестабильности, когда законодательные решения, мягко говоря, диктуются отнюдь не здравым смыслом или дальновидностью. Уже сама непредсказуемость действий регуляторов и законодателей серьезно замедляет технологический прогресс в сфере криптовалют.

В ближайшее время нам потребуются законодательные инициативы — база, которая позволит понять, как вписать организационные и управленческие модели на основе блокчейна в рамки традиционных правовых систем. Как нам определить права собственности на цифровой актив, если они сводятся к владению приватным анонимным ключом? Как провести границы юрисдикций, когда блокчейн-реестр распределен между пользователями из разных стран или когда невозможно отследить, какие именно компьютеры глобальной сети исполняют случайно назначенные операции в рамках смарт-контракта? Сторонники этих технологий могут отрицать необходимость новых законов, но совсем вывести их из сферы правового регулирования невозможно. Цифровой мир — не отдельная вселенная; на него, как

и на любое поле человеческого взаимодействия, распространяются законы и нормы, которые складывались тысячелетиями.

[74] Анархически настроенные криптоэнтузиасты, которые мечтают жить исключительно по законам самого блокчейна и полностью выйти из-под власти государства, любят цитировать фразу «Код есть закон», брошенную профессором Лоуренсом Лессигом [26]. Впрочем, они склонны вкладывать в нее свой смысл. Лессиг вовсе не имел в виду, что программный код может заменить человеческие законы или что любые споры будет решать машина. Он всего лишь хотел сказать, что код отчасти подобен юридическому кодексу, поскольку регулирует «поведение» вычислительных компонентов. Считать код полноценной альтернативой закону означает сводить последний к чему-то гораздо меньшему, чем он есть в действительности. Будь закон всего лишь сводом инструкций и правил — тогда да, вероятно, мы смогли бы положиться на компьютеры и прописать алгоритмы, которые выполняли бы и регулировали наше взаимодействие в цифровой среде. Но понятие закона намного глубже и шире. На философский вопрос «что есть закон?» можно ответить по-разному, но чем дольше изучаешь это понятие, тем труднее становится отделить закон от юнговского «коллективного бессознательного»: набора представлений о том, как относи́ться друг к другу, унаследованного нами от предыдущих поколений и понемногу меняющегося на протяжении нашей истории [27]. Столь древнее и сложное явление нельзя свести к программному коду.

Ничто не иллюстрирует это ярче, чем печально известная атака на фонд The DAO в июне 2016 года. DAO расшифровывается как «децентрализованная автономная организация» (ДАО). Выбрав это название, основатели проекта присвоили акроним, который прежде использовался как общее обозначение ряда новых, многообещающих систем автоматического корпоративного менеджмента и был предельным выражением техноанархических идеалов. Этот децентрализованный венчурный фонд основала команда стартапа Slock.it — группа разработчиков смарт-контрактов во главе со Стефаном Туалем, бывшим коммерческим директором Ethereum. Весь проект должен был управляться исключительно автоматикой — без администраторов, совета директоров и менеджеров какого-либо звена. О подобных системах уже давно велись разговоры, однако создатели The DAO первыми рискнули опробовать новый принцип на практике. Платформа должна

была позволить инвесторам распределять средства с помощью голосования, — то есть выбирать и отмечать один из предложенных проектов. Предполагалось, что в итоге возникнет новая, более демократичная и эффективная логика инвестирования, чем в традиционных фондах, где интересы руководства и вкладчиков не всегда совпадают.

Сказать, что планы были грандиозными, значит ничего не сказать. Инвесторам предлагалось покупать токены DAO, расплачиваясь за них эфирами — изначальной валютой платформы Ethereum. Таким образом они приобретали долю в фонде The DAO. Решения по инвестициям должны были приниматься путем голосования по представленным бизнес-проектам. В дальнейшем все взносы, дивиденды и отчисления должны были автоматически распределяться системой «умных» контрактов платформы Ethereum. Этот проект вызвал небывалый ажиотаж среди адептов децентрализации в криптосообществе. Им уже виделась возможность доказать, что эффективные экономические решения могут приниматься без помощи посредников — частных или государственных.

Многих юристов беспокоило отсутствие механизма компенсаций в случае потерь. Предупреждали о недостатках кода, из-за которых взломщики могут «увести» из фонда все средства, и такие признанные специалисты по криптографии, как создатель Zcash Зуко Уилкокс и профессор Корнеллского университета Эмин Гун Сирер [28]. Но, несмотря на это, инвесторы всего за 27 дней раскупили токены DAO на сумму 150 миллионов долларов. На тот момент The DAO оценивали как самый крупный краудфандинговый проект в истории.

Как выяснилось впоследствии, затея изначально была обречена на провал из-за дефектов, не замеченных учредителями и инвесторами, которые, вероятно, были ослеплены излишней самоуверенностью, помноженной на идеализм. В первичных документах, где излагались условия сделки, компания Slock.it прописала: «Алгоритм смарт-контракта DAO управляет созданием токенов DAO и отменяет любые публичные заявления о создании токенов DAO, сделанные третьими сторонами или лицами, ассоциированными с Фондом, в прошлом, настоящем и будущем» [29]. Это было весьма смелое и, как мы теперь знаем, опрометчивое заявление, основанное на радикальной, чересчур *буквальной* трактовке фразы Лессига «код есть закон». Создатели фонда хотели целиком и полностью избавиться от человеческого фактора, от наших расплывчатых, субъективных представлений и оценок.

Ущербность этой логики вскоре проявилась во всей красе. Ранним утром в пятницу, 17 июня 2016 года, наблюдатели заметили, что с криптовалютного счета The DAO стремительно выводятся средства. Неидентифицируемый участник проекта сумел написать и запустить программу, которая вступила во взаимодействие со смарт-контрактом, постоянно требуя и получая средства, а затем отправляя их на ложную версию DAO, специально созданную взломщиком. Получилось нечто вроде взбесившегося виртуального банкомата, который не могла выключить полностью автоматизированная система DAO. Прежде чем удалось заблокировать доступ к средствам, хакер вывел со счета почти 55 миллионов долларов в криптовалюте.

Ошеломленные организаторы проекта с юридической точки зрения оказались в патовой ситуации, поскольку сами же ранее заявили, что код стоит над законом. Предполагалось, что любая операция, выполненная программой, допустима. В данном случае программа, повинуясь правилам собственного кода, перенаправила средства фонда на счета одного ловкого пользователя. «Я даже не уверен, что это можно квалифицировать как взлом, — писал у себя в блоге профессор Гун Сирер. — Чтобы назвать некое действие взломом, кражей или хакерской атакой, — то есть нарушением закона, — для начала нужно определить, что такое соблюдение закона. В документах The DAO никаких определений не было. Более того, сам код и объявлялся основным документом. Просто хакер прочел его гораздо внимательнее, чем сами разработчики, и обнаружил лазейку. ...Если бы он, наоборот, лишился денег из-за ошибки программы — я более чем уверен, разработчики без колебаний распределили бы его средства и сказали: мол, такова жизнь в новом мире электронных финансовых потоков. Однако хакер не потерял деньги, а вывел их из фонда. Остается только похвалить его за сообразительность» [30]. По правилам самих основателей The DAO, взломщик не сделал ничего плохого. Он просто нашел и воспользовался новой *функцией* программы.

В реальном мире дух закона всегда стоит выше его буквы — намерение для нас важнее, чем соблюдение формальностей. В данном случае преступные намерения хакера явственно ощутили обладатели токенов (и отреагировали соответственно). У них-то не возникло сомнений, что их ограбили. Они пришли в ярость и потребовали вернуть средства. Но как? На кого в этом случае подавать в суд? У фонда не было

официально зарегистрированного владельца. Все пользователи были равноправными членами децентрализованной организации без руководства. Однако, как заявляли многие юристы, закон всегда найдет виновного. И самыми очевидными «крайними» оказались сотрудники Slock.it, а также основатели и разработчики платформы Ethereum, которые всячески рекламировали и продвигали The DAO [31]. Даже без судебного преследования их репутация, как и репутация популяризируемой ими системы, сильно пострадала.

Однако год спустя инцидентом заинтересовались и правоохранительные органы. Расследуя взлом The DAO, Комиссия по ценным бумагам и биржам США постановила: поскольку токены фонда не были официально зарегистрированы в качестве ценных бумаг, их выпуск можно считать противозаконным. К счастью для команды Slock.it, комиссия в итоге решила не передавать дело в прокуратуру, но пресс-релиз, где пояснялись итоги расследования, послужил своего рода предупредительным выстрелом [32] и не только дал понять, что продавцам криптотокенов пора задуматься об отношениях с законом, но и напомнил о рамках полномочий регуляторных органов, за которыми стоит правовая система США.

Перед нами неизбежно встает вопрос: как встроить доверительные отношения в блокчейн? Радикальные приверженцы биткоина считают, что пользователям не нужно думать о благонадежности тех, с кем они обмениваются криптовалютой. Запись любых транзакций автоматически генерируется распределенной программой, и, когда средства переводятся другому пользователю, это подтверждается децентрализованной системой без «доверенной третьей стороны». Следовательно, нет необходимости идентифицировать пользователей. Однако в реальности пользователям биткоина неизбежно приходится кому-то или чему-то доверять. Во-первых, платеж — только часть транзакции; программное обеспечение никоим образом не гарантирует, что продавец действительно отправит вам товар или окажет требуемую услугу. Во-вторых, пользователям нужно удостовериться, что данные, вносимые в общий реестр, будут соответствовать истине. Откуда нам знать, что смартфон или компьютер, с которого мы входим в биткоин-кошелек, не был взломан? Откуда нам знать, что, набирая на клавиатуре 6f7Hl92ej, мы действительно передаем эти символы в сеть Биткоин? Остается лишь верить и надеяться, что Apple,

Samsung и другие производители оргтехники строго отслеживают цепи поставки и не позволяют хакерам заразить чипы какой-нибудь программой-шпионом. Нет, впадать в панику, конечно, не стоит: невзирая на частые взломы, большинство из нас все же полагаются на милость компьютера, и ничего особо ужасного не происходит. Однако считать, что блокчейн-системы полностью снимают или отменяют проблему доверия, было бы неверно и несколько наивно.

Если не сводить транзакции к обмену криптовалютой и переводить через блокчейн другие ценности и активы, без посредников не обойтись. К примеру, подлинность документов о праве собственности на землю должна заверяться уполномоченным лицом — сотрудником кадастровой службы. Криптовалютные пуристы полагают, что такая зависимость от посредников подрывает основы блокчейна как системы безопасности. С их точки зрения, блокчейн непригоден для многих нефинансовых операций. Однако мы считаем, что при разумном компромиссе блокчейн может стать вполне надежной платформой для фиксации прав собственности и цифрового отображения материальных активов. Тем не менее о проблеме благонадежности нельзя забывать, поэтому нам понадобятся стандартные протоколы для сбора данных из официальных источников и внесения их в систему на основе блокчейна.

Технология блокчейн не отменяет потребности в доверии — даже наоборот, позволяет выстроить более доверительные отношения. В каком-то смысле она расширяет наш «периметр доверия». Само устройство блокчейн-платформ делает проверку благонадежности и ведение реестров децентрализованными процессами. Это значит, что каждому из нас нужно выдать некий кредит доверия человеку «на другом конце сети». Нам придется принять на веру, что продавец исполнит обещание и в срок отгрузит нужный товар; что источник ценной информации — например, о котировках акций — выдаст нам точные сведения или что компьютеры и смартфоны, которыми мы пользуемся для ввода данных, не заражены программами-шпионами еще на заводе. При разработке новых систем управления на основе блокчейна необходимо тщательно продумать защитные алгоритмы, которые можно будет применять на периферии сети — или, как иногда говорят, «на последнем рубеже верификации». Внедрение технологии блокчейн должно дать толчок разработке стандартов, правил и критериев для оценки соблюдения контрактных обязательств в новом цифровом контексте.

Наконец, существует еще один потенциально спорный момент, связанный со структурой рынка, — это вопрос о том, какие компьютеры должны контролировать блокчейн и какие полномочия при установке цен и уровня доступа, а также доли рыночного присутствия дает этот контроль. Закрытые блокчейны — то есть требующие допуска от администраторов — по определению содержат в себе контролирующие механизмы, а значит, риск появления монопольных или олигархических структур здесь выше, чем в одноранговой цепи, которую в идеале представляет собой биткоин. (Мы говорим «в идеале», потому что, как будет показано в следующей главе, ряд функций ПО биткоина уже привел к нежелательной концентрации власти в системе — недостаток, который сейчас устраняют разработчики.)

Закрытые блокчейны подразумевают наличие доверенной третьей стороны — тот самый тип посредничества, которого надеялся избежать Сатоши Накамото. Они уполномочены решать, какие компьютеры могут участвовать в процессе валидации. Такой принцип подходит для различных предприятий, которые хотели бы внедрить технологию блокчейн, но в силу отраслевой специфики не могут себе этого позволить. Пока не внесены изменения в законодательство, банки будут сталкиваться с неразрешимыми юридическими и регуляционными проблемами, например при попытках использовать системы вроде блокчейна Биткоина, где ответственность за разные стадии ведения отчетности случайным образом приписывается анонимным компьютерам по всему миру. Но это не означает, что компании другого профиля не заинтересованы в переосмыслении принципа работы закрытых цепей. Если распределенный реестр окажется под властью консорциума самых влиятельных банков мира, то будет ли он служить интересам широких слоев населения? Несложно представить, какая опасность кроется в «нерушимом огромном блокчейне»: мы можем вновь оказаться в заложниках у крупных организаций из-за сбоев в общей учетной системе. Вероятно, такой исход можно предотвратить с помощью строгих правил или общественного надзора над подобными системами. В любом случае нам необходимо удостовериться, что контроль над блокчейнами будет осуществляться исходя из общих интересов и потребностей, иначе блокчейн станет всего лишь новым орудием в руках олигархических сил.

Очень важна разработка закрытых реестров на базе ПО с открытым исходным кодом: ею занимаются, например, R3 CEV — консорциум под управлением ряда крупных банков — и поисковая лаборатория Hyperledger, в которую входят сотрудники таких техногигантов, как IBM, Intel и Cisco. Новые технологии выявляют и подчеркивают недостатки старых централизованных работающих моделей. Некоторые находки, несомненно, окажутся очень ценны для всей блокчейн-индустрии. Однако мы полагаем, что «открытый» идеал, намеченный биткоином и воспроизведенный в многочисленных альткоинах* и блокчейнах, сейчас жизненно необходим всему миру.

Как мы отмечали в книге «Эпоха криптовалют», Биткоин просто был первым пробным шаром — попыткой разрешить извечную проблему доверия и создать открытую дешевую архитектуру для прямых глобальных транзакций с помощью распределенных вычислений и децентрализованных реестров. Эта платформа может выполнить свою задачу, а может и не выполнить. Не исключено, что появится и другая технология, которая сыграет в эпоху криптовалют ту же роль, что пара протоколов TCP/IP сыграла в эпоху интернета. Возникнет некий стандартный, базовый протокол, который определит, как именно компьютеры могут обмениваться ценностями между собой. Будет ли это Биткоин, Ethereum или нечто совершенно иное — новый протокол, который позволит компьютерам с цифровыми активами любой из этих конкурирующих цепей свободно торговать друг с другом без посредников? Такова опасность и привлекательность открытых разработок: кто угодно может скопировать, а затем усовершенствовать ваше изобретение. Хорошая новость в том, что на доработку и улучшение ныне существующих технологий будет направлена безграничная творческая энергия. Возможно, русло инновации снова выведет нас к Биткоину и окончательно закрепит за ним преимущество первопроходца. Или же право на создание ценностей распределится между несколькими платформами до тех пор, пока не будет найдено принципиально новое решение. Подобные вопросы мы обсудим в следующей главе, обозревая стремительную эволюцию сферы блокчейна.

* Все криптовалюты, которые представляют собой альтернативу биткоину. *Прим. ред.*

Глава

3

Платформы и политика

Формирование децентрализованной экономической системы для сети независимых анонимных пользователей, где каждый будет работать в интересах всего сообщества, представляет собой весьма сложную техническую задачу. Но не менее сложны и задачи политического характера. Парадоксальным образом выясняется, что создание сети вне традиционной политической системы требует принятия множества политических решений.

Успех децентрализованной криптовалютной сети или другого блокчейна зависит от разработки правильного набора правил — то есть программного протокола, — согласно которому будет происходить взаимодействие участников. Биткоин, новаторский проект Сатоши Накамото, впервые показал, как достичь подобного результата даже при обмене крупными денежными суммами, конфиденциальной деловой информацией и прочими ценностями. Однако по мере роста и изменения сообщества пользователей биткоина новички начинают требовать более разнообразных функций и более мощных приложений; звучат настойчивые призывы усовершенствовать протокол и упростить принципы работы. Увы, в поистине открытой и децентрализованной системе без руководства крайне сложно привести к консенсусу множество людей с очень разными индивидуальными запросами.

Внедрением блокчейн-протоколов сейчас заняты несколько тысяч блестящих программистов и предпринимателей. В каком-то смысле они напоминают отцов-основателей американской нации: перед ними

лежит нечто новое и неизведанное, что могло бы изменить мир, если им удастся настроить это «нечто» должным образом. Постулат «все люди созданы равными» не родился сам по себе в июле 1776 года на просторах одной британской колонии. В нем выкристаллизовалась вся суть классической либертарианской идеологии, которая и до того насчитывала уже несколько десятилетий. В наши дни технофилософы блокчейна обрабатывают множество версий одной и той же идеи. Нужно лишь найти ее лучшие выражения.

Святой Грааль шифропанков

Чтобы понять, как работают блокчейны, а также какие технические и политические дебаты они порождают, для начала нужно рассмотреть первую рабочую блокчейн-платформу — Биткоин. Основополагающие принципы Биткоина — полная децентрализация и открытость. Позволив сообществу автономных пользователей выработать единую историю транзакций, Биткоин показал: компьютерная программа, не управляемая отдельными лицами или корпорациями, может взять на себя роль «доверенной третьей стороны», которую при финансовом взаимодействии традиционно играют банки. Чтобы общество могло осознанно принять (или отвергнуть) эту поистине прорывную технологию, надо сначала понять, что такое Биткоин и чем он для нас важен [1].

Однако прежде чем мы это сделаем, давайте начнем с общего определения блокчейна: это распределенный реестр, который обновляется только путем присоединения новых записей и отображает доказуемо подписанные, непрерывно связанные и криптографически защищенные транзакции. Каждый реестр многократно воспроизведен и хранится на независимых друг от друга компьютерах; каждое обновление синхронизируется на основе алгоритма консенсуса.

Что же значит весь этот набор слов? Давайте рассмотрим ключевые смысловые единицы.

1. *Распределенный*: это значит, что реестр хранится не на одном компьютере, а на всех компьютерах сети одновременно.

Каждая машина по отдельности отвечает за его обновление и синхронизацию с остальными версиями. Как только один регистратор (в данном случае компьютер) обновляет базу данных и предоставляет доказательство легитимности записи, все остальные устройства вносят то же самое обновление в свои реестры. В результате получается регулярно обновляемая, общепринятая запись без централизованной главной версии.

2. *Обновляется только путем присоединения новых записей (append-only)*: информацию можно добавлять, но не удалять. Это важно, поскольку никто не может вернуться к старым записям и подкорректировать их. То, что однажды было принято и утверждено как истинное, им же и останется. Разночтения здесь невозможны.
3. *Доказуемо подписанные*: для обмена и управления данными блокчейны используют инфраструктуру открытых ключей (ИОК), где каждый пользователь распоряжается двумя отдельными, но математически связанными последовательностями букв и чисел, или «ключами». Первый — секретный, или «закрытый», ключ — известен только владельцу. Второй — «открытый» ключ — доступен всем пользователям и отображает некую ценную информацию. В системе Биткоина, например, она связана с количеством криптовалюты. Когда пользователь «подписывает» открытый ключ с помощью секретного ключа, эта операция математически доказывает, что он имеет право распоряжаться данными и может перевести их на открытый ключ другого пользователя. В случае Биткоина владелец таким образом пересылает валюту со своего «кошелька» (открытого ключа) на другие кошельки. (Личный ключ можно сравнить с паролем или ПИН-кодом для управления средствами на счете. Аналогия не идеальная, но достаточно близкая.)
4. *Непрерывно связанные и криптографически защищенные транзакции*: некоторые инструменты из криптографического арсенала используются для отображения записи в реестре определенным способом. Любые транзакции записываются в строго хронологическом порядке с помощью функции хеширования, которая позволяет подтвердить достоверность

всей цепочки. В итоге получаются бесконечные цепочки блоков (или «кусочков информации»), чья целостность защищена криптографическим методом. Такая структура обеспечивает высокую степень уверенности в том, что ни одна запись в реестре не будет отклоняться от общей, согласованной версии.

5. *Реестр многократно воспроизведен*: каждый узел сети хранит свою копию реестра (согласно принципу распределения из пункта 1).
6. *Алгоритм консенсуса*: программа, которую выполняет каждый компьютер сети, побуждает синхронизировать запись транзакций с другими устройствами. Можно сказать, что узлы сети достигают соглашения по поводу того, какие записи вносить в общий реестр. «Консенсус» — ключевой термин технологии блокчейн, описывающий процесс, в рамках которого каждая отдельная копия реестра согласовывается со всеми остальными и вырабатывается общая для всех версия истины. Суть консенсуса сводится к тому, что любое обновление должно быть подтверждено и одобрено большинством участников.

Ну что, разобрались? Если нет, не пугайтесь — скоро мы проясним все детали.

Важно понять, что общее описание блокчейна не отдает должного блестящим находкам Накамото. В системе Биткоина присутствуют элементы, которые воплотили в жизнь идеал шифропанков — полностью децентрализованную криптовалюту, неподконтрольную ни одному частному лицу, учреждению или консорциуму.

Калифорнийское сообщество шифропанков, которое билось над проблемой децентрализации лет двадцать до появления биткоина, прекрасно знало, что любой системе электронных денег необходим общий реестр для фиксации активов и пассивов пользователей. Он нужен для предотвращения «двойного расходования», то есть мошенничества. Но чтобы система стала полностью децентрализованной, каждый пользователь должен иметь доступ к реестру. Запись транзакций должна быть открытой, с алгоритмом консенсуса, на который нельзя повлиять в одностороннем порядке. Тогда никакая контролирующая инстанция не сможет блокировать, изменять или фильтровать содержимое реестра и он станет *неуязвимым для цензуры.*

До появления биткоина все попытки достичь этой цели неизменно упирались в неразрешимую дилемму: без контролеров, подтверждающих личность и права того, кто ведет реестр, любой мошенник мог нарушить консенсус, создав множество узлов сети под вымышленными именами. (Чтобы понять, насколько это легко, вспомните бесчисленные фейковые аккаунты в Twitter.) Застолбив сотни узлов сети, злоумышленник отдаст сам себе более 50 процентов голосов и добьется одобрения ложной «двойной транзакции», то есть, например, оплатит покупку несуществующими или уже на что-то потраченными деньгами. Эту проблему можно решить путем создания контролирующей инстанции, которая идентифицировала бы пользователей и авторизовала операции. Но тогда разработчики вернулись бы в исходное положение и не достигли бы великого идеала шифропанков — открытости и отсутствия цензуры.

Новаторское решение Сатоши Накамото, в сущности, опиралось на метод кнута и пряника — систему поощрений и наказаний, которые должны гарантировать честную работу валидаторов. Любой компьютер в любой точке земного шара может подключиться к процессу валидации и в качестве стимула и награды за работу будет получать биткоины, распределяемые по принципу лотереи. Вознаграждение выплачивается каждые 10 минут, как только один из компьютеров успешно добавит новый блок подтвержденных транзакций в блокчейн-реестр. (Эти компьютеры, а также их владельцы называются «майнерами» — от английского слова *miner*, или золотодобытчик, — потому что в надежде заполучить свою долю биткоинов они словно пускаются в погоню за цифровым золотом. На момент написания книги вознаграждение составляло 12,5 биткоина — 50 тысяч долларов по текущему курсу. Децентрализованный протокол автоматически начисляет эту сумму выбранному майнеру. Кроме того, майнеры получают комиссию за операции, о чем мы поговорим чуть позже.)

Поскольку в системе не предусмотрены ограничения допуска, любой мог попытать счастья и повысить шанс на получение награды, добавив к сети как можно больше узлов. Поэтому Накамото был необходим децентрализованный механизм, который бы помешал майнерам-мошенникам захватить более 50 процентов вычислительных мощностей. С этой целью он потребовал, чтобы каждый вовлеченный компьютер предоставлял «доказательство выполнения работы», то есть

решал сложную математическую задачу, предполагающую серьезные вычислительные ресурсы.

Доказательство выполнения работы стоит недешево, поскольку на него уходит много электроэнергии и вычислительных мощностей. Это означает, что, если майнер попытается захватить 51 процент мощностей и контролировать систему консенсуса, ему придется потратить довольно круглую сумму. Благодаря таким функциям, как «коррекция уровня сложности», которая усложняет вычислительные задачи по мере роста общей мощности сети, система Накамото гарантирует, что стоимость так называемой атаки 51 процента на порядки повысится, если взломщик подойдет к порогу контроля над консенсусом. Иными словами, мошенничество и двойная трата в системе Биткоина не запрещены — они просто чрезмерно до́роги. На данный момент, согласно оценкам сайта GoBitcoin.io, «контрольный пакет» в сети Биткоин обойдется примерно в 2,2 миллиарда долларов: столько будут стоить компьютерное оборудование и электроэнергия, которые нужны для захвата таких мощностей.

За несколько лет майнинг криптовалют превратился в настоящую индустрию, где лидирующую роль играют гигантские «фермы». Могут ли эти крупные игроки вступить в сговор, объединить ресурсы и захватить власть над реестром? Теоретически да. Но на практике это повлечет весьма неприятные последствия для них самих. Например, успешная атака обрушит курс биткоина и резко понизит стоимость криптовалюты, которой завладеют злоумышленники. По крайней мере, за девять лет существования биткоина этот реестр еще никто не взломал. Очевидно, метод кнута и пряника — весьма эффективное средство защиты.

Если рассматривать биткоин с этой стороны — а не просто как новую, непривычную денежную единицу, которую компьютерные гики почему-то считают хорошей заменой доллару, евро или иене, — становится очевиден подлинный масштаб изобретения Накамото. Криптовалюта биткоин (со строчной буквы «б») — это прежде всего ценность, которой вознаграждаются люди, обеспечивающие безопасность системы Биткоин (с прописной буквы «Б»). Ее суть и главное предназначение именно в этом, а не в надежде, что однажды она станет повседневным средством оплаты. Такое поощрение заставляет пользователей честно фиксировать и подтверждать обмен ценной

информацией, а без него открытый распределенный реестр Сатоши просто не смог бы работать.

[88] Конечно, для того чтобы система жила и развивалась, майнеры должны считать биткоин ценностью — то есть знать, что смогут обменять его на другие признанные ценности: товары, услуги, фиатные деньги, например доллары. Чтобы понять, почему они (и миллионы людей по всему миру) решили, что биткоины *чего-то стоят*, следует поговорить о том, как человеческие сообщества назначают себе универсальное средство обмена, меру стоимости товаров и услуг и расчетную единицу — иными словами, деньги. (За историческим материалом мы, опять же, беззастенчиво отошлем вас к книге «Эпоха криптовалют».) Нужно отметить, что вопреки расхожему мнению валюте не всегда требуется *обеспечение* — будь то правительственные гарантии или золотой запас. Ее нужно лишь официально признать единицей измерения ценности и средством платежа. Это может показаться иррациональным, ведь мы привыкли считать деньги материальным объектом (бумажной купюрой, золотой монетой и пр.), который каким-то образом содержит ценность *в себе самом*. Однако на деле любая валюта всего лишь обозначает, символизирует ценность, приписанную ей коллективной волей общества. Именно общество постановило считать эту купюру или монету носителем ценности. Подобный статус можно присвоить любому символу или объекту при условии, что с этим согласна значительная часть общества. Так и произошло с биткоином.

Структура реестра также важна для статуса биткоина. Накамото изначально задумывал свой реестр как постоянно растущую, непрерывную цепь блоков, каждый из которых отображает группу связанных друг с другом транзакций, подтвержденных в течение десятиминутного «наградного периода». Отсюда и возник термин "блокчейн", который так полюбился начальникам IT-отделов. (Надо сказать, слово «блокчейн» вообще не употреблялось в первой версии рабочей брошюры Накамото. Следовательно, нет причин отдавать системе Биткоин эксклюзивное право на этот термин.)

В течение десяти минут каждый майнер, вовлеченный в состязание за биткоины, одновременно собирает новые входящие транзакции и «укладывает» их в собственный блок. Детали каждой транзакции — дата, время, адреса отправителя и получателя, сумма перевода

и т. д. — фиксируются и прогоняются через особый криптографический алгоритм, чтобы получить так называемый *хеш* — строку из буквенных и цифровых символов. Алгоритм хеширования может преобразовать любое произвольное количество данных (входной массив) в строку фиксированной длины, тем самым математически подтверждая существование исходной информации. Владея данными о транзакции, любой пользователь может обработать их с помощью того же алгоритма, чтобы подтвердить, что создатель оригинального хеша владел теми же данными.

Ключевая особенность хеш-кодов — их сверхчувствительность к изменениям входного массива. Например, мы обработали текст предыдущего абзаца с помощью SHA-256 — алгоритма, на котором построен биткоин-майнинг, — и получили следующую строку:

63f48074e26b1dcd6ec26be74b35e49bd31a36f849033bdee4194b6be8505fd9

Если мы всего-навсего удалим последнюю точку в абзаце и повторим процесс, алгоритм сгенерирует уже совершенно иную последовательность:

8f5967a42c6dc39757c2e6be4368c6c5f06647cc3c73d3aa2c0abdec3c6007a5

Теперь представим, что некий злоумышленник решил потихоньку изменить данные транзакции. Если он хоть немного подправит запись, остальные майнеры немедленно поймут, что новый хеш не совпадает с тем, который отражен в их версии блокчейна, и отвергнут изменения. Вот почему функция хеширования так важна для защиты реестра.

Кроме того, мы можем объединить два хеша и получить конечный, или корневой, хеш, содержащий в себе оба подтверждения данных. Этот процесс можно повторять до бесконечности, создавая хеши хешей хешей в виде древовидной структуры, известной как дерево Меркла. Таким образом, транзакции внутри каждого блока криптографически связываются между собой.

Биткоин выводит эту связующую функцию на новый уровень. С помощью другого алгоритма хеширования майнер-победитель привязывает свой вновь созданный блок к предыдущему, что превращает весь блокчейн в бесконечную, математически связанную

последовательность хешированных транзакций, восходящую непосредственно к первичному блоку от 3 января 2009 года. Если внести исправление, скажем, в транзакцию от 15 января 2011 года, изменится вся цепочка хешированных записей, сделанных за последующие семь лет. В каком-то смысле это напоминает окрашивание купюр, применяемое банками для их защиты: если вор захочет потратить меченые банкноты, то немедленно изобличит себя.

Непрерывная запись транзакций — основа, используемая майнерами для проверки легитимности операций в новом блоке счастливчика, получившего награду в биткоинах. Если майнеры удовлетворены содержимым блока, они согласятся присоединить к нему свой следующий блок в случае удачи и выигрыша. Если их что-то не устраивает, они присоединят новый блок к более раннему, в достоверности которого убеждены, оставляя подозрительный блок в одиночестве, словно сироту. Такие варианты решения лежат в основе логики консенсуса, которая опирается на критерий под названием «длиннейшая цепь». Основной принцип следующий: пока ни один майнер не захватил более 50 процентов общих вычислительных мощностей, математическая вероятность гарантирует, что любая сомнительная ветка, созданная криминальным меньшинством, вскоре безнадежно отстанет от «правильной», одобренной большинством цепочки, и отомрет. Ловушка, конечно же, в том, что, если злоумышленники сумеют захватить больше половины мощностей, они получат возможность создать длиннейшую цепь, которую остальные майнеры поневоле примут за легитимную. Однако, как мы уже объяснили, такой уровень мощности непомерно дорог. Защита биткоина объединяет в себе математический и финансовый фактор.

В этой взаимосвязи принципов и кроется новаторская суть изобретения Накамото — децентрализованного, избавленного от цензуры архива. Если признать, что все системы бухгалтерского учета приблизительны (то есть абсолютно точное отображение реальности невозможно), то новая система, фиксирующая коллективное мнение сообщества без центральных инстанций, предлагает самый объективный механизм отображения *истины* из всех ныне известных.

Решив проблему двойного расходования, Биткоин заодно создал понятие «цифровой актив». До этого все цифровое слишком легко воспроизводилось, чтобы считаться собственностью, имуществом.

Именно поэтому цифровые продукты вроде музыкальных записей и фильмов обычно продаются с лицензией и правом доступа, а не правом собственности. Исключив возможность воспроизведения ценностей — в данном случае биткоинов, — система Накамото нарушила привычное положение вещей, создав *цифровую уникальность*. Этот принцип крайне важен для оценки биткоина как валюты и для прочих криптоактивов, которые появились чуть позже.

Однако хотя Биткоин и превосходит многие другие системы, он пока далек от совершенства. Ничто не проявило это столь явно, как внутренний конфликт по поводу, казалось бы, мелкого технического вопроса. По крайней мере, раскол начался с небольших разногласий, но быстро перерос в полноценную борьбу за контроль в системе, которая задумывалась как абсолютно независимая. Оказалось, что управлять Биткоином не значит просто вести реестр. Вопрос касался управления сообществом. Настало время политики.

«Гражданская война» Биткоина

Серьезные изменения в коде — извечная проблема открытых проектов, в особенности таких, как Биткоин. У них нет признанного руководителя, который может разрешать споры, к тому же в условиях практически полной анонимности невозможно даже понять, с кем именно ты споришь и каков статус этого человека в системе. При этом предмет спора — вполне реальные, солидные суммы. Любое новшество может повлиять на ценность криптовалюты. Словом, ситуация взрывоопасная. И конечно же, взрывы происходят, порождая длительные, ожесточенные дискуссии.

Поводом для самого серьезного конфликта послужил небольшой фрагмент программного кода — максимальный объем данных, установленный для каждого блока в цепочке. С 2010 года он ограничивался одним мегабайтом. Этот лимит означал, что в системе Биткоина можно совершать не более семи транзакций в секунду — серьезный недостаток в глазах провайдеров, которые надеялись, что Биткоин сможет конкурировать с платежными системами вроде Visa, обрабатывающими около 65 тысяч транзакций в секунду [2].

К 2016 году количество операций с биткоинами выросло настолько, что уже не позволяло уложиться в отведенный мегабайт на каждый блок. Транзакции, которые должны были выполняться за несколько минут, растягивались на час, а то и дольше. Чтобы сократить период ожидания, пользователи стали предлагать майнерам повышенную комиссию за включение их транзакции в блок. Возник искусственно созданный «рынок комиссионных», и пользователи начали конкурировать друг с другом. К июню 2017 года средняя комиссия в системе Биткоин достигала пяти долларов, что вполне выгодно при переводе 20 тысяч долларов, но недопустимо при оплате чашки кофе за два доллара [3]. Расходы ложились на плечи пользователей и становились дополнительным источником прибыли для майнеров, помимо обычного вознаграждения в 12,5 биткоина за блок. Майнеры неожиданно оказались в роли тех самых банкиров-посредников, от которых стремились избавиться создатели криптовалюты. С точки зрения пользователей, позиционируемая как открытая и безбарьерная система теперь ставила им преграды на каждом шагу.

Многие стартапы, избравшие Биткоин как платформу для бизнеса — например, электронные кошельки и обменные сервисы, — жаловались на невозможность быстро и качественно провести транзакции клиентов. «Я стал доверенной третьей стороной», — горько шутил Уинчес Казарес, CEO кастодиальной службы «Харо» [4], имея в виду, что взаимодействие его компании с клиентами часто приходится совершать «вне системы», а потом задним числом проводить транзакции через блокчейн Биткоина.

Требовались срочные меры. Некоторые предлагали увеличить емкость блока. Однако не все считали небольшое изменение в коде лучшим выходом. Критики этого решения указывали на то, что увеличение блока потребует больше памяти, а это сделает майнинг еще дороже. Следовательно, многие майнеры выйдут из игры и Биткоин окончательно станет достоянием нескольких крупных игроков, что повысит вероятность сговора в целях подтасовок. На первый взгляд казалось, что оба лагеря в чем-то правы. Партия «большого блока» хотела, чтобы любой мог себе позволить расплачиваться биткоинами и высокая комиссия не мешала заплатить за чашку кофе. Партия «малого блока» хотела отстоять два главных принципа — децентрализацию и безопасность. Их позиции были непримиримы, к тому же финансовый

масштаб проекта только обострял разногласия. Из небольшой любительской затеи Биткоин вырос в глобальную систему рыночной стоимостью около 50 миллиардов долларов (осенью 2017 года). За неимением владельца или совета директоров было крайне сложно определить, чья стратегия эффективнее защитит активы.

Предлагались различные решения, но ни одно не помогало достичь консенсуса — святыни Биткоина. Отчасти проблема крылась в отсутствии механизмов, которые позволили бы определить долю сторонников каждой идеи. Псевдонимная структура Биткоина, без формальных идентификаторов для пользователей и кошельков, лежит в основе всего проекта и гарантирует конфиденциальность. Однако она же мешает организовать голосование по ключевым вопросам. Без знания, кто есть кто и кто чем владеет, невозможно узнать предпочтения большей части сообщества, включающего рядовых пользователей, предпринимателей, инвесторов, разработчиков и майнеров. В итоге дискуссия свелась к потоку гневных комментариев в соцсетях.

Обе партии безнадежно увязли в конфликте. Накал страстей достиг апогея и привел к тому, что биткоин-сообщество на сайте Reddit раскололось пополам и завело две отдельные ветки форума для каждой фракции. Поскольку примирение казалось невозможным, все больше пользователей стало склоняться к мысли о радикальном, на первый взгляд почти невыполнимом решении: разделить пополам и саму сеть Биткоина.

Суть идеи сводилась к созданию так называемого форка Биткоина. «Форк», или ответвление, — это просто новая версия программы, например Microsoft Word. Существует два вида форков — хардфорк и софтфорк. При софтфорке старая версия программы не поддерживает новые опции, но все же совместима со свежей версией. При хардфорке новая программа лишена «обратной совместимости», то есть не работает с прежними версиями. Таким образом, хардфорк ставит пользователя перед необходимостью обновить все ПО. Это не слишком удобно даже в случае текстового редактора, а для криптовалютной системы становилось настоящей проблемой, поскольку биткоины из старой версии кошелька нельзя было перевести получателю, у которого установлена новая версия. Два Биткоина. Две версии истины.

Затем творческая фантазия разработчика Биткоина Питера Вейля породила альтернативное решение: небольшое обновление кода

под названием SegWit [5], которое можно внедрить щадящим методом софтфорка. Это не удвоило бы лимит блока как таковой, но увеличило
[94] бы его пропускную способность, а значит, почти удвоило бы количество информации, которую можно уместить в один мегабайт. Что еще важнее, обновление SegWit исправляло давние недостатки кода, которые мешали внедрить очень ценное новое изобретение — протокол Lightning Network (LN).

Протокол LN, разработанный Таддеусом Дрийя и Джозефом Пуном, позволил бы Биткоину соревноваться в скорости операций с платежной системой Visa. Он дает пользователям возможность совместно подписать смарт-контракт, который временно создаст двунаправленный платежный канал для перевода на заранее согласованную сумму, после чего они смогут переводить средства в рамках этого оговоренного баланса [6]. Кроме того, появится возможность переводить средства третьим лицам через систему взаимосвязанных вторичных каналов. Таким образом, должна возникнуть сеть платежных операций, которые не нужно подтверждать в блокчейне Биткоина. Следовательно, исчезнут комиссии майнерам и ограничения на количество транзакций в единицу времени. Смарт-контракты предотвратят обман между пользователями, а блокчейн понадобится только для записи и подтверждения итогового баланса при открытии и закрытии каналов. Он сохранится как главное свидетельство — гарантия подлинности «внесетевых» транзакций по протоколу LN.

Многие программисты горячо поддержали внедрение SegWit и Lightning Network — особенно разработчики Bitcoin Core вроде Питера Вейля, связанные с влиятельным биткоин-стартапом Blockstream. С их точки зрения, именно этого требовал ответственный подход к инновации. Они считали своим долгом избежать резких, чересчур масштабных изменений в коде и создать приложения, которые оптимизировали бы работу изначальной платформы. Классический, осторожный подход к разработке протоколов: оставить базовую систему простой, надежной и почти неподвластной изменениям (как говорят программисты, «намеренно тупой»), чтобы инновация происходила на уровне обновлений и надстроек. При благополучном исходе можно убить сразу двух зайцев: обеспечить и надежность, и новизну.

Тем не менее одна влиятельная группа майнеров, возглавляемая китайской компанией Bitmain, которая не только занимается майнингом

биткоинов, но и производит для него весьма востребованное оборудование, была категорически против SegWit и LN-протокола. Не совсем понятно, что именно так не понравилось CEO компании Цзянь Ву, но он заключил союз с одним из первых инвесторов Биткоина Роджером Вером и занялся активным продвижением «больших блоков» [7]. Возможно, руководство Bitmain опасалось, что «внесетевые» технологии Lightning отнимут у майнеров кровно заработанные комиссионные. Есть и другая версия: транзакции, проведенные через двунаправленный канал, не столь прозрачны, как «сетевые», поэтому китайские майнеры побоялись, что правительство запретит их деятельность. Репутация Bitmain сильно пострадала, когда выяснилось, что интегральные схемы их производства Ant-miner поставлялись сторонним майнерам с уязвимостью, которая позволяла майнеру-производителю вывести из строя оборудование конкурента. Немедленно заговорили о теории заговора: Bitmain планирует саботировать SegWit. Компания открестилась от подобных намерений и пообещала устранить уязвимость, но доверие уже было подорвано.

Противостояние длилось до весны 2017 года. В конце концов после многочисленных предложений по софтфорку и хардфорку группа предпринимателей во главе с давним биткоин-инвестором Барри Силбертом выбрала компромиссное решение — проект SegWit2x [8], который поддержали почти все крупные игроки биткоин-сообщества (кроме команды Blockstream). Это был двухступенчатый план — к середине июля предполагалось убедить хотя бы часть майнеров принять протокол SegWit, а затем, в ноябре, увеличить объем блока до двух мегабайтов. Для «партии большого блока» это была всего лишь возможность сохранить лицо, ведь в открытом анонимном сообществе никто не мог гарантировать, что обещанное удвоение объема состоится. Тем не менее план сработал. Незадолго до первого намеченного дедлайна по SegWit2x было установлено, что более 80 процентов компьютеров в сети готовятся принять протокол SegWit после 31 июля — достаточно, чтобы признать дело сделанным. Однако в последний момент победа команды Силберта была омрачена. Взбунтовавшаяся китайская группа (вероятно, поддерживаемая компанией Bitmain) заявила, что все-таки создаст свой хардфорк биткоина. Итак, 1 августа 2017 года, когда многим уже казалось, что болезненный развод можно предотвратить, сеть Биткоина раскололась пополам.

В этот день была запущена новая версия под названием Bitcoin Cash; эта валюта получила обозначение BCH (у старого биткоина — BTC). Емкость блока в новой системе составила 8 мегабайт. Как только майнеры — противники SegWit начали создавать блоки с такими параметрами, форк был запущен. Это напоминало раздел ценных бумаг: с формальной точки зрения все держатели биткоинов имели право и на свою валюту, и на равную долю в BCH, вот только на практике две валюты были несовместимы. Если такая идея равноценных, но разных денежных единиц кажется вам странной, вы не одиноки. Для биткоин-бирж она тоже была в новинку. Некоторые из них согласились вести операции с BCH, однако рынок с трудом переварил раздвоение биткоина. Поначалу стоимость новой версии подскочила с 300 до 700 долларов за 1 BCH, но затем, когда выяснилось, что форк поддерживает лишь одна крупная майнинговая компания, курс упал до 200 долларов и в течение лета 2017 года остановился у отметки 350 долларов. Тем временем курс изначального биткоина взмыл до небес, увеличившись за две недели более чем на 50 процентов и достигнув рекордной отметки в 4400 долларов США. Судя по поведению двух валют на рынке, сторонники малого блока и протокола SegWit победили.

Bitcoin Cash по-прежнему торгуется на биржах, но ему явно не по силам вытеснить первый биткоин. Что до компромиссного плана SegWit2x, в рамках которого предполагалось увеличить емкость блока до двух мегабайт, то к ноябрю 2017 года от него решили отказаться, поскольку прийти к полному консенсусу так и не удалось. Одна из сторон покинула поле боя основательно потрепанной, тогда как вторая ликовала. Многим сторонним наблюдателям казалось, что весь этот хаос неизбежно подорвет репутацию биткоина: кто же захочет иметь дело со столь непредсказуемой валютой? Тем не менее изначальная версия биткоина брала все новые высоты. Буквально за год ее курс вырос на 650 процентов!

Почему? Во-первых, биткоин прошел проверку на прочность. Несмотря на «гражданскую войну», его реестр уцелел. И хотя сложно назвать вражду и ожесточение преимуществом, сам факт того, что код так сложно переписать, а систему — изменить, многие расценили как важное свидетельство устойчивости и надежности биткоина. Невосприимчивость к цензуре стала самой привлекательной чертой биткоина; именно благодаря ей цифровую валюту начали считать возможной

заменой старым, уязвимым фиатным системам, которые до сих пор правят миром. Фактически можно сказать, что неспособность к компромиссу и эволюции, вызывающая скепсис у многих наблюдателей, — едва ли не главное достоинство биткоина. Как и простая, неизменная основа протокола TCP/IP, неповоротливые механизмы биткоина защищают систему от чересчур резких перемен и закрепляют инновацию на уровне надстроек.

Еще один урок, вынесенный из «раздвоения» биткоина, показал, куда направляются денежные потоки в условиях кадрового голода. Выяснилось, что они текут туда, где собираются лучшие разработчики, наиболее вероятна инновация и будут вовремя продуманы, опробованы и приняты меры безопасности. За изначальной версией биткоина (BTC) стоят многочисленные таланты. «Младшему» биткоину этот человеческий ресурс недоступен, поскольку сообщество майнеров-прагматиков никогда не привлечет к себе пылких энтузиастов. Мы не хотим сказать, что разработчики старшей ветви — Bitcoin Core — сплошь святые подвижники; многие предприниматели заслуженно осудили их несговорчивость в ситуации, когда простое и быстрое увеличение блоков могло бы снять напряжение в системе. К тому же существуют опасения, что компания Blockstream при поддержке инвесторов оказывает слишком большое влияние на процесс разработки.

Тем не менее Биткоин — далеко не единственный носитель технологии блокчейн. В деловом мире все больше крупных организаций, как финансового, так и нефинансового профиля, исследуют возможности закрытых блокчейнов. В системах такого рода некий центральный орган, например консорциум банков, решает, кто может принять участие в процессе валидации. Это во многом отступление от идеалов Накамото, поскольку участники закрытой системы вновь попадают во власть доверенной третьей стороны. Такие сети иногда называют не блокчейнами, а «системами на основе блокчейна» или же применяют к ним общий термин «распределенный реестр». Однако они действительно используют многие революционные находки Биткоина и справляются с проблемами доверия, которые в противном случае могли бы возникнуть при обмене информацией в сети. Что самое важное, закрытые блокчейны намного легче масштабировать, чем Биткоин (по крайней мере, на данный момент), так как для этого не требуется согласие тысяч анонимных пользователей по всему миру; достаточно просто

заранее договориться повышать вычислительную мощность по мере разрастания сети. Однако, как мы увидим в главе 6, закрытые системы
[98] в силу своей природы обладают ограниченными возможностями для инновации.

С нашей точки зрения, наиболее перспективны открытые блокчейны. Вероятно, закрытые системы — необходимая промежуточная ступень на пути к внедрению открытых реестров, однако мы полагаем, что открытость и общедоступность — тот идеал, к которому нужно стремиться, невзирая на подводные камни, выявленные «гражданской войной» Биткоина. Вот почему мы уделяем открытым системам так много внимания в этой книге.

Открытые блокчейны тоже стремительно эволюционируют; возникают новые модели, которые призваны усовершенствовать находки Биткоина. Многие из них предназначены не только для обмена криптовалютой, но и для широкого спектра операций, связанных с распределенными вычислениями. Можно считать их конкурентами Биткоина или интересными вариациями на ту же тему, но в любом случае они показывают, насколько динамичным стал поиск новых решений с момента появления Биткоина.

Эфириум: вечный глобальный компьютер... с багами

Платформа, которая привлекла к себе почти столько же внимания, как и Биткоин, — это, конечно же, детище русско-канадского вундеркинда Виталика Бутерина под названием Эфириум. Одна из первых и главных «больших идей» Биткоина заключается в возможности использовать блокчейн-сеть не только для прямых денежных переводов. Все, что может быть оцифровано — документ о праве собственности, контракт, история болезни, договор авторского права, личный документ, даже свидетельство о регистрации фирмы, — можно сделать частью транзакции и записать в неизменяемый блок. Это означает появление нового механизма автоматического однорангового взаимодействия. Проблема в том, что Биткоин как платформа, разработанная для обмена криптовалютой, мало подходит для нефинансовых

операций. Поэтому Бутерин взял основные принципы распределенного реестра и создал новую программу, оптимизированную для смарт-контрактов, которая будет поддерживать специальные децентрализованные приложения (Dapps), позволяющие пользователям обмениваться чем угодно.

Идея заключается в том, что компьютеры в сети Эфириум будут конкурировать за право выполнять инструкции Dapps по созданию и передаче цифровых активов. В награду за вычислительную работу компьютеры получат эфиры — криптовалюту сети Эфириум. Поскольку сеть децентрализована, приложения смогут работать абсолютно независимо, не поддаваясь влиянию извне. Это гарантирует полное соблюдение условий договора. Если бы концепцию Бутерина удалось воплотить в жизнь, его система фактически стала бы глобальной, децентрализованной *виртуальной машиной*, которая повинуется только программному коду и не контролируется ни одним отдельно взятым компьютером.

В декабре 2013 года, когда Бутерин впервые представил свой проект, его идея вызвала бурный энтузиазм [9]. В ней тут же признали первую поистине многофункциональную платформу для децентрализованных приложений. За несколько лет открытый проект привлек множество активных и талантливых разработчиков. «Тут можно встретить кого угодно: веб-дизайнера, сисадмина, ученого, экономиста, транссексуала, ярого поклонника Трампа, китайского бизнесмена, нью-йоркского инвестора или технаря в толстовке, у которого набралось эфиров миллионов эдак на пять», — так блогер под псевдонимом owaisted описывает собравшихся на Devcon — крупнейшей конференции разработчиков Эфириума [10].

И это неудивительно, поскольку спектр идей, которые подсказала новая децентрализованная платформа, столь же широк и разнообразен. Вот лишь их малая часть: «суверенная» цифровая идентичность; децентрализованная база медицинских документов; автоматизированные солнечные мини-электросети; децентрализованный товарообмен; краудфандинг и инвестиционные фонды «без владельца»; сертифицированные блокчейном свидетельства о браке; сверхнадежные системы онлайн-голосования; децентрализованные цепи поставок и логистические платформы; надежные протоколы для «интернета вещей». Список можно продолжать до бесконечности.

Внутренний язык программирования Эфириума иногда называют «сбывшейся мечтой Тьюринга». Это означает, что он очень гибок, универсален и позволяет писать программы самого разного предназначения.

Помимо легкого и доступного языка у структуры есть еще одно принципиально важное достоинство — поддержка работы смарт-контрактов. Как сформулировал криптотеоретик Ник Сабо еще до появления биткоина, смарт-контракт — это способ записать на языке программного кода инструкции по выполнению сделок согласно ранее достигнутой договоренности. Юристов нередко настораживает слово «контракт», употребленное в этом контексте. В конце концов, контракт — это имеющее законную силу соглашение между людьми. Машины могут лишь исполнять условия, прописанные в этих документах. Однако «проблемное» название не должно отвлекать от сути: досконально и гарантированно выполненное соглашение всегда очень полезно.

Возьмем простой пример: две стороны вступают в «контракт на разницу цен» — соглашение, напоминающее игру на бирже. Если приток данных с биржи уведомляет компьютер о падении или повышении цены некоего актива выше оговоренного уровня (обычно это уровень изначальной стоимости), то одна сторона должна выплатить второй разницу в цене. С помощью смарт-контракта на базе Эфириума сделки такого рода можно выполнять автоматически, не привлекая юристов, депозитных агентов и прочих посредников, поскольку обе стороны могут твердо рассчитывать, что сверхнадежная система будет функционировать именно так, как задумано. Смарт-контракты могли бы, например, немедленно передавать право собственности на товар в обмен на платеж в цифровой валюте, когда чип с поддержкой GPS определит, что партия товара попала на нужный склад. Такие компьютеризованные контракты, вероятно, произведут революцию в логистике и управлении цепями поставок.

После запуска Эфириума на Североамериканской конференции по вопросам Биткоина в январе 2014 года Бутерин сказал, что хотел бы создать нечто вроде «андроида для децентрализованных приложений» [11]. Это должна быть открытая платформа, напоминающая операционную систему Google для смартфонов, на базе которой пользователи смогли бы создавать и запускать любое новое приложение

на свой вкус — не на единственном сервере какого-нибудь провайдера, а в децентрализованной, «бесхозной» сети Эфириум. Тогда Бутерину было всего 19 лет; он бросил учебу на факультете кибернетики в Университете Ватерлоо, осознав, что развитие криптовалют идет полным ходом и не намерено его ждать. Потому он и решил создать общедоступный, децентрализованный глобальный суперкомпьютер. Это была дерзкая, поистине революционная идея. Сейчас, когда на платформе Эфириум работают более шестисот децентрализованных приложений, такой поступок кажется оправданным. Только за первые семь месяцев 2017 года внутренняя валюта системы — эфир — подорожала с 8 до 290 долларов. На тот момент полная рыночная капитализация эфира составляла около 25 миллиардов долларов, то есть половину стоимости Биткоина. Успех мгновенно сделал вундеркинда Бутерина мультимиллионером и возвел на пьедестал в глазах разбогатевших владельцев эфира и связанных с ним токенов. Однако в сфере, где сосредоточение власти в руках одной фигуры или организации считается худшим из грехов, многим кажется, что культ Виталика Бутерина зашел слишком далеко.

Технология Эфириума пока молода, недостаточно проработана и подвержена сбоям. Будучи открытой, общедоступной и универсальной, она дает злоумышленникам широкий простор для маневра. Система постоянно подвергается DDOS-атакам, при которых взломщики используют уязвимости кода, чтобы перегрузить сеть ведущих реестр компьютеров и парализовать их работу. Поскольку платформа изначально создавалась как общедоступная, с огромным количеством надстроенных программ, возникло множество лазеек, позволяющих злоумышленнику нанести вред сети.

Сооснователь Эфириума Джозеф Лубин еще больше усложнил ситуацию в результате запуска стартапа ConsenSys, чья главная задача — поиск новых применений для платформы Эфириум и разработка децентрализованных приложений. Команда Лубина выполнила очень важную миссию: продемонстрировала огромный потенциал этой технологии, что привлекло в сферу блокчейна многочисленные новые таланты. Кроме того, деятельность ConsenSys помогла внедрить идею децентрализованной архитектуры в сферу массовых компьютерных технологий. Сотрудничество с такими компаниями, как Microsoft, привело к появлению инструментов, позволяющих

разработчикам из стартапов и более солидных организаций создавать собственные децентрализованные приложения на базе Эфи-
[102] риума. Однако вместе с сотнями новых электронных кошельков и смарт-контрактов появляются и новые лазейки для злоумышленников, которые могут вывести систему из строя, а в худшем случае совершить крупную кражу. Так, из электронного кошелька Parity Wallet, разработанного сооснователем и главным инженером-архитектором Эфириума Гэвином Вудом для проведения платежей по смарт-контрактам напрямую через браузер, хакеры похитили 30 миллионов долларов [12].

Такие инциденты, безусловно, парализовали бы любую банковскую систему. Однако в сфере открытых разработок их скорее воспринимают как полезный урок, шанс сделать платформу надежнее. До сих пор каждый пользователь Эфириума действует по принципу *caveat emptor* — на свой страх и риск. По согласию сторон процесс обкатки и притирки рассматривается как совместное усилие, позволяющее улучшить и адаптировать Эфириум к нуждам пользователей. По крайней мере, так обстоят дела в теории. На практике же, если речь заходит о крупных суммах, владельцы всегда готовы защищать свои активы. Следовательно, успешные открытые проекты вроде Эфириума и Биткоина становятся ареной борьбы интересов. Бутерина и других основателей Эфириума — Лубина, Вуда и операционного директора Стефана Туаля — нередко критикуют за то, что они поставили личные интересы во главу угла. Конечно, такие трения ожидаемы, однако любопытно сравнить, как на них реагирует сообщество Эфириума и сообщество Биткоина.

Проект Эфириум с самого начала возглавляла вполне определенная группа лиц с продуманной стратегией развития и продвижения продукта. Создатели Эфириума были более склонны рассматривать свой проект как стартап, чем ранние энтузиасты Биткоина. Последний возник чуть ли не как подпольная ячейка — с анонимным создателем, который понемногу открывал свое детище узкому кругу добровольных пользователей и разработчиков, медленно, но верно готовясь к выходу в большой мир. Токены биткоина были созданы в первый день работы системы с нулевым балансом, и каждый, кто о них знал, мог подключиться к раздаче. Однако Эфириум провел «предварительный майнинг», заранее выпустив почти 70 миллионов токенов, которые

затем были проданы и распределены для сбора средств на разработку, управление, маркетинг и вознаграждение основателям. В 2014 году в ходе крупнейшей краудфандинговой распродажи такого рода Эфириум выручил за токены 18,4 миллиона долларов [13]. При этом 16,5 процента заранее созданных токенов (общей стоимостью 3,5 миллиона долларов по тогдашнему курсу) были отложены в отдельный фонд для основателей и разработчиков. Бенефициары фонда сказочно обогатились: к августу 2017 года те же самые токены стоили порядка 3,2 миллиарда долларов. Невероятный прирост почти на 100 тысяч процентов всего за три года!

Такая динамика развития при очень высоких ставках нередко порождает опасения, что интересы основателей перестанут совпадать с интересами рядовых пользователей. Во избежание этого была учреждена некоммерческая организация Ethereum Foundation, которая взяла на себя управление фондом криптовалюты и прочими активами, полученными от премайнинга и предпродаж; принцип переняли многие продавцы ICO-токенов. На данный момент Эфириум приносит такие богатства, что владельцы токенов склонны считать его создателей героями. Пожалуй, самая большая проблема — это культ успеха и уверенность, что разработчики никогда не ошибутся. Ведущие разработчики Эфириума исполняют роль руководителей компании в гораздо большей степени, чем команда Биткоина, хотя у них нет такой исполнительной власти, как у обычных директоров, поскольку сообщество пользователей может, как и в случае Биткоина, отклонить программные обновления. Но на практике они намного больше влияют на политику Эфириума, чем разработчики Биткоина.

Это стало особенно очевидно после взлома фонда The DAO, описанного в предыдущей главе. С помощью «белых хакеров» разработчикам удалось заблокировать счет The DAO, прежде чем взломщик вывел оттуда все средства, но ведь нужно было что-то делать с хищением 55 миллионов долларов! Руководство Эфириума знало, что похищенное можно вернуть, переписав программный код и изменив права на доступ к фондам, если действовать быстро, до истечения двадцати семи дней: на такой срок «заморозили» токены DAO. Вопрос был в том, нужно ли это делать? Когда небольшие изменения кода не дали результата, было решено пойти на радикальный шаг: основная группа разработчиков создала хардфорк блокчейна, выполнив обновление,

не имевшее обратной совместимости. Таким образом, все транзакции взломщика оказались недействительными с определенной даты. В криптовалютном сообществе это вызвало ряд вопросов. Многие пользователи посчитали, что задет ключевой принцип Эфириума — неизменяемость. Если группа разработчиков может аннулировать действия пользователя (пусть даже и неблаговидные), изменив реестр, то где гарантии, что в следующий раз его не подправят в интересах самих разработчиков или какой-нибудь другой группы? Разве это не подрывает саму основу системы?

Что ж, во многих отношениях лидеры Эфириума поступили как настоящие политики в ходе кризиса: пошли на непопулярные меры, которые кое-кому навредили, но все же были приняты для общего блага. Пожалуй, в этом случае процесс принятия решений можно назвать вполне демократичным. Организаторы не пожалели сил на объяснение своего шага, чтобы набрать голоса в поддержку хардфорка. Так же как в случае с планом Segwit2x и другими предложениями по реформе Биткоина, эта инициатива была бы отклонена, если б ее не поддержало большинство майнеров. В каком-то смысле меры, принятые командой Эфириума, оказались более демократичными, чем решения, принимаемые политиками от лица граждан, но без их участия. А поскольку сообщество Эфириума состоит преимущественно из инженеров-программистов, а не криптовалютных инвесторов, их споры по поводу хардфорка были куда менее ожесточенными, чем в сообществе Биткоина.

Более того, выяснилось, что недовольные пользователи Эфириума тоже не совсем лишены власти. Небольшая группа решила продолжать майнинг старой, исходной версии эфира, где средства взломщика по-прежнему фигурировали в истории транзакций. Они назвали свою версию Ethereum Classic, присвоили валюте обозначение ETC и начали торговать ею наряду с новым эфиром (ETH). Теперь Эфириумов стало два. Это раздвоение вызвало изрядную путаницу и привело к интересным арбитражным решениям, а кроме того, позволило трейдерам биткоина извлечь для себя кое-какие уроки к моменту разделения их собственной валюты. Однако его можно рассматривать и как ненасильственную акцию группы диссидентов, которые решили отстоять право на собственный путь. Сегодня, больше года спустя, Ethereum Classic по-прежнему существует, хотя его стоимость

по сравнению с новой валютой невелика. Это значит, что активы взломщика The DAO, чьи транзакции тщательно отслеживаются в открытом реестре Эфириума, сейчас стоят намного меньше, чем если бы их конвертировали в ETH.

Все эти кибератаки и мучительные попытки залатать дыры кажутся чистым безумием. Но давайте попробуем трезво оценить их масштаб. Разве они сравнимы с финансовым кризисом 2008 года? Или с размахом последующих скандалов на Уолл-стрит? Кроме того, каждый новый взлом становился ценным опытом и позволял улучшить платформу Эфириума, повышая ее надежность. Кибератаки также привели к появлению протокола Plasma, разработанного лично Виталиком Бутериным в тандеме с Джозефом Пуном — одним из создателей Lightning Network [14]. Подобно LN у Биткоина, Plasma выводит крупные транзакции и операции по смарт-контрактам в защищенную «внесетевую» зону, тем самым разгружая блокчейн. Если новый протокол заработает, Эфириум можно будет использовать в корпоративных масштабах. На фоне инновационного взрыва, подпитываемого миллиардными капиталовложениями, кибератаки кажутся мелкими и незначительными.

Тем не менее опыт Биткоина и Эфириума ясно показал, что управлять открытыми платформами и децентрализованными системами нелегко. Любые решения и перемены требуют консенсуса между разрозненными группами, чьи интересы часто конфликтуют. Однако творческая фантазия разработчиков в этой сфере такова, что любой барьер немедленно вызывает желание его преодолеть. Вот почему самые смелые и интересные находки возникают как отклик на проблемы и недостатки первых блокчейн-платформ.

На заре существования интернета немало прорицателей утверждало, что независимые компьютеры никогда не смогут безопасно подключаться друг к другу — главным образом потому, что на тот момент не существовало криптографических, юридических и прочих защитных механизмов. В итоге интеллектуальная мощь, брошенная на борьбу с этими проблемами, их успешно победила. Дальнейшее мы знаем из истории. Вероятно, аналогичного исхода надо ждать и в случае с блокчейном. В конце главы мы вкратце рассмотрим еще несколько новых решений, которые приближают нас к достижению таких целей.

Лучший Биткоин?

Один из главных недостатков биткоина и других ранних криптовалют сводит с ума криптографов, однако часто упускается из виду широкой публикой, — отсутствие конфиденциальности. Несмотря на расхожее представление о Биткоине как об анонимной платежной системе и резонансные истории о том, как хакеры и прочие злоумышленники с помощью криптовалюты заметают следы, в действительности блокчейн Биткоина — абсолютно открытый реестр. И хотя в нем не видно имен, а только численно-буквенные адреса, каждая транзакция видима и легко отслеживается. Это означает, что кто угодно (в том числе и представитель закона) может в итоге добраться до вас, особенно теперь, когда регулируемые обменники биткоинов должны придерживаться политики ЗСК («знай своего клиента»). Вот что вызывает тревогу у всех, кому небезразлично фундаментальное право человека на частную жизнь. Без подлинной конфиденциальности безграничный доступ в сферу экономики и социального взаимодействия так и останется зыбкой мечтой, полагают защитники личного пространства. Ведь принудительный «выход на публику» ограничивает нашу способность к самовыражению и свободной торговле. Поэтому многие программисты сейчас разрабатывают менее прозрачные криптовалюты.

Наверное, вы задаетесь вопросом: а разве нам не нужна возможность ловить хакеров-вымогателей в тот момент, когда они пытаются обменять полученный «выкуп» на доллары? Конечно нужна, но... Во-первых, если некая порция криптовалюты будет фигурировать в уголовном деле, это может изменить ее ценность по сравнению с другими единицами той же валюты. (Не забывайте, что история транзакций, в том числе и криминальных, заносится в блокчейн на веки вечные.) Как объясняет Зуко Уилкокс, создатель валюты Zcash, необходимо гарантировать полную равнозначность валютных единиц. Иными словами, «если вы хотите кому-то чем-то заплатить и у вас есть две одинаковые платежные единицы, то должно быть абсолютно все равно, какую из них вы отдадите» [15]. Например, каждая купюра номиналом в один доллар, один фунт или одну йену полностью равнозначна другой такой же купюре вне зависимости

от серийного номера. С биткоином так бывает не всегда. Когда ФСБ выставило на продажу 144 тысяч биткоинов (стоимостью 460 миллионов долларов по состоянию на август 2017 года), конфискованных у Росса Ульбрихта — владельца интернет-рынка нелегальных товаров Silk Road, эти «монеты» ушли по значительно более высокой цене, чем другие их эквиваленты [16], поскольку пользователи посчитали, что эта порция биткоинов официально «отмыта» правительством США. И наоборот, другие биткоины с запятнанной репутацией могут стоить меньше из-за риска потенциальной конфискации. Представьте, что наличность в вашем кошельке внезапно обложили десятипроцентным налогом только потому, что пять лет назад эти купюры побывали в руках наркоторговца, которого вы и в глаза не видели. По-вашему, это справедливо? По-нашему, не очень. Чтобы избежать подобных перегибов и приблизить криптовалюту к равнозначным наличным деньгам, Zcash использует сложный протокол «доказательства с нулевым разглашением», позволяющий подтвердить, что транзакция совершена без возможности отследить сумму, отправителя и получателя.

Zcash, как и другие анонимные валюты с высоким уровнем криптозащиты, такие как Monero и Dash, в последнее время привлекает к себе повышенное внимание, причем не только интернет-вольнодумцев и прочих любителей приватности, но и банкиров. Эти технологии манят их по вполне простой и понятной причине: банки не хотят, чтобы их сделки с клиентами выставлялись на всеобщее обозрение, поскольку это помешает вести дела. Вообще, в финансовом секторе наблюдается вспышка интереса к решениям, связанным с защитой конфиденциальности. В феврале 2017 года семь крупнейших банков мира, включая J.P. Morgan и UBS, объединились с компаниями CME Group, Intel и Microsoft для создания союза предпринимателей на базе платформы Эфириум и «разработки программного обеспечения коммерческого масштаба», отвечающего высоким стандартам мощности и, главное, конфиденциальности, в которой нуждаются крупные корпорации [17].

Не будем забывать и о технической проблеме, над которой бьются команды Биткоина и Эфириума: как добиться масштабируемости без риска, то есть проводить больше транзакций в секунду без создания уязвимой централизованной платформы. Есть и еще один сложный

момент, касающийся организации демократической правящей структуры, которая сможет решать проблемы безопасности. Два новых блок-
[108] чейн-стартапа, Tezos и EOS, активно ищут ответы на эти вопросы. Всего за 12 дней в июле 2017 года им удалось собрать 232 и 185 миллионов долларов соответственно, ненадолго заняв первое и второе места в истории краудфандинга [18]. (Вскоре рекорд побил стартап Filecoin, который собрал 252 миллиона долларов, причем бóльшую часть суммы — всего за один час.)

EOS — детище Дэниела Ларимера, одного из первых создателей децентрализованных приложений и распределенных организаций. В проекте также задействован известный криптограф Йен Григг, разработчик системы тройной записи. Block.one — компания, запустившая EOS, — позволяет майнерам заверять записи и подтверждать транзакции путем просмотра данных в сообщениях, что гораздо легче, чем просматривать всю историю баланса, как требуют другие открытые блокчейны. При меньшей вычислительной нагрузке EOS может обработать до 50 тысяч транзакций в секунду, а в будущем дойдет и до миллиона, как обещают создатели платформы [19].

Архитектура Tezos упрощает поиск консенсуса при изменении протокола. Система позволяет владельцам токенов Tez голосовать за специально назначенных делегатов, которые уполномочены одобрять пошаговые изменения протокола, и включает в себя гибкие и динамичные правила, позволяющие пользователям определять и развивать собственные модели управления. Когда книга готовилась к печати, жизнеспособность Tezos оказалась под вопросом из-за внутреннего скандала, о котором мы расскажем в главе 4. Доверие пользователей к новой платформе было подорвано, тем не менее вклад Tezos в развитие надежных систем управления все же следует признать весомым [20].

Безусловно, у каждой новой идеи есть недостатки, но, если привлечь команду талантливых инженеров, любая задумка может на шаг приблизить нас к идеалу децентрализации, функционального руководства, высокой пропускной способности и конфиденциальности. Так произошло с альтернативными криптовалютами вроде лайткоина, чей нестандартный подход к алгоритмам доказательства работы продемонстрировал, что отстранить крупных, «промышленных» майнеров от участия в добыче монет вполне возможно. Другие

валюты — в особенности верткоин, о котором мы поговорим в следующей главе, — улучшили и доработали модель лайткоина. Верткоину удалось избежать печального опыта биткоина, когда ничем не ограниченная борьба за награды породила множество энергоемких, дорогостоящих майнинговых предприятий.

Возникают также различные версии так называемого алгоритма доказательства доли, который наделяет пользователей правами на одобрение транзакций в зависимости от количества валюты на счету. Идея заключается в том, что, имея «шкурный интерес», валидаторы не станут мошенничать с реестром, который обеспечивает ценность их собственных активов. Критики этого алгоритма опасаются, что без дорогостоящего доказательства работы злоумышленники просто создадут многочисленные блоки и тем самым повысят свой шанс на внедрение фальшивых блоков в реестр. Однако недавно была разработана новая делегированная модель доказательства доли (ее преимущественно использует EOS) с более высоким уровнем защиты, которая так и называется — «делегированное доказательство доли». Она позволяет пользователям назначать ряд владельцев компьютерных узлов делегатами, чтобы они путем голосования оценивали работу и добросовестность майнеров. Таким образом, возникает представительный орган самоуправления в противовес исполнительным структурам.

Аналогия со структурами государственной власти отнюдь не случайна. Правила блокчейн-протокола, как мы уже не раз подчеркивали, в известной степени управляют нашим экономическим поведением. Многие организации делают ставку на то, что в будущем эта технология сформирует новый управленческий механизм для цифровой экономики в целом. Вот почему нам жизненно необходимо понять, как лучше всего управлять самими платформами. Есть хорошая новость: открытое, динамичное, глобальное состязание идей и изобретений почти ежедневно порождает новые инструменты. Возможно, «большие», признанные блокчейн-платформы вроде Биткоина и Эфириума позаимствуют что-то у новичков и внедрят в свою модель. Или, может быть, сочтут ставки чересчур высокими, откажутся от перемен и в итоге утратят нынешний статус. Не исключено и появление принципиально нового криптографического инструмента, который обеспечит совместимость и взаимодействие любых платформ.

Это позволило бы всем остаться на плаву и не допустило бы появления лидеров-тяжеловесов.

Что ж, будущее покажет. Главное, что нужно понять сейчас, — конкуренция между платформами важна и необходима. От того, кто будет решать, какие изменения вносить в новые экономические системы, зависит не только судьба биткоин-майнеров в Китае или технарей-криптографов в Кремниевой долине, но и наше общее будущее.

Глава

4

Экономика токенов [1]

В 14:32 по Гринвичскому меридиану 31 мая 2017 года компания из Сан-Франциско Brave Software, специализирующаяся на веб-инфраструктурах, открыла окно онлайн-продаж [2]. На торги было выставлено всего лишь одно наименование «товара», и через двадцать четыре секунды весь его запас — миллиард единиц — был распродан, а опоздавшие кусали локти от досады. Что же за товар вызвал такой ажиотаж? Компания Brave Software собрала около 35 миллионов долларов в ходе первичного предложения монет, или ICO, продавая токены базового доступа (basic access token, или BAT).

В конце весны и начале лета 2017 года мир охватила настоящая ICO-мания. За первые семь с половиной месяцев года в эту новую сферу инвестиций влилось почти полтора миллиарда долларов [3]. Подобно биткоинам, токены представляют собой уникальный конвертируемый цифровой актив, транзакции которого подтверждаются через открытый, децентрализованный блокчейн. Но, в отличие от биткоина, токены чаще всего предназначены для сделок в рамках отдельной отрасли или группы, использующей определенное приложение Dapp. Кроме того, токены не добываются путем постоянного майнинга, а создаются за счет однократной эмиссии специально для ICO.

Другие ICO-проекты собирали суммы, в шесть раз превосходящие выручку Brave Software. За один год было побито несколько рекордов краудфандинга. Однако распродажа токенов Brave (в намеренно ограниченном количестве, что редко бывает при крупных ICO)

примечательна невероятной скоростью. Очевидно, инвесторы поверили, что Brave предлагает токен, который может полностью изменить захиревшую отрасль контекстной и медийной рекламы. В качестве платежного средства для стремительной распродажи компания выбрала криптовалюту эфир, что вызвало некоторые опасения насчет инвесторов-тяжеловесов, которые могли вытеснить с поля менее крупных игроков. Однако этот выбор во многом объясняет и заманчивость уникального предложения Brave. За ним кроется первая серьезная попытка придать ценность ресурсу, который мы обычно раздаем бесплатно или с минимальной выгодой для себя, — нашему вниманию. Вот в чем подлинная сила новой идеи токенов. Они позволяют переосмыслить и переопределить саму природу обмена ресурсами, лежащую в основе любой экономики.

Дивная новая экономика рекламы

Любой, кому доводилось сражаться с надоедливыми всплывающими окнами, из-за которых виснет браузер и невозможно прочесть выбранную статью, знает, что рынок медийной и контекстной рекламы функционирует далеко не лучшим образом. Когда-то нам обещали исключительную точность, отличную аналитику, адресный маркетинг и более высокий доход от качественного контента. Сейчас же можно с уверенностью сказать, что у всех трех субъектов рекламной отрасли — авторов контента, рекламодателей и пользователей (зрителей/читателей) — есть основания для жалоб. Рекламные баннеры и непрошеные видеоролики не только мешают просматривать сайты, но и буквально пожирают трафик. (По некоторым подсчетам, абоненты мобильных операторов США платят около 23 долларов за просмотр ненужных им рекламных роликов [4].) Что касается рекламодателей, то «боты», которые генерируют ложные данные трафика, завышают стоимость объявлений на сомнительных сайтах. В итоге, согласно подсчетам Ассоциации рекламодателей США, в 2016 году индустрия потеряла 7,2 миллиарда долларов [5]. Между тем падение CPM — цены за 1000 просмотров баннера или ролика, базовой единицы ценообразования в области медийной рекламы — вредит крупным

интернет-изданиям, которые вынуждены конкурировать с бесчисленными альтернативными площадками для размещения контента: блогами, соцсетями и т. п. В итоге потребитель почти неизбежно выбирает блокировку рекламы: в 2017 году соответствующие программы были установлены на 600 миллионах мобильных и стационарных устройств [6]. Если так пойдет и дальше, крупные информационные агентства останутся без притока средств, необходимых для качественной работы журналистов.

Все это приводит к ухудшению качества информации и нездоровой системе поощрений, которая помогает авторам «фейковых новостей» завоевывать рынки и получать деньги за рекламу — главным образом благодаря лжи. Ложно все: и контент, предлагаемый читателям, и данные о трафике, предоставляемые заказчику рекламы. Таким образом, в выигрышном положении оказывается тот, кто сознательно распространяет заведомо ложные сведения ради власти или наживы. Вероятно, все мы, вне зависимости от политической позиции, согласимся, что подорванное доверие к качеству информации в среде, где некогда неоспоримые факты приходится подвергать сомнению, крайне опасно для демократических процессов и общества в целом.

Все это возвращает нас к невероятно успешной распродаже токенов Brave Software. Команда Brave во главе с Бренданом Эйхом (создателем универсального языка JavaScript Web) полагает, что токены, которые делают внимание публики ценным ресурсом, могут исправить перекосы в экономике медийной рекламы. Суть идеи — в разработке ценовых сигналов, которые побудят участников генерировать более качественный контент и предоставлять точную информацию об активности потребителей [7]. Эти (и многие другие) токены можно рассматривать как механизм поощрений и стимулов для общественно полезных видов поведения.

Как работают токены? Так же как протокол Биткоина побуждает пользователей к определенным действиям, которые служат интересам сообщества — в данном случае созданию и поддержке надежного, защищенного реестра транзакций, — программы, управляющие токенами, включают в себя стимулы и ограничения, поощряющие поступки, нацеленные на общее благо. Постепенно вырабатывается новое понятие — экономика токенов, основанное на убеждении, что в «программируемые» виды денег можно встроить механизм, позволяющий

направить сообщество к желанной и благотворной для всех цели. Возможно, токены помогут нам справиться с «трагедией общин». Если так, их роль в истории будет огромна.

Термин «трагедия общин» ввел в 1968 году эколог Гаррет Хардин [8]. В одной из своих статей он рассказал печальную историю о том, как английские фермеры XIX века истощили общественную землю, поскольку каждый фермер из-за опасений, что соседский скот съест больше, чем положено, стремился выгнать на пастбище как можно больше голов. Эта история давно уже воспринимается как напоминание о необходимости контролировать доступ к общественным ресурсам, например к земле. После появления статьи Хардина слово «общины» стало означать практически любую открытую «площадку», наделенную материальной или нематериальной ценностью, требующую охраны. Поэтому об интернете часто говорят как об «открытом творческом пространстве», которое, несмотря на свободу слова, должно быть защищено законами, соглашениями и гражданской активностью. Здесь прослеживается очевидная связь с давней экономической проблемой «внешних эффектов» (экстерналий): никакой рыночный механизм не может регулировать издержки, которые несет все население вследствие истощения некоего общего ресурса (например, когда завод загрязняет воздух).

Какое отношение все это имеет к медийной и контекстной рекламе? Самое прямое, ведь у этой отрасли есть свой, уже практически истощенный общий ресурс — «внимание пользователей», как называет его компания Brave. В интернет-среде идет ожесточенная борьба за глаза и уши публики, которую нужно завлечь и «развести на покупку», будь то рекламируемый товар или подписка на онлайн-газету. Увы, этим ценным ресурсом — вниманием — распоряжаются крайне бездарно. Начнем с того, чем нам, читателям и зрителям, возмещают затраченное время. По идее за внимание к рекламе нам должны «платить» доступом к новостям и прочей якобы бесплатной информации, которую мы желаем получить. Между тем рекламодатели платят авторам контента, чтобы частично перенаправить наше внимание на свой продукт (обычно против нашей воли). Пожалуй, в этом есть что-то нечестное.

Из-за ложной статистики просмотров и стихийного увеличения количества контента механизмы ценообразования в сфере медийной

рекламы становятся все менее точными. При этом подлинная цена пользовательского внимания, вероятно, растет. Как мы отмечали
[116] в главе 2, пользователи генерируют эксабайты ценных личных данных — часть активов нового типа, роль которых, по оценке журнала The Economist, в XXI веке будет сопоставима с ролью нефти в прошлом столетии [9]. Мы предоставляем ценнейший ресурс, а взамен получаем досадные помехи. Тем временем интернет-издания и рекламодатели, которые не способны даже адекватно измерить, а не то что привлечь внимание пользователей, на ощупь продираются сквозь груды бессмысленных цифр и придумывают ценовые механизмы, даже приблизительно не отражающие доступное количество ресурса. В этом и кроются причины сбоев, перекосов и общего нездоровья отрасли.

Компания Brave предлагает применить двунаправленную стратегию к решению проблемы. Команда создала новый браузер, полностью поддерживающий работу с токенами. Он по умолчанию блокирует любую рекламу и с помощью сложного аналитического алгоритма собирает и анонимизирует данные пользователей, показывающие, сколько времени они тратят на просмотр того или иного контента. Это позволяет адекватно оценить количество времени, не идентифицируя пользователя. Установив браузер Brave, вы сможете зарабатывать токены базового доступа. Для этого нужно выборочно отключить блокировку рекламы и просматривать объявления; токены будут поступать на встроенный кошелек, доступ к которому есть только у вас. Вы, в свою очередь, можете их использовать для вознаграждения авторов понравившегося вам контента, то есть фактически оставлять им электронные чаевые. А вот для размещения рекламы на интернет-площадках сначала нужно будет приобрести токены, а затем расплатиться ими с издателями, авторами или хостами. Цены на рекламные объявления будут определяться исходя из «статистики внимания» для каждого конкретного интернет-ресурса.

Все эти новые инструменты позволяют создать экосистему, в которой внимание вознаграждается непосредственно и по заслугам. Конечно, это вряд ли покончит с «журналистикой клика»: если Ким Кардашьян останется медийной звездой, то и посты о ней будут собирать рекордное количество токенов. Но возможность оставлять чаевые за контент интернет-изданиям позволит посылать им более тонкие,

информативные сигналы. Нельзя в точности предсказать поведение аудитории, но, скорее всего, пользователь охотнее станет платить за вдумчивую, тщательно проделанную работу, чем за откровенное фото, на которое кликнул, повинуясь мгновенному порыву.

Вне зависимости от того, добьемся мы повышения качества контента или нет, поощрение токенами кажется более справедливым механизмом оценки пользовательского внимания, чем те, которыми мы сейчас располагаем, так как непосредственно его вознаграждает. Пользователь получает токены за просмотр рекламы, и если спрос на оплачиваемые токенами объявления вырастет, то и цена их будет расти по мере перехода новых рекламодателей на эту модель. Соответственно, повысятся и доходы пользователей. Такие результаты гораздо больше отвечают всеобщим интересам, чем нынешняя система, при которой мы вроде бы просто соглашаемся посмотреть рекламу в обмен на доступ к нужному контенту, а на самом деле расплачиваемся своим временем и ценной информацией о себе и своих предпочтениях в интернете.

Эффективным было бы такое применение токенов, при котором обмен ими в определенной сфере влиял бы на экономическое поведение пользователей так, чтобы их интересы совпадали с интересами более крупных групп. Любители книг серии «Фрикономика», конечно же, знают, что экономическая наука прежде всего изучает стимулы — то, как ожидаемый результат заставляет нас покупать одни товары, воздерживаться от других или действовать различными способами [10]. Увы, нередко наши интересы и ожидания идут вразрез с ожиданиями других людей. Скажем, премии руководства фондов зависят от краткосрочной прибыли, тогда как инвесторы выиграли бы гораздо больше от долгосрочных стратегий. Экономика токенов — это попытка решить подобные проблемы, создавая программируемый эффект ценности (иными словами, рост цен), вознаграждающий тех, чьи действия приносят пользу обществу. В результате все интересы уравновешиваются.

В то время как обычной валютой можно по взаимному согласию обменяться где угодно и с любыми целями, криптотокен подчиняется внутренней программной логике, которая может ограничивать и регламентировать его использование. В экосистеме Brave за рекламные объявления разрешается расплачиваться только токенами базового

доступа. Другие подобные модели включают в себя, например, децентрализованную платформу хранения данных Storj, позволяющую пользователям, у которых закончилось место на диске, занять лишнее пространство других пользователей в обмен на токены. Существует также токен Gamecredits, который позволяет зарабатывать на продаже виртуального товара, такого как оружие и снаряжение, в сообществах геймеров, но только при условии, что продавец подтвердит наличие и качество товара. Для этого необходима история продукта и его программного кода, занесенная в журнал на основе блокчейна. По заявлению Gamecredits, мошенничество продавцов — главная проблема 15-миллиардного рынка виртуальных игровых принадлежностей [11].

В подобных системах деньги перестают быть морально нейтральным платежным средством; теперь они могут отображать общие ценности и интересы всех сторон, которые согласились их использовать. В системе Brave статистика внимания, отображенная браузером, диктует, кто получит токены и в каком количестве. Таким образом, рыночная стоимость внимания определяется гораздо адекватнее, чем при расчетах в традиционной валюте. Если проект Brave окажется успешным, цена на токены вырастет, что побудит больше пользователей присоединиться к сообществу и соблюдать правила просоциального поведения. Конечная цель — сетевой эффект, который будет подпитывать цикл общих стимулов и вознаграждений на рынке интернет-контента.

Подобные сетевые эффекты стали важнейшим источником силы для многих компаний в эпоху цифровой экономики. На них полагаются Amazon, Alibaba, Uber и другие цифровые гиганты, ведь успех всецело зависит от того, насколько широко распространяется идея и насколько эффективна обратная связь. Чем больше пассажиров используют Uber, тем больше водителей регистрируются в системе и тем легче становится найти попутную машину, что привлекает в систему новых пользователей, и так далее.

Эмитенты токенов утверждают, что могут стимулировать сетевые эффекты и циклы положительной обратной связи, хотя убедительных доказательств пока нет. Вероятно, успех будет зависеть от ликвидности каждого конкретного токена, то есть того, как часто им станут расплачиваться. В случае проекта Brave опасность состоит в том, что миллиарды выпущенных токенов будут расцениваться как долгосрочное

капиталовложение и инвесторы предпочтут их накапливать, изымая из оборота. Если это произойдет, цена токенов не сможет адекватно отобразить рыночную стоимость пользовательского внимания. Здесь необходима критическая масса *используемой* валюты, а не накопленные запасы.

Модель Brave предусматривает стратегию выпуска токенов для решения подобных проблем. Компания отложила 300 миллионов токенов в отдельный фонд «для привлечения пользователей». Так, например, планируется переводить небольшое количество токенов на встроенный электронный кошелек пользователя, когда он устанавливает браузер. Соответственно, токен становится инструментом поощрения и раскрутки, создания сетевого эффекта.

«Мы с самого начала хотели заложить в программу механизм, который позволит выдавать пользователям небольшое стартовое вознаграждение», — говорит CEO Brave Брендан Эйх [12]. Эту стратегию подсказал Эйху многолетний опыт работы в Кремниевой долине, где он создал универсальный язык программирования JavaScript, а затем стал одним из основателей компании Mozilla. Со временем он осознал, что инвесторы неохотно финансируют маркетинговые уловки по привлечению пользователей и что издержки на раскрутку уменьшают долевое участие основателей и первых вкладчиков. «Однако токены позволяют поощрить пользователей без всяких финансовых последствий», — добавляет Эйх и уточняет, что токен, в отличие от доллара, — «валюта социального кредита, не вызывающая девальвации фондов».

Давайте разберем это утверждение. Расходы (каковы бы они ни были) на выдачу токенов новым пользователям ложатся на плечи уже существующих их держателей; конечно, за счет этого их доля в общем фонде уменьшится. Но если, как предполагает компания Brave, вознаграждение новичков породит мощный сетевой эффект от расширения охвата, рост цен на токены с лихвой покроет все убытки. Суть идеи в том, что все издержки и риски несут пользователи Brave как сообщество (*социум*), а не сторонние инвесторы. Вот что подразумевает Эйх, когда говорит о социальном кредите.

Однако молниеносная распродажа токенов Brave вызывает и другие опасения. В частности, крупные инвесторы моментально перехватили инициативу, предложив высокие комиссии майнерам эфира. Майнеры

биткоина, ограниченные размером блока в 1 мегабайт, предпочитали транзакции на бóльшие суммы. Примерно так же и смарт-контракты Brave быстро вывели крупных покупателей вперед очереди. После того как миллиард токенов разлетелся за двадцать четыре секунды, выяснилось, что они осели всего-навсего на 130 счетах и двадцать самых крупных закупок покрыли более двух третей от общего количества. Такой дисбаланс вызвал неудовольствие многих инвесторов.

Некоторые полагают, что проблему породила предварительная фандрайзинговая распродажа на сумму 35 миллионов долларов, оставившая слишком мало доступных токенов, что и объясняет агрессивную стратегию анонимных покупателей, которым удалось добиться преимущества в системе [13]. Однако, по мнению других экспертов, компания Brave, решив ограничить прием средств, поступила с инвесторами справедливее, чем, скажем, блокчейн-стартап Tezos, у которого после рекордного сбора в 232 миллиона долларов на счетах оказалось гораздо больше, чем требовалось, из-за чего доли инвесторов обесценились [14]. Что же касается Брендана Эйха, то в интервью порталу CoinDesk он пожаловался, что было сложно нанять «таланты из Эфириума», отчасти из-за девятизначных сборов, которые позволили стартапам вроде Tezos обойти Brave в погоне за лучшими программистами [15].

Успех или неудача всех этих стратегий продажи будет в первую очередь определяться тем, помогут они или помешают развитию токенов в верном направлении: стать не средством финансирования, а «полезными» токенами (utility tokens). Иными словами, помогут ли они расширить сеть и гарантировать соответствующую работу каждого конкретного децентрализованного приложения. Но для того чтобы избежать столкновения с законом и обеспечить дальнейшее развитие платформы, эмитентам ICO придется доказать, что их токены — не инструмент спекуляций, а полноценный «продукт», программное обеспечение с определенной функцией. Вопросы статуса уже давно интересуют юристов и регуляторов, которые выясняют, можно ли отличить эти новые и пока спорные единицы обмена от ценных бумаг и освободить их от бремени законов и ограничений, применяемых к последним. От дальнейшего развития событий будут зависеть прибыли или потери инвесторов и пользователей, а также юридические последствия.

Золотая лихорадка

Внезапная вспышка ICO-мании тесно связана с успехом Эфириума. За 2016–2017 годы Эфириум стал основной платформой для работы приложений на базе смарт-контрактов и выпуска соответствующих токенов. Бурное развитие вызвало столь же мощный цикл положительной обратной связи, что привело к стабильному росту стоимости эфириума в первые восемь месяцев 2017 года.

Тридцатого июля 2017 года команда Эфириума отметила второй день рождения проекта шумной вечеринкой в одном из баров Манхэттена. С тех пор как девятнадцатилетний компьютерный гений осмелился мечтать о глобальной вычислительной системе без единого контролера, был проделан долгий путь. В то время многим казалось, что идея Виталика Бутерина неосуществима. И даже после присоединения к проекту разработчиков мирового класса, в частности англичанина Гэвина Вуда, Эфириум пережил несколько потрясений, включая потерю почти всей выручки от ICO из-за резкого падения цены биткоина [16]. Но к 2017 году многое изменилось. Эфириум начали обсуждать директора компаний из списка Fortune 500 и правительственные чиновники. Угловатое лицо Бутерина и его слегка растерянная улыбка стали появляться на обложках журналов. Об Эфириуме — его возможностях и ограничениях, потенциально судьбоносной роли — заговорили взахлеб (и часто без всякого понимания предмета).

Во многих отношениях залогом успеха Эфириума, как и биткоина, стало сообщество, которое собралось вокруг платформы и вложило всю свою веру и энтузиазм в мечту о децентрализованной глобальной экономике. Особенно важную роль сыграли встречи рабочей группы, оргкомитет которых в Нью-Йорке и устроил праздничную вечеринку 2017 года.

Сначала группа продала на праздник 300 билетов, а потом еще 40, поскольку спрос оказался огромным. Бар, в котором ожидали не более 50 человек, едва вместил всю толпу. Что же привлекло на вечеринку столько гостей? Цена эфира, внутренней валюты сети Эфириум, которая подскочила с 8 до 400 долларов за первые шесть месяцев 2017 года. И хотя потом курс упал до 200 долларов, те, кто купил эфиры в конце предыдущего года, все равно существенно разбогатели.

Неудивительно, что нашлось столько желающих присоединиться к проекту.

[122] День выдался великолепный: теплый, но не душный, с безоблачным ярко-голубым небом. Туристы с удовольствием позировали для фотографий на фоне Нью-Йорка: на востоке — позолоченный купол Нью-Йорк-лайф-билдинг, на юге — башня Метлайф-тауэр, на севере — внушительная громада Эмпайр-стейт-билдинг. На вечеринке собралось множество энтузиастов, от криптоветеранов вроде Джозефа Лубина, который помог Бутерину запустить Эфириум, а теперь возглавляет крупную поисковую лабораторию ConsenSys, до программистов-новичков. Как всегда в технических кругах, преобладали мужчины, однако и женщин нашлось немало, причем самого разного возраста. Гости обсуждали взлеты и падения биткоина и эфира, грядущие задачи, а заодно феномен ICO и цены на токены. Визитки раздавались тоннами. Гости на глазах сбивались в рабочие группы, строили планы, с ходу придумывали новые продукты, которые, по их представлениям, могли принести немалую выгоду.

Мы познакомились с молодой женщиной, которая несколько месяцев назад ушла с работы, чтобы открыть бизнес на платформе Эфириум. Затем поговорили с пожилым мужчиной, который двадцать семь лет проработал финансовым консультантом и теперь решил продать свою фирму, чтобы создать сервис на основе блокчейна. Паренек из поколения миллениалов — сотрудник Morgan Stanley — долго и терпеливо ловил момент, чтобы поговорить с Лубином: он мечтал присоединиться к Эфириуму, написать собственное децентрализованное приложение и заработать серьезные деньги. Мы спросили, есть ли среди его знакомых, друзей или коллег те, кто тоже интересуется платформой. «Да практически все», — ответил он.

Как финансовые журналисты мы наблюдали и описывали множество инвестиционных бумов. На наших глазах произошла первая вспышка серьезного интереса к биткоину в 2013 году, однако мы застали и куда более крупное событие: взлет и крах доткомов в 1990-х. Атмосфера того июльского вечера в Нью-Йорке как будто перенесла нас на десятилетия назад. Та же пульсирующая, физически ощутимая энергия, то же предвкушение скорого богатства. Как и при большинстве технологических прорывов, в воздухе витала смесь утопических мечтаний с жаждой наживы. Одни хотели изменить мир, другие — просто

разбогатеть. Многие полагали, что смогут получить и то и другое. Отчасти в этой лихорадке были повинны гигантские скачки́ цен. Курс биткоина за 2017 год вырос втрое. Эфир подорожал на 5000 процентов. Однако эти рывки были не единственным фактором. Подлинная суть перемен 2017 года заключалась в трех буквах — ICO.

Аббревиатура ICO (*initial coin offering*), как мы уже говорили, означает первичное предложение монет, то есть предпродажу криптовалюты или токенов на базе блокчейна. Распределение фондов в этом случае отличается от модели биткоина, где «монеты» изначально зарабатывались майнерами за счет вычислительных мощностей, используемых при выполнении доказательства работы, и выпускались по графику, заданному компьютерной программой без контролеров. В случае ICO, напротив, токены порождает сама распродажа, объявленная основателями платформы. В отличие от биткоинов, которые могут использоваться для любых целей, у токена узкое целевое предназначение и он применяется в рамках того приложения, для которого выпущен. Иными словами, эмиссии ICO непосредственно вливаются в проект, запущенный и управляемый основателями платформы, — прежде всего, чтобы покрыть стоимость разработки, а также чтобы вознаградить их и их инвесторов за взятый на себя предпринимательский риск.

Эта идея витает в воздухе уже несколько лет. Подобным способом были собраны 18,4 миллиона долларов для Ethereum Foundation; к нему прибегали и другие ранние блокчейн-стартапы. Но для того чтобы метод заработал на полную мощность, понадобился новый инструмент, созданный в лабораториях Эфириума под руководством немецкого программиста Фабиана Фогельштеллера, — прозрачная система смарт-контрактов для токенов, известная как ERC-20.

Новый стандарт инструкций для смарт-контрактов позволяет токенам сохранять единый, неизменный формат в ходе ICO и последующих продаж. Токенам больше не нужны собственные блокчейны и сообщества майнеров, поскольку теперь токены стандарта ERC-20 торгуются *на основе* Эфириума. Они генерируются смарт-контрактом, который отслеживает каждый выпуск и транзакцию. Как биткоину и любой криптовалюте, токенам по-прежнему требуется неизменяемый реестр, подтверждающий их статус как невоспроизводимого цифрового актива. Но благодаря стандарту ERC-20 для них не нужно создавать собственный блокчейн-реестр и затрачивать на это

отдельные вычислительные мощности. Вместо этого подтверждением операций займется уже существующая компьютерная сеть Эфириума.

Столь удобное и дешевое решение проблемы двойного расходования запустило целый конвейер ICO, проложив эмитентам легкий путь в глобальное инвестиционное сообщество. Больше никаких мучительных переговоров с инвесторами по поводу размытия долей или управления проектом. Никакой погони и никаких ухаживаний за банкирами с Уолл-стрит, чтобы встать в очередь за вложениями. Теперь не нужно ждать отмашки от Комиссии по ценным бумагам и биржам. Можно просто выйти к публике и сказать: «Вот мои токены. Они очень удобные. Покупайте их!» Появился простой, малозатратный алгоритм действий, который понизил входной барьер для многих блестящих новаторов с революционными идеями. Увы, он же оказался весьма привлекательным для мошенников.

Самый красноречивый пример того, что можно сделать с помощью стандарта ERC-20, оказался и самым скандальным — уже упомянутая нами кража средств из фонда The DAO в 2016 году. Когда Стефан Туаль, основатель Stock.it — стартапа, который запустил The DAO, — планировал ICO с токенами стандарта ERC-20, он предполагал собрать около 20 миллионов долларов — достаточно, чтобы поэкспериментировать с новой, непривычной моделью капиталовложения [17]. В итоге было собрано 150 миллионов. Отчасти это и послужило причиной катастрофы, ведь во время кибератаки на счетах были не только «экспериментальные» деньги, поэтому вкладчики потребовали возмещения. Тем не менее тот же результат показал другим желающим провести ICO, что вложения в нестандартные идеи для децентрализованных приложений не заставят себя долго ждать.

По иронии судьбы, именно уязвимости The DAO спасли Эфириум от последствий атаки. Эфир, который на момент взлома торговался в районе 20 долларов, просел до 8 долларов за следующий месяц. Ситуацию усугубил и хардфорк Эфириума. Но токены стандарта ERC-20 пишутся исключительно на основе платформы Эфириум, и смарт-контракты, которые их регламентируют, требуют оплаты в эфирах. Поэтому спрос на токены, резко возросший после рекордных сборов The DAO, более чем компенсировал падение курса. Появление стандарта ERC-20 поставило эфир в исключительно выигрышное положение.

Прежде биткоин был единственной валютой, в которой производился сбор средств при продаже токенов. Так было при первой распродаже токенов Эфириума в 2014 году и при других ранних ICO, в том числе провайдера децентрализованных хранилищ Maidsafe. Теперь же главной валютой ICO стал эфир. Чтобы инвестировать в очередную порцию токенов, нужно было покупать эфир; так образовалась восходящая спираль, которая благотворно повлияла на всех разработчиков в экосистеме Эфириума. Во-первых, созданные ими токены ERC-20 росли в цене, а во-вторых, теперь у них на счетах образовались запасы эфира. Часть была получена в награду за майнинг, еще часть приобретена как долгосрочное вложение или же как своего рода «топливо» для работы смарт-контрактов. А курс эфира взмыл в небеса. В свою очередь, позитивная отдача вдохновила других разработчиков на базе Эфириума создавать свои токены и выходить с ними на рынок, проводя ICO, что подстегивает спрос на эфир и ускоряет рост цен.

Ощущение, что происходит нечто экстраординарное, окончательно закрепилось в ноябре 2016 года, когда сайт под названием Golem, предлагавший платформу для торговли излишками вычислительных мощностей (он позиционировался владельцами как «Airbnb для компьютеров»), собрал 8,6 миллиона долларов за полчаса [18]. После этого стало казаться, что деньги сами придут в руки любому, у кого есть идея для приложения и горстка токенов. Первая заоблачная высота была взята в апреле 2017 года, когда стартап Gnosis, чья платформа позволяет пользователям создавать рынки прогнозов для любых ставок, продала 5 процентов своих токенов и выручила 12,5 миллиона долларов за 12 минут. Учитывая, что остальные 95 процентов были на руках у основателей, такие цены означали, что предполагаемая оценка проекта достигала 300 миллионов долларов. Эта цифра вскоре преодолела отметку в миллиард, поскольку на вторичном рынке токены Gnosis подорожали в четыре раза [19]. По меркам Кремниевой долины, это был первый ICO-стартап со статусом «единорога» (то есть достигший стоимости свыше миллиарда долларов). Правда, в отличие от других сверхприбыльных стартапов вроде Uber и Airbnb, компания Gnosis так ничего и не продала.

Между тем идеи для ICO продолжали поступать — порой блестящие, иногда крайне нестандартные или весьма сомнительные; многие, казалось, были явно рождены желанием попробовать и посмотреть, что

получится. По мере наполнения нашего почтового ящика в Wall Street Journal бесчисленными пресс-релизами очередных ICO на ум все чаще приходили сравнения с Pets.com — одним из самых печально известных доткомов 1990-х. Каких проектов нам только не присылали! REAL — риелторский сервис на базе криптовалюты. Prospectors — компьютерная игра, действие которой происходит во времена золотой лихорадки; токены игры предсказуемо именовались золотом. Paquiarium — группа, планирующая собрать десятки миллионов долларов и построить «самый большой в мире аквапарк». Инвесторы должны были выбрать место строительства путем онлайн-голосования и получить пожизненный бесплатный абонемент. Еще был некий «клуб для джентльменов» в Лас-Вегасе и токен под названием «кенкоин», который обещал полную анонимность при оплате интимных услуг. Компания Ahoolee мечтала создать поисковую систему для покупок онлайн. Все как один уверяли (хотя и не всегда убедительно), что их токены вознаградят сообщество пользователей, запустят цикл положительной обратной связи и обусловят масштабный сетевой эффект по мере разрастания сообщества.

Каждый день приходили новые электронные письма от частных лиц, которые тоже хотели «устроить ICO». Кто-то мечтал основать новую лигу регби. Кто-то собирал на производство переносного персонального кондиционера. Еще один пытался создать новую бюджетную авиакомпанию. Как-то раз Полу позвонил предприниматель, который прочел одну из его статей в Wall Street Journal и хотел побольше узнать о том, с чего начать ICO и как получить юридическую консультацию. По его словам, он пытался дозвониться Марко Сантори — одному из партнеров в юридической фирме Cooley, которая упоминалась в статье, — но так и не смог. Позже Сантори объяснил, что ему поступало так много звонков по поводу ICO, что он просто физически не мог ответить на все [20].

Почему же все эти люди решили запрыгнуть в один и тот же вагон? Ответ становится очевиден, если изучить данные портала CoinDesk. За первые семь с половиной месяцев 2017 года в ходе различных ICO было собрано свыше полутора миллиардов долларов [21]. Это намного больше, чем удавалось собрать любым блокчейн-компаниям традиционными методами привлечения капитала. И когда четыре предложения — Bancor, Tezos, EOS и Filecoin — в сумме получили 830 миллионов

долларов за два месяца, стало казаться, что приток средств будет лишь расти. В августе курс биткоина и эфира снова подскочил. На таком фоне ничто не могло омрачить общего настроения, даже июльское предупреждение от Комиссии по ценным бумагам и биржам, которая заявила, что часть предложений могут рассматриваться как ценные бумаги и подлежать регулированию.

И все же когда эта тенденция пойдет на спад? Когда переменится рынок и инвесторы осознают, что многие из купленных ими монет на самом деле пустышки. Вероятно, тогда мы все увидим, как лопнет гигантский мыльный пузырь.

«Большинство из них обречены на провал, — говорит Олаф Карлсон-Уи, глава инвестиционной компании Polychain Capital, о плохо продуманных затеях с недостаточной технической базой. — Многие по определению неудачны» [22]. Тем не менее Карлсон-Уи основал Polychain исключительно в целях инвестиций в ICO-проекты. В сущности, многие вкладчики подходят к ICO с характерных позиций венчурного инвестора. Они понимают, что большинство проектов пойдут ко дну, но надеются, что все же сумеют поставить несколько фишек на будущего победителя.

Надо отметить, что ICO — явление вполне демократичное. Если разработчики честно предупреждают о возможных проблемах, а инвесторы понимают, что делают высокорисковое вложение, ICO можно рассматривать как быстрый способ получить большую прибыль при высоких рисках, доступный не только венчурным инвесторам, но и широкому кругу желающих. В конце концов, почему только крупные инвесторы должны иметь преимущество на начальных стадиях? Эмин Гун Сирер, эксперт по криптографии и криптовалютам из Корнеллского университета, отмечает: «Венчурные инвесторы уже почуяли потенциальную угрозу. Это видно даже по их жестам» [23]. Когда речь заходит о традиционных формах вложений в ценные бумаги, венчурные фонды, частные инвестиционные фонды, хедж-фонды и тому подобное всегда обгоняют мелких инвесторов, поскольку свободны от ограничений, налагаемых на малый бизнес. Венчурные инвесторы имеют статус «аккредитованных инвесторов», что дает им право вкладываться в ценные бумаги, которые не выставляются на открытые торги, то есть обходиться без письменных предложений и других публичных процедур. Такие привилегии помогли им перехватить

инициативу во всех крупнейших начинаниях двух последних десятилетий: Facebook, Google, Uber.

[128] В наши дни, утверждает Гун Сирер, «маленький человек» тоже хочет получить свою долю и токеномания позволяет ему вступить в игру. Откуда взялись такие запросы? «У широких масс практически нет возможности удачно пристроить свои деньги. Им нужна отдача. Банки дают один, максимум два процента. Люди начали осознавать, что новые модели бизнеса приносят крупным инвесторам куда более высокую прибыль. Они готовы идти на риск». Сирера не смущает, что многие потеряют деньги. Это обычные издержки капиталовложения. «Да, кто-то примет решение, о котором впоследствии пожалеет. Но сообщество ICO-вкладчиков вполне самостоятельно и готово нести ответственность за свои поступки. По крайней мере, никто не бунтует, не протестует и не требует вмешательства закона. Процесс, который мы наблюдаем, очень интересен сам по себе».

Невероятно интересно было увидеть замкнутый мир венчурного капитала Кремниевой долины — почти исключительно мужской, известный сексизмом и громкими обвинениями в рукоприкладстве, — под сильным давлением извне. Дельцы с Западного побережья, всегда учившие робких предпринимателей и чиновников из восточных штатов жить по принципу «атакуй первым или атакуют тебя», внезапно сами оказались под прицелом, причем с разных сторон. Возникло даже некое противостояние Севера и Юга: если прежде инвестициями на ранних стадиях правили финансовые круги из Северной Калифорнии, то теперь несколько фондов, инвестирующих в токены, расположились в Лос-Анджелесе. В их числе CoinCircle во главе с Эриком Миллером и компания Crypto, применяющая под руководством чемпиона мира по покеру Рейфа Ферста особую стратегию вложений в токены, частично позаимствованную из предыдущего проекта Ферста — фонда Crowdfunder, который направляет средства мелких инвесторов в различные холдинги и стартапы, чтобы приоткрыть им ряд возможностей для венчурного инвестирования. Пока, конечно, рано делать прогнозы, но тем не менее забавно думать, что «Кремниевый пляж» в один прекрасный день может перегнать Кремниевую долину.

Неудивительно, что многие венчурные инвесторы решили вспомнить давнюю, проверенную стратегию: если не можешь разгромить, организуй и возглавь. Такие крупные компании, как Andreessen

Horowitz, Sequoia Capital, Union Square Ventures и Bessemer Venture Partners, объявили о планах инвестировать в токены через хедж-фонд Metastable Capital, созданный в 2014 году CEO краудфандинговой платформы AngelList Навалем Равикантом и другими известными предпринимателями [24]. В то же время ряд профильных блокчейн-инвесторов, таких как Pantera Capital под руководством Дэна Морхеда и Blockchain Capital во главе с братьями Бартом и Брэдом Стивенс, учредили фонды для вложения в токены. В игру вступили и ведущие юридические фирмы: Cooley, Perkins Coie, BakerHostetler, Debevoise Plimpton, MME и Sullivan Worcester. Они консультируют клиентов ICO по поводу отношений с законом. Похоже, профессионалы финансового мира все же захватывают площадки в сфере криптоактивов. Несмотря на лихорадочное состояние рынка токенов, крупные игроки привнесли в него не только новый размах, но и флер респектабельности.

Невзирая на все сетования о судьбе маленького человека в бизнесе, стоит отметить: как только в отрасль влились деньги инвесторов-тяжеловесов, результаты резко пошли вверх. Так произошло, например, с легендарным инвестором Тимом Дрейпером из Draper Fisher Jurvetson, чей дед Уильям Дрейпер и отец Билл Дрейпер практически создали венчурную индустрию в Кремниевой долине, а сын Адам Дрейпер стал одним из первых крупных инвесторов в биткоин и блокчейн-стартапы. Когда стало известно, что Дрейпер скупил часть токенов Bancor — платформы для запуска и продаж других токенов, — их ICO быстро побило все рекорды, собрав более 153 миллионов долларов [25]. Однако и этот результат вскоре был превзойден. Когда разнесся слух, что Дрейпер также заинтересовался Tezos — проектом супружеской пары Артура и Кэтлин Брейтман, — инвесторы немедленно вложили 232 миллиона в их новый блокчейн-стартап. «В декабре мне приснилось, что мы собрали 30 миллионов, — вспоминает Кэтлин Брейтман. — Я проснулась и подумала: как жаль, что это невозможно» [26].

Не исключено, что сейчас Брейтман жалеет о том, что реальная цифра превзошла самые смелые фантазии. Из-за гигантского сбора они с мужем оказались в зоне пристального внимания. Стали очень заметны и досадные задержки в разработке ПО, которые только увеличились из-за внутреннего конфликта четы Брейтман с Йоханом Геверсом — председателем якобы независимого фонда Tezos, отвечавшего за распределение средств [27]. Ссора стала достоянием

общественности и породила слухи, что Комиссия по ценным бумагам и биржам собирается расследовать деятельность компании [28]. Артур
[130] и Кэтлин Брейтман попытались пресечь эти слухи, заявив, что комиссия даже не пыталась с ними связаться.

Супруги Брейтман и подобные им предприниматели управляют стартапами в начальной фазе, когда обычно ищут финансовую поддержку бизнес-ангелов, а также друзей и родных. Но здесь мы наблюдаем нечто беспрецедентное — сбор огромных средств от широкого круга инвесторов, что, как правило, возможно лишь через несколько лет успешной деятельности и стабильного роста компании. Владельцам обычных стартапов, которые подолгу обивают пороги самых разных фирм в Пало-Альто и Маунтин-Вью только для того, чтобы выпросить ничтожные первые вливания в 500 тысяч долларов, это может показаться весьма несправедливым. То же относится и к более крупным компаниям, которым приходится осаждать юристов и регуляторов с Уолл-стрит, чтобы провести IPO — первичное публичное предложение акций.

Вспомним, например, на что пришлось пойти компании Blue Apron — изготовителю пищевых полуфабрикатов, — чтобы выставить акции на продажу и собрать 300 миллионов долларов в июне 2017 года. Изначально руководство компании намеревалось продавать акции по цене от 15 до 17 долларов за штуку, однако покупателей не нашлось [29]. Тогда цену понизили. Потом понизили еще раз. В итоге при первичном предложении акции торговались по 10 долларов. К тому времени компания Blue Apron продержалась на рынке около восьми лет. Ее выручка за предыдущий год составила 800 миллионов. У нее был свой продукт и неплохая история. А месяцем позже стартап под названием block.one, не проживший и года, провел ICO и собрал 185 миллионов долларов. В качестве продукта предлагалась еще не запущенная блокчейн-платформа EOS, разработанная для предпринимательских нужд. У создателей block.one имелись весьма интересные идеи, кроме того, они утверждали, что их блокчейн будет обрабатывать миллионы транзакций в секунду. Однако никто не давал гарантий, что результат совпадет с обещаниями.

И все же сравнивать децентрализованные платформы с традиционными компаниями вроде Blue Apron не совсем правильно. Теоретически любой владелец токенов получает прибыль от расширения

сервиса, сетевого эффекта и повышения стоимости. Платформы устроены не так, как традиционные организации с четко выделенным руководством и акционерами, у которых есть строго определенное право голоса в зависимости от доли в компании и конкретный источник выручки. Будущий «доход» (если его можно так назвать) от платформы block.one составит растущая стоимость токенов, прибыль от которой получат и пустят в оборот майнеры, разработчики и пользователи EOS; таким образом, обогатится каждый. В подобных сетевых проектах размываются границы между компанией, владельцами, руководителями, сотрудниками и потребителями. Поэтому можно сказать, что параллели с традиционными акционерными обществами здесь некорректны. Фактически именно это несоответствие ключевых принципов и понятий лежит в основе ожесточенных юридических дебатов.

Комиссия по ценным бумагам: предупреждение или зеленый свет?

Самую большую тревогу в сфере ICO вызывают действия государственных регуляторов, которые в любой момент могут «прижать» торговцев токенами и объявить о необходимости регистрации токенов в качестве ценных бумаг. Это может привести к краху рынка. В сентябре 2017 года прозвенел первый тревожный звонок: китайское правительство полностью запретило ICO [30]. Цены на все криптовалюты, включая биткоин и эфир, тут же упали. После этого шага многим популярным обменникам криптовалюты в Китае пришлось отказаться от работы с десятками токенов.

Что касается американской Комиссии по ценным бумагам и биржам, то хотя она и не предприняла официальных действий после краха The DAO, тем не менее свое мнение высказала четко. Токены, подразумевающие инвестиционные обязательства, могут рассматриваться как ценные бумаги и, следовательно, требуют регистрации, оглашения и прочих процедур, которые почти никогда не проводятся при ICO [31]. Правда, какие токены соответствуют стандартам The DAO, до сих пор непонятно. Комиссия не утверждала, что *все* токены будут рассматриваться как

незарегистрированные ценные бумаги, а заявила, что «этот вопрос будет решаться в зависимости от фактов и обстоятельств».

[132] Отдельные юристы, представляющие эмитентов токенов, оптимистически отметили: комиссия дала понять, что не станет автоматически приравнивать токены к ценным бумагам, и даже выразила поддержку инновациям на рынке капитала. Тем не менее высказывания чиновников негативно повлияли на сферу ICO. Гонконгская биржа Bitfinex весьма серьезно отнеслась к словам комиссии о том, что биржи и обменники токенов тоже могут подпасть под санкции, если позволят торговать незарегистрированными ценными бумагами на своей платформе, и предпочла не допускать американских инвесторов к торгам определенными активами, включая токены EOS.

Одна из причин такой правовой коллизии — невозможность вписать токены в традиционное определение. Многие из них (например, эфир) можно вполне убедительно представить как «продукт», необходимый разработчикам для создания новых приложений на децентрализованной платформе, связанной с определенным токеном. С другой стороны, цель большинства ICO — сбор средств. И судя по переговорам трейдеров на сайтах для торговли криптовалютой, многие инвесторы рассматривают токены как чисто спекулятивное вложение, от которого надеются получить прибыль. Их не интересует применение токена в качестве инструмента. Пока сложно сказать, повлияет ли такое отношение на работу Комиссии по ценным бумагам. Возможно, в результате она применит так называемый тест Хоуи и решит, что большинство токенов подпадают под определение ценных бумаг. Тест Хоуи — это американский правовой критерий, выработанный в 1946 году по итогам сложного судебного разбирательства. Согласно ему, если некая коммерческая операция подразумевает *вложение денег в общее предприятие*, от которого *ожидается прибыль*, полученная *усилиями третьих лиц*, то она подпадает под определение ценной бумаги.

Каковы бы ни были действия регуляторов, вся отрасль отчаянно нуждается в более развитой инфраструктуре инвестиций. Coinlist — проект Наваля Равиканта — разрабатывает стандартизированные подходы к продаже токенов, которые обеспечат инвесторам твердую юридическую почву и нечто вроде официального разрешения. Консалтинговые фирмы, в частности Coinfund, помогают инвесторам и эмитентам разобраться в принципах работы токенов. Уже появился бюллетень для

инвесторов Token Report — вероятно, первый из множества будущих изданий в этой сфере. Портал ICORatings.com проводит независимую оценку ICO и присваивает им рейтинг: «положительно», «стабильно», «рискованно», «отрицательно», «неосуществимо» или «мошенничество».

Инновации происходят и в юридической сфере. Компания Cooley предложила новый правовой инструмент под названием «Специальное соглашение по будущим токенам» (Special Agreement for Future Tokens, или SAFT), чтобы обеспечить юридическую поддержку и гарантировать соответствующее использование (на разработку и совершенствование платформ) стартапами собранных средств. Прообразом для соглашения послужил контракт под названием SAFE (Специальное соглашение по будущим ценным бумагам, Special Agreement for Future Equity), который профессиональные инвесторы иногда заключают с компаниями, планирующими выпуск акций. Соглашение SAFT будет заключаться с аккредитованными инвесторами, чьи ликвидные активы должны составлять не менее миллиона долларов, а доход — более 200 тысяч. Тем самым операция получит легальный статус с первых же дней. «В дальнейшем эмитенты будут использовать собранные средства для разработки платформы и сети, — поясняет Марко Сантори, юрист фирмы Cooley. — Только когда сеть будет отлажена, а токены начнут функционировать как полноценный продукт, их можно будет выставлять на продажу» [32]. Подобный контракт снимает риск, что регуляторы расценят ICO как выпуск *ценных бумаг*, если токены в момент продажи еще не станут частью работающей децентрализованной платформы. Многие инвесторы, очевидно, скупают токены в надежде на прибыль, которая должна стать результатом труда разработчиков. По словам создателей SAFT, это означает, что два критерия из теста Хоуи будут выполнены, и токены встанут в один ряд с ценными бумагами. Проблема в том, что, ограничиваясь только аккредитованными инвесторами, SAFT на шаг отдаляет нас от демократизации финансовой сферы, о которой мечтают многие сторонники ICO, например вышеупомянутый Гун Сирер.

Впрочем, похоже, ограничение доступа для инвесторов не слишком сократит доступ к фондам для смекалистых разработчиков. При первом же применении контракта сделка в рамках SAFT принесла команде стартапа Filecoin рекордный сбор в 252 миллиона долларов, затмив предыдущее достижение команды Tezos [33]. Файлкоины продаются как поощрительные токены для пользователей, готовых предоставить свой

жесткий диск в распоряжение IPFS — Межпланетной файловой системы. Это распределенная система веб-хостинга, которая в один прекрасный день, возможно, преобразит структуру Всемирной паутины.

Есть и другой способ распространить токены, выстроить сетевое сообщество и финансировать разработку платформы, избежав санкций Комиссии по ценным бумагам и не уронив себя в глазах сторонников криптовалюты, — применить старый добрый криптографический метод: внедрить токены в экосистему путем постоянного майнинга. В этих случаях отсутствует механизм предварительных продаж, которые вознаграждают основателей и финансируют дальнейшие операции. Разработчикам приходится состязаться с остальными майнерами за доступ к периодически выпускаемым токенам — так же как делал Сатоши Накамото с каждым новым блоком Биткоина.

При этой модели разработчики становятся и первыми пользователями, поэтому обычно получают фору в процессе накопления монет. Однако это не снимает проблемы справедливого распределения, особенно если задействован алгоритм доказательства работы. Ведь приоритетный доступ к токенам тогда получают владельцы более мощных компьютеров. И все-таки не каждая криптовалюта на основе майнинга непременно должна прийти к тому же, что и биткоин: доминированию крупнейших вычислительных комплексов промышленного уровня. Ряд новых альткоинов разработан так, чтобы противостоять «диктату мощностей». Это означает, что их встроенный алгоритм консенсуса — задачи, которые майнер должен выполнить, чтобы заработать монеты, — вынуждает компьютеры совершать различные действия, не всегда поддерживаемые супермощными интегральными схемами, по умолчанию установленными на машинах крупнейших майнеров биткоина. Суть идеи — не давать особых преимуществ владельцам дорогих однозадачных компьютеров. Следовательно, пользуясь относительно недорогими графическими процессорами (GPU), можно будет заработать вполне достойное количество «монет». Кроме того, возникает возможность более широкого распространения токенов.

Как правило, в итоге разработчики процессоров отвечают созданием новой интегральной схемы, способной обойти ограничения. Так произошло с оборудованием для майнинга, специально разработанным под алгоритм s-crypt системы лайткоина. Однако создатели верткоина вскоре доказали, что можно справиться с диктатом мощностей,

кое-что позаимствовав из практики реальных, а не цифровых организаций, а именно взаимное соглашение сторон, деловой пакт, то есть с самого начала прописать в механизмах управления платформой пункт о том, что пользователи обязуются признавать форк (изменение в коде), который будет добавлять новые защитные элементы каждый раз при появлении нового вида интегральных схем. Тогда сообщество пользователей сможет защитить распределенную демократическую структуру майнинговой сети на графических процессорах.

Тем не менее ICO, или распродажи токенов — называйте как хотите, — могут сыграть и, несомненно, сыграют немалую роль в реформировании рынка капиталов. И то, что вокруг этого революционного новшества уже формируется сообщество вкладчиков, диктуя более высокие стандарты, — хороший знак. Все больше профессиональных инвесторов выходят на рынок и осознанно применяют долгосрочные стратегии капиталовложения. Остается надеяться, что эти вливания породят фидуциарные стандарты, которые обяжут эмитентов проводить объективную оценку, отчитываться о расходовании средств и гарантировать попечительское управление полученными фондами.

Если все это сбудется, сфера ICO наконец перестанет напоминать Дикий Запад. Вероятно, сначала придется пойти на довольно болезненные жертвы, но они не будут напрасны и сыграют стимулирующую роль. Вспомним, что поистине новаторские интернет-технологии пришли в нашу жизнь лишь после того, как лопнул пузырь доткомов и закрылись проекты вроде Pets.com. Их неудачи проложили путь таким гигантам, как Google, Facebook и Amazon.

Золотой век открытых протоколов

Наибольшее внимание публики, разумеется, привлекает огромная выручка ICO. Однако самое ценное в нарождающейся экономике токенов — это перспектива появления новой экономической парадигмы, новых способов сохранить и приумножить общественные блага. Фред Уилсон, основатель венчурной компании Union Square Ventures, весьма убедительно описывает один из этих аспектов в своем блоге, утверждая, что токены приведут нас «в золотой век открытых протоколов» [34].

В свое время программистам не удалось заработать на открытых протоколах, которые легли в основу интернета, таких как базовая пара TCP/IP, веб-протокол HTTP и протокол электронной почты SMTP. А вот у нынешних разработчиков протоколов для новых децентрализованных платформ хорошие шансы разбогатеть, хотя их продукты вроде бы и находятся в свободном доступе. Таким образом, по мнению Уилсона, мы получаем мощный стимул для очередной волны инноваций, которая может изменить фундаментальную инфраструктуру цифровой экономики.

«Создатели открытых платформ, — пишет он, — больше не прикованы к университетам, правительственным лабораториям и прочим некоммерческим организациям, которым нет необходимости заботиться об акционерах». Если раньше эти учреждения чаще всего проигрывали коммерческим структурам в борьбе за инженерные таланты, то теперь платформы вроде Эфириума с легкостью привлекают лучшие умы. В их распоряжении — «коллективный разум» Всемирной сети: тысячи сообществ программистов, занятых разработкой открытого кода. Вот еще один аргумент в пользу того, что токены — как стимул для сохранения общих ресурсов — могут спасти человечество от трагедии общин и произвести эпохальный сдвиг в экономической реальности.

Экосистема токенов и открытых платформ пока очень мала в сравнении с традиционными рынками капитала и, несомненно, будет выглядеть совсем иначе, когда лопнет пузырь ICO. Однако уже сейчас в ней угадываются очертания принципиально новой, децентрализованной экономики будущего. Стартапы обещают нам, что вскоре все — от платформ для хранения цифровых данных и приложений для каршеринга до солнечных энергосетей и медийной рекламы — перейдет на децентрализованную модель и будет управляться с помощью токенов. Не исключено, что цифровые активы даже станут главным носителем ценности и средством обмена для всего человечества.

Цифровой бартер?

Многим из нас потребовался скачок в познании, чтобы понять: запись в никем не контролируемом цифровом реестре может исполнять роль денежного знака. Теперь нужно усвоить еще один урок: токены еще

сильнее изменят наше представление о деньгах. «Биткоиновые максималисты» полагают, что любые операции, связанные с цифровым выражением ценности, в конце концов перейдут на основу биткоина (если, конечно, сеть удастся масштабировать, не потеряв при этом в безопасности). Мечта об экономике токенов, напротив, предполагает фрагментацию инструментов оплаты. Если довести ее до логического завершения и разработать системы, которые обеспечат свободную конвертацию любых токенов, необходимость в общей криптовалюте для обмена может и отпасть.

Чтобы все это стало явью, понадобится мощная компьютерная программа, которая способна в режиме реального времени создавать рынки и генерировать перекрестную оценку любых двух вещей. Такая программа нам, например, подскажет, за сколько токенов Basic Attention можно приобрести право на треть картины Джексона Поллока. Мы окажемся в мире цифрового бартера — мире без денег в нашем нынешнем понимании.

Хотя эти планы могут показаться утопическими, уже сейчас есть немало желающих построить новый, альтернативный мир. По их представлениям, все наши материальные активы (машины, дома, яхты), равно как и нематериальные вроде брендов, можно отображать в виде надежно защищенных цифровых активов в неизменяемом блокчейн-реестре, а затем напрямую обменивать на другие подобные активы, устанавливая цену с помощью сети из миллиардов покупателей и продавцов. Эта идея давно заинтересовала швейцарского финансового технолога Ричарда Ольсена, чьи соображения мы приводили в конце книги «Эпоха криптовалют». Ко времени выхода книги из печати Ольсен уже начал претворять свою мечту в жизнь. Отчасти с помощью токенов он собрал 5 миллионов долларов и запустил стартап Lykke, чья задача — «разработать оценочно-поисковую систему, которая будет предлагать справедливую рыночную цену за любую цифровую монету вне зависимости от ее характера» [35]. Будучи уверенным, что проблема масштабирования блокчейнов так или иначе решится, Ольсен убежден, что открытые данные и свободные от посредников рынки на основе блокчейна позволят совершать любые транзакции цифровых активов с нулевой комиссией. Поэтому он намеревается развернуть на отлаженном новом рынке сеть высокоскоростных компьютеризованных механизмов для торговли. Подобно трейдерам с Уолл-стрит, они

будут «создавать рынки», обеспечивая финансовую ликвидность любым парам токенов: продавать одни, покупать другие. Так что, если найдется желающий обменять сотню токенов на треть картины Поллока, он сможет быть уверен, что платит разумную рыночную цену.

Мы как финансовые журналисты слишком хорошо знакомы с уловками крупных банков, которые намеренно делают ценовые механизмы непрозрачными, чтобы эксплуатировать инвесторов. Поэтому нам с трудом верится, что такая изощренная система может быть выгодной и эффективной. Однако Ольсен уверяет, что его «рыночным ботам» необязательно придерживаться людоедских правил Уолл-стрит, чтобы приносить прибыль. Машины будут вполне прозрачным образом зарабатывать на естественных краткосрочных колебаниях рынка, что станет возможным за счет высокой эффективности блокчейн-среды и низкой стоимости транзакций. По словам Ольсена, в этой прозрачной, свободной от эксплуатации системе ликвидность будет бесплатной. «Ведь в природе пчеле не нужно платить за нектар. Она просто садится на цветок и заодно опыляет его. А эффективная бизнес-модель — та, где есть пищевая цепочка».

Утопия? Конечно. Возможно ли это? Кто знает. Примечателен сам факт, что люди с глубоким пониманием рынка и технологий собирают средства на разработку систем, которые сделают деньги излишними. Похожие (хотя и менее стройные, чем у Lykke) концепции свободного обмена активами без помощи привычных денег возникают у многих экспертов, занятых проблемой совместимости реестров. Например, в лабораториях компании Ripple идет работа над проектом Interledger, который позволяет заключать двусторонние соглашения на основе смарт-контрактов с тем, чтобы обмениваться активами из двух отдельных реестров — открытых или закрытых [36]. Тем временем компания Tendermint уже представила протокол совместимости под названием Cosmos, который разработчики описывают как новый «интернет блокчейнов» [37]. У компании Web 3 Foundation есть похожая идея — «парачейн» Polkadot. Еще одно интересное решение проблемы совместимости может родиться из проекта сайдчейнов компании Blockstream или находок Таддеуса Дрийя, позволяющих протоколу Lightning Network совершать транзакции между разными реестрами. Можно предположить, что в будущем у нас не останется «валюты № 1», будь то биткоин или доллар.

Токены репутации

Идея цифровой системы ценностей с разнородными активами порождает представления о мире, где в токены можно конвертировать не только материальную собственность, но и нематериальное достояние вроде бренда или личной репутации. Фактически процесс конвертации уже идет.

Ряд стартапов — например, компания Loyyal из ОАЭ — разрабатывают на основе блокчейна новую систему вознаграждения за потребительскую лояльность с конвертируемыми баллами и бонусами. Если сейчас, скажем, покупая лекарства в местной аптеке, вы можете потратить накопленные баллы только в той же сети аптек, то токены Loyyal можно обменять на другие токены или на деньги. Вы спросите, почему продавцы позволяют клиентам это делать? Петер Рейшель, глава берлинской компании Leondrino Exchange, которая разрабатывает и продает брендовые токены, поясняет: «Стоимость токена — очень точная, поминутная мера успеха вашего бренда на рынке. Разумный и активный руководитель будет использовать ее как важный индикатор и стимул к развитию» [38].

А как насчет личной репутации? Стартап TokenStars планирует перевести в токены тот капитал известности, которым обладают звезды [39]. Таким образом, фанаты смогут приобрести, например, «кусочек» Роджера Федерера. Но что же тогда делать парикмахерам, юристам, строителям? Все ли профессионалы смогут воспользоваться токенами, чтобы монетизировать свой талант? Возможно, когда-нибудь не только сотрудники сферы услуг, но и вообще любой из нас сможет выставить свою репутацию для оценки на рыночной основе. Каждый человек сам по себе станет ценным активом.

Безусловно, подобные идеи порождают не только надежды, но и мрачные антиутопии о том, что в один прекрасный день наша способность прокормить семью будет зависеть от чужой предвзятой оценки нашей репутации. Что если общество станет еще более уязвимо для тирании масс — например, орды фанатов кинутся раскупать персональные токены Кэти Перри или Джастина Бибера, игнорируя при этом всех остальных? Тем не менее при адекватной системе поощрений, встроенной в алгоритм управления токенами, у нас есть шанс

превратить эту модель в нечто более ценное — дисциплинирующий рыночный механизм, который гарантирует прозрачность и ответственность. В эпоху, когда политики самого высокого ранга запросто торгуют «альтернативными фактами», а ученые уже открыто говорят об «обществе постправды», создание машины правды, которая сможет по достоинству вознаградить честность, выглядит весьма заманчиво.

Блокчейн-стартап Augur уже исследует подобные идеи. Компания создала на платформе Эфириум децентрализованный криптовалютный рынок прогнозов, где каждый участник может сделать ставку на исход того или иного события, причем результат зависит от подтверждения со стороны определенных лиц. Подтверждающая сторона ставит на кон свои репутационные токены и утверждает, что говорит правду. Если большинство пользователей согласно, что правда именно такова, система возвращает токены и выплачивает денежное вознаграждение. Есть риск, что большинство сможет заставить систему играть против «продавцов истины», однако для поощрения честности с обеих сторон существуют и другие бонусы и выплаты. В статье для журнала Wired Кейд Метц рассуждает о будущем этого проекта и приходит к выводу, что благодаря ему могли бы появиться специальные «проверочные комиссии», которые либо подтверждали, либо опровергали бы заявления политиков; за подобную услугу, пожалуй, охотно бы платили информационные агентства [40]. Нам бы очень пригодилась система, в которой материальная выгода совпадает с потребностью в правде, — если, конечно, такую систему действительно можно создать.

На пути к экономике токенов

Рассуждая о том, каким образом токены могут поощрить нас за честность и открытость, а также помочь сохранить общественные блага, нельзя не задаться вопросом: помогут ли токены в борьбе с самой серьезной угрозой, нависшей над нами?

Изменение климата — наибольшая опасность для человечества. Эрик Миллер выдвинул идею, как ее предотвратить. Миллер — предприниматель и венчурный инвестор из Лос-Анджелеса; работал

в Голливуде, вкладывался в первые доткомы и сыграл важную роль в разработке «умных» очков Snapchat. Теперь он мечтает «токенизировать» мир с помощью инвестиционного фонда CoinCircle. В ходе работы Миллер и его партнеры сформулировали понятие «экономики криптоэффекта» (crypto-impact-economics).

Исходя из этой концепции, команда Миллера, куда входят профессор экономики из Калифорнийского университета Бхагван Чоудхри и специалист по охране вод Мирового океана Грегори Стоун, разработала два специальных токена — Ocean Health Coin и Climate Coin, — которые будут распределяться между важнейшими инстанциями в сфере охраны климатических ресурсов: корпорациями, правительствами, потребителями, неправительственными и благотворительными организациями [41]. Они, в свою очередь, смогут использовать токены для оплаты ряда программ, связанных с углеродными квотами и уменьшением выброса вредных веществ. Предполагается также создать резерв токенов и передать его под контроль Всемирного экономического форума, чтобы вручную управлять стоимостью этой валюты. Суть идеи — в безвозвратном уничтожении части резерва всякий раз, когда международные научные организации будут докладывать о достигнутом прогрессе в борьбе с загрязнением и выбросами углерода. Уничтожение токенов с помощью криптографической функции создаст их дефицит и, следовательно, повысит ценность. Таким образом, у владельцев появится стимул действовать в интересах окружающей среды сейчас, а не в отдаленном будущем.

Сложно предсказать, сработает ли эта идея. Однако в ней есть нечто новое и свежее — стремление напрямую обратиться к истинной проблеме, которая стоит за нашей неспособностью обуздать климатические изменения, — а именно столкновению экономических интересов. Многие правительства — например, администрация Трампа — до сих пор остаются заложниками добывающей промышленности, что не позволяет им всерьез заняться вопросами экологии. Так почему бы не обойти правительственный уровень и не сменить политику с помощью компьютерных рычагов воздействия на финансовые потоки?

В печальном состоянии нашей планеты прежде всего повинно нынешнее устройство глобального капитализма, при котором деньги стали не просто средством обмена, а фетишем, статусным символом, призванным демонстрировать власть и силу. Ради будущих поколений

мы должны хотя бы попытаться перекроить систему и навести порядок на земле. Возможно, в этом нам помогут цифровые деньги, ведь
[142] они представляют собой не конечную цель, а просто инструмент для обмена и коллективного созидания ценности, то есть то, чем деньги по определению и должны быть.

Конечно, загрязнение окружающей среды — не единственная претензия, которую мы можем предъявить глобальному капитализму и поддерживающему его политическому строю. Налицо явный разрыв между стремлением политиков принимать законы в угоду своих корпоративных спонсоров и интересами избирателей, которые они по логике должны защищать. Массовое представление о выходе на пенсию как о желанной конечной цели породило когорту фондовых менеджеров, которые ежеквартально получают краткосрочную прибыль; при этом почти никого не волнует, что произойдет с теми же активами, когда старение общества еще сильнее понизит экономическую продуктивность. Подобные конфликты интересов подпитывают терроризм, насилие, страхи за будущее и реальный риск того, что эта гремучая смесь протекционизма, национализма и ксенофобии в один далеко не прекрасный день выльется в полномасштабный вооруженный конфликт.

Однако с цинизмом отнестись к перспективе перемен — значит заранее сдаться. Поэтому мы призываем всех читателей поразмышлять об альтернативных моделях посткапиталистического общества и представить новые технологии в качестве платформы для будущего, в котором человечеству уже не придется выбирать между рухнувшей коллективистской утопией социализма и централизованной политической экономикой крупных монополий, охраняемых государством. Изложенные нами идеи предлагают выход из ловушки, но для этого необходимо изменить представления о создании ценности. Вместо актов обмена — услугами, активами, идеями, — определяющих нашу жизнь, которые мы склонны рассматривать как средство для приобретения денежных сумм, символически выраженных банкнотами и прочими знаками, мы должны исследовать новые модели создания ценности (на основе токенов или чего-то другого), которые поощряют сотрудничество для общего блага.

Накопление богатства никогда не бывает игрой с нулевой суммой. Если активно участвовать в схеме, запускающей положительный цикл

инклюзии, инновации и эффективности, можно накопить капитал путем его создания, а не отъема. При правильном подходе новые экономические системы могли бы мобилизовать энергию рынка для максимально эффективного использования ресурсов планеты в целях всеобщего процветания, чтобы больше не поощрять управленцев с завышенной зарплатой к строительству гигантских теплоэлектростанций. В следующей главе мы подробнее поговорим о том, как технология блокчейн помогает переосмыслить экономическое устройство мира.

Глава

5

Четвертая промышленная революция

Вы, наверное, думаете, что если человек сидит перед 65-дюймовым телевизором с функцией Smart TV и запоем смотрит свежие эпизоды «Ходячих мертвецов» на канале Netflix, то он просто любитель хороших историй о зомби. На самом деле он еще и футурист. Знаете почему? Потому что его «умный» телевизор не только показывает программу, которая идет в эфире, — это один из миллиардов приборов, подключенных к так называемому интернету вещей: огромной сети устройств, таких как телевизоры, автомобили, электросчетчики, камеры видеонаблюдения и т. д., запрограммированных на обмен информацией — фактически «разговоры» друг с другом. Вероятно, в последние несколько лет вы уже не раз слышали об «интернете вещей», но пока не осознали, что его время уже пришло.

С тех пор как в середине XX века появились первые машины, которые можно назвать компьютерами, прогресс движется семимильными шагами. Уже 20 лет назад любой студент-кибернетик мог собрать полупроводниковую микросхему, превосходившую по вычислительной мощности первые ЭВМ, занимавшие целую комнату, не говоря уже о крошечных процессорах в современных гаджетах, которые в тысячи раз мощнее. Процесс обработки данных больше не привязан к одиночным компьютерам; вычисление все чаще происходит в сети устройств. Вот почему «интернет вещей» так важен. Дело не в том, что мы поставили себе на службу миллиарды новых вычислительных устройств, а в том, что, объединяясь, они создают вычислительную махину,

которая бесконечно больше суммы своих частей. На заре интернета знаменитый программист Джон Гейдж из Sun Microsystems бросил меткую фразу: «Сеть и есть компьютер». В наши дни его слова сбылись. Мы придумываем новые способы управлять мощью этих систем, а тем временем вычислительные способности «всеобъемлющего компьютера» растут с каждым очередным добавленным устройством. Наступил важный момент в жизни всего общества. Пойдет ли вся эта мощь на благо или во вред человечеству, пока сложно определить. Надежный и добротный механизм установления истины, встроенный в новые сети, помог бы нам гарантировать, что грандиозные виртуальные машины станут нашими друзьями.

Перенос вычислительных мощностей в сеть изначально стал возможен благодаря проводному интернету, затем продолжился с помощью мобильных технологий, а теперь разнообразные беспроводные соединения связали все это воедино. Однако не будем забывать, что рост сетевых мощностей также обусловлен программным обеспечением, которое раскрывает безграничный информационный потенциал сетей. Анализ данных усложняется все больше: компьютеры добывают и обрабатывают огромные массивы информации, порожденной бесчисленными сетями, чтобы вывести алгоритм поведения самых разных групп. Вспомним, с какой точностью и скоростью транспортные приложения вроде Waze прокладывают оптимальные маршруты и рассчитывают время в пути или насколько важен анализ публикаций в Twitter для политических кампаний. Самообучение машин выводит аналитику на принципиально новый уровень, поскольку каждый отдельно взятый компьютер подстраивает свою работу под те данные, которые получает из сети, и становится все мощнее за счет цикла обратной связи.

Однако мы полагаем, что новые виды ПО, которые максимально обогатят наши знания социальных явлений, будут основаны на базе блокчейна либо созданы по его подобию. Без протоколов распределенного доверия сфера применения виртуальных машин останется ограниченной. Данные, контролируемые централизованными, доверенными третьими сторонами, ограниченны по определению. Во-первых, они доступны широкому сообществу только за отдельную плату. Во-вторых, недоверие к монополистам может привести к сокрытию информации провайдерами. «Всемирный мозг» не может

появиться в экономике, где доминирует централизованная модель доверия. Разработки блокчейн-сетей едва ли привлекут такое же внимание СМИ, как «умные» двери и беспилотные автомобили, однако именно на их основе сложатся вычислительные мощности «интернета вещей», где десятки миллиардов устройств — от дверных замков до автомобилей — смогут самостоятельно «общаться» и торговать друг с другом.

По словам основателя Всемирного экономического форума Клауса Шваба, мы стоим на пороге «четвертой промышленной революции» не потому, что вот-вот появится определенная линейка новых продуктов, а потому, что сочетание различных технологий начинает порождать принципиально новые системы: мобильные устройства, сенсоры, нанопроцессоры, возобновляемые энергоресурсы, нейроисследования, виртуальную реальность, искусственный интеллект и т. п. [1]

Объединив миллиарды собирающих и обрабатывающих данные машин в глобальную, всеобъемлющую сетевую архитектуру, мы в корне изменим принципы взаимодействия с миром. Это означает, что *материальный* аспект нашей жизни в плане как природных ресурсов, так и произведенных товаров будет всесторонне измерен, проанализирован и объяснен, что позволит достигнуть его полного *дематериализованного* понимания.

Новая сеть вычислительных и сенсорных систем поможет нам четко представить, как функционирует мир вещей: насколько быстро работают, до какой температуры нагреваются или охлаждаются наши устройства, насколько они эффективны и надежны и насколько нам хватит определенного ресурса, будь то заряд аккумулятора, источник воды или запас кислорода. Столь подробная, актуальная и достоверная картина могла бы научить нас более бережному обращению с ресурсами планеты (отнюдь не безграничными), а также подсказала бы, как отладить экономические процессы, нарастить или хотя бы улучшить производство товаров (например, продуктов питания, инструментов), чтобы привнести комфорт и процветание в жизнь землян.

Представьте себе мир, где сеть наземных датчиков и сверхточный механизм обработки данных могут выявлять проблемы с мостом задолго до того, как он рухнет. Представьте себе мир без пандемий, поскольку врачи отслеживают распространение вирусов в режиме

реального времени и купируют их в момент заражения. Что ж, такая революция не состоится — оптимизировать информационный поток будет просто невозможно, — пока мы не создадим распределенную архитектуру, способную решить проблему доверия. Если выстроить централизованный «интернет вещей», огромные хранилища собранных устройствами данных будут монополизированы компаниями-гегемонами. Эти лакомые куски неизбежно привлекут грабителей и вызовут кибератаки беспрецедентного масштаба. Ущерб от взломов будет намного серьезнее, чем сейчас. Когда хакеры получают доступ к вашей почте — это уже плохо. А теперь представьте, что они получили доступ к вашему термостату, автомобилю или муниципальной системе управления транспортом. В эпоху интернета безопасность уже стала проблемой мирового масштаба, и без повышения уровня киберзащиты нас ждет настоящий хаос.

Итак, давайте для начала рассмотрим саму структуру «интернета вещей» и то, каким образом принцип распределенного доверия из сферы технологии блокчейн можно применить в новом подходе к управлению материальным миром.

Спасти «интернет вещей» от самого себя

Как только возник ажиотаж вокруг «интернета вещей», эксперты по кибербезопасности начали оценивать риски от бездумного внедрения технологии, которую практически невозможно контролировать. Худшие сценарии представить было несложно: взломщики получают доступ к вашему жилью, автомобилю, телефону, телевизору, истории болезни и судимостей, политическим взглядам. При поддержке правительства хакеры дистанционно управляют самолетами, автострадами, кабинками для голосования, электросетями. Террористы убивают тысячи жертв, просто отключив им кардиостимуляторы. В 2016 году киберэксперт Брюс Шнайер подробно изложил возможные последствия в статье для журнала Motherboard: «Одно дело, если ваш "умный" замок используют, чтобы отследить, кто сейчас дома. И совсем другое — перенастроить его так, чтобы он впустил вора или не позволил вам открыть дверь. Хакер, который может перехватить управление вашим

автомобилем, гораздо опаснее того, кто может подслушать ваш разговор или отследить ваши перемещения» [2].

[150] По словам Шнайера, «интернет вещей» и другие киберфизические системы «дают интернету руки и ноги, то есть способность напрямую воздействовать на физический мир. Сегодня мишенью для кибератак служат данные и информация. Завтра ею могут стать плоть и кровь, сталь и бетон». Необходимость постоянных обновлений лишь усугубляет проблему. Мы уже сейчас едва успеваем загружать новые патчи безопасности для Microsoft и разных приложений, а представьте, что вам придется обновлять ПО на подключенном к интернету холодильнике. (Эту проблему со всей наглядностью выявила атака на серверы DNS-провайдера Dyn, осуществленная с помощью плохо защищенных устройств.) Чтобы сделать «интернет вещей» инструментом, который помогает, а не мешает нам жить, необходимо переосмыслить основные принципы его безопасности.

Используя наработки в сфере аналитики, облачных вычислений и других программных технологий для коммерческого применения, компания IBM стала крупным игроком в создании инфраструктуры для «интернета вещей» и сейчас активно осваивает блокчейн. В широко известной статье под названием «Демократия устройств: спасаем будущее “интернета вещей”» двое научных сотрудников компании сосредоточились на центральной этической проблеме — как обеспечить доверие [3]. Как и кому можно доверить управление глобальной сетью из миллиардов устройств, которые будут курировать буквально каждое наше действие? Одно дело, когда частная компания (например, Comcast) предлагает миллионам клиентов относительно простой сервис — скажем, кабельное вещание, и совсем другое — когда монополисту предоставляются все конфиденциальные данные, которые проходят через ваши устройства. Если вас уже сейчас беспокоит тот факт, что о вас слишком много знают Google, Amazon, Facebook и Apple, представьте, что будет в эпоху централизованного «интернета вещей». Когда все транзакции проходят через две-три гигантские корпорации, это, во-первых, неэффективно с точки зрения обработки данных и управления системой, а во-вторых, дает контролирующим инстанциям такую полноту власти, что ужаснулся бы даже Джордж Оруэлл. Мы действительно хотим, чтобы Amazon Web Services или другой крупный провайдер облачных хранилищ располагал нашими ценными

данными? Тогда эта корпорация не только окажется в беспрецедентно выгодной позиции для наблюдения за нашим имуществом и поведением, но и возьмет на себя исполнение миллиардов транзакций в токенах и криптовалюте. Только представьте, что будет в случае сбоя или неполадки!

В качестве альтернативы можно было бы передать контроль правительственным структурам. Но если вам стало не по себе от заявлений Эдварда Сноудена — «АНБ прослушивает телефоны граждан», — то вообразите, что спецслужбы получили неограниченный доступ к личным данным, поступающим с ваших устройств. Нет уж, спасибо! «Интернет изначально строился на принципе доверия, — пишут сотрудники IBM Вина Пуресваран и Пол Броди. — Но после разоблачений Сноудена стало очевидно, что эра доверия в сети закончилась. Концепция "интернета вещей" как централизованной системы с доверительными отношениями между партнерами — не более чем фантазия».

По мнению Пуресваран и Броди, технология блокчейн — единственная основа, на которой можно выстроить «интернет вещей» так, чтобы никто не мог его контролировать. Блокчейн обеспечил бы ему полную неуязвимость. В ситуации, когда устройства регулярно обмениваются ценностями, блокчейн нужен для того, чтобы их владельцы доверяли друг другу. Как только структура децентрализованного доверия будет создана, перед нами откроются совершенно новые горизонты.

Давайте немного помечтаем о будущем. Представьте, что вы поехали на электромобиле Tesla за город, чтобы погулять на природе, и на обратном пути обнаруживаете, что запас энергии почти на нуле, а ближайшая станция подзарядки далеко. В условиях шеринговой экономики на основе блокчейна у вас не возникнет ни малейших проблем. Вы сможете подъехать к любому дому, чьи владельцы согласны предоставить доступ к зарядке, и заплатить им за электричество в любой криптовалюте. Для оплаты вы используете скоростной протокол вроде Lightning Network, и токены моментально уйдут с электронного кошелька вашей машины на кошелек домового электросчетчика. Однако при этом вы понятия не имеете, кому принадлежит дом, что за люди его владельцы, не обкрадут ли они вас, не заразят ли компьютер вашего автомобиля каким-нибудь вирусом, который уведет с кошелька все средства. У хозяев дома возникнут аналогичные вопросы на ваш счет,

к тому же они никак не смогут проверить вашу платежеспособность. Но вот в чем дело: при наличии системы распределенного доверия —
[152] например, на основе блокчейна — легитимность транзакций и надежность устройств будут подтверждаться благодаря неуязвимому реестру, которому смогут доверять обе стороны. В такой ситуации недостаток знаний друг о друге не имеет значения. Система распределенного доверия позволяет совершенно незнакомым людям — и, что еще важнее, их гаджетам — обмениваться ценностями.

Системы, за которые ратуют Пуресваран и Броди, должны обеспечить легитимность миллиардам транзакций в общей глобальной сети объединенных устройств. При такой модели мы будем обмениваться лишь теми данными, которые необходимы для подтверждения надежности каждого устройства, а не выплескивать в открытое пространство целый поток конфиденциальной информации. Иными словами, когда ваш автомобиль обменяется криптовалютой с электросчетчиком, ни вы, ни хозяин дома, ни любой другой пользователь или валидатор блокчейна не получит доступа к личным данным участников сделки.

«В нашей концепции децентрализованного "интернета вещей" блокчейну отводится роль платформы, которая облегчит обработку транзакций и взаимную координацию подключенных устройств», — пишут Пуресваран и Броди и далее объясняют, каким образом система распределенного доверия поможет гораздо эффективнее использовать устройства и технологии, поскольку не нужно будет опасаться, что устройство-партнер сработает нам во вред. «Каждое устройство исполняет свою роль и контролирует собственное поведение. В результате получается *интернет децентрализованных, независимых вещей*, то есть происходит демократизация всего цифрового мира». В каком-то смысле общество машин начнет создавать и накапливать свою версию социального капитала.

«Доверенные» вычисления

И все же остается одна проблема: необходимо как-то убедиться, что само устройство не взломано и не испорчено, что «идентичность» машины — на всех этапах ее истории, вплоть до изготовления отдельных

деталей — заслуживает доверия. Решить эту проблему непросто. Производители устройств, описывая свои усилия по ее устранению, часто используют словосочетание «доверенные вычисления». Этот термин введен изготовителями процессоров AMD и Intel в сотрудничестве с IBM, Microsoft, Cisco и другими компаниями. Их консорциум получил название Trusted Computing Group (Группа доверенных вычислений).

В своем нынешнем виде доверенные вычисления предназначены для обеспечения адекватного выполнения команд, то есть для гарантии, что компьютер передаст именно ту последовательность символов, которую набрал пользователь, и никакую другую и машина не поражена вредоносным кодом. Для этого в первую очередь необходимо достичь полной безопасности в лабораториях разработчиков и на производстве комплектующих. Поясняя сложность задачи, исследователи из Мичиганского университета недавно продемонстрировали, как злоумышленник мог бы встроить микроскопическую «лазейку» в микросхему, сдвинув всего лишь один транзистор [4]. Теоретически мы с вами можем использовать смартфоны со встроенным прослушивающим устройством, установленным без ведома изготовителя. Предотвратить подобные диверсии — жизненно важная задача.

Как только будет обеспечена неуязвимость на производстве, необходимо предпринять следующий шаг: установить на любое устройство криптографические инструменты, которые позволят ему безопасно обмениваться сигналами со своим программным обеспечением.

Согласно нынешней концепции доверительных вычислений, аппаратные и программные компоненты устройства обмениваются криптографически подписанными сообщениями, чтобы подтвердить, что ни один из них не поврежден. Но этот принцип вызывает вопросы у многих защитников конфиденциальности. В частности, для того чтобы исключить ошибки, связанные с человеческим фактором, такие системы не позволяют владельцу устройства контролировать и даже прочитывать сообщения, которыми обмениваются компоненты его же гаджета. Это вынуждает пользователя доверяться компаниям-изготовителям, установившим в устройство систему внутренней коммуникации. Большинство производителей — крупные корпорации вроде Intel, поэтому их авторитет и власть так или иначе будут определять работу системы безопасности. Получается, мы вновь возвращаемся к проблеме посредников, причем в данном случае они станут

управлять процессами, которые происходят на *наших с вами* устройствах. Однако на сегодняшний день такая система доверенных вычислений — все, что у нас есть, и в целом она работает.

Доверенные вычисления — лишь часть сложной программы по обеспечению безопасности «интернета вещей». Очень важно фиксировать деятельность устройства: историю транзакций; каждый случай ввода пароля для выполнения различных задач; какие манипуляции и кем с ним производились с момента сборки и поставки и вплоть до утилизации. Точно так же как запись человеческих действий помогает предотвратить мошенничество, надежный регистр позволяет убедиться, что определенное устройство заслуживает доверия и не подделывает цифровую валюту, которую перечисляет на кошелек другого устройства. И если блокчейн уже доказал свое превосходство над централизованными архивами человеческих транзакций, то есть все основания задействовать его для транзакций в «интернете вещей». В конце концов, машины ведь не юридические лица и не организации и не могут завести счет в банке или использовать Paypal, Venmo и другие регулируемые электронные кошельки [5].

Идеальный сценарий, при котором устройства «интернета вещей» смогут платить за краткосрочный доступ к сервисам, контролируемым другими устройствами — например, за то, чтобы воспользоваться Wi-Fi-точкой соседа и отправить срочное сообщение, — предполагает многосторонние и очень быстрые микроплатежи. Подобная схема физически невозможна при нынешней сложной системе платежей в рамках централизованной финансовой модели, с трехдневным периодом зачисления и высокими комиссиями. Чтобы обмениваться ценностями между собой, узлам «интернета вещей» нужна более децентрализованная система учета и записи, например блокчейн. Многие компании уже пытаются ее создать.

Одним из первопроходцев в этой сфере стала корпорация Intel. Производители процессоров разработали блокчейн-технологию под названием Sawtooth Lake, надстраиваемую поверх уже существующего модуля доверенных вычислений, известного как Software Guard Extensions (IntelSGX) [6]. Система задумана как «блокчейн-агностик», а это означает, что ее можно запустить как на базе приватного корпоративного блокчейна с ограниченным доступом, так и на базе открытой сети устройств. Особо ярые пуристы могут заявить, что, поскольку

система Sawtooth целиком привязана к технологиям Intel, это частично сводит на нет преимущества открытого децентрализованного блокчейна, ведь пользователи будут вынуждены полагаться на ПО компании Intel. Тем не менее возможность встроить в открытый блокчейн защитные механизмы, специально разработанные для «интернета вещей», крайне важна. Она открывает перед ним гораздо более широкие горизонты, чем власть двух-трех мегакорпораций.

Рассмотрим ситуацию, которая вполне вероятна в мире «интернета вещей». Один беспилотный автомобиль, которому нужно как можно быстрее добраться до места назначения, платит небольшую сумму другому беспилотному автомобилю, чтобы тот его пропустил. Как мы уже говорили, для того чтобы удостоверить валидность этой транзакции, необходима распределенная система доверия, поскольку речь идет о передаче большого количества данных, а не просто о переводе средств. Например, нужно удостовериться, что обгоняющая машина может развивать высокую скорость с должным уровнем безопасности, а также что система одного из автомобилей не заражена вредоносным ПО и не передаст его другому. Все эти подтверждения, а также справку о средствах на кошельке автомобиля-плательщика можно пропустить через блокчейн-реестр и проверить истинность заявлений каждой стороны, гарантируя валидность сделки без централизованного контроля. При этом, однако, возникает ряд вопросов. Легко ли будет обработать такую транзакцию на основе приватного блокчейна? Какова вероятность (в стране, где более 230 миллионов автомобилей), что обе машины подключены к одной и той же закрытой сети под управлением группы валидаторов? Если же они подключены к разным сетям, программное обеспечение может оказаться несовместимым и платеж не пройдет. Где гарантия, что все производители авто станут пользоваться одной и той же системой верификации? А если они объединятся и создадут консорциум, чтобы самим управлять единой системой, не перекроет ли это доступ на рынок молодым компаниям, стартапам в сфере автопрома? Вдруг мы породим гигантский механизм, который в щепки перемелет конкуренцию?

Вероятно, решить проблему барьеров и монополий помогла бы поистине децентрализованная, открытая система, в работе которой может участвовать любое устройство, но при этом каждый пользователь будет уверен в сохранности информации,

оборудования и передаваемых ценностей. Открытая система создала бы гораздо более гибкую инфраструктуру для «интернета вещей» и избавила бы от диктата посредников (а также от их любви к высоким комиссиям).

Однако проблема в том, что возможности нынешних открытых блокчейнов довольно ограниченны. Пропускная способность и размер блоков в системе Биткоин позволяют выполнять лишь несколько транзакций в секунду, хотя «внесетевой» протокол LN должен значительно улучшить ситуацию. Система Эфириум хотя и быстрее обрабатывает блоки, но тоже подвержена сбоям при большой загруженности сети. Эти ограничения — если их не устранить в ближайшее время — затормозят развитие «интернета вещей», который должен справляться с мощнейшим трафиком микроплатежей между миллиардами устройств.

В этой сфере также ведутся активные разработки. Стартап IOTA использует нестандартный алгоритм консенсуса, который в меньшей степени нагружает вычислительную сеть, чем обыкновенный блокчейн. В этой системе каждое устройство не только совершает транзакции, но и является валидатором — в отличие от Биткоина, где майнеры и пользователи разделены. Принцип таков: чтобы одно устройство могло обменяться данными с другим — отправить деньги в форме токенов IOTA или переслать другую ценную информацию, — оно должно само подтвердить валидность двух транзакций в сети, назначенных ему случайным образом. Две транзакции из миллионов, очевидно, требуют намного меньших мощностей, чем в системах Биткоина и Эфириума, где майнерам приходится обрабатывать каждый блок целиком. Поэтому система IOTA опережает их в плане масштабируемости. Однако ее успех — и вообще безопасность всей сети IOTA — зависит от сетевого эффекта. Если к сети будет подключено небольшое количество устройств, то злоумышленник, оперирующий одним из них, рано или поздно получит на подтверждение собственную транзакцию и сможет авторизовать двойное расходование или другой вид мошенничества. С другой стороны, по мере разрастания сети такая вероятность убывает в геометрической прогрессии, а надежность системы резко повышается. Разработчики компании IOTA уверяют: чем сеть шире, тем лучше она масштабируется и тем больше дает гарантий. В этом она прямо противоположна Биткоину.

Наработки компании IOTA были встречены с бурным энтузиазмом, и многие их сторонники инвестировали в токен IOTA, который стал одним из самых успешных на рынке. Однако эйфория прошла, когда криптографы исследовательского сообщества медиалаборатории Массачусетского технологического института (MIT's Digital Currency Initiative) обнаружили в алгоритме хеширования транзакций серьезную уязвимость [7]. Вместо того чтобы применять стандартные инструменты хеширования, например алгоритм SHA-256, как у биткоина и прочих криптовалют, разработчики IOTA предпочли создать собственную версию, где и нашлись «лазейки» для мошенников. Это открытие обесценило токены IOTA и поставило пользователей перед выбором: либо загрузить новую версию ПО, либо выпасть из системы. Иными словами, произошел хардфорк. После того как группа МТИ опубликовала свои выводы и на примере IOTA пояснила необходимость более жесткого контроля безопасности, курс токенов IOTA рухнул. Инвесторы — разумеется, недовольные обесцениванием своих токенов — устроили «разбор полетов» в соцсетях и обвинили лабораторию МТИ в намеренном нагнетании страхов ради собственной выгоды [8]. Досталось и журналисту Forbes, написавшему статью об уязвимости IOTA [9]. Сооснователь компании Сергей Иванчегло выступил в тематическом блоге с весьма неожиданным заявлением, что уязвимость заложена в код специально для «защиты от копирования», чтобы недобросовестные конкуренты, которые решат позаимствовать открытый код IOTA, столкнулись с проблемами [10]. Эти слова вызвали шквал критики со стороны криптографического сообщества, у которого стало традицией открыто разбирать наработки друг друга, чтобы исправить недочеты и сделать код надежнее.

Между тем, хотя проект IOTA и утратил доверие ряда уважаемых криптографов в блокчейн-сообществе, у многих крупных компаний интерес к нему не угас. Вероятно, потому, что вне зависимости от криптографических удач или промахов экономическая модель IOTA весьма привлекательна. Если удастся исправить код, то сам принцип, на котором основана система, обещает быть менее сложным и затратным в плане вычислительных мощностей, чем устройство Биткоина и Эфириума, где каждый компьютер в огромной сети валидаторов должен обработать и подтвердить полный список транзакций в каждом новом блоке. Немецкий гигант инженерии

и электроники — компания Bosch — проводит серию экспериментов с системой IOTA, в том числе изучая возможность платежей между беспилотными грузовиками, выстроенными в линейный энергосберегающий «взвод». Суть идеи в том, что грузовики, едущие в задних рядах, попадают в воздушный поток от тех, что едут впереди и в результате тратят намного меньше энергии на передвижение, поэтому они должны перечислять токены IOTA передним грузовикам, чтобы компенсировать разницу в расходе энергии. При этом компании IOTA и Bosch входят в консорциум под названием Trusted IoT Alliance («Ассоциация доверенных вычислений для "интернета вещей"») [11], задача которого — выстроить надежную и безопасную блокчейн-инфраструктуру для своей отрасли. В нем также состоят компании Foxconn, Cisco, BNY Mellon и ряд блокчейн-стартапов, в том числе логистическая фирма Skuchain и поисковая лаборатория ConsenSys. Сайт консорциума продвигает «интернет вещей для бизнеса», обещая «стать катализатором четвертой промышленной революции». Технология IOTA, возможно, и не идеальна, но такие подходы к задаче масштабирования сети однозначно вызывают интерес.

Даже правительство США не осталось в стороне. Министерство национальной безопасности выделило компании Factom — строителю блокчейн-инфраструктур — грант в размере 199 тысяч долларов на разработку протокола безопасности для «интернета вещей» [12]. По меркам ICO-сборов сумма очень скромная, однако сам факт ее выдачи можно рассматривать как обнадеживающий вотум доверия со стороны правительственных организаций. Система компании Factom должна создать уникальный журнал данных для каждого устройства: серийный номер, дата и место производства, история обновлений, выявленные проблемы с безопасностью и полномочия, которыми устройство наделено. Суть идеи в том, что, если запись о технических параметрах, транзакциях и сертификации устройства будет храниться в неизменяемом реестре, хакеры не смогут ее подправить, чтобы скрыть уязвимость, которой воспользовались. До какой степени правительство США намерено контролировать ход проекта, пока неизвестно.

Лаборатория Context в Кембридже ведет похожие программы, чтобы добиться того, что она называет «правдивостью данных». На ее базе взаимодействуют представители различных отраслей,

заинтересованные в единых стандартах открытых данных для API (программных интерфейсов приложения), которые позволили бы сторонам обмениваться информацией с уникальным криптографическим хешем, подтверждающим идентичность устройства и его владельца. Собирая и обрабатывая информацию с помощью блокчейна, команда лаборатории Context надеется повысить уровень доверия к данным, производимым узлами «интернета вещей», например датчиками климатических изменений. Как утверждает CEO лаборатории Дэн Харпл, если консорциум с достаточно большим числом представителей от каждого сегмента индустрии сможет достичь согласия и внедрить единый стандарт для открытых API, это поможет оградить приватные блокчейны от захвата монополиями и олигополиями. Теоретически это бы облегчило решение проблемы масштабирования гигантской сети «интернета вещей».

Однако подобные утверждения — как почти все в нарождающейся блокчейн-индустрии — еще должны пройти проверку действием. Пока у нас есть набор базовых идей, которые сулят огромные возможности. Что примечательно, эти идеи, позволяя вообразить мир децентрализованного доверия, заодно обещают в корне изменить принципы нашей экономики. Обеспечив безопасность «интернета вещей», мы можем запустить такую волну инноваций, какой еще никогда не видели. В результате не только сам интернет заработает эффективнее, но и производители с потребителями смогут более взвешенно распоряжаться любыми ресурсами. В итоге мы увидим значительное снижение тарифов и улучшение экологической обстановки. Давайте рассмотрим, что это означает для производства самого важного ресурса в мире — энергии.

Энергетика блокчейна

В октябре 2015 года, во время парижской конференции ООН по климату премьер-министр Индии Нарендра Моди сформулировал крайне амбициозную задачу для своей страны: ввести дополнительно 175 ГВт (гигаватт) мощностей возобновляемой энергетики до 2022 года [13]. Исходя из общей пропускной способности энергосети около 280 ГВт,

озвученное премьер-министром количество энергии покроет нужды 600 миллионов индийцев. Это заметно приблизит страну к другой важнейшей цели: обеспечить электроэнергией 300 миллионов человек, у которых на сегодняшний день нет постоянного доступа к ней. Таким образом совмещаются две задачи, которые человечество должно решить, чтобы избежать самоуничтожения и не разрушить планету: резкое сокращение углеродных выбросов и неуклонный рост благосостояния четырех миллиардов беднейших жителей Земли.

Сейчас мы сделаем одно смелое заявление, которое (пока) не прозвучало в залах заседания индийского правительства: запланированный рывок невозможно совершить без проведения одновременной децентрализации энергосетей и передачи производства и потребления энергии на нижний уровень. Необходимо выстроить систему, которую иногда называют «энергетической демократией».

Изменение климата на планете вызвано не только повсеместным использованием насыщенного углеродом топлива для электростанций, но еще и крайней непродуктивностью централизованной модели энергоснабжения — от географической структуры и уровня безопасности до долгосрочных политизированных программ финансирования. Если наша цель — поставлять как можно больше энергии по низкой цене и при этом эффективно использовать возобновляемые ресурсы, источник производства энергии необходимо максимально приблизить к источнику потребления. Быстрое развитие фотоэлектрических технологий дает нам надежду достичь этой цели; в последнее время мощность солнечных панелей и батарей растет почти по закону Мура*, а цены падают такими темпами, что в 2016 году китайско-японский консорциум выиграл тендер на строительство солнечной электростанции в Абу-Даби с рекордно низкой ценой на энергию: 2,42 цента за кВт/ч [14]. Это примерно вполовину меньше средних расценок по США; благодаря такой разнице солнечная энергия сможет конкурировать с полученной от ископаемого топлива. Конечно, электростанция в Абу-Даби — централизованный проект — это огромное поле солнечных панелей, которое должно бесперебойно

* Закон Му́ра — эмпирическое наблюдение, сделанное Гордоном Муром, одним из основателей Intel, согласно которому количество транзисторов, размещаемых на кристалле интегральной схемы, удваивается каждые 24 месяца. *Прим. ред.*

снабжать энергией один из эмиратов. Однако оно дает представление о будущем локальных солнечных микросетей.

Преимущества децентрализованных энергосетей очевидны. Если любое местное сообщество будет само производить и распределять энергию, например, через микросети, объединяющие солнечные панели на каждом доме, то это значительно сократит ее потери при передаче на большие расстояния (а они иногда доходят до 30 процентов). Децентрализованные микросети менее уязвимы для кибератак, поскольку последовательный взлом каждого узла обойдется хакерам гораздо дороже, чем взлом главного сервера в централизованной региональной сети. Кроме того, децентрализованная сеть позволяет подстраховаться на случай стихийного бедствия. (Найдите в интернете фотографии ночного Манхэттена после урагана «Сэнди»: весь район ниже 34-й улицы — сплошная черная дыра, кроме одного светлого пятнышка вокруг Вашингтон-сквера. Там находится Нью-Йоркский университет, корпуса которого объединены в децентрализованную энергосеть [15].) Есть и еще один плюс: хотя полностью искоренить коррупцию очень сложно, маленькие локализованные инициативы будут не столь лакомым куском для продажных чиновников и теневых банкиров, как гигантские энергетические проекты. Без тридцатилетних контрактов, навязанных нам крупными международными банками и политическими силами, можно будет значительно сократить лишние издержки и снизить цены на энергию для рядовых граждан.

Еще важнее то, что децентрализованный подход к строительству энергосетей позволяет гораздо эффективнее управлять расходом электричества. С помощью компьютерного мониторинга, «умных» счетчиков и оптимизированного индивидуального графика работы каждого устройства домашние «наносети» смогут выйти на такой уровень микроменеджмента, какой и не снился большим муниципальным структурам. Революция, которая началась с появления «умных» термостатов Nest и Ecobee, совершит следующий рывок. Однако мечта о дешевой и экологически чистой энергии может стать явью лишь при наличии двух вещей: децентрализованного управления энергосистемой (производством, поставками и потреблением) и сети взаимосвязанных «умных» счетчиков и прочих устройств с выходом в интернет, которые будут принимать счета за потребленное электричество. Иными словами, подобное возможно лишь в эпоху «интернета вещей».

Однако нам придется продумать организационную сторону вопроса. Кто будет контролировать оплату? Крупная управляющая компания — то есть, по сути, очередной посредник или «банкир», который отслеживает потребление энергии и выписывает платежные документы, — не может заниматься бесчисленными микротранзакциями между солнечными панелями, холодильниками, кондиционерами и т. п. Это была бы не просто чудовищная нагрузка на ее сотрудников; такой метод управления явно противоречит интересам сообщества, которое стремится потреблять как можно меньше энергии. Но если управляющие компании не смогут контролировать микросети, перед нами вновь встанет проблема доверия. Разумеется, интересы продавцов энергии, для которых важна прибыль, не совпадут с интересами потребителей, которые хотят сэкономить. Следовательно, соседи не смогут просто довериться друг другу, и чем крупнее сообщество, тем больше возникнет вопросов. Как доказать, что один из соседей не «подкручивает» электросчетчик, а другой не берет лишнего за поставку энергии?

Кроме того, чтобы система работала должным образом, все расчеты следует производить в специальной внутренней криптовалюте — токенах, чей плавающий курс привязан к киловатт-часам и которые любой пользователь может конвертировать в обычные деньги. Это поможет оптимизировать процесс управления локальной сетью. Таким образом сложится механизм рыночного ценообразования, с помощью которого будут выполняться все функции, возложенные сегодня на управленцев регионального уровня. Конвертируемый токен будет отображать местную, внутрисетевую цену на электричество и, как любой ценовой показатель, сообщать определенную информацию — передавать сигнал пользователям сети. Но поскольку этот сигнал цифровой, пользователи смогут настроить под него свои электроприборы. Например, станут заряжать аккумуляторы электромобиля лишь в часы, когда сеть мало загружена и электричество дешево; или же выстроят систему приоритетов для разных устройств, чтобы одни выключались автоматически (телевизор), а другие продолжали работать (холодильник). Те же ценовые сигналы, которые будут отображать баланс спроса и предложения для энергии, могут заставить программу, управляющую сетью, направлять излишки электричества в аккумуляторы или подключать эти резервы в случае его нехватки. Но все же кто (или что) будет контролировать работу этого внутреннего рынка и платежной

системы? По причинам, которые мы уже упоминали — высокие комиссии; неэффективные механизмы зачисления средств; риск вмешательства посредника (например, управляющей компании), чьи интересы не совпадают с интересами пользователей, — децентрализованным сообществам понадобятся децентрализованные решения.

Именно к этому выводу пришли специалисты из компании LO3, когда разрабатывали модель Transactive Grid в Бруклине — экспериментальную сеть из нескольких домохозяйств и предприятий, пользующихся энергией от солнечных панелей. Сообщество намеревалось предоставить экологически сознательным потребителям возможность покупать чистую энергию местного производства, а не просто помогать своим управляющим компаниям брать кредиты и строить «зеленые» электростанции в других регионах США.

В рамках проекта Transactive Grid владельцы зданий устанавливают на крыше солнечные панели, которые объединяются с панелями соседей в общую систему; при этом используются недорогие модели «умных» счетчиков и аккумуляторов, а также инверторы, которые позволяют направлять излишки электричества в городскую сеть (за плату). Однако главный «ингредиент» — приватный блокчейн, регулирующий обмен электроэнергией между «умными» счетчиками, чьи данные заносятся в распределенный реестр. Летом 2017 года компания LO3 сделала следующий шаг: разработала «эксергетический токен», который должен стимулировать рыночные механизмы внутри бруклинской сети и между аналогичными ей децентрализованными микросетями [16]. (*Эксергия* — ключевое понятие для измерения энергоэффективности и сокращения лишних трат. Это предельное значение энергии, которое может быть выгодно использовано в термодинамическом процессе, а также объем полезной работы, выполненной для производства каждого заданного количества энергии.)

Отметим, что в основе сети LO3 лежит приватный блокчейн. Энергетические микросети — один из тех случаев, когда эта модель вполне пригодна, ведь сообщество состоит из ограниченного количества пользователей, которые согласились с правилами производства и потребления. Это снимает проблему масштабирования, присущую крупным сетям вроде Биткоина и Эфириума. Таким образом, транзакции можно быстро и эффективно проводить через блокчейн, не прибегая к протоколам типа Lightning Network и другим «внесетевым»

технологиям масштабирования. Закрытый блокчейн может обрабатывать микротранзакции, запускать и поддерживать смарт-контракты, которые позволят, например, подключаться к источнику питания в зависимости от того, сделан платеж в криптовалюте или нет, а также производить одноранговый обмен энергии на токены. Следовательно, блокчейн позволит создать децентрализованный рынок с ценовыми сигналами, необходимыми микросети для максимальной эффективности. Это означает, что система сможет работать без централизованного руководства, решающего, кто и по какой цене получит энергию. Кроме того, мощность сети будет естественным образом возрастать по мере установки всеми членами сообщества новых панелей и прочего оборудования, приносящего дополнительный доход. Подобный сценарий закономерен, поскольку пользователи будут знать, что система сможет эффективно инкорпорировать любое устройство.

LO3 — отнюдь не единственный игрок на этом поле. Внедрением блокчейна в сферу энергетики активно занимается и берлинская компания Grid Singularity в союзе с некоммерческой лабораторией Rocky Mountain [17]. Их задача — ускорить выход технологии блокчейн на промышленный уровень. Сотрудники Grid Singularity в первую очередь фокусируются на применении блокчейнов для чтения и обработки гигантских массивов данных, получаемых от тысяч независимых устройств. С их помощью можно было бы получить предельно точные сведения об использовании электроэнергии и повысить эффективность управления локальными и региональными сетями. Подобные инициативы говорят о назревшей потребности использовать блокчейн для обработки и подтверждения ключевых данных, которые потребуются правительствам, предприятиям и прочим заинтересованным структурам для решения проблемы климатических изменений. Однако учитывая, что пока ситуация только усложняется, подобные механизмы управления энергией — вернее, даже эксергией — жизненно необходимы для выработки эффективной стратегии.

Особую актуальность таким технологиям придают последствия ураганов «Ирма» и «Мария», которые практически уничтожили энергосети в странах Карибского бассейна. Спустя два месяца после удара стихии некоторые возможные решения были представлены на форуме разработчиков в рамках 23-й Конференции ООН по проблемам изменения климата в Бонне.

Финансирование — одна из самых сложных задач при создании микросетей. Несмотря на то что стоимость аккумуляторов понемногу снижается, их установка в жилом квартале или коттеджном поселке стоит немало. Кроме того, пока не совсем ясно, каким образом владельцы солнечных панелей смогут монетизировать свои вложения. До сих пор коммерческие проекты такого рода в основном проводились на отлаженных, хорошо развитых рынках, где владельцы оборудования могут использовать сетевые счетчики для продажи излишков энергии региональным сетям. Для этого нужны не только дорогостоящие современные приборы и надежные линии передач, но и добросовестные регуляторы, которые обяжут коммунальные службы покупать электричество по разумной цене, даже если это противоречит их сиюминутным интересам. Все козыри у энергетических компаний, поэтому владельцы солнечных панелей целиком зависят от политики местных властей.

Тем не менее ситуация может в корне измениться в результате революции в технологиях накопления энергии. Во многом благодаря усилиям и средствам, вкладываемым компаниями вроде Tesla в разработку нового поколения аккумуляторов, топливных элементов и накопителей тепловой энергии, мобильность и эффективность накопительных систем неуклонно растет, тогда как себестоимость понижается. И вскоре, вероятно, можно будет говорить о полной энергетической независимости. Представьте себе автономное сообщество, которое совместно владеет децентрализованной солнечной электростанцией, управляемой на основе блокчейна. Оно могло бы создать полноценную систему хранения и транспортировки аккумуляторов (с помощью беспилотных электромобилей), а также обмена с другими автономными группами.

Подобные решения будут полезны для самых разных общин: индийских деревень, нередко отрезанных от крупных энергосетей; независимых этнических поселений, таких как коренные народы США и австралийские аборигены, которые стремятся к энергетической независимости; или же фермеров и прочих жителей малонаселенных районов, которые испытывают сложности из-за низкого местного спроса на энергию, но не в состоянии осилить затраты на установку генераторов и проведение ЛЭП. До сих пор в большинстве подобных случаев поставки энергии субсидируются государством — фактически

за счет городских пользователей, которым приходится платить по завышенным расценкам.

[166] Однако остается еще одна проблема: как финансировать изначальную установку децентрализованных микросетей в местах, где отсутствует надежная кредитная инфраструктура? Технология блокчейн могла бы помочь и здесь. Подробнее мы расскажем об этом в главе 7, где рассмотрим реестры активов, альтернативное залоговое обеспечение и новейшие финансовые решения для развивающихся стран.

Управление энергоресурсами — не единственная сфера материальной экономики, где блокчейн и «интернет вещей» открывают перед нами новые горизонты. С каждым днем растет интерес к применению блокчейна в логистике, а именно в управлении цепями поставки. Цепи поставок — это последовательные, взаимосвязанные операции, которые определяют весь путь, пройденный товаром от стадии добычи сырья до полки в супермаркете. Повысив прозрачность таких цепей, можно увеличить конкурентоспособность мелких производителей, сделать доступнее финансирование и страхование, снизить расход ресурсов и вселить в потребителей уверенность, что купленный ими продукт высокого качества.

Отслеживаем товары

В октябре 2015 года 55 клиентов ресторана Chipotle Mexican Grill заразились кишечной палочкой, из-за чего репутация бренда серьезно пострадала, продажи упали, а стоимость акций компании снизилась на 42 процента и начала немного расти лишь три года спустя [18]. Главной причиной инцидента стала извечная беда компаний, вынужденных полагаться на множество внешних поставщиков, — недостаточная прозрачность логистики и нечетко определенные зоны ответственности. Многие посетители ресторанов Chipotle, наверное, решили, что все произошло из-за антисанитарных условий в одном из заведений сети. Однако, как ни прискорбно для репутации бренда, истинное положение дел было еще хуже: руководство компании не имело возможности установить, как кишечная палочка попала в ее продукты; выяснить удалось только то, что ею была заражена говядина, полученная

от кого-то из многочисленных сторонних поставщиков, предположительно австралийских. Как и в любой глобальной цепи поставок, система оказалась слишком запутанной, чтобы найти истинного виновника. Следовательно, компания не могла ни предотвратить, ни локализовать заражение.

Цепи поставок состоят из отдельных, часто независимых друг от друга звеньев, но у них один общий интерес — максимизировать продажи конечного продукта. Например, изготовители транзисторов, микросхем, дисплеев и прочих комплектующих смартфона Samsung получат бóльшую прибыль при росте спроса на продукцию компании Samsung. Но при этом они связаны между собой закупочными контрактами, и здесь интересы высших и нижних звеньев цепи часто не совпадают. Поэтому они не спешат делиться друг с другом информацией, и по молчаливому согласию каждая сторона ведет собственный учет данных касательно внутреннего рабочего процесса и условий производства. Конечно, любая компания может посылать запросы остальным, однако практика в этой сфере похожа на банковскую, где все платежные системы ведут свой реестр и прозрачность стремится к нулю. Следовательно, сеть ресторанов не может просмотреть реестры австралийских ферм и убедиться, что забой скота производился с соблюдением всех обязательных процедур и гигиенических стандартов. Штрихкоды и RFID-метки несколько упростили отслеживание партий товара в глобальной логистике, но истинная проблема состоит в закрытости каждого отдельного поставщика. Конечные производители — и, что еще важнее, потребители — по-прежнему покупают кота в мешке.

Технология блокчейн с ее способностью вовлекать изначально не доверяющих друг другу людей в работу на общее благо предлагает возможное решение проблемы. Компании, предпочитающие не делиться конфиденциальной информацией, могли бы использовать криптографическое хеширование для подтверждения выполнения ключевых процедур без разглашения своих секретов. Полученные хеши можно заносить в блокчейн-реестр, доступ к которому будет открыт для всех участников цепи поставок. Таким образом, возникнет единая, прозрачная, неизменяемая запись, принятая всеми сторонами делового соглашения. Соответственно, повысится и уровень доверия к информации. Все больше стартапов, банков и даже крупных

производителей начинают исследовать этот инструмент, видя в нем потенциальное решение проблем открытости и подотчетности, которые раньше были невозможны для поставщиков, разбросанных по всему миру. При обновлении реестра данных в режиме реального времени (если нужно, в анонимизированном или зашифрованном формате) отпадает необходимость в длительной, не всегда объективной сверке внутренних записей. Каждый участник цепи сможет составить более полную и четкую картину общих действий. При такой системе владельцы ресторана Chipotle в любой момент могли бы проверить, кто из поставщиков мяса соблюдает все требования к его обработке. Конечно, вероятность, что поставщик внесет в реестр запись о работе, которую не выполнял, остается, но уже сам факт наличия единой, общедоступной учетной книги должен оказать дисциплинирующее воздействие.

Распространение такого механизма обеспечения прозрачности и моментального отслеживания на всю сферу международной торговли позволит создать глобальную систему поставок с более эффективным использованием ресурсов. И это может радикально изменить условия торгового обмена в мировой экономике. Предоставляя свободный доступ к данным и закрепляя за каждым этапом производства цифровой токен, технология блокчейн высвободила бы дополнительную ценность для обмена на промежуточных стадиях многопрофильного производства и процесса реализации. В результате предприниматели получили бы гораздо большую свободу для маневра при поиске рынков и в ценовой политике на любом этапе производства и смогли бы оперативнее реагировать на запросы потребителей, которые хотят все знать о покупаемых товарах. Вместо жестко выстроенных цепей поставок возникли бы куда более гибкие *цепи спроса*, что позволило бы эффективнее распределять ресурсы.

Реклама британского стартапа Provenance сообщает об использовании технологии блокчейн для того, чтобы «оживить историю вашего продукта» и «проследить путь каждой его партии от истока до полки в магазине» [19]. Сеть супермаркетов Walmart совместно с компанией IBM и пекинским университетом Цинхуа разрабатывает систему отслеживания партий китайской свинины с помощью блокчейна [20]. Горнодобывающий гигант BHP Billiton применяет эту технологию для проверки анализа минералов, выполненного сторонними

подрядчиками [21]. Стартап Everledger загрузил в блокчейн-реестр уникальные идентифицирующие данные для миллиона драгоценных камней, чтобы помочь ювелирам соблюдать требования закона и пресекать сделки по «кровавым бриллиантам» [22].

Все эти решения неразрывно связаны не только с технологией блокчейн, но и с «интернетом вещей». Они невозможны без датчиков, штрихкодов, RFID-меток, которые все чаще используются на производстве и в логистике для отслеживания партий товара, запуска рабочих процессов и своевременной оплаты. Следовательно, нам и здесь понадобится «всезнающая машина», которая сможет распознать все эти устройства и убедиться в их безупречной работе. Когда к системе добавятся смарт-контракты, сигналы от каждого устройства смогут автоматически исполнять заданные условия оплаты и доставки, подтвержденные всеми сторонами. Подобным образом таможенные службы, администрация портов, обеспечители торгового финансирования и прочие заинтересованные структуры могли бы объединиться в сети для управления собственными рабочими процессами.

Преимущества полной прозрачности и автоматизации касаются не только материальных объектов; блокчейны могли бы помочь и с учетом человеческих ресурсов. Персоналу и администрации различных компаний-поставщиков можно раздать специальные криптографические коды доступа, которые играли бы в блокчейн-среде роль уникальных, легко отслеживаемых идентификаторов. (Здесь, конечно, понадобится очень высокая степень криптографической защиты, чтобы обезопасить личные данные сотрудников.) Тогда все участники цепи поставок смогут отслеживать деятельность зарегистрированных работников на любом этапе процесса. Скажем, администрация ресторана Chipotle могла бы в режиме реального времени убедиться, что сертифицированный сотрудник мясоперерабатывающего цеха провел соответствующую стерилизацию и дезинфекцию говядины.

Доказуемая прозрачная сертификация подобного рода особенно важна для так называемого аддитивного производства — трехмерной печати промышленного уровня. Эта технология лежит в основе динамичной, интерактивной отрасли, известной как «индустрия 4.0». Так стало принято обозначать новый сектор производства, способный моментально реагировать на изменения потребительского и иного спроса. Произведенные 3D-принтерами детали уже сейчас намного легче

и крепче изготовленных традиционным способом. К тому же их гораздо проще и быстрее изготовить по требованию, причем даже для самых сложных механизмов: космических ракет NASA, истребителей и пр. Однако для продуктов стратегического назначения существует и особый риск. Джеймс Редженор, директор отдела аддитивного производства и инновации компании — производителя высокоточных деталей Moog, задается вопросом: «Каким образом экипаж американского авианосца сможет удостовериться, что программа, загруженная в 3D-принтер для печати деталей истребителя, не взломана и не переписана противником?» [23] В поисках решения Редженор и его команда запустили многофункциональный сервис Veripart, использующий среди прочего технологию блокчейн, чтобы отследить разработку исходного ПО и последующих обновлений, выполненную различными операторами 3D-печати на всех этапах производства и сборки. В дальнейшем предполагается добавить ряд функций, которые позволят защитить интеллектуальную собственность и превратить ее в более гибкий и динамичный актив. Научная команда Moog планирует привлечь к разработке сервиса всех участников своей глобальной цепи поставок. Тем временем гигант оборонной промышленности Lockheed Martin — один из крупнейших клиентов компании Moog — также оценил потенциал блокчейна для повышения безопасности в стратегически важных отраслях [24] и объявил о начале совместного проекта с виргинской компанией GuardTime Federal в целях внедрения технологии блокчейн в управление рисками, связанными с цепью поставок.

Если рассматривать цепь поставок как интерактивную последовательность договорных функций, то список отраслей, которые могли бы воспользоваться этим новым подходом к информации, будет весьма обширным. К примеру, стартап Keyturn планирует применить технологию блокчейн в строительной индустрии, чтобы помочь застройщикам управлять цепями поставок на каждом отдельном объекте и отслеживать затраченные часы и материалы, тем самым сокращая расход ресурсов и понижая цену для конечного потребителя [25]. Кроме того, инновация могла бы обеспечить адекватную оплату труда нелегальным мигрантам и улучшить почти катастрофическое положение группы, которая составляет 7 процентов мировой рабочей силы в отрасли, генерирующей 13 процентов мирового ВВП (по оценкам Глобального института McKinsey) [26].

Распределенная структура цепей поставок очень помогла бы и при сверке счетов. Компания IBM ежегодно разбирает и улаживает около 25 тысяч спорных платежей. В 2016 году, используя закрытый распределенный реестр, ей удалось сократить время разбирательств с 44 до 10 дней [27]. Общая история платежей и поставок, которую все участники могут просмотреть и подтвердить в режиме реального времени, позволяет быстрее достигать соглашения всех сторон. И дело не только в скорости. По словам представителей IBM, на данный момент разбирательства ежегодно обходятся компании в 100 миллионов долларов.

Таким образом, налицо огромный потенциал для экономии средств и повышения эффективности, который может сказаться на каждом участнике цепи поставок — от добытчика сырья до конечного потребителя. Вопрос в том, как этот потенциал будет монетизирован и кто основной выгодополучатель. Одна из ключевых возможностей кроется в сфере финансирования и страхования.

У предприятий малого и среднего бизнеса по всему миру весьма ограниченный доступ к аккредитивам и другим видам торгового финансирования, используемым для покрытия периода доставки товаров экспортера зарубежному покупателю. Основная причина — в недостаточном доверии кредитующих организаций документам, например портовым накладным, предоставляемым в качестве дополнительного обеспечения. В наши дни малейшая тень подозрения, что предъявитель накладной уже брал средства под залог этой партии товара, обычно ставит крест на кредитной заявке. Если все эти документы и обязательства по ним можно будет загрузить в блокчейн-реестр, который докажет, что они не использовались дважды, у малого и среднего бизнеса появится шанс подтвердить свою кредитоспособность и тем самым повысить конкуренцию на глобальном рынке. Сингапурская компания Standard Chartered уже разработала возможное техническое решение [28].

Кроме того, подобная технология позволила бы основным участникам цепи поставок фактически стать банкирами или страховыми агентами для своих поставщиков. Опираясь на детальную, подтвержденную блокчейн-реестром информацию о наличных товарах поставщиков, они могли бы разработать для каждого из них индивидуальные условия оплаты, например, сократив срок с 90 до 30 дней. Это помогло бы основным поставщикам высвободить средства, которые

в противном случае надолго «зависают в воздухе». Научный поиск в этой сфере возглавляет китайская корпорация Foxconn — производитель и сборщик электроники для ведущих мировых брендов, в том числе Apple. Корпорация развернула пилотный проект для тысяч поставщиков, вовлеченных в различные цепи, и в скором времени объявила, что эксперимент позволил получить кредиты на сумму 6,5 миллиона долларов [29].

Более радикальный способ высвободить капитал с помощью блокчейн-решений в сфере логистики — эмиссия уникальных токенов того вида, о котором мы говорили в предыдущей главе: особых цифровых активов, символически представляющих товары и сервисы в цепи поставок. Это привнесло бы гибкость в бизнес-модели в сфере импорта и экспорта и способствовало внедрению инновационных стратегий. Токенизация в сочетании с данными GPS и прочей информацией, записанной в блокчейн-реестре, позволит владельцу товара передать право собственности любому покупателю в любой момент без необходимости регистрировать партию груза в порту или ином пункте перегрузки. Те компании, чьи товары оказались среди огромной партии, застрявшей в море после банкротства южнокорейской судоходной компании Hanjin Shipping в 2016 году, горячо одобрили бы такое решение. Только представьте, что рынки оптовых и промежуточных товаров смогли добиться той же ликвидности и гибкости ценовых механизмов, что и рынок ценных бумаг. Управление рисками тогда тоже вышло бы на качественно новый уровень.

Цифровые токены, подтвержденные блокчейн-реестром, подготавливают почву для того, что Пиндар Вонг — предприниматель и эксперт в сфере технологии блокчейн — назвал «пакетизацией риска» [30]. Эта новаторская концепция позволяет ввести передачу права на разных этапах поставки. Промежуточные товары, обремененные задолженностями и неисполненными контрактами, можно будет выставлять на торги в поисках покупателей, готовых принять связанные с ними права и обязательства. Это привлечет альтернативные источники спонтанного спроса, что существенно облегчит управление ресурсами. Повышенная прозрачность коммерческих операций в сочетании с возможностью быстро находить ликвидные рынки для связанных с товарами цифровых активов, дала бы промышленникам мощнейший стимул объединить финансовую выгоду с защитой

окружающей среды. Такая модель аналогична вышеописанному механизму, где ценовые сигналы служат оптимизации солнечной энергосети. Если токены позволят устанавливать цену на товары и услуги, прежде не имевшие альтернативного источника спроса, производители смогут принимать более выверенные решения в сфере распределения ресурсов. Вот почему многие эксперты считают, что идеал «круговой экономики», где все материалы и источники энергии используются многократно, можно воплотить в жизнь лишь за счет прозрачности информационных потоков, которую обеспечивают блокчейн-системы.

Главной проблемой по-прежнему остается пропускная способность сети. Общедоступные открытые блокчейны вроде Биткоина и Эфириума пока просто не готовы к расцвету глобальной торговли. Чтобы все поставщики мира смогли проводить транзакции через открытый блокчейн, нужен гигантский рывок в сфере масштабирования — будь то с помощью сетевых или внесетевых решений. Имеющиеся же на данный момент перспективные технологии, например протокол Lightning Network, описанный в главе 3, пока далеки от совершенства. Поэтому сегодня большинство компаний проявляют интерес к приватным блокчейнам, о которых мы поговорим в следующей главе. Такой выбор легко объясним, поскольку крупные производители склонны рассматривать цепь поставок как *статичное* явление — структуру, в которой строго определенные участники уполномочены поставлять те или иные компоненты для конечного продукта. Однако в стремительно меняющемся мире «четвертой промышленной революции» такой подход, вероятно, не самый выигрышный. Новые технологии — например, аддитивное производство, которое можно осуществить где угодно и поручить любому изготовителю с доступом к нужному ПО и достаточно мощным 3D-принтером, — предвещают создание более гибкой и динамичной среды, где поставщики будут с легкостью сменять друг друга. В этой среде закономерно возникнет потребность в открытых реестрах. Когда проблемы масштабирования будут решены, а надежные механизмы криптозащиты и отслеживания позволят гарантировать качественную работу поставщиков, открытые цепи на основе блокчейна смогут значительно демократизировать сферу глобального производства.

Вторая важная проблема связана с юридическими аспектами поставок. На данный момент права собственности и владения в ходе

поставок регулируются очень сложным набором нормативных актов, морским правом, торговым кодексом различных государств. Весьма непросто приспособить все это «дореволюционное» законодательство и охраняющие его организации к цифровой, дематериализованной, автоматизированной и транснациональной системе блокчейн и смарт-контрактов. Например, какие стандарты будут использовать портовые чиновники, чтобы подтвердить, что право собственности на партию товара перешло к импортеру, если в блокчейне понятие собственности определяет не владение материальным объектом, а доступ к приватному криптографическому ключу, привязанному к цифровой записи о товаре?

Разработка блокчейн-приложений для цепей поставок улучшит коммерческие возможности, предоставит малому бизнесу более широкий доступ к финансовым инструментам, сократит неоправданные затраты и позволит потребителю отслеживать историю продукта. Однако для этого требуется и определенный уровень стандартизации. Разумеется, конкуренция желательна, но стандарты позволяют широкому кругу пользователей подключаться к процессу, вызывая сетевой эффект. Исторически так было со всеми новыми технологиями, от метрической системы мер до железной дороги. Интернет смог достичь нынешнего масштаба лишь после получения большой группой пользователей единых протоколов для передачи данных, отправки электронных писем, обмена файлами и защиты информации. На сегодняшний день ни одна крупная организация не взяла на себя разработку подобных стандартов для блокчейна, однако в разных отраслях — логистике, транспортировке, электронике, пищевой промышленности — возникают различные союзы и консорциумы для изучения общих технологий.

Опять же, децентрализованная природа блокчейна несколько осложняет координацию процесса. Но здесь тоже полезен опыт интернета. Например, работающая в Гонконге группа компаний под общим названием Belt and Road Blockchain Consortium [31] исследует метод интернет-администрирования, предложенный и опробованный ICANN (Корпорация по управлению доменными именами и IP-адресами) — международной некоммерческой организацией, регулирующей вопросы, связанные с доменными именами и прочими идентификаторами и играющей одну из ключевых ролей в управлении интернетом.

Ее полномочия по назначению и администрированию доменных имен — главной «недвижимости» Всемирной паутины — ограничиваются не правительством или законом, а разнообразными интересами множества участников процесса, что в итоге и гарантирует общедоступность интернета.

Работа консорциума Belt and Road Blockchain важна уже своей широкой сферой охвата. В группу входят такие гиганты, как KPMG и HSBC, а также крупные логистические компании, в частности гонконгская Li & Fung. Своим названием группа обязана глобальному инвестиционному проекту китайского правительства «Один пояс, один путь». В его рамках предполагается инвестировать три триллиона долларов в совместное развитие высокотехнологичного производства в шестидесяти пяти странах, через которые проходят три торговых пути, соединяющие Азию с Европой и Африкой. Отдельные эксперты уже успели назвать проект «китайским планом Маршалла» [32], однако, как отмечает Кевин Снидер из консалтинговой компании McKinsey, амбициозная программа правительства КНР в 12 раз превосходит по масштабу знаменитый проект восстановления Европы после Второй мировой войны. Пиндар Вонг, основатель консорциума Belt and Road Blockchain, убежден: «Нам предстоит создать огромную сеть поставок между шестьюдесятью пятью государствами с очень разным уровнем открытости и доверия; это можно сделать лишь с помощью распределенной структуры обмена информацией». Теперь технология блокчейн возьмет на себя функцию системы международного управления. Ключевую роль будет играть Гонконг, ведь британские юридические традиции и уважение к правам собственников уже сделали эту территорию респектабельным центром управления интеллектуальной собственностью и прочими договорными обязательствами в рамках международной торговли. Если блокчейну суждено встроиться в глобальные торговые потоки, именно этот регион может стать прекрасной стартовой площадкой для его внедрения. Тем жителям Гонконга, которые мечтают сохранить британский правовой уклад, особая миссия их региона сулит защиту от влияния Пекина.

Яркие новые проекты для глобальной экономики XXI века с супермощными технологиями и динамичными цепями поставок открывают новые горизонты, но при этом представляют большую опасность

для компаний, которые правят деловым миром с прошлого столетия. И эти компании не будут сидеть сложа руки. Но воспримут ли они радикальную, революционную модель экономических отношений, которую предлагает Биткоин? В следующей главе мы рассмотрим, как всевозможные коммерческие и некоммерческие организации исследуют технологию блокчейн и ищут свое место в децентрализованной экономике будущего.

Глава

6

Новый мундир старой гвардии

Пятого августа 2015 года биткоин пришел на Уолл-стрит. Или, если точнее, на Уолл-стрит пришла его новая, причесанная и приглаженная версия.

Поначалу банкиры, которые что-то слышали о биткоине, воспринимали его как занятную диковинку. Гигантские скачки курса обещали высокий спекулятивный доход, но нестабильность не позволяла рассматривать биткоин как альтернативную валюту. С точки зрения банкиров, биткоин не мог претендовать на место в сложившейся финансовой системе. Банковские структуры процветают за счет непрозрачности: наша неспособность доверять друг другу ставит нас в зависимость от их посреднических операций. Банкиры могут скрепя сердце пойти на небольшую реформу внутренней системы, но отдать ее во власть какой-то стихийной силы вроде биткоина — полная ересь. Подобное и в голову никому бы не пришло.

В тот период энтузиасты биткоина тоже не особо интересовались делами на Уолл-стрит. В конце концов, биткоин задумывался как альтернатива банковской системе. Как новая ступень эволюции. По правде говоря, несмотря на широкое движение, которое сформировалось вокруг молодой криптовалюты за семь лет, предшествовавших августу 2015 года, техническую инновацию, десятки новых криптовалют, все сообщества и возможности, порожденные биткоином, старый режим был непоколебим. Денежная машина Уолл-стрит оставалась сердцем глобальной экономики — и до сих пор не сдала позиций. Если вы вдруг

решите использовать технологический прогресс, чтобы улучшить мир финансов (например, понизить системный риск на рынке облигаций или облегчить малоимущим перевод и получение средств), вам все равно придется обивать пороги на Уолл-стрит.

Именно этим и занялась группа технологов из стартапа Symbiont в августе 2015 года. Они принесли в сердце финансового мира собственную, менее радикальную версию биткоина. И хотя их модель правильнее было бы назвать не разновидностью, а свободной вариацией на тему биткоина, она все же обещала произвести революцию, пусть и контролируемую. С биткоином ее роднил ряд ключевых элементов: распределенный реестр, возможность переводить цифровые активы в режиме P2P, а также низкая стоимость и почти мгновенное исполнение транзакций. Однако разработчики компании Symbiont отказались от других характеристик биткоина, включая те, что устраняют посредническую функцию банков при операциях. Система не предполагала собственной криптовалюты для вознаграждения майнеров и поддержки открытого процесса валидации. Иными словами, разработчики Symbiont предложили «блокчейн без биткоина»: сохранили быструю, надежную и дешевую модель распределенной сети с машиной правды, подтверждающей транзакции, но их система не была открытой, общедоступной и лишенной руководства. Таким блокчейном могли управлять банкиры с Уолл-стрит.

Но давайте попробуем выяснить, можно ли отделить биткоин, эфир или другие криптовалюты от блокчейна. Некоторые поклонники цифровых активов уверяют, что отказ от внутренней криптовалюты уничтожит саму сущность блокчейна. Без «родной» расчетной единицы нечем будет вознаграждать и поощрять валидизацию, следовательно, не возникнет открытая сеть, которая, по мнению многих экспертов, лежит в основе децентрализованной системы обмена. Лишенные криптовалюты системы неизбежно превратятся в закрытые приватные блокчейны, где все действия компьютеров одобряются компанией или группой компаний, ведущей реестр. У такого подхода есть свои преимущества: зарегистрированных участников легче собрать в единое управляемое сообщество, чем анонимную массу пользователей биткоина. Это означает, что масштабировать пропускную способность тоже будет проще. Однако приватные системы обычно закрыты для технических экспериментов, а доступ к данным и ПО целиком и полностью

зависит от воли официального куратора. Все это неизбежно тормозит инновацию. Поэтому многим кажется, что «приватный блокчейн» — это оксюморон. Весь смысл данной технологии — в создании открытой, прозрачной, общедоступной системы. Некоторые эксперты предлагают использовать общий термин «технология распределенного реестра» и отказаться от слова «блокчейн», когда речь идет об ограниченном доступе.

Однако банкиры, которым в тот августовский день показали техническую новинку, не вникали в такие тонкости. В целом идея им понравилась. Они понимали, что их собственная система взаимообмена почти парализована из-за проблемы *централизованного доверия*. Взаимное недоверие между банковскими структурами заставляет их утаивать информацию, хранить данные в закрытых, недоступных ячейках, что увеличивает время и стоимость транзакций, повышает вероятность ошибок и риск взлома.

Сложный, многосоставный механизм современной финансовой сферы лишь усугубляет положение. Каждая транзакция проходит длинную цепочку: банк-отправитель, банк-корреспондент, клиринговая организация, брокер, банк-гарант, платежная система и т. д. Прекрасно понимая уровень риска и издержек, банкиры негласно признавали проблемы, которые создатель биткоина Сатоши Накамото пытался разрешить. Может быть, они и не хотели, чтобы простой обыватель мог переслать деньги с Восточного побережья на Западное без всяких посредников, но уж точно осознавали, что в финансовой системе происходит слишком много лишних процессов, из-за которых обмен замедляется, издержки растут, а клиенты теряют терпение.

В 2009 году Накамото писал:

> Ключевая проблема привычной нам валюты — в требовании огромных резервов доверия. Мы должны верить, что Центробанк не обрушит ее курс, но в истории фиатных валют немало случаев, когда это доверие было обмануто. Мы должны верить, что банк сохранит наши деньги и отправит их куда нужно, но банки используют деньги вкладчиков для сомнительных кредитных операций и лишь малую часть оставляют в резерве. Мы вынуждены доверять им конфиденциальную информацию и надеяться, что

> они не позволят злоумышленникам присвоить нашу идентичность и опустошить счета. Огромные банковские комиссии делают микроплатежи невозможными [1].

Накамото писал все это в разгар финансового кризиса. Мировая банковская система стала настолько запутанной и непрозрачной, что заявлениям банкиров уже веры не было. Подлинную стоимость активов было невозможно определить. И в один прекрасный день мыльный пузырь лопнул. Изначально биткоин создавался, чтобы избавить нас от этого хаоса, однако нельзя было с уверенностью заявлять, что ключевой механизм — та самая машина правды, не подвластная манипуляциям изнутри, — сам не окажется под контролем Уолл-стрит.

Тогда, в августе 2015 года, компания Symbiont представила новую торговую платформу Smart Securities. И по иронии судьбы, презентация проходила на верхнем этаже небоскреба с видом на Зукотти-парк — небольшую зеленую площадку, где четырьмя годами ранее родилось движение «Захвати Уолл-стрит» (Occupy Wall Street). Используя распределенный реестр с теми же функциями, что и у блокчейна системы Биткоин (только без внутренней криптовалюты), платформа должна была реорганизовать работу глобальной системы финансового рынка с активами свыше 200 триллионов долларов. Она обещала рационализировать страхование, покупку, продажу и передачу акций, облигаций и прочих ценных бумаг — иными словами, процессы, которые кормят бесчисленное племя инвестиционных банкиров, брокеров и финансовых консультантов Нью-Йорка, Лондона и Гонконга. Можно ли в этом случае говорить о кооптации? Технология, с помощью которой группа киберанархистов мечтала обойти сборщиков дани из глобальной банковской системы, теперь подавалась как перспективный продукт для тех же самых финансовых учреждений.

Четырьмя годами ранее в парке у небоскреба стояли серые палатки, а ораторы с дредами на голове влезали на деревянные ящики и призывали отправить дельцов с Уолл-стрит в тюрьму. Многие активисты стихийного движения — особенно те, у кого вызывала протест гегемония Уолл-стрит и крупных корпораций в целом, — с восторгом приняли биткоин. Цифровая валюта появилась в октябре 2008 года, в разгар банковского кризиса, как своеобразный ответ на самые острые проблемы. Финансовая неразбериха послужила Накамото наглядным

примером риска, на который мы идем, доверяя неблагонадежным банкам вроде Lehman Brothers. И вот теперь CEO Symbiont Марк Смит предлагал приемы из арсенала биткоина тем самым организациям, которые последовали бы в могилу за Lehman Brothers, если бы не деньги налогоплательщиков (по подсчетам Bloomberg News, на спасение банков ушло 12,8 триллиона долларов) [2].

Среди слушателей Смита были руководители UBS, Morgan Stanley и DTCC — финансовой корпорации, которая отвечает за проведение большинства сделок по ценным бумагам в США. Присутствовал и Дункан Нидерауэр, бывший CEO Нью-Йоркской биржи (хотя и не как представитель «старой гвардии», а скорее как инвестор в новый стартап).

Смит начал презентацию с очень простого обещания: сэкономить банкирам время и деньги — много денег. Он представил продукт, который мог сократить весь длинный и сложный процесс продажи и передачи ценных бумаг (занимающий дни, а то и недели) до нескольких кликов мышью и пары минут. Аудитория увидела платформу Smart Securities, слегка похожую на страницу оплаты сервиса Amazon. Там были поля для всех параметров долгового инструмента: имя эмитента, сумма, процентная ставка, срок погашения, когда вступают в силу обязательства эмитента и т. п. В данном случае продавалась облигация, выпущенная компанией-инвестором SenaHill Partners, владевшей долей акций Symbiont. Марк Смит заполнил все нужные поля, нажал кнопку «Выполнить» и продолжил презентацию. Несколько минут спустя он сообщил, что уже пришло подтверждение. Облигация была продана и куплена; вся транзакция заняла буквально две минуты — резкий скачок по сравнению со стандартным сроком проведения таких операций на финансовых рынках США, составлявшим на тот момент двое суток.

Это означало, что риск невыполнения корреспондентом или посредником своих обязательств можно значительно снизить. А риск весьма серьезен — по оценкам DTCC, такие сбои ежедневно уносят более 50 миллиардов долларов на одном только рынке бумаг Казначейства США [3]. Инвесторы нередко используют двухдневное «окно» для выдачи краткосрочных займов из тех средств или ценных бумаг, которые уже обещаны по сделке, но не успевают собрать долг, когда приходит пора оплатить счет. Случается, что третья сторона, которой «одолжили» ценные бумаги, решает сыграть на понижение, то есть продать бумаги в надежде, что их цена упадет, а затем не может найти того, кто

продал бы их обратно по сниженной ставке. Все это оборачивается убытками для истинного владельца активов. Решение этой проблемы позволило бы высвободить триллионы долларов, которые инвесторам приходится держать про запас для покрытия подобных рисков.

В тот день компания Symbiont впервые показала возможный путь будущего развития. За прошедшие несколько лет было предпринято много попыток создать блокчейн-систему для традиционной индустрии финансов. Теперь Уолл-стрит уже не смеется над биткоином, а пытается разработать собственную версию.

Уолл-стрит ищет альтернативу: приватные блокчейны

Хотя поклонники биткоина весьма скептически относятся к закрытым блокчейнам, Уолл-стрит продолжает экспериментировать с этим форматом. «Усеченные» версии биткоина сохраняют элементы мощной криптографической защиты и принципы работы сети, но вместо энергоемкой модели консенсуса с «доказательством проделанной работы» опираются на старые, предшествовавшие биткоину протоколы. Пропускная способность прежних моделей была выше, хотя они не могли обеспечить сравнимый уровень защиты без централизованного механизма контроля, отвечающего за идентификацию и авторизацию пользователей.

Банковские модели в основном применяли созданный в 1999 году алгоритм консенсуса, известный как PBFT (practical byzantine fault tolerance, или «задача византийских генералов»). Он гарантировал всем авторизованным контролерам реестра, что их действия не скомпрометируют общую запись, даже если в их рядах окажется злоумышленник. При такой системе компьютеры вносят обновления в реестр только после сбора определенных свидетельств подтверждения со всей сети.

Закрытые, приватные блокчейны с ограниченным доступом вызывали у разработчиков куда меньше энтузиазма, чем глобальный посыл Эфириума — избавить мир от любых посредников — или распродажи токенов, собиравшие десятки и сотни миллионов долларов. Помогать банкам сэкономить на операциях с ценными бумагами куда скучнее.

Однако у Уолл-стрит толстые кошельки, а это всегда привлекает кадры. К примеру, в разгар «гражданской войны» Биткоина инвесторам удалось переманить нескольких крупных разработчиков и поклонников криптовалюты. Их утомило отсутствие прогресса в эксперименте Накамото, а финансисты предложили возможность создать нечто собственными руками, не впутываясь в мучительные дебаты с аморфным раздробленным сообществом.

Наибольшую пользу из ситуации извлекла исследовательская компания R3 CEV, ориентированная на финансовый сектор. Руководство R3 мечтало о распределенном реестре, который, с одной стороны, собрал бы все плюсы мгновенной проводки ценных бумаг и межотраслевой синхронизации учета, а с другой — встроился бы в сложную систему банковских правил и позволил бы всем участникам сохранить конфиденциальность данных. К весне 2017 года консорциум, возглавляемый R3 CEV, насчитывал более ста компаний. Каждая платит годовой членский взнос в размере 250 тысяч долларов и получает доступ к новейшим разработкам лабораторий R3. Кроме того, в 2017-м основатели компании привлекли около 107 миллионов долларов инвестиций, преимущественно от финансовых структур. Частично эти средства ушли на наём таких специалистов, как Майк Хирн — один из главных разработчиков Биткоина, который расстался с криптовалютным сообществом из-за ожесточенных внутренних конфликтов [4]. Кроме того, R3 привлекла к работе другого знаменитого криптобунтаря — Йена Грigга, позже перешедшего в компанию EOS. В 2017 году научно-технический отдел R3 возглавил весьма известный и уважаемый в блокчейн-сообществе Ричард Гендал Браун. Таким образом, в компании подобрались весьма ценные инженерные кадры.

Еще раньше научным директором лабораторий R3 стал Тим Суонсон — блокчейн-аналитик, который пережил краткий период увлечения биткоином, но позже разочаровался в идеологах криптовалюты и превратился в яростного критика биткоина, злорадствовавшего по поводу всех его неудач. Примерно на тех же позициях стоял Престон Бирн, главный юрисконсульт компании Eris Ltd, позже переименованной в Monax. Компания разрабатывала закрытые блокчейны для банков и прочих организаций. Когда Бирн в соцсетях не выражал свои весьма пестрые политические взгляды — в поддержку Трампа, против выхода Британии из ЕС, за Вторую поправку, за криптографию, против

открытого ПО, — он по обыкновению высмеивал фанатов биткоина. Для Суонсона, Берна и их единомышленников раскол и хаос в лагере Биткоина стали настоящим праздником.

Однако все их насмешки над биткоином можно было адресовать и им самим. Хоть консорциум на базе R3 и заработал очки в сфере высоких технологий, наняв Хирна, Гендал-Брауна и Григга, само его руководство буквально просилось на карикатуру с подписью: «Клуб старожилов Уолл-стрит». Все его девять банков-основателей — Barclays, BBVA, Австралийский банк Содружества, Credit Suisse, Goldman Sachs, J.P. Morgan, Королевский банк Шотландии, State Street и UBS (кроме двух — BBVA и Австралийского банка Содружества) — фигурировали в списке Совета по финансовой стабильности 2016 года как глобальные системообразующие банки. Это не просто крупные банки, чья непомерно раздутая отчетность опасна для внутреннего рынка их страны; здесь речь идет об особой категории. Кредитные портфели этих банков настолько велики, что в случае краха может пострадать вся мировая экономика. А ведь некоторые из них уже столкнулись с многомиллионными штрафами.

Тем, кто внимательно следит за развитием финансовых технологий, это знакомо. Уолл-стрит не впервые присваивает технические новинки, чтобы нейтрализовать потенциальную угрозу. В конце 1990-х появление электронных систем для торговли валютой, ценными бумагами и прочих малопрозрачных операций на рынке капитала едва не породило прямые схемы инвестиций, которые бы покончили с посреднической ролью банкиров. Крупнейшие банки мира немедленно сплотились и запустили собственные онлайн-биржи. В результате банковские контракты по продаже акций, облигаций и прочих активов остались основой инвестиционных сделок, а сами банки сохранили привилегированное положение и возможность диктовать цены.

У регуляторов со свежими воспоминаниями о кризисе 2008 года интерес Уолл-стрит к приватным закрытым блокчейнам тоже вызвал ряд опасений. На слушаниях, организованных Советом по финансовой стабильности (международный регуляционный орган под эгидой G-20), представители центробанков и государственных комиссий по ценным бумагам попытались выяснить, какие системные риски несет будущая рыночная структура на основе блокчейна, может ли она спровоцировать финансовую нестабильность. С одной стороны,

регуляторы вполне уютно себя чувствовали в знакомой компании из глав консорциума R3. Разумеется, им привычнее работать с банкирами, чем с одетыми в джинсы и футболки адептами криптографии. С другой — сама мысль о том, что консорциум крупнейших мировых банков сможет решать, кто и как будет допущен к единому (и единственному!) распределенному реестру всей финансовой системы, незамедлительно вызвала в памяти давние страхи. Что если банки получат чрезмерную полноту власти? Что если вновь придется прибегнуть к непопулярным мерам и спасать их за счет налогоплательщиков? Вдруг Уолл-стрит снова выстроит систему, которая слишком велика, чтобы позволить себе рухнуть?

Панацея от финансовых кризисов?

Давайте посмотрим правде в глаза: хотя было бы неплохо увидеть, как «старички с Уолл-стрит» теряют статус финансовых посредников, законодательные и экономические барьеры делают столь радикальные перемены практически невозможными. По крайней мере, они неосуществимы изнутри. Тем не менее разработчики из лабораторий консорциума R3, а также входящих в него банков и блокчейн-стартапов вроде Digital Asset Holdings и Symbiont порой буквально творят чудеса в попытке отладить нашу перегруженную финансовую систему.

В наши дни процесс перевода активов между разными организациями настолько сложен, что приходится прибегать к услугам специально созданных посредников: клиринговых палат, расчетных агентств, банков-корреспондентов, депозитных банков и т. п. Отчасти они разрешают проблемы доверия, однако они же увеличивают время операций, повышают издержки и риск. Окончательное оформление сделки по облигациям казначейства США занимает два дня. На оформление синдицированного займа может потребоваться месяц. Процесс нередко сопровождается ошибками и сбоями. Что еще важнее, задержки в оформлении парализуют триллионы долларов капитала, которые замирают на депозитных счетах или залоговых соглашениях до тех пор, пока все стороны не согласуют отчетность и не закроют сделку. Более эффективная, синхронизированная система высвободила бы эти

активы и обеспечила мощный приток средств на мировые рынки. Да, банкиры обогатились бы еще больше, но предпринимателям и физическим лицам стало бы гораздо легче получить кредит. Теоретически распределенный реестр компании R3 может осилить все вышеперечисленное и «развязать» денежные потоки.

Скорость оформления сделок — важный фактор финансового кризиса, отчасти способствовавший всемирной панике 2008 года. Отсутствие гарантий того, что контрагент выполнит свои обязательства и переведет средства или ценные бумаги, в любые времена заставляет инвесторов призадуматься. Но когда рынок начинает падать, а страх — пересиливать жажду наживы, чрезмерная осторожность может толкнуть инвесторов на превентивные меры, которые, в свою очередь, запустят порочный круг уничтожения капитала.

Именно системная проблема риска заставила Блайт Мастерс — горячую сторонницу внедрения блокчейна на Уолл-стрит — обратить внимание на распределенные реестры. В 2014 году Мастерс возглавила компанию Digital Asset Holdings, предоставляющую блокчейн-платформы для внутрибанковских операций. Имя Мастерс прежде всего ассоциируется с одним из самых спорных финансовых инструментов нашего времени — кредитным дефолтным свопом, или КДС. Это кредитное соглашение, при котором «покупатель» уплачивает разовые или регулярные взносы «продавцу», а тот обязуется погасить выданный «покупателем» кредит третьей стороне в случае, если он не будет погашен самим должником (дефолт третьей стороны). Работая в команде банка J.P. Morgan, двадцатипятилетняя Блайт Мастерс создала концепцию КДС в качестве инструмента, позволяющего инвесторам застраховать себя от риска и тем самым высвободить капитал, прежде зарезервированный для его покрытия. Кроме того, другие инвесторы, банки и структуры, выпускающие КДС, получили возможность делать ставки на оговоренные в свопе активы, не будучи при этом их фактическими обладателями. Соглашения подлежат купле-продаже, поэтому участники при желании могут продать их третьей стороне.

Такая система значительно повысила ликвидность и упростила работу кредитного рынка, и рынок самих свопов стремительно вырос, достигнув к моменту кризиса их общей номинальной стоимости в 600 триллионов долларов. Проблема, по словам финансового аналитика Майкла Льюиса, заключалась в том, что никто не представлял, как

риск, связанный с обязательствами перед одной из сторон, повлияет на *ее* способность расплачиваться с другими организациями и т. д. [5]. Сделки по свопам проводились фактически «мимо кассы» — не регистрировались на официальных биржах и почти никак не регулировались. Их невозможно было отследить. Когда кризис набрал обороты, этот гигантский, донельзя запутанный клубок обязательств стал причиной всеобщей тревоги, подтверждающей предсказание Уоррена Баффета, который еще в 2002 году назвал свопы «финансовым оружием массового поражения» [6]. Вполне предсказуемое обрушение КДС поставило под вопрос платежеспособность многих банков. Рынки заволновались не только из-за риска дефолта по сомнительным ипотечным кредитам, но и по поводу более глобальной проблемы — исполнения перекрестных обязательств. Банки, сомневающиеся в платежеспособности партнеров, начали выводить кредитные средства с рынка. Паника нарастала как снежный ком, и, чтобы ее обуздать, потребовались государственные гарантии, дотации, дополнительная эмиссия денег. В общей сложности спасительные меры обошлись в десятки триллионов долларов.

Создатели КДС не предвидели подобного исхода — в первую очередь потому, что к нему привели не изъяны в самих контрактах, а недостаточная прозрачность рынка. Именно после кризиса Блайт Мастерс обратила внимание на технологию блокчейн, позволяющую отследить каждую транзакцию на любом рынке, и задалась вопросом: а если бы в 2008 году существовала подобная система, удалось бы избежать глобального кризиса? «Я почувствовала себя Ньютоном — как будто меня ударило яблоком по голове», — вспоминает Мастерс [7]. Она внезапно осознала, что «общедоступный, защищенный и неизменяемый реестр не просто уменьшает проволочки, риски и издержки, но и дает мгновенный доступ к системно значимой информации».

«В посткризисном мире, — утверждает Мастерс, — от решения подобных проблем зависит выживание индустрии финансовых услуг. Я почти тридцать лет проработала на финансовом рынке и имела возможность поразмыслить об управлении, структуре и рисках. В технологии распределенного реестра мне видится инновационная мощь, которая и заставила меня сменить гигантский инвестиционный банк на небольшой стартап. Я сделала это в надежде изменить мир, к которому мы привыкли».

Уже сам факт того, что специалисты уровня Мастерс и разработчиков R3 обратились к недостаткам финансовой системы, чрезвычайно важен. Как мы отмечали, открытые и закрытые блокчейны помогают решить проблему социального доверия. А ведь именно она приводит к системному обрушению рынков. В данном случае речь идет о недостатке взаимного доверия во внутрибанковских структурах и между финансовыми учреждениями. Однако следует отметить, что в поисках решения нынешние разработчики распределенных систем отобрали те свойства изобретения Накамото, которые меньше всего угрожают статусу крупных финансистов (например, криптографическую защиту), и отказались от более радикальных и, пожалуй, более ценных механизмов, — главным образом от общедоступной децентрализованной системы консенсуса.

Конечно, разработчики, нанятые крупными банками, в первую очередь должны обслуживать традиционные финансовые институты. Поэтому их нельзя винить за отказ от революционного подхода к децентрализации, присущего Биткоину. Да и проблема масштабирования сети вызывает серьезные опасения. Например, Депозитарная трастовая и клиринговая корпорация (DTCC), которая проводит бóльшую часть сделок по американским ценным бумагам, обрабатывает 10 тысяч транзакций в секунду. Биткоин на данный момент может обработать только семь. И как бы хорошо ни зарекомендовала себя система безопасности Биткоина, нельзя гарантировать, что миллионные издержки на майнинг остановят злоумышленников, если на кону будут стоять миллиарды долларов в ценных бумагах. Возможно, сам рынок поднимет цены на криптовалюту и ее добычу, тем самым устанавливая новые, более высокие преграды для мошенников. Но этого может и не произойти. В любом случае такой уровень риска недопустим для клиентов R3 и Digital Asset — банков, управляющих пенсионными и зарплатными фондами, государственными ценными бумагами и т. п. В своем нынешнем состоянии — по крайней мере до тех пор, пока такие протоколы, как Lightning, существенно не повысят пропускную способность — Биткоин даже близко не готов обслуживать внутренние транзакции Уолл-стрит.

Нельзя забывать и о юридических проблемах. Научный директор лабораторий R3 Тим Суонсон утверждает, что сама возможность «атаки 51 процент», то есть сценарий, при котором один майнер захватывает 51 процент вычислительных мощностей сети и изменяет реестр

в преступных целях, означает, что в криптовалютных операциях в принципе не бывает «окончательных расчетов» [8]. А на такое состояние вечной неопределенности юристы Уолл-стрит не согласятся никогда. Можно, конечно, возразить, что дотации и прочие спасительные меры, с помощью которых банки фактически отменили собственные потери во время кризиса, лишают смысла всякий разговор об «окончательности». Да, реестр Биткоина намного прозрачнее и надежнее бухгалтерии Уолл-стрит. Тем не менее замечания Суонсона встретили живой отклик среди банкиров. В конце концов, они услышали именно то, что хотели услышать.

С помощью такой логики — то есть игнорируя саму проблему централизованного посредничества, которая и довела финансовую систему до кризиса, — банкиры смогли принять приватный реестр как (условно) идеальную альтернативу недоработанным, технически несовершенным открытым блокчейнам. В системе с ограниченным правом доступа у всех участников есть стимул подтверждать и выверять единый реестр, поскольку это служит их общим интересам. Они не состязаются друг с другом за криптовалюту, поэтому не нуждаются в энергоемкой компьютерной инфраструктуре в духе Биткоина. Кроме того, в закрытой системе не возникнет политических и экономических проблем, которые приходится решать при масштабировании открытого реестра. Ведь здесь не нужно приводить к консенсусу аморфное интернациональное сообщество из тысяч анонимных пользователей; любое предложенное новшество обсуждает небольшая комиссия из знакомых друг с другом специалистов.

Собственно, суть проблемы кроется в этом последнем пункте: маленькая группа избранных решает, что делать, а что нет. Закрытая система во главе с банкирами будет обслуживать интересы тех самых структур, которые уже контролируют финансовый мир и несут ответственность за системные риски, входные барьеры и политические кризисы, то есть все то, с чем борются сторонники криптовалюты. Есть основания утверждать, что внедрение закрытых реестров в банковское дело просто вернет нас в 2008 год — к тому краху системных и общественных институтов, который и обусловил запрос на альтернативные средства и каналы обмена.

Вот почему мы полагаем, что частным лицам, предпринимателям и правительственным структурам необходимо поддержать

радикальные технические меры, предлагаемые разработчиками открытых реестров вроде Биткоина и Эфириума в надежде решить проблемы масштабирования, безопасности и внутренней политики. Мы обсуждали эти предложения в главе 3: внесетевые протоколы Lightning Network у Биткоина и Plasma у Эфириума; сетевые решения в духе SegWit, которые «сжимают» информацию и позволяют децентрализованной системе контролировать, хранить и верифицировать крупные массивы данных, используя намного меньше вычислительных ресурсов. Законодатели должны не ограничивать научно-технический поиск, а, напротив, предоставить разработчикам простор для экспериментов и разрешить инвесторам финансовую поддержку лабораторий. Конечно, не стоит — да и невозможно — препятствовать банкам, которые ищут способ упорядочить внутренний хаос. Однако всем нам пора усвоить урок недавнего кризиса и обратить внимание на блокчейн-системы (хоть открытые, хоть закрытые), ограничивающие власть крупных финансовых структур над рынком. Общество заинтересовано в разработке открытых платформ и свободной инновации. Без нее мы вряд ли преобразим ослабленную финансовую систему и откроем доступ новым участникам игры.

Другая модель: фиатная криптовалюта центробанка

Нельзя упускать из виду еще один фактор, который может спутать все карты финансовым учреждениям. Помимо открытых, функционально совместимых блокчейн-систем, у них есть и другие весьма серьезные конкуренты — центробанки. Если центробанки мира и дальше будут проявлять интерес к внедрению криптовалютных технологий, то в итоге сильнее всех будет задета именно банковская сфера.

В финальной главе книги «Эпоха криптовалют» мы предположили, что правительства и центробанки могут начать выпуск собственных цифровых монет. Что ж, к январю 2017 года уже 26 центробанков запустили поисковые проекты, связанные с технологией блокчейн [9], в том числе Банк Англии, Банк Японии и Банк Канады, как сообщает финансово-технический портал Finextra. Банки многих других стран

проводят предварительные исследования. Никто не знает, чем увенчается этот поиск, но его результаты могут существенно изменить финансовый мир.

В лабораториях Массачусетского технологического института также реализуется международный проект по разработке экспериментальной фиатной криптовалюты, которую смогут применять центробанки и правительства. В основе разработок лежит блокчейн-инструмент под названием Cryptokernel, или CK, созданный массачусетским исследователем Джеймсом Лавджоем. CK — продукт с открытым исходным кодом, поэтому с ним может экспериментировать любой желающий. «Это очень важный момент, — отмечает Роблех Али, научный сотрудник, который присоединился к группе после работы над аналогичным проектом Банка Англии, — поскольку это означает, что разработка финансовых механизмов будущего открыта лучшим умам мира. С приходом каждого нового участника повышаются шансы создать поистине децентрализованную финансовую систему, которая будет подвластна народу, а не банкам» [10].

Первый продукт, созданный на базе Cryptokernel, — экспериментальная цифровая валюта под названием K320 — существенно отличается от биткоина. В то время как для эмиссии биткоинов установлен жесткий лимит — максимум 21 миллион монет к 2140 году, — у K320 таких ограничений нет. Разработчики надеются, что при уменьшении фактора редкости пользователи перестанут накапливать монеты, как это происходит с биткоином. Многие эксперты полагают, что биткоин прежде всего будет играть роль капиталовложения (как золото или драгоценности), а не обыкновенной денежной единицы для повседневных платежей. Однако обществу нужно, чтобы граждане тратили деньги, а не держали их про запас, а накопительский инстинкт — это своего рода память о многочисленных финансовых кризисах (самым тяжелым из которых в истории США, разумеется, был период Великой депрессии). Чтобы не превратиться в мертвый груз, K320 должна выпускаться регулярно, с поправкой на небольшую инфляцию. Это означает, что после фазы активной эмиссии в первые восемь лет запас криптовалюты будет стабильно пополняться на 3,2 процента в год. Ставка намеренно сделана несколько выше, чем стандартные 2 процента, которые большинство центробанков намечают для индекса потребительских цен в своей стране. Разработчики K320 стремятся избежать

как чрезмерной дефляции (которая может привести к массовому накоплению, как во времена Великой депрессии), так и бурной инфляции (когда население стремится быстрее расстаться с деньгами, как в Германии периода Веймарской республики 1920-х годов).

Хотя график эмиссий K320 отображает стратегию большинства центробанков, маловероятно, что национальные банки развитых стран возьмут на вооружение криптовалюту, чей выпуск не смогут контролировать. Скорее всего, их пробные проекты будут иметь больше общего с нынешней системой, чем K320. Зато немало аргументов в пользу того, что первыми алгоритмическую эмиссию денежных единиц опробуют центробанки развивающихся стран, где плюсы политического контроля над валютой отнюдь не очевидны в силу частых финансовых кризисов. В любом случае тот факт, что центробанки всех мастей проявляют интерес к цифровым активам, открывает путь к серьезным изменениям в системе фиатных валют.

Если бы существовали криптовалюты, выпущенные правительством или центробанком, то физические лица или организации, откладывая средства исключительно в кастодиальных целях, предпочли бы хранить их непосредственно у эмитента. Это было бы гораздо дешевле и надежнее, чем доверять деньги частным структурам и выплачивать комиссии, которые они устанавливают, чтобы не потерять прибыль. Иными словами, центробанк станет грозным конкурентом коммерческим банкам, если домохозяйства и корпорации смогут выбирать, где хранить средства для бюджетных расходов, будь то «продовольственные» деньги или зарплатный фонд. Для примера возьмем корпорацию Apple. В конце декабря 2016 года у нее на бюджетных счетах скопилось 246 миллиардов долларов. Бóльшая часть этих средств была инвестирована в краткосрочные инструменты вроде казначейских векселей США, однако и тот «скромный» остаток, что ушел на депозитные счета, составлял огромную сумму. Логично предположить, что при наличии выбора подобные компании переместили бы значительную часть активов под присмотр центробанка. Вот почему исследовательская группа Банка Англии утверждает, что желательно установить различные процентные ставки: более низкие для криптовалют центробанка и более высокие для депозитов [11]. Это предотвратит резкий отток фондов и обеспечит плавный переход на цифровую валюту.

Тем не менее руководители многих центробанков согласны, что постепенный вывод коммерческих банков из платежного процесса может оказать оздоровительный эффект. Теоретически он должен снизить издержки и риски, ведь жаждущие прибыли банки (кое-кто, пожалуй, сказал бы, что они жаждут ренты) перестанут взимать плату за коммерческую деятельность. Важно и то, что правительствам и центробанкам не придется любой ценой выкупать коммерческие банки, как это было в 2008 году, когда казалось, что надвигающийся коллапс похоронит под собой всю платежную систему экономики. Центробанки прекрасно знают, до какой степени этот кризис, вынудивший до нуля понизить процентные ставки, ограничил их способность стимулировать экономический рост. Один из самых мощных доводов в пользу выпуска криптовалюты центробанками — это обещание финансовой стабильности в будущем.

Таким образом, появление криптовалюты выявило конфликт между интересами центробанков и контролируемых ими коммерческих структур. В течение многих лет они пребывали в отношениях симбиоза: частные банки пользовались правом эксклюзивного доступа к государственным финансовым инструментам, а взамен претворяли в жизнь политику центробанков. Этот союз породил немало конспирологических теорий и мифов (нередко замешанных на антисемитизме) о тайных ложах и обществах, которые правят миром. Действительность, конечно же, была намного сложнее. Однако теперь, когда технология блокчейн предлагает новые модели эмиссии, обмена и обслуживания денежных единиц, интересы двух сторон могут оказаться прямо противоположны.

Hyperledger: борьба с самим собой

Не только «старая гвардия» финансового сектора вынуждена приспосабливаться к переменам. Множество некоммерческих структур тоже рассматривают технологию блокчейн, пытаясь понять, что она может изменить в их жизни. Один из самых интересных и значимых проектов в этой сфере носит название Hyperledger. Он проводится под эгидой большого корпоративного консорциума и предназначен

для открытой совместной разработки отраслевых блокчейнов. Однако главная цель проекта куда амбициознее — создание общей распределенной инфраструктуры для глобальной экономики, пригодной не только для банковского дела, но и для «интернета вещей», логистики и производства.

Учреждая консорциум, руководство корпораций-участников выразило общую заинтересованность в превращении глобальной цифровой экономики в более мощную и открытую. На сайте проекта разрабатываемая технология описывается как «операционная система для рынков, информационных сетей, микровалют и децентрализованных цифровых сообществ» [12]. При этом утверждается, что Hyperledger «может значительно удешевить и упростить рабочие процессы в реальном мире». Столь глобальный образ мышления, безусловно, требует внимания к любым моделям, которые могут хорошо зарекомендовать себя в будущем. Поэтому неудивительно, что среди членов консорциума (а к концу 2016 года их насчитывалось уже более сотни) немало компаний, ориентированных на биткоин и децентрализованные криптовалютные системы в целом. В их числе можно назвать Blockstream, разработчика блокчейн-приложений Bloq, а также Blockchain.info — сервис виртуальных биткоин-кошельков и обозреватель блоков. И все же тон в консорциуме задают крупные корпорации, и это порождает координационные проблемы. Бизнес-модели этих компаний изначально опираются на централизованную обработку данных и роль доверенных посредников при транзакциях клиентов. Потому и здесь закономерно разгорелся спор о преимуществах открытых и закрытых реестров.

Крупнейшие основатели Hyperledger, включая IBM, Digital Asset, Accenture, DTCC и Intel, привлекли к управлению проектом знаменитый консорциум Linux Foundation. Именно он создал ядро ОС Linux, которая установлена на 90 процентах мировых серверов, широко применяется для работы роутеров, ресиверов цифрового телевидения и легла в основу операционной системы Android. История Linux — наглядный пример того, как открытая разработка ПО может привлечь ярчайшие таланты мира и породить удобную, надежную, универсальную технологию. К тому же для проекта Hyperledger был выбран исполнительный директор, известный своей любовью к *открытым* платформам: Брайан Белендорф, один из главных разработчиков веб-сервера

Apache и член совета директоров Mozilla Foundation и Electronic Frontier Foundation.

[196] Все это очень важные сигналы. Имея перед собой чистый лист и сложнейшую задачу — разработать новую операционную систему для глобальной цифровой экономики, жизненно необходимо поощрять открытые инновации, чтобы революционные идеи не подавлялись напуганными контролерами. Джой Ито, глава медиалаборатории Массачусетского технологического института, напоминает: «В онлайн-экономике победили не первые замкнутые "интранеты" вроде системы Minitel от France Telecom или внутренние сети компаний AOL и Prodigy, а общедоступная сеть, возникшая благодаря паре открытых протоколов TCP/IP» [13]. С тех пор открытую структуру интернета защищает ряд глобальных некоммерческих организаций (хотя полнота их власти вызывает некоторые опасения). Похоже, что и проект Hyperledger будет опираться на аналогичные принципы.

Тем не менее «звездный состав» руководителей Hyperledger вызывает организационные проблемы. Каждая компания должна защищать интересы своих акционеров, то есть настаивать на внедрении тех элементов программного кода, которые наилучшим образом подходят для их рода деятельности. Конечно же, в привилегированном положении оказываются компании с лучшими кадровыми ресурсами: они просто создают бóльшую часть кода. Когда их интересы идут вразрез с интересами других участников проекта, внутренняя политика каждой компании перевешивает стремление к общей цели. «Подписать пресс-релиз легко. Трудно сделать все, на что замахнулись, — сказал Джим Землин, исполнительный директор Linux Foundation на первом собрании группы разработчиков Hyperledger в январе 2016 года. — Мы пытаемся руководить открытым проектом. Мы искусственным образом объединили людей, которые работают в очень разных местах. Так давайте же прислушиваться к точке зрения каждого из них» [14]. Землин рассказал собравшимся, какой урок компания IBM извлекла из сотрудничества с Linux Foundation. Поначалу она вознаграждала разработчиков Linux в зависимости от количества строк кода IBM, внесенных в проект. Предполагалось, что IBM получит максимальную прибыль, если код операционной системы Linux будет оптимизирован для работы с продуктами компании: компьютерами, серверами и различными IT-решениями, которые IBM предлагает клиентам (особенно если тот

же код будет не слишком совместим с продукцией конкурентов). Однако, по словам Землина, руководство IBM вскоре осознало, что выбрало далеко не самый удачный способ взаимодействия с открытым сообществом Linux. В итоге было решено поощрять программистов за работу, которая улучшает общее качество ПО. Оказалось, что это гораздо выгоднее и для IBM.

Пример был приведен неспроста, ведь к тому моменту IBM уже явно претендовала на ключевую позицию в проекте Hyperledger. На том же собрании в январе 2016 года корпорация представила 44 тысячи строк «чейнкода» для автоматизированных смарт-контрактов, фактически сделав безвозмездный взнос в разработку общего ПО для распределенного реестра Hyperledger, ныне известного как Fabric [15]. С одной стороны, это можно расценивать как щедрый жест. С другой — это означает, что корпорация изначально пыталась повлиять на формат проекта. Со временем у многих сложилось впечатление, что система, которую представляло себе руководство IBM, «заточена» под узкий профиль компании: облачные сервисы и хранилища. Отвечало ли это интересам сообщества?

Конечно, и другие участники консорциума вносят вклад в форме кода и идей. Компания Digital Asset представила инструмент Global Synchronization Log для финансовых структур; разработчики Intel предложили программу Sawtooth Lake для подтверждения благонадежности вычислительных устройств. Однако мощный ход IBM сделал корпорацию ключевым игроком в экосистеме Hyperledger и повысил вероятность того, что именно ее интересы будут определять параметры кода и диктовать экономические приоритеты всего проекта. Подобные факторы тревожили и сообщество биткоина в период «гражданской войны». Пользователи по обе стороны баррикад знали, какие гонорары выплачивают компании некоторым разработчикам, и понимали, что те будут ратовать за или против увеличения блока в зависимости от взглядов своего работодателя.

Что касается проекта Hyperledger, то здесь интересы IBM прежде всего связаны с возможным применением блокчейнов в сфере логистики. Как упоминалось в предыдущей главе, компания уже использует свой код для оптимизации механизма разрешения споров между заказчиками и поставщиками. Когда Джерри Куомо, вице-президент IBM по вопросам технологии блокчейн, отчитался перед сообществом

Hyperledger об успехе этого начинания, он представил веские аргументы в пользу приватных блокчейнов. Оказалось, что применить технологию блокчейн к последовательной записи транзакций можно и без помощи открытых систем. Однако Джерри Куомо невольно показал и другое: как деловые интересы наиболее влиятельных членов могут отвлечь консорциум от разработки по-настоящему инновационной открытой системы. Вскоре стало очевидно, что руководство IBM увидело в совместном проекте прежде всего возможность вернуть себе клиентов — особенно тех, кто бился над оптимизацией цепей поставок. Через год компания запустила собственный блокчейн-сервис, благодаря чему слово «блокчейн» впервые прозвучало в телевизионной рекламе. Клиентам предлагалось объединиться с контрагентами в цепи поставок и создать приватный блокчейн со структурой, полностью интегрированной с уже существующим облачным сервисом IBM. Поручить IBM хранить данные из вашего реестра — то есть обратиться к «доверенной третьей стороне» — значит отказаться от революционной, свободолюбивой природы блокчейна.

Подобная манипуляция стала отчасти возможна за счет ложных представлений, связанных с термином «облачные хранилища». Когда IBM, Amazon, Google или любой другой провайдер облачных технологий хранит ваши файлы или предоставляет вам доступ к сторонним облачным сервисам, все операции выполняются на вполне конкретных серверах, принадлежащих этой компании. Они хозяева, а мы арендуем у них место на сервере. Многим кажется, что «облако» — это аморфная, децентрализованная система, однако на самом деле это предельно централизованная технология, целиком зависящая от посредника.

Огромный потенциал технологии блокчейн кроется в децентрализации, которая делает пользователя не зависящим от какой-либо промежуточной инстанции, выполняющей нужное ему действие. (На самом деле на базе блокчейн-архитектуры уже сейчас разрабатываются специальные приложения, которые позволят полностью децентрализовать хранение файлов и предоставят внесетевые сервисы.) Модель блокчейна, предложенная компанией IBM, скорее, ограждает процветающий централизованный бизнес от угрозы со стороны децентрализующих технологий. С точки зрения акционеров IBM, это вполне оправданная, рациональная и грамотная стратегия, однако она

противоречит духу открытых платформ, который пропагандирует сам же концерн Hyperledger. Кроме того, возникает и ряд правовых вопросов: если ключевые данные из блокчейн-реестра хранятся на компьютерах некоей компании, то может ли государство, согласно нынешнему закону о хранении данных, контролировать этот блокчейн?

Вышеупомянутые проблемы показывают, как сложно заставить корпоративный консорциум, многие члены которого уже давно забыли о собственных бунтарских стартапах и обзавелись крупным бизнесом, уязвимым для радикальных инноваций, действовать в интересах широкой межотраслевой группы производителей и их будущих клиентов. Это важно, поскольку реализовать заявленные цели, очевидно, смогло бы лишь сообщество, разделяющее нашу веру в децентрализацию. Разнообразие, богатство возможностей и совместный творческий поиск в конце концов породят открытую систему, которая отвергает чрезмерное влияние любых инстанций, противостоящих внедрению инноваций, если они угрожают их интересам.

Границы доступа

Квазицентрализованные приватные блокчейны, с которыми сейчас экспериментируют крупные финансовые структуры и корпорации-техногиганты, по своей сути не так уж плохи и непродуктивны. Идеи и открытия, родившиеся в ходе исследований на базе консорциумов R3 и Hyperledger, войдут в фонд знаний, с помощью которого технологи и предприниматели всего мира выстроят новую, улучшенную глобальную систему доверительного управления. Но если принять во внимание уроки истории — например, о победе открытых интернет-протоколов TCP/IP над «огороженными» микросетями вроде Minitel, AOL или Prodigy, — становятся заметны внутренние ограничения приватных блокчейн-систем. Как напомнил Джой Ито, маленькие закрытые сети проиграли из-за невозможности справиться с наплывом программ и приложений, созданных для работы в общей, глобальной экосистеме интернета. Какой пользователь или разработчик захочет мучиться с громоздким и медленным почтовым клиентом AOL, когда есть множество открытых, общедоступных сервисов, к которым

ежедневно добавляются новые опции? Примерно ту же расстановку сил скоро можно будет наблюдать в битве открытых и закрытых блокчейнов, полагает Ито.

Открытые системы, такие как Биткоин и Эфириум, по своей природе способствуют творческому поиску и инновации, поскольку ни одна компания или группа компаний не может наложить вето на то или иное новшество. Даже если кураторы приватных систем заявят о готовности открыть свои платформы для всех желающих, сам факт наличия «хозяев и охранников» будет чреват ограничениями для посторонних. И это, несомненно, оттолкнет многих разработчиков открытого ПО, которые могли бы внести свой вклад в развитие платформы. Ведь именно гарантия открытого доступа порождает бурный энтузиазм и тягу к «свободным» сетям, о чем говорит количество и качество разработчиков, вовлеченных в создание открытых блокчейн-приложений. Вероятно, и у приватных блокчейнов появится своя ниша — хотя бы потому, что ими гораздо проще управлять и на данной стадии развития технологий они лучше справляются с крупными многочисленными транзакциями. И все-таки нашей главной целью должна стать дальнейшая эволюция открытых, функционально совместимых платформ.

В наших интересах построить мир открытых реестров и распределенных моделей доверия, в котором у каждого пользователя будет право голоса. Давайте же приложим к этому все усилия!

Глава

7

Блокчейн как сила добра

В трущобах вокруг стадиона Сан-Лоренцо в Буэнос-Айресе (домашнего стадиона любимой футбольной команды папы Франциска) нашли приют сотни тысяч беднейших иммигрантов из Боливии. Многие живут в лачугах, которые запросто может смыть при разливе реки Матанса. Между тем посередине этого бедняцкого района есть крохотная улочка длиной буквально в два квартала, где дома выделяются своей добротностью. Здесь находится школа, больница и несколько учреждений культуры боливийской диаспоры. Географически улица Чаруа ничем не отличается от остальных. Так почему же семьям, живущим в этих двух кварталах, настолько повезло? Почему это место стало центром боливийской культуры?

Ответ можно сформулировать в двух словах: право собственности.

В 1991 году после многолетней «войны» с городскими властями 200 семей, проживающих на улице Чаруа, наконец получили то, что послужило мощнейшим толчком к развитию района, — свидетельство о собственности на жилье [1]. Доход этих семейств был ничуть не выше, чем у соседей, социальный статус и уровень образования тоже. Единственное различие состояло в том, что им удалось официально подтвердить право собственности. «Волшебные бумаги» открыли перед ними многие двери. Как налогоплательщики и домовладельцы они получили определенное положение в обществе, а следовательно, могли требовать услуг от местных властей. Так появились школа и больница. Кроме того, под официально оформленную недвижимость можно

взять кредит и открыть свое дело, поэтому улица Чаруа обросла магазинами и ресторанчиками. Конечно, гостям из престижных районов Буэнос-Айреса все это покажется довольно жалким, но для местных боливийцев эти два квартала — наглядный пример того, что их собратьям может улыбнуться судьба.

Какое отношение все это имеет к блокчейну? Чтобы ответить на этот вопрос, давайте поговорим не о счастливцах с улицы Чаруа, а о сотнях тысяч боливийцев и прочих обитателей трущоб Буэнос-Айреса и других городов развивающегося мира, у которых нет никаких официальных документов на жилье. Конечно, соседи признáют их хозяевами дома, но это ничего не значит в глазах правительства или банка. Бюрократические органы в бедных странах, как правило, коррумпированы и некомпетентны. Обитатель индийских или филиппинских трущоб может попробовать взять кредит под залог дома, однако ни один банк не примет такое обеспечение. Даже более обеспеченные домовладельцы часто сталкиваются с проблемами: например, покупают квартиру у застройщика, а затем обнаруживают, что тот дал чиновникам взятку, чтобы объект по-прежнему числился за ним. Подтвердить право собственности в подобных условиях настолько сложно, что банки весьма неохотно дают ипотечные кредиты, по крайней мере под разумный процент.

Однако в последнее время начали появляться стартапы, пытающиеся разрешить бюрократические проблемы с помощью технологии блокчейн. И это неудивительно, ведь распределенный реестр неизменяем, все транзакции в нем имеют отметку о времени и открыты для общественного контроля. Кроме того, блокчейн позволяет почти мгновенно совершить передачу права собственности и подтвердить сделку с помощью уникальных криптографических ключей. Поэтому изменить реестр в одностороннем порядке практически невозможно. В вышеописанном случае застройщик (теоретически) не смог бы подкупить чиновника, чтобы удалить информацию о сделке, потому что ни у одного из них не было бы криптографического ключа для подтверждения отмены.

Мы говорим «теоретически», потому что все эти идеи пока не прошли проверку в крайне сложной и политизированной сфере права на недвижимость. Не исключено, что с помощью взяток в реестр все же будет попадать заведомо ложная информация. В странах

третьего мира, где реестры придется выстраивать с нуля, высок риск того, что продажные чиновники с самого начала постараются обеспечить себе простор для маневра. Чуть позже мы обсудим способы снизить такой риск. Однако если реестр рассматривается как истина в последней инстанции, вопрос о том, какие данные в него внесены, становится жизненно важным.

Тем не менее, если взглянуть на ситуацию максимально широко и предположить, что в большинстве случаев блокчейны будут использоваться с добрыми намерениями, преимущества криптографически защищенного реестра недвижимости выглядят весьма заманчиво. По оценке перуанского экономиста Эрнандо де Сото, «мертвый капитал», то есть недокументированный жилищный фонд по всему миру, приблизительно равен 20 триллионам долларов [2]. Если бы малообеспеченные граждане смогли брать кредиты под залог этого капитала, совокупный эффект от притока средств обеспечил бы развивающимся странам 10-процентный экономический рост, что составило бы более половины мирового ВВП.

Недвижимость — это далеко не все. Технология блокчейн позволяет задуматься о том, как помочь беднейшему населению подтвердить право на разные виды имущества, такие как мелкий инвентарь и транспортные средства, а также доказать благонадежность и кредитоспособность, реализовать избирательные права и т. д. Есть надежда, что блокчейн станет тем необходимым свидетельством репутации, которое позволит миллионам людей активно включиться в глобальную экономику, куда доступ им до сих пор был закрыт.

Доказательство

Наше общество разработало систему проверок, которые каждый из нас должен пройти, чтобы участвовать в торговом обмене и социальном взаимодействии. До тех пор пока человек не доказал, что он именно тот, за кого себя выдает, и пока его имя не увязано с историей платежей, правом на имущество и прочими индикаторами благонадежности, он не может завести счет в банке, взять кредит, проголосовать на выборах и т. п. Ему доступны разве что электричество и мобильная связь.

Вот почему технология блокчейн настолько важна для глобальной финансовой инклюзии: она может помочь с подтверждением репутации. Проще говоря, каждому из нас нужна возможность объяснить и доказать, *кто я, чем занимаюсь и чем владею*. Прежде чем нанять сотрудника или заключить сделку с партнером, в любом учреждении всегда задают вопросы об идентичности, репутации и прочих персональных активах.

Успех любого начинания в конечном счете зависит от нашей способности доказать благонадежность. Вы бы взяли на работу человека, о котором ничего не знаете? Одолжили бы ему денег? С такими людьми рискованно иметь дело, потому им приходится платить непомерно дорого за доступ к любым финансовым услугам. Им выдают кредиты под самый высокий процент, а в ломбардах они вынуждены соглашаться на ничтожную долю от истинной цены закладываемого имущества. За любую транзакцию они платят большую комиссию. То, что мы с вами можем приобрести по кредитной карте, причем безо всяких процентов в первые 25 дней, они должны сразу же оплатить наличными. Бедность — дорогое «удовольствие», вот почему с ней так сложно покончить.

Иногда осторожность финансистов продиктована строгостью закона, а не их личным нежеланием помочь. Например, в США и других развитых странах банкиры обязаны назначать повышенную ставку при сомнительном обеспечении кредита. И все же большинство отказов и ограничений обусловлено страхом за свои вложения. В любом случае инструмент, который позволит представить более понятную и прозрачную картину сложной человеческой жизни, должен помочь финансовым институтам снизить стоимость кредитования и страховки.

Эта проблема присуща не только развивающимся странам. В США 7,7 процента населения не охвачены банковскими услугами, то есть не имеет банковских счетов; 17,9 процента считаются частично охваченными, то есть пользуются услугами микрофинансовых организаций, берут кредиты под ежедневный процент и т. п. [3]. В Балтиморе 14 процентов жителей не имеют доступа к финансовым инструментам; в Мемфисе таких жителей 17 процентов, в Детройте и Майами — 20 процентов. Даже представители среднего класса не всегда могут успешно подтвердить свою благонадежность. Например, многие виды выплат по кредитам не фигурируют в скоринговой модели FICO,

которой банки по умолчанию пользуются для оценки кредитоспособности клиента. И все же большинство из нас воспринимают свидетельство о рождении, водительские права, выписку со счета и кредитную историю, то есть главные доказательства благонадежности, как нечто само собой разумеющееся. Поэтому самые серьезные перемены, конечно, произойдут в развивающихся странах.

По оценкам Всемирного банка, более двух миллиардов взрослых жителей Земли лишены доступа к банковским услугам [4]. Однако есть и хорошие новости: сочетание гуманитарных и коммерческих интересов породило массовое движение за допуск беднейших слоев населения в мир современных финансов. Это, несомненно, порадует и тех, кто ищет новые рынки сбыта, — если задачу удастся решить, нас ожидает беспрецедентный экономический бум. Надо лишь свести воедино новые рынки, новых потребителей, новые продукты и триллионы долларов неучтенного капитала, который они с собой принесут.

Хотя термин «не охваченные банковскими услугами» используется широко, он не совсем точен. Отчасти, конечно, он отображает реальное положение дел: эти люди действительно не могут воспользоваться стандартными банковскими предложениями, что серьезно осложняет им экономический обмен. Однако он же создает впечатление, будто достаточно просто открыть им банковские счета. Но, как показал опыт применения биткоина и блокчейнов, одноранговая система цифрового обмена, избавленная от громоздких, дорогих и по определению недемократичных банковских механизмов, может предложить более эффективный путь развития.

Тем не менее в наши дни банки активно участвуют в дебатах о «финансовой инклюзии». Среди ключевых пунктов в долгосрочном плане ООН по искоренению нищеты числится «поощрение и расширение доступа к банковским, страховым и финансовым услугам для всех категорий населения» [5]. А Всемирный банк предлагает особую инициативу под названием «Всеобщий доступ к финансовым услугам к 2020 году» (UFA2020). Как утверждает Консультативная группа по оказанию помощи беднейшим слоям населения, в 2013 году ряд финансовых структур, коммерческих и благотворительных организаций, инвестиционных фондов и тому подобного направил 31 миллиард долларов на расширение финансовой инклюзии. Ожидается, что ежегодно сумма отчислений будет возрастать на 7 процентов.

Чем здесь может помочь технология блокчейн? Давайте вспомним, что изначально хотели создать ее разработчики — улучшенную универсальную систему записи и хранения данных, которая не поддается фальсификации и в любой момент будет доступна всем желающим. Такой замысел существенно меняет расстановку сил между крупными институтами — правительствами или корпорациями — и тем населением, которому они в идеале призваны служить. Контроль над собственными данными позволяет нам реализовать свои гражданские права и обеспечивает незыблемую основу для взаимодействия с окружающими. И наоборот, если мы не можем контролировать информацию, если она переменчива и недостоверна (идет ли речь о данных, связанных с нашим имуществом, или об истории платежей по коммунальным счетам), это ставит нас в заведомо проигрышную позицию по сравнению с теми, кто обладает всей полнотой власти. Такое неравенство сил как раз и объясняет — позволим себе воспользоваться подзаголовком книги Эрнандо де Сото, — «почему капитализм торжествует на Западе и терпит поражение во всем остальном мире» [6]. Сейчас у нас появилась возможность решить проблему дисбаланса, и от одной лишь этой перспективы уже захватывает дух.

Цифровая метка

В сущности, главная ценность блокчейна — это система цифровых меток, которую он предоставляет. Когда житель развитой страны покупает дом или машину, регистрирует собственное дело или заводит семью, это всегда подтверждается официально: контрактами, патентами, свидетельствами, актами приемки-передачи и пр. Каждая бумага заверена уполномоченной инстанцией. Печать на ней, конечно, всего лишь символ, но очень могущественный. Фактически это символ «истины».

Вероятно, вам и в голову не приходит, что кто-то может оспорить ваше право собственности на дом или машину, или законность вашего бизнеса, или факт рождения вашего ребенка. Но если бы такое случилось, то вы бы просто предъявили официальный, нотариально заверенный документ. Его наличие автоматически делает вас полноправным и законным хозяином или попечителем. Самое же главное

в документе — это проставленная дата, поскольку она свидетельствует: произошло важное событие (рождение, вручение диплома, свадьба, передача имущественных прав). Благодаря ей вырабатывается общая, единая версия истории, на которую может сослаться любой из нас.

Первые печати датируются 7600 годом до н. э. и появились на территории современной Сирии. Это были вырезанные из камня небольшие цилиндры (цилиндрическая печать), которые цепляли на ожерелья, браслеты или просто прикалывали к одежде. Они использовались как личная подпись и были у каждого — от царя до раба [7]. Позже печати приобрели знакомую нам плоскую форму, однако их предназначение не изменилось: оттиск на глине или воске удостоверял подлинность документа и личность подписавшего. Эта традиция жива до сих пор, хотя мы, жители развитых стран, о ней даже не задумываемся. Скорее при слове «печать» мы думаем о неудобствах, связанных с походом в официальные инстанции. А ведь сила печати огромна. Именно ее нам и предлагает блокчейн. Открытый, общедоступный и общепризнанный реестр, который можно проверить в любое время, играет примерно ту же роль, что и печать: подтверждает, что некое действие совершено в указанное время при определенных обстоятельствах. Причем делает это таким образом, что изменить запись в одностороннем порядке не сможет ни частное лицо, ни правительственная структура.

Вполне вероятно, что блокчейн заменит нотариальные конторы (возможно, в виде отдельных государственных платформ или общей универсальной платформы, неподвластной отдельным правительствам). Неудивительно, что первые попытки применить блокчейн вне криптовалютных систем связаны как раз с нотариальными услугами. Специалисты из техасской компании Factom быстро осознали, что официальные документы можно заносить в неуязвимый реестр, и создали аудиторский сервис, чтобы отслеживать любые изменения в финансовых документах. Если эта модель приживется, она позволит перевести все процедуры ежеквартального и ежегодного аудита в режим реального времени. Отдельного упоминания заслуживает компания Stampery — детище талантливого молодого предпринимателя из Испании Луиса Куэнде, запустившего в возрасте 12 лет свой первый проект по разработке ПО, а к 21 году заслужившего репутацию одного из самых смелых инноваторов мира. Stampery собирает хеши различных документов и фиксирует все их изменения в блокчейн-реестре,

предоставляя отчет об их статусе компаниям, вовлеченным в переговоры или судебные разбирательства. Таким образом можно, например, отследить историю правки, которую различные юристы и подписанты вносили в контракт на разных стадиях обсуждения будущей сделки.

Однако подобная модель сертификации может иметь гораздо более широкое применение и уж точно заинтересует не только юристов и предпринимателей. Подумайте о сфере кредитования, где цена, как говорят банкиры, «привлечения клиента», то есть всех тех работ, которые нужно выполнить, чтобы убедиться в его кредитоспособности, часто непомерно высока, и это в развитых странах. А что уж говорить о третьем мире? Огромное количество времени, которое нужно потратить на сбор информации о человеке, у которого нет официальной финансовой истории, а иногда даже удостоверяющих личность документов, и вовсе делает кредитование нецелесообразным. Микрофинансовые организации, которые предоставляют небольшие займы малоимущим, пытаются решить эту проблему с помощью кредитных специалистов, которые знакомятся с потенциальными клиентами, изучают условия их жизни, поручаются за них и занимаются сбором и доставкой выплат. Однако такой штат требует огромных расходов и понижает рентабельность. Потому не стоит удивляться, что вскоре после того, как основатель банка Grameen Мухаммад Юнус получил Нобелевскую премию мира за идею микрофинансирования, высокий процент непогашения кредитов и ряд скандалов выявили все недостатки этой отрасли [8]. Миллиарды жителей планеты по-прежнему не охвачены программами кредитования в силу информационного хаоса.

Именно эту проблему и может устранить блокчейн — навести порядок в информационном поле. Наиболее широкий подход к технологии предложили те разработчики, которым хватило фантазии превратить блокчейн Биткоина из платформы для обмена криптовалютой в универсальный инструмент, применимый к любым активам. Эта трансформация породила множество взаимосвязанных идей и решений, которые завладели умами инноваторов в самых разных сферах и теперь заполняют страницы этой книги.

У истоков движения стояла группа разработчиков во главе с Алексом Мизрахи. В 2013 году команда запустила версию «Биткоин 2.0» под названием Colored Coins, взяв за основу наброски Мени Розенфельда, опубликованные годом ранее. Идея заключалась в следующем: записать

уникальные, подтвержденные метаданные о материальном объекте — например, серийный номер автомобиля или географические координаты земельного участка — и связать их с именем законного владельца, который получит персональный ключ доступа к биткоин-аккаунту. Для выполнения операций в системе Биткоин необходимо заполнить информационные поля, и при передаче права собственности на автомобиль новому владельцу хеш этого документа можно будет вставить в транзакцию, подтвержденную сетью майнеров. (Алгоритм хеширования здесь аналогичен используемому майнерами биткоина, за исключением того, что его выполняет владелец имущества или тот, кто уполномочен обновлять эту информацию. По сути, текст документа, в который внесены новые сведения относительно прав и обязанностей, включая новое имя собственника и условия владения имуществом, обрабатывается с помощью необходимых инструментов и на выходе дает численно-буквенную последовательность — хеш. Затем этот хеш вносится в параметры блокчейн-транзакции.)

В данном случае количество использованной криптовалюты не имеет значения. Можно перевести несколько центов, хотя, вероятно, понадобится еще заплатить майнерам за включение транзакции в блок. Однако сама транзакция — не более чем способ передать информацию о некоем праве или соглашении. Это стало возможным потому, что, как мы уже говорили, криптовалюта в блокчейне обладает рядом свойств, которые отличают ее от привычных нам денег: она поддается программированию и может передавать данные и инструкции. Заметим, что владельцу активов необязательно использовать этот инструмент только для передачи права собственности. Он может сделать перевод между своими же биткоин-кошельками исключительно для того, чтобы неопровержимо подтвердить факт владения домом, автомобилем или иным видом имущества.

На практике Биткоин оказался не самым удобным инструментом для таких операций, поскольку его язык программирования имеет ограниченные функции. Именно поэтому более гибкий и многофункциональный Эфириум и другие блокчейн-платформы привлекли внимание многих разработчиков. Но если говорить о замысле, то проект Colored Coins — чьи авторы уже успели основать новый блокчейн-стартап Chromaway, который регистрирует сделки с недвижимостью в Швеции, — был прорывным. Он поставил вопрос о создании

защищенного от фальсификаций реестра активов и объединил новую идею децентрализованного доверия с многовековой практикой отслеживания собственности: истории правообладателей, документов, актов передачи.

Если вы когда-нибудь покупали жилье, то наверняка знаете, что такое проверка юридической чистоты объекта (хотя, возможно, и не до конца представляете, зачем она нужна). Историей объекта недвижимости занимается целая когорта специалистов. (Вряд ли вам захочется выложить сотни тысяч долларов — причем, скорее всего, кредитных — за квартиру, в которой вы не сможете жить, потому что в последний момент объявился ранее не учтенный правообладатель!) Что происходит, когда вы платите за проверку юридической чистоты? Нанятая вами команда изучает историю жилищного объекта, чтобы убедиться, что в ней нет «черных пятен», например поддельных документов об одной из предыдущих сделок. Если бы любое изменение сведений о владельцах хешировалось и заносилось в блокчейн-реестр, такая проверка занимала бы секунды и ничего бы не стоила, а число мошеннических сделок заметно бы сократилось.

Даже в развитых странах с относительно эффективным кадастром недвижимости порой сложно проследить всю историю объекта. У каждого из американских штатов своя система регистрации прав на недвижимое имущество (так называемый титул Торренса). Это означает, что кадастр создается и поддерживается властями штата. Первичная запись занимает много времени, поскольку в ней должны фигурировать максимально полные сведения о новом объекте. Дальнейшие записи вносить проще, однако чем их больше, тем труднее отследить исторические детали — оформление и передачу права собственности. В каком-то смысле блокчейн-реестр предоставил бы автоматизированную версию этой абстрактной системы — титул Торренса с облегченным поиском. Однако для создания распределенного реестра нужно, чтобы записи о купле-продаже постоянно добавлялись, а в случае с недвижимостью такие сделки совершаются один раз при жизни поколения. Поэтому правительственным структурам гораздо проще заключить договор с компанией, которая бы перевела уже существующие архивы в формат, необходимый для их записи в блокчейн-реестр. В любом случае предстоит очень серьезная юридическая работа. Появление распределенных реестров может в корне изменить всю сферу

имущественного права. Например, страховые компании, которые гарантируют домовладельцам возмещение убытков в случае юридических осложнений, просто прекратят работу. А вот жилищные инвесторы, которые сейчас вынуждены месяцами держать крупные суммы на депозитных счетах, смогут высвободить этот капитал, что весьма положительно скажется и на рынке недвижимости, и на рынке ценных бумаг.

Великое обещание: высвобождение мертвого капитала

Реструктуризация жилищного и страхового рынка развитых стран — заманчивая перспектива. Однако, как мы уже говорили, самые вдохновляющие перемены ожидаются в странах третьего мира. Ведь здесь речь идет не просто о новом способе записи данных, а о возможности изменить уклад жизни, о выработке доверия к общественной системе хранения информации — без чего невозможно создать социальный капитал и увеличить масштаб и интенсивность экономического обмена.

Эрнандо де Сото, увидевший в технологии блокчейн возможность осуществить свою давнюю мечту и гарантировать малоимущим право собственности, описывает потенциальные перемены в моделях поведения так: «Главная причина, по которой жители постсоциалистических и развивающихся стран неохотно предоставляют сведения о себе, кроется даже не в неэффективности бюрократической системы. Проблема в недостаточном доверии к тем, кто распоряжается данными. Люди боятся, что предоставленная информация будет использована против них. Вот чем так привлекателен неуязвимый блокчейн. Если подать эту идею в нужном свете, многие захотят внести туда сведения о себе» [9].

Сейчас перуанский экономист работает над осуществлением своей мечты в альянсе со стартапом BitFury. Он проводит пилотный проект в Грузии — переводит кадастр недвижимости страны на блокчейн-платформу [10]. Подобные инициативы осуществляются и в других странах: компания Chromaway ведет аналогичный проект в Швеции, а стартап BitLand — в Гане. Даже в США происходят весьма

интересные сдвиги. Например, блокчейн-стартап Ubitquity заключил контракт с виргинской риелторской компанией Priority Title & Escrow с целью «упростить процесс отслеживания и записи данных для проверки юридической чистоты объекта», как пояснил CEO компании Натан Воснак [11].

Эти начинания внушают надежду, однако проводить их в беднейших странах мира нелегко. Не стоит впадать в безудержный оптимизм и рассматривать блокчейн как панацею от всех бед, включая нищету. Чтобы население бедных регионов планеты обзавелось социальным капиталом и построило функциональную экономику, нужно создать немало «физических» структур. Неплохо отрезвляет пример африканского государства Сьерра-Леоне, где больше десятка правительственных учреждений с 1999 года пытаются навести порядок в сфере имущественного и земельного права. В своем нынешнем состоянии кадастровая система Сьерра-Леоне ущемляет в правах большинство граждан, обслуживая интересы узкого круга землевладельцев, получивших наделы еще от британских колониальных властей [12]. Гибридная постколониальная система, выстроенная после обретения независимости, не в состоянии уладить многочисленные споры и разобраться с противоречивыми свидетельствами. Хаос достиг такого масштаба, что Министерство земельных ресурсов было вынуждено наложить мораторий на любые сделки по купле-продаже участков с 2008 по 2011 год. С 2015 года государство проводит новую земельную политику, которая должна нормализовать отношения частной собственности. Проблема в том, что никто не представляет, с чего начать. Хватит ли правительству политической воли, чтобы довести реформы до конца? Поддержат ли их те, кто в итоге понесет убытки? А ведь это лишь одна отдельно взятая страна.

Возможно, вы заметили, что все вышеупомянутые пилотные проекты — за исключением реализуемого в Гане — опираются на уже существующие, более или менее достоверные архивы. Нужно лишь занести их в блокчейн-реестр. До сих пор не предпринимались попытки оформить право собственности там, где записей о нем не существует или где архивы находятся в бедственном состоянии. Дело в том, что при создании архивов «с нуля» очень велик риск закрепить и легитимизировать давние правонарушения, ведь первичные документы, как правило, недоступны. Эта проблема освещена в работе профессора

Университета Британской Колумбии Виктории Лемье [13]. Она анализирует опыт ныне замороженного проекта компании Factom по регистрации имущественных прав в Гондурасе и предупреждает об опасности чрезмерного доверия к цифровым технологиям. С ее точки зрения, технология блокчейн полезна для отслеживания транзакций, однако «может негативно сказаться на достоверности информации». Фактически проблема сводится все к тому же извечному вопросу о благонадежности и посредничестве, которого в данном случае невозможно полностью избежать. Можно ли верить тому, кто заявляет права собственника на жилье? Кому в принципе можно верить в этих случаях? Это «внесетевая» проблема, связанная не с хешированием данных в блокчейне, а с сомнительностью источника информации.

Во многих странах третьего мира бюрократический хаос длится веками, поэтому есть все основания опасаться, что внесение ложных данных в блокчейн-реестр закрепит права богатых коррупционеров и окончательно обездолит рядовых граждан. Битва за честность и прозрачность может привести к конфликтам, насилию, запугиванию и вообще оказаться на руку преступникам. В беднейших кварталах право собственности по обыкновению определяют местные криминальные группировки. Хотим ли мы, чтобы блокчейн увековечил их картину мира?

Тем не менее улучшенная система отчетности и аудита, которую обещает нам новая технология, сама по себе может стимулировать законопослушность. Блокчейн, конечно, не отобразит дачу взятки наличными, но неопровержимым образом зафиксирует манипуляции с реестром, которые можно будет использовать как улики против продажных чиновников. Каждый этап в истории жилищного объекта — землеустройство, переговоры с владельцами соседних участков, подписание акта купли-продажи и т. п. — можно будет отобразить в блокчейн-реестре. Столь подробная запись — мощный инструмент для подтверждения законного права, чего нельзя сказать о привычных нам реестрах. Их можно фальсифицировать, чтобы скрыть следы мошенничества. Как правило, люди ведут себя более законопослушно и осмотрительно, если знают, что каждый их шаг можно проследить.

Эрнандо де Сото полагает, что нельзя пасовать перед социальными проблемами, которые могут возникнуть при записи имущественных прав. Общественные и экономические выгоды от наличия

достоверных свидетельств значительно перевешивают риск легитимизации давних нарушений. К тому же культурная традиция сообщества, как правило, включает и знание об имуществе его членов. Это знание во многих случаях можно конвертировать в надежные цифровые данные.

Джулиус Акинеми, научный сотрудник медиалаборатории Массачусетского технологического института, также решает проблему установления собственников с помощью древних культурных практик. Он просит деревенских старейшин Камеруна и Сенегала определить, что и кому принадлежит в их поселении, а затем заносит данные в цифровой реестр (его собственной системы, а не на основе блокчейна). Интересно, что к каждой записи прилагается рейтинговая шкала, которая должна гарантировать добросовестность старейшин. Если кто-то из них обманом припишет земельный участок или стадо своему родственнику, пострадавшая сторона может выразить протест с помощью рейтинга [14]. По словам Акинеми, налицо положительный эффект: старейшины стремятся повысить авторитет в глазах общины, набирая высокие рейтинги.

Не только земля

Раз уж мы упомянули о проекте Джулиуса Акинеми, нужно отметить и другое его начинание, которое опирается на весьма широкое понимание права собственности, не сводимое к одному лишь владению землей или жилищем. Сейчас Акинеми разрабатывает блокчейн-реестр для учета интеллектуальной собственности в странах третьего мира, богатых природными ресурсами. Пилотный проект разворачивается на острове Маврикий при поддержке правительства страны. Его задача — провести перепись ресурсов тропического леса и других природных зон, а затем занести их в блокчейн как собственность местных сообществ, что позволит населению страны увереннее отстаивать свои права в противостоянии с иностранными фармацевтическими и косметологическими компаниями, которые запатентовали уже тысячи препаратов, полученных из местного сырья. Проект пока находится в начальной стадии, и мы упомянули о нем, только чтобы показать, что

недвижимость — не единственный вид активов, который можно занести в блокчейн-реестр. Не исключено, что другие активы отобразить даже легче, поскольку они меньше связаны с политикой, а их история прозрачней.

Все чаще ведутся разговоры о создании блокчейн-реестров для движимого имущества, например автомобилей, вероятно, с помощью сигналов со встроенных RFID-чипов, которые переносят уникальный серийный номер в блокчейн. Такие реестры можно создать в пунктах продажи и немедленно предоставлять кредит под залог актива, что во много раз сократило бы процедуру его оформления.

В медиалаборатории Массачусетского технологического института реализуется еще один проект с участием нашего коллеги Марка Вебера [15]. Его команда в сотрудничестве с Межамериканским банком развития разрабатывает блокчейн-платформу для открытого публичного реестра, который мог бы подтверждать право собственности на различные виды активов, такие как товары, платежные документы, оборудование и недвижимость. Пилотная версия реестра должна предоставить малоимущим фермерам в странах третьего мира неопровержимое свидетельство о количестве сданного на склад урожая. Складская квитанция — один из главных документов в сфере сельскохозяйственной торговли, но в развивающихся странах банки давно не хотят их принимать как обеспечение кредитов, поскольку они выписываются на примитивных, незащищенных от подделки бланках, поэтому нет уверенности в том, что под тот же самый документ уже не взят другой заем. Блокчейн-реестр может гарантировать выдачу на каждую сданную партию урожая всего одной квитанции и фиксировать все полученные займы. Технология блокчейн предотвратит двойное расходование и в этом случае.

В сфере солнечной энергетики команда под руководством Майкла Кейси исследует концепт, который определит права пользования электроэнергией в локальной микросети. Это облегчит задачу самофинансирования внесетевых сообществ, у которых сейчас нет внятного юридического статуса и механизмов правообладания. В команду входят разработчики стартапа Filament, фондовой биржи Nasdaq и компании IDEO. Им уже удалось интегрировать данные «умного» электросчетчика с блокчейн-системой. Это позволяет доказать, что определенная фотоэлектрическая панель произвела и направила в сеть точно

установленное количество солнечной энергии. Измеренный и подтвержденный поток энергии можно отобразить как своего рода энергетический сертификат, который затем можно продать или использовать как обеспечение. Если подключить устройство вроде счетчика Filament к электронной платежной системе и смарт-контракту и добавить к системе переключатель, регулирующий доступ к энергии, получится некий вид «умной» собственности, управлять которым можно дистанционно. Если система обнаруживает, что платежи в криптовалюте прекратились, смарт-контракт блокирует доступ к энергии, пока оплата не возобновится, либо перенаправит энергию в хранилище или любую другую часть системы, в которой платежи производятся бесперебойно. Это потенциально может в корне изменить все нынешние принципы финансирования.

Разумеется, условия такого соглашения должны быть справедливы для всех сторон. (Уже сегодня обсуждаются вопросы этики и безопасности, связанные с применением подобных самовыключающихся систем для автокредитов в США.) Разумно ли доверять контроль над энергосетью децентрализованному алгоритму? Однако если все стороны согласятся с условиями контракта и признают, что беспристрастный блокчейн гарантирует его соответствующее выполнение, эта модель сможет заменить привычную несовершенную систему и значительно понизит расценки в сфере энергетики.

Представьте себе мелкого инвестора, скажем экологически сознательного пенсионера из штата Орегон, который вкладывает свои накопления в блокчейн-проект, чтобы частично финансировать микроэнергосеть в одном из бедных районов Индии. Долю в этом проекте можно продать другим инвесторам, чьи вклады будут защищены тем же смарт-контрактом. Теперь представьте, что будет, если объединить этот вклад с другими займами микросетям: от местных банков, МФО, кредитных кооперативов и пр., создав неуязвимые для взлома «криптосолнечные» финансовые активы, которые можно продать инвестиционным компаниям и прочим крупным организациям. В данном случае блокчейн необходим, поскольку он обеспечивает такой уровень детализации и микроуправления инвестиционными и энергетическими потоками, какой физически невозможен в нецифровом мире, где относительная непрозрачность и высокие комиссии традиционной финансовой системы не позволяют выполнять микротранзакции.

Однако при наличии сети компьютеров с блокчейном в роли децентрализованного автоматического менеджера, который способен отследить путь даже самой малой доли финансового пакета микросети, можно задуматься о комплексной системе микроинвестиций.

Перед нами стоит весьма амбициозная задача — превратить крошечные частицы активов третьего мира в общий пул, который может заинтересовать инвестиционные банки Уолл-стрит. В идеале должна получиться уменьшенная, но более надежная и стабильная версия рынка ипотечных ценных бумаг, посредством которого финансисты Уолл-стрит создали инвестиционно привлекательные бонды из большого фонда жилищных кредитов. Сможем ли мы совершить подобную финансовую революцию, чтобы поддержать строительство децентрализованной энергетической инфраструктуры по всему миру? Энергия — самый ценный ресурс любого сообщества. Что если мы разработаем алгоритм справедливого ценообразования для малоимущих жителей планеты и обеспечим им доступ к возобновляемым видам этого ресурса? Возможно, тогда мы сможем одновременно спасти природу и подарить беднейшим слоям населения платформу для экономического развития, которая позволит запустить динамичные локальные бизнес-проекты.

Деньги, которые доступны всем

Надежды на финансовую инклюзию стран третьего мира во многом проистекают из стремительного распространения мобильных телефонов и, как следствие, мобильных платежных систем. Первый такой сервис под названием M-Pesa был запущен в Кении в 2007 году. Сейчас мобильные платежи в той или иной форме доступны жителям 93 развивающихся стран; уже работает 271 сервис и еще 101 готовится к запуску [16]. Но многие из них лишь скользят по поверхности потенциального рынка, а статистика указывает на более глубинную проблему. «От 60 до 90 процентов счетов, открытых клиентами мобильных банков, почти тут же переходят в "спящее" состояние без единой транзакции», — пишет эксперт по мобильному банкингу Кэрол Реалини [17]. Почему? Потому что большинство таких систем опираются

на традиционную банковскую инфраструктуру, а организации, которые ими управляют, плохо представляют себе нужды клиентов, не охваченных банковским обслуживанием. Многих клиентов требования банка ставят в тупик. Возникает конфликт между теми, кто жаждет любой ценой приобщиться к сфере банковских услуг, и теми, кто отказывается предоставить такую возможность. Чаще всего источник проблемы — сами банки или по крайней мере их регуляторная система и модель управления рисками. Может быть, рост числа банковских клиентов и не нужно делать главной целью?

Сложнее всего оказалось расширить программы мобильного кредитования, и здесь основным препятствием тоже стала банковская парадигма. Когда речь заходит о займах, мобильные платежные системы вроде M-Pesa, которые, как правило, вынуждены опираться на государственные финансовые институты, возвращаются к традиционным моделям и параметрам одобрения кредитов. Поэтому слабо разработанные, субъективные механизмы подтверждения личных данных и платежеспособности вновь становятся непреодолимой преградой, особенно если учесть, что крупные операторы мобильной связи используют свое привилегированное положение посредника, чтобы максимально повысить цены на услуги. Ведущие операторы, включая кенийскую компанию Safaricom, не стремятся к совместимости своих систем с другими провайдерами. Поэтому межсетевые и международные транзакции приходится проводить через африканскую банковскую инфраструктуру — малоэффективную, громоздкую и дорогую. Эти локальные платежные системы ничуть не похожи на открытые, общедоступные инновационные платформы, о которых мечтают поклонники блокчейна и биткоина. Да, они несколько облегчили малоимущим жителям процесс перевода денег, по крайней мере в рамках местной мобильной сети, но нынешняя модель банковской системы по-прежнему им недоступна, особенно при необходимости получить кредит (порой единственный выход в кризисной ситуации). Будучи не в состоянии подтвердить, кто они, чем занимаются и чем владеют, жители беднейших районов мира остаются заложниками финансовых акул, которые всеми силами удерживают их за чертой бедности.

Если бы в широком доступе имелись универсальные криптовалюты вроде биткоина, которые не требуют никаких документов и личных данных, малоимущим было бы легче вырваться из кабалы банков

и мобильных операторов. Кроме того, у инноваторов появился бы стимул разрабатывать новые блокчейн-сервисы, включая кредитные программы, которые помогли бы беднейшим слоям населения.

В мире высоких технологий уже довольно давно обсуждаются способы поддержки тех, кто лишен доступа к финансовым услугам (или вообще отрезан от мира высоких технологий). К сожалению, через девять лет после изобретения криптовалюты уровень ее использования за пределами научно-технического сектора довольно низок. Отчасти потому, что в глазах широкой публики криптовалюта до сих пор ассоциируется с преступными махинациями. Ее репутация еще сильнее пострадала в 2017 году, когда создатели вируса WannaCry взломали компьютерные системы больниц и прочих общественных заведений, зашифровали жизненно важные файлы и потребовали выкуп в биткоинах. (В ответ на многочисленные призывы запретить биткоин, которые закономерно последовали за этой атакой, мы хотели бы отметить, что обыкновенные купюры гораздо чаще используются для преступных махинаций и отмывания денег, причем их путь отследить намного сложнее, чем историю транзакций в биткоинах. Однако когда речь идет о коллективном восприятии, все эти доводы теряют смысл. Из-за хакерских атак на репутации биткоина образовалось пятно.)

Второй тормозящий фактор — высокая волатильность биткоина, с которой могло бы справиться дальнейшее техническое развитие. Большинство из нас привыкло считать деньги в национальной валюте, поэтому скачущий курс криптовалюты не позволяет рядовым гражданам рассматривать ее как платежное средство. Кто же захочет покупать товары за денежную единицу, чья цена может в любой момент упасть и сделать потребительскую корзину процентов на тридцать дороже? Вот почему биткоин пока не реализовал свой огромный потенциал в качестве инструмента финансовой инклюзии. Иммигранту с Ямайки, возможно, и выгоднее отправить деньги родственникам в биткоинах почти без комиссии, чем выложить девять процентов за перевод через Western Union [18]. Однако пока его родня будет искать, где обменять биткоины на ямайские доллары, курс может рухнуть и обесценить всю сумму.

Тем не менее оригинальные решения, почти ежедневно появляющиеся в инновационной экосистеме Биткоина, понемногу начинают избавлять нас от неудобств. Молодые сервисы денежных переводов — такие как компания Veem (ранее Align Commerce) — уже используют

биткоин и технологию блокчейн как своего рода «рельсы» для валютных переводов, минуя дорогостоящую банковскую систему. Благодаря грамотным инструментам страхования обменного курса, возможным ввиду прозрачности блокчейн-реестра и низкой стоимости транзакций, компании удалось минимизировать собственный риск от краткосрочных операций с биткоином. Это позволяет предложить доступные расценки клиентам, которые работают исключительно с местной валютой. Подобный метод уже приносит дивиденды, что со всей очевидностью можно наблюдать на примере BitPesa — кенийского сервиса биткоин-переводов. Компания, проводящая трансграничные платежи и операции с иностранной валютой в Кении, Нигерии, Танзании и Уганде, сообщила о 25-процентном ежемесячном росте. Объем ее транзакций достиг десяти миллионов долларов еще в первой половине 2017 года (в 2016 году был всего миллион долларов) [19]. Кроме того, есть сведения, что 20 процентов переводов, которые филиппинские мигранты в Южной Корее отправляли своим семьям, производились в биткоинах [20].

Весьма оригинальное решение проблемы волатильности предложила компания Abra. Ее сервис позволяет абоненту из одной страны перевести деньги на номер абонента в другой стране без всякого посредничества. С помощью смартфона абонент покупает биткоины, при этом специальное приложение устраняет риск колебаний курса благодаря высокотехнологичной страховой системе, работающей за счет полной прозрачности и низкой стоимости блокчейн-транзакций. Пользователь даже не задумывается о курсе. Приложение использует смарт-контракт на основе блокчейна, чтобы автоматически сделать отчисление третьей стороне, если курс биткоина вырастет с момента покупки, или, напротив, получить недостающие средства, если курс упадет. Этот так называемый контракт на разницу цен (немного похожий на биржевые финансовые инструменты) закрепляет стоимость используемого биткоина. У потребителя на экране отображается лишь та сумма в фиатной валюте, например в долларах, которую он изначально зачислил на счет в системе Abra. Скажем, филиппинский иммигрант, проживающий в Сан-Франциско, переведет некую сумму родственникам в Маниле. Тогда смартфон принимающего абонента на Филиппинах запустит аналогичный процесс, только на этот раз контракт будет работать с биткоином и филиппинским песо. Такая система стала

возможна благодаря применению блокчейна и смарт-контрактов, что отменяет необходимость в банках, юристах, депозитных агентах и прочих посредниках, которые обычно управляют конвертацией валюты. Возникает гораздо более дешевый инструмент для страхования обменного курса.

Есть и еще одна весьма серьезная проблема — финансовые регуляции. Их важность повысилась после того, как Департамент финансовых услуг Нью-Йорка впервые выдал банковскую лицензию на проведение операций в биткоинах в 2015 году [21]. Сам акт выдачи лицензии свидетельствовал о том, что финансовые регуляторы считают себя ответственными за транзакции между фиатными валютами и криптовалютой, несмотря на готовность предоставить полную свободу инновационному процессу в рамках криптовалютной среды. В результате возник целый набор правил, которые существенно повысили стоимость покупки и использования цифровой валюты. Стартапы, предлагавшие конвертацию долларов в биткоины, заявили, что новые регуляции ограничат возможность предоставления недорогих услуг конечным потребителям. Многие предпочли прекратить операции в штате Нью-Йорк. Однако деловую столицу просто так не обойдешь. Значительная часть денежных потоков попадает под юрисдикцию нью-йоркских властей. К тому же Нью-Йорк — один из центров мирового капитала, следовательно, его модель послужит примером для регуляторов других стран. (Хотя многие все же не рискнули применить столь драконовские меры.)

Главная проблема при выдаче лицензии — доказать, что компания может идентифицировать личность потребителей. Это требование («знай своего клиента») в наши дни предъявляется ко всем поставщикам финансовых услуг. Его цель — воспрепятствовать отмыванию денег, финансированию терроризма, уклонению от уплаты налогов и т. п. Прежде чем финансовое учреждение начнет работать с новым клиентом, необходимо выяснить, какой риск это может повлечь. Уровень риска определяется (довольно-таки расплывчато) с помощью ответа на вопрос «кто этот человек?». Во главу угла ставится привычное, сформулированное государством понятие личности, которая может подпасть под некие санкции, например оказаться в черном списке авиакомпаний. Государство не может подтвердить твою личность и репутацию? Значит, у тебя проблемы. Если к биткоин-провайдерам

начнут предъявлять аналогичные требования, пользоваться их услугами станет ничуть не проще, чем банковскими.

По мере ужесточения правил из-за финансовой нестабильности, террористической угрозы и наркотрафика банкам приходится все больше средств и усилий тратить на идентификацию клиентов. Ситуация усугубляется еще и тем, что международные банки и прочие финансовые институты должны гарантировать, что их контрагенты и/или посредники в других странах проверяют *своих* клиентов надлежащим образом. Этот пункт уже привел к выплате крупных штрафов. Так, финансовый гигант HSBC был вынужден заплатить правительству США 1,9 миллиарда долларов, когда выяснилось, что мексиканские наркодельцы отмывали деньги через один из банков конгломерата. Из-за сложности системы многие финансисты впадают в отчаяние и решают, что игра не стоит свеч. В результате возникает такое явление, как *de-risking*, или перестраховка, — систематический отказ в предоставлении кредита и оказании банковских услуг лицам и организациям, которые кажутся сомнительными клиентами. Это откровенно противоречит курсу ООН и Всемирного банка на расширение доступа к финансовым услугам.

Рассмотрим, к примеру, ситуацию в Сомали. В этом «несостоявшемся государстве» с его террористами, пиратами и боевиками практически невозможно установить личность по всем стандартам западного мира. Мало у кого из граждан найдется полный пакет документов. Поэтому американские банки, следуя указаниям казначейства США, фактически прекратили операции по переводу средств в Сомали. В результате население целой страны, и прежде крайне бедное, вынуждено использовать дорогие и ненадежные «теневые» каналы для международных транзакций. Трудно представить себе более подходящую среду для вербовщиков аш-Шабаб — самой активной группы сомалийских исламистов. Иными словами, все попытки добиться прозрачности и легальности с треском провалились.

Чем же здесь поможет блокчейн? Прежде всего предоставит возможность анализировать публичные данные о транзакциях и определять уровень риска для отдельных узлов или биткоин-кошельков, не выясняя при этом имени пользователя. Блокчейн-стартапы, такие как Chainalysis, Elliptic и Skry, уже сотрудничают с правоохранительными органами, применяя анализ «больших данных», теорию сети

и искусственный интеллект для оценки финансовых потоков в сети Биткоин, так же как телеканалы вроде Netflix используют «большие данные» для обработки информации о запросах аудитории, чтобы предложить каждому зрителю фильмы на его вкус. Анализ биткоин-транзакций может очень многое рассказать о поведении, а возможно, и о намерениях пользователя. Конечно, новые зашифрованные криптовалюты вроде Zcash и Monero, разработанные как «ответ» поклонников анонимности на усилия Chainalysis и прочих, могут помочь преступникам замести следы. Однако программа, которую мы сейчас обсуждаем, нацелена не столько на поимку преступников, сколько на то, чтобы помочь добропорядочным гражданам *доказать обратное*. Если гражданину нечего скрывать, хотя он и не имеет надлежащих документов, то при хранении и переводе средств в биткоинах история транзакций подтвердит его законопослушность.

Финансовые механизмы сообщества

На протяжении всей истории человечества сообщества выстраивают собственные финансовые и банковские системы, которые сводят заемщиков с кредиторами. Эти системы легко масштабируются, когда решена проблема доверия. Некоторые разработчики блокчейн-платформ ищут способ упорядочить и развить инструменты финансовой взаимопомощи, которые в один прекрасный день могут избавить нас от потребности в банках.

Одна из наиболее привлекательных практик в этом отношении — так называемая касса взаимопомощи: добровольное объединение членов сообщества в целях создания материального (финансового) фонда поддержки. В разных странах такие ячейки носят разные названия, но основной принцип у всех один. Группа знакомых между собой и доверяющих друг другу людей заводит общую копилку, куда все периодически вносят определенную сумму, скажем 50 долларов ежемесячно. Затем накопленные средства выдаются одному из членов группы как своего рода кредит. После этого взносы продолжаются, пока не настанет очередь следующего участника, и т. д. В рамках этой системы каждый (за исключением последнего в очереди) фактически получает

беспроцентную ссуду. Единственная форма возврата — это те взносы, которые нужно продолжать платить после выдачи займа.

Такие системы традиционно основаны на доверии, возникающем благодаря узам дружбы и родства. Если тебя хорошо знает вся группа, намного сложнее нарушить обязательства и перестать вкладываться в общую кубышку после того, как получишь свою порцию. Однако эта модель доверия физически ограничивает масштаб операций. Вспомним число Данбара: антрополог Робин Данбар утверждает, что наибольшее число стабильных межличностных связей, которые способен поддерживать человек, равно 150 [22]. Это означает, что группа взаимопомощи по определению должна быть довольно мала, ведь каждый ее участник должен входить в круг ста пятидесяти доверенных лиц любого другого участника. Вероятность этого совпадения снижается по мере роста группы.

И вот здесь как раз могут помочь блокчейны, смарт-контракты и токены. Стартап WeTrust, который консультирует Майкл Кейси, использует технологию блокчейн для автоматизации, структурирования касс взаимопомощи и встраивания в них поощрительных механизмов на основе токенов, что должно стимулировать добросовестное выполнение обязательств всеми участниками группы. Более того, возникает возможность добавления новых участников — не обязательно знакомых со всеми остальными, как в традиционных «кубышках». В отличие от банковских процедур, которые требуют все новых и более изощренных подтверждений идентичности, этот механизм понижает барьер доступа, перекладывая часть задач на саму систему, так что «знать клиента в лицо» уже не столь важно.

Вне зависимости от того, насколько эффективной окажется модель WeTrust, она в любом случае подскажет, как увязать новые системы алгоритмического распределенного доверия со старыми, глубоко укоренившимися структурами общественных отношений. На наш взгляд, крайне важно, чтобы проблемы беднейшего населения Земли не решались «сверху» инвесторами из Кремниевой долины, которые уверены, что знают, как это делать. Все решения должны приниматься в индивидуальном порядке, с учетом культурной специфики и социального устройства каждого отдельно взятого сообщества.

Безусловно, такие инициативы, как WeTrust, с их стремлением понизить барьеры доступа и обеспечить финансовую инклюзию, нужно

приветствовать. Но не будем забывать, что в каждой культуре своя система идентификации. В той или иной форме вопрос об идентичности возникает всегда. Однако если подумать, чтó мы вкладываем в понятие «идентичность», о котором пойдет речь в следующей главе, мы обнаружим, что оно весьма неоднозначно, а в эпоху интернета связано с проблемой безопасности и социальных конфликтов. Именно в этой сфере сегодня рождаются наиболее радикальные идеи относительно применения технологии блокчейн.

Глава

8

Суверенная идентичность

До недавнего времени пятерку крупнейших институтов, занимающихся подтверждением личности, по умолчанию составляли правительства пяти крупнейших государств с самым большим населением — Китая, Индии, США, Индонезии и Бразилии. Однако в наши дни эту миссию выполняют новые, весьма могущественные инстанции, причем не прибегая к стандартным государственным инструментам вроде свидетельств о рождении, паспортов, удостоверений личности и т. п. Поразительно, что три из этих новых структур уже вошли в ту самую пятерку мировых лидеров, — это Facebook, Google и Twitter. Теперь они верифицируют наши заявления о том, кто мы такие. Заводя аккаунты в социальных сетях, мы фактически создаем онлайн-идентичность, которую третьи стороны могут использовать для проверки наших личных данных. Отсюда и растущая популярность технологии единого входа (SSO, single sign-on), позволяющей переходить с сайта на сайт без повторной авторизации. Сколько же «идентичностей» обслуживают эти техногиганты? Число подписчиков Facebook уже превысило два миллиарда; Google и Gmail насчитывают 1,2 миллиарда пользователей; платформой Twitter регулярно пользуются около 320 миллионов человек. Если существует объективная мера влияния этих компаний на нашу жизнь, то она, пожалуй, такова: информация, которой они располагают, в буквальном смысле определяет, кто мы есть.

Этот вид корпоративного вторжения в частную жизнь вызвал бурную негативную реакцию в странах Запада. Обнародованная Эдвардом

Сноуденом информация о мониторинге персональных данных спецслужбами США затрагивала и подобные компании, что вывело проблему в публичную плоскость. В пьесе Джеймса Грэма «Частная жизнь» со знаменитым Дэниелом Рэдклиффом в главной роли зрителям весьма наглядно объясняют, каким образом в их смартфонах и планшетах накапливаются персональные данные и как эта информация может быть использована против них — например, когда компания Uber выводит карту поездок пассажира на гигантский дисплей посреди городской улицы. (Кстати, в пьесе использован и документальный видеоролик с участием самого Сноудена.)

Однако если в развитых странах слишком пристальное внимание к нашим «цифровым следам» вызывает протест, то третий мир сталкивается с противоположной проблемой — недостатком подтвержденной информации. Даже вполне законопослушным гражданам нередко бывает нелегко подтвердить свое имя и репутацию. По данным Всемирного банка, 2,4 миллиарда человек во всем мире не имеют официальных документов, что лишь усугубляет проблему [1]. И дело не только в том, что они не могут открыть счет в банке, подать заявку на кредит, выехать за границу и т. д. Отсутствие документов делает их легкой мишенью для преступников. В результате исследования, проведенного под эгидой ЮНЕСКО в горных районах Таиланда, выяснилось, что отсутствие внятного гражданского статуса и удостоверяющих бумаг — *величайший фактор риска* для детей, вовлекаемых в торговлю живым товаром [2]. В глазах закона эти дети не существуют; их передвижения крайне сложно отследить. Поэтому они регулярно становятся жертвами чудовищных преступлений. Любой лагерь для беженцев как магнит притягивает к себе торговцев детьми, готовых воспользоваться их уязвимым положением.

Бывший банкир и финансовый технолог Джон Эдж ощутил потребность заняться решением этой проблемы после просмотра документального фильма «Мина» о судьбе индийской девочки, похищенной из дома и вовлеченной в проституцию. Когда Эдж изучил работу групп, занятых спасением «неучтенных» детей, ему пришла в голову мысль, что технология блокчейн могла бы стать универсальным средством подтверждения личности, если создать на ее основе глобальный, защищенный от фальсификации реестр персональных данных. Эдж основал организацию под названием ID2020, поскольку ее изначальной

целью было обеспечить надежные цифровые удостоверения личности всем детям мира к 2020 году. (Позже формулировка задачи была изменена, чтобы вписать ее в более реалистичный проект ООН: выдачу официальных документов всему населению планеты к 2030 году.) Конечно же, Джон Эдж понимал, какие проблемы придется решить, прежде чем его мечта об универсальном блокчейн-реестре станет явью. Например, кто гарантирует достоверность сведений о ребенке? Кто будет отвечать за сохранность и неразглашение уникального ключа, дающего доступ к личной информации, до совершеннолетия ребенка?

В мае 2016 года Эдж заключил договор с ООН, в рамках которого предполагалось вызвать представителей пятидесяти технологических компаний и аналогичное количество дипломатов и эмиссаров неправительственных организаций на саммит ID2020, чтобы обсудить, как цифровые технологии, и прежде всего блокчейн, могут помочь в решении проблемы идентификации. Вскоре, однако, выяснилось, что воззрения «технарей» существенно отличаются от убеждений и методов правительственных чиновников. В глазах дипломатов официальные, выданные государством документы — паспорт, водительские права, свидетельство о рождении — наделены едва ли не сакральной силой. Выпуск таких бумаг и подтверждение личности гражданина — прерогатива государственных органов. Инженеры, напротив, скептически относятся к государственным институтам и не хотели бы давать им в руки неограниченную власть. Поэтому из их лагеря неоднократно доносилось словосочетание, которое в итоге стало лейтмотивом саммита, — «суверенная идентичность». Суть идеи вкратце такова: людям лучше самим заняться подтверждением персональных данных, используя тот массив информации о себе, который каждый из нас накапливает и хранит в течение жизни (а не отдавать его в распоряжение правительства). Как видим, это гораздо более автономная концепция, чем у чиновников.

Тем не менее обе стороны оказались единодушны в одном: «аналоговая идентификация», то есть осуществляемая с помощью бумажных документов вроде паспорта, свидетельства о рождении или водительских прав, безнадежно устарела. Необходимы нормы и стандарты «цифровой идентификации». Без них и отдельные лица, и целые организации будут лишены доступа к инструментам современной экономики. Поскольку количество услуг, предоставляемых в электронном

виде, растет, нужен улучшенный цифровой интерфейс, способный быстро идентифицировать пользователей, организации и устройства. Доступ к услугам должен обеспечиваться без долгой проверки не всегда надежных бумажных документов.

Отправной точкой на пути к новой цифровой модели идентификации может служить система открытых криптографических ключей — математически связанных ключевых пар, — которые, как мы говорили в главе 3, позволяют пользователям авторизовать транзакции в Биткоине и других блокчейнах. (Эта система шифрования, изобретенная в 1976 году Уитфилдом Диффи и Мартином Хеллманом, намного старше Биткоина и широко применяется для обеспечения безопасности в различных интернет-приложениях, включая электронную почту.) Открытые ключи позволяют пользователям Биткоина «подписывать» биткоин-адрес, то есть публичную часть ключа, с помощью приватной последовательности символов, тем самым подтверждая право совершать операции. Аналогичным образом учреждение, заверяющее личные данные граждан, может предоставлять к ним доступ с помощью цифровых подписей. Сопоставление «половинок» ключа послужит неопровержимым доказательством того, что вы оплатили все коммунальные счета, университет выдал вам диплом, а регистрационная служба выписала свидетельство о рождении вашего ребенка.

Многие разработчики блокчейн-платформ, в том числе и в лабораториях таких техногигантов, как Microsoft, стараются оптимизировать систему цифровых подписей, включая официально заверенные подтверждения в блокчейн-транзакции [3]. Таким образом добавляется новый уровень защиты, ведь заверяющая организация не сможет отозвать свою подпись после внесения документа в реестр, изменяемый лишь путем добавления. (Любое действие в нем необратимо, как и транзакция в Биткоине.) Однако сама идея применения блокчейна в подобных целях вызывает горячие дебаты среди специалистов по идентификации. О причинах разногласий мы поговорим чуть позже.

Независимо от того, какие инструменты мы в итоге выберем, общество должно перейти к децентрализованной цифровой автономной модели идентификации. Даже если личные данные и не будут храниться в блокчейн-реестрах, их перевод в цифровой формат и внедрение криптографических методов защиты весьма ощутимо повлияют

на разработку блокчейн-сервисов, не связанных с идентификацией напрямую. Есть и более важные причины настаивать на внедрении систем, которые позволят гражданам самостоятельно решать, где и как использовать и хранить конфиденциальную информацию. Хакерская атака на бюро кредитной истории Equifax в сентябре 2017 года, когда злоумышленники получили доступ к именам, номерам социального страхования и банковским счетам 143 миллионов граждан США, со всей очевидностью показала, что, полагаясь на компании, которые размещают наши данные (в том числе и строго конфиденциальные) в больших централизованных хранилищах, мы становимся легкой мишенью для преступников. Как говорилось в главе 2, для хакера нет более лакомой добычи, чем единая локализованная база данных. Автономная модель идентификации могла бы решить эту проблему.

Тот факт, что правительства начали проявлять интерес к этой сфере, вызывает сдержанный оптимизм, хотя чиновники охотнее говорят о «цифровой» части процесса, чем о его автономизации. Многие государственные структуры делают ставку на подконтрольные *им* электронные идентификаторы, причем наибольшей популярностью пользуются биометрические решения — сканирование отпечатков пальцев или сетчатки глаза для подтверждения идентичности.

По мнению многих правительственных чиновников, ориентиром и флагманом в этой сфере нужно считать Индию. Индийское правительство приступило к выполнению титанической работы по идентификации каждого гражданина: на него создается цифровое досье с биометрическими маркерами (главным образом отпечатками пальцев), а затем эта информация заносится в огромную централизованную базу данных. Система под рабочим названием Aadhaar уже включает 1,1 миллиарда уникальных регистрационных номеров, причем 400 миллионов из них привязаны к банковским счетам [4].

У такой системы есть неоспоримые преимущества. Она может обеспечить быструю и легкую авторизацию для доступа к самым разным цифровым сервисам, будь то открытие банковского счета или просмотр медицинской истории. В нескольких городах (Хайдарабаде, Бангалоре и др.) уже возникла новая отрасль программирования — разработка приложений на базе Aadhaar. В начале 2017 года индийский банк IDFC запустил сервис Aadhaar Pay, позволяющий продавцам с помощью мобильного приложения для Android получать платежи

с номеров Aadhaar, привязанных к банковскому счету [5]. Индийским гражданам для оплаты больше не понадобятся кредитные карты или телефоны, достаточно отпечатка пальца и регистрационного номера. Сервис идеально вписывается в программу премьер-министра Нарендры Моди, задавшегося целью построить новую безналичную экономику на базе трех взаимодополняющих технологий. Первая — новая система банковских счетов, предназначенных только для проведения платежей, вторая — база данных Aadhaar и третья — мобильная телефония.

Столь же далеко продвинулась по пути цифровой идентификации другая страна — намного меньше, но гораздо богаче — Эстония. Здесь удостоверение личности пока еще имеет форму пластиковой карты, но встроенный в нее микрочип обеспечивает взаимный доступ между широким спектром социальных услуг и системой идентификации граждан. Правительство приглашает и частных предпринимателей из сферы услуг присоединиться к системе. К тому же Эстония предлагает цифровую идентификацию иностранцам: в стране весьма успешно работает программа «электронное гражданство», благодаря которой любой гость может зарегистрироваться в качестве «электронного резидента», даже если не проживает в Эстонии постоянно. Это существенно облегчает предпринимательскую деятельность. Благодаря цифровому идентификатору можно моментально подтвердить свое право на доступ к самому широкому спектру предложений — от медицинских услуг до революционной программы онлайн-голосования, позволяющей гражданам участвовать в выборах с помощью смартфона или компьютера. Появление этой инфраструктуры также привело к инновационному взрыву. Многие разработки нацелены на то, чтобы связать эстонскую систему цифровой идентификации с наиболее престижными блокчейн-сервисами. Например, биржа Nasdaq ввела программу на основе блокчейна для голосования акционеров [6].

Но какими бы передовыми ни были эстонская и индийская системы, централизованные базы данных неизменно находятся в зоне риска. Сейчас обе страны управляются вполне благосклонными властями, которые уважают частную жизнь своих граждан. Однако всегда есть опасность, что нечистоплотный чиновник — или даже коррумпированное правительство будущего — получит доступ к конфиденциальным данным и использует их для шантажа или чего похуже.

Индийский премьер Моди — умеренный консерватор, но его партия БДП («Бхáратия джáната пáрти») известна поддержкой индуистских националистов в ущерб мусульманским меньшинствам. Если в будущем к власти придет менее толерантный лидер, что помешает ему использовать базу биометрических данных для ущемления граждан по этническому или религиозному признаку? Что касается Эстонии, у нее сложные отношения с советским прошлым и его наследием, в том числе с бюрократическим. К тому же ряд западных экспертов уже предупреждали, что системы электронного голосования могут стать мишенью для хакеров [7].

Недавнее подтверждение этому мы наблюдали в Нью-Йорке, когда возникли вполне мотивированные опасения, что администрация Дональда Трампа может принудить городские власти раскрыть данные о мигрантах, которые зарегистрировались в муниципальной программе идентификации. Программа задумывалась с самыми благими намерениями — предоставить недокументированным мигрантам (многие из которых прожили в городе несколько десятков лет) доступ к социальным и финансовым услугам, а также помочь городским властям контролировать оказание этих услуг. В итоге же получилось, что либеральный мегаполис, объявивший себя «городом-убежищем» в пику антимиграционной политике Трампа, невольно создал ресурс, позволяющий чиновникам выявить, найти и при желании депортировать тех самых людей, которые искали здесь защиты. Этот случай дает нам повод вспомнить суровое предостережение эксперта по кибербезопасности Стивена Спрага, CEO компании Rivest Co.: «На протяжении всей истории человечества личные данные не раз становились оружием» [8]. Уязвимость единых хранилищ информации — мощный аргумент в пользу децентрализованных механизмов управления личными данными. Для их создания нам и нужен блокчейн.

Идентичность по-новому

Мы склонны ассоциировать идентичность с официальными документами. Исторически государство так долго играло ключевую роль в подтверждении личности, что постепенно влилось в наши представления

о самих себе. Тем не менее, как отмечает эксперт Дэвид Берч, существует три типа, или три грани, идентичности: правовая, которая связана с идентификацией гражданина; социальная, которая вырабатывается в процессе взаимодействия с окружающими и включает в себя межличностные отношения и то, как нас воспринимают другие члены сообщества; и личная — то есть то, кем мы сами себя считаем [9]. Последние две категории становятся все более изменчивыми по мере того, как новые технологии и культурные сдвиги заставляют нас иначе взглянуть на человеческую природу, будь то вопросы сексуальной ориентации, пола, религии, расовой принадлежности или этнического происхождения. Что особенно примечательно, новые технологии, которые сделали возможными эти перемены, теперь позволяют использовать наиболее динамичные аспекты нашего «я» как средство *подтверждения* — прежде всего в сфере социальной идентичности. Ваш круг общения и взаимодействия образует сеть доверия, которая обладает немалой информационной ценностью. Если эта сеть объединяет благонадежных, добропорядочных людей, можно с высокой степенью вероятности заключить, что и вы сами — человек добропорядочный. По крайней мере на ваш «личный счет» можно записать несколько плюсов и посмотреть, подтвердят ли эту оценку другие данные.

Однако для того, чтобы воплотить в жизнь концепцию «суверенной идентичности», нужно передать контроль над ценными личными данными в руки самих граждан, а не правительств и крупных корпораций вроде Facebook и Google. Некоторые разработчики пытаются доказать, что технология блокчейн обладает всеми задатками для достижения этой цели. Но прежде чем говорить о конкретных проектах, давайте представим, как бы мы обращались с информацией, обретя желанную самостоятельность. Например, мы могли бы выборочно предоставлять лишь те сведения, которые необходимы для получения определенных услуг.

В наш век постоянных нарушений конфиденциальности защита личных данных приобретает жизненно важное значение. Цифровой формат, который позволяет разбивать массивы данных и выделять из них нужные фрагменты, очень полезен в этом отношении. «Аналоговые» удостоверения — например, водительские права и паспорт — статичны и монолитны. Вы не можете предъявить лишь одну их часть или графу. Когда мы протягиваем бармену водительские

права, подтверждая совершеннолетие, бармен узнает не только наш возраст, но и имя, пол, адрес, дату рождения, рост и даже цвет глаз. (Бог
[236] его знает, зачем в штатах Нью-Йорк и Нью-Джерси требуют вносить в права эту деталь!) Конечно, человек едва ли это запомнит, а вот сканеры, которые часто используют в ночных клубах, считают и сохранят информацию. Вас обрадует, если какой-нибудь вышибала получит скан документа с вашим именем и адресом? Давно пора отказаться от модели, где для доступа к определенным услугам требуется полный пакет личных данных, и перейти к формату, который позволяет подтверждать лишь конкретные параметры (или *атрибуты*), необходимые для каждого отдельного случая, например, что на банковском счете имеется определенная сумма; что наш диплом выдан именно тем университетом, который мы указали; что мы родились больше двадцати одного года назад. Доказуемые цифровые данные, связанные с нашими достижениями и отношениями, со всеми документами, которыми мы обросли в течение жизни, могли бы нам предоставить такую возможность.

Всемирный экономический форум внес вклад в развитие новой модели цифрового подтверждения атрибутов личности [10]. В отчете под названием «На пути к цифровой идентичности» авторы указывают, что в нашем нынешнем понимании идентичности можно выделить три типа атрибутов. *Сущностные атрибуты* присущи человеку от природы и, как правило, неизменны; это такие свойства, как рост, отпечатки пальцев, дата рождения. *Приобретенные атрибуты* со временем изменяются; к ним можно отнести состояние здоровья, уровень образования, предпочтения при выборе товаров. Наконец, *назначенные атрибуты* приписываются гражданину внешними инстанциями, наделенными разного рода полномочиями. Например, номер паспорта нам дает государство, а электронный адрес — провайдер почтового сервиса.

Выборочно демонстрируя свои атрибуты, мы подтверждаем не статичную, монолитную идентичность в традиционном смысле слова, а скорее разные аспекты *персоны*, как сейчас принято говорить среди разработчиков цифровых технологий. Четверо наших коллег из Массачусетского технологического института — Алекс Пентленд, Томас Харджоно, Дэвид Шрайер и Ирвинг Владавски-Бергер, — пожалуй, нашли самую удачную формулировку, когда писали статью для комиссии

по вопросам кибербезопасности при Американском национальном институте стандартов и технологий:

> Полноценная цифровая идентичность. Идентичность, будь то личная или групповая, — это ключ к данным и всем функциям обмена данными. Цифровая идентичность включает в себя не только уникальные подтверждающие механизмы, которые работают всегда и везде, но и возможность распоряжаться всей информацией, связанной с вашим именем, и управлять «персоной», которую вы предъявляете окружающим в различных ситуациях. Эти псевдоличности, или персоны, включают в себя «вас на работе», «вас в медицинском учреждении», «вас как гражданина» и все прочие ипостаси, в которых вы пребываете в ходе общения с любым отдельно взятым контрагентом. Каждая псевдоличность будет иметь доступ к данным, необходимым именно ей. Весь массив данных целиком будете контролировать только вы, то есть личность «биологическая» [11].

Наиболее радикальная часть этих теорий (та, что особенно противоречит понятию «официальной идентичности», из которого исходят чиновники) гласит: наши цифровые следы и виртуальные действия предоставляют о нас гораздо больше сведений, чем бумажные документы вроде паспорта и свидетельства о рождении. В наш век «больших данных» и сетевого анализа — теперь дополненных системой распределенного доверия, которая помогает защитить и подтвердить информацию, — цифровая запись становится более надежным индикатором поведения и репутации, чем паспорта и карточки. Их, в конце концов, не так уж сложно подделать. Используя данные GPS, накопленные телефоном, любой, кто каждый день проводит около восьми часов в одном и том же месте вне дома, может подтвердить факт трудоустройства. Возможно, этот человек получает «серую» зарплату в конверте или у него нет счета в банке, но уже само наличие работы — как минимум один фактор, позволяющий претендовать на ссуду и ряд других услуг.

Возникают два проблемных момента. Первый: как хранить и обрабатывать эти данные так, чтобы нужные сведения о нас были доступны

в любой момент, но при этом не нарушались границы частного пространства и личные свободы? Этот вопрос относится не только к накоплению наших цифровых следов в реальном и виртуальном мире, но и ко всем свидетельствам и поручительствам, предоставляемым третьими сторонами — банками, университетами и пр.

За эти годы криптографы придумали множество приемов, которые позволяют использовать математическое доказательство для подтверждения правильности некоего заявления, даже если детали заявления не разглашаются. Такой метод в криптографии называется «доказательство с нулевым разглашением»: сторона А может использовать математические инструменты, чтобы доказать стороне Б, что ей известен некий пароль или другой секретный код, не раскрывая при этом самого пароля. Для наглядности часто приводят такой пример «из жизни»: дальтоник, который не верит другу, что шарики, лежащие перед ним, разные — один красный, другой зеленый. Каким образом друг может доказать свою правоту? Он может попросить дальтоника взять шарики и несколько раз поменять их местами за спиной, отслеживая при этом, где какой шарик. Затем дальтоник должен по очереди предъявлять ему то один, то другой шарик и спрашивать, какого он цвета. Поскольку друг всякий раз будет называть шарик № 1 зеленым, а шарик № 2 красным, дальтонику придется принять его версию — хотя бы потому, что теория вероятностей не допускает такого количества случайных совпадений.

Еще один вариант доказательства с нулевым разглашением — так называемое гомоморфное шифрование, которое позволяет компьютеру получать нужную информацию, работая с комбинированным массивом данных, но при этом не зная его отдельных компонентов. Возьмем еще один упрощенный пример. Допустим, сотрудники одной компании хотели бы узнать ее общий зарплатный фонд и среднюю зарплату, но никто из них не хочет разглашать сумму своего заработка. Способ есть: первый сотрудник берет произвольное число и прибавляет к нему свою зарплату, а затем по секрету сообщает полученный результат сотруднику № 2. Тот добавляет к сумме свой заработок и передает результат третьему коллеге, и так далее. По завершении опроса итоговая цифра сообщается тому, кто начал процесс, он вычитает свое произвольное число, чтобы узнать общую сумму выплат, а затем делит ее на количество сотрудников и получает среднее арифметическое.

Получается очень простая «человеческая» вычислительная цепочка. Все эти математические операции легли в основу куда более сложных шифровальных программ, позволяющих криптографам буквально творить чудеса с информацией, которая должна оставаться секретной. А поскольку компьютер сводит любые данные — будь то фрагмент текста, фотография, GPS-координаты или ценный актив вроде зарплаты — к последовательности символов, те же технологии можно использовать для защиты личной информации в цифровой вселенной.

Второй проблемный момент — как сохранить единоличный контроль над своими данными, но при этом убедить контрагентов, что они верны? Именно над этой задачей сейчас бьются разработчики блокчейн-платформ. В идеале, если валидизация данных поручается децентрализованной сети, управляемой алгоритмом консенсуса, то ни одно частное лицо или учреждение (государственное или коммерческое) не может изменить информацию после ее подтверждения и записи в соответствующем формате. Кроме того, распорядитель данных — человек, институт, компьютер — должен обладать эксклюзивным правом на выдачу необходимых (желательно зашифрованных) сведений третьим лицам. Осуществить все это непросто даже технически, однако над проблемой сейчас работают десятки исследовательских центров, включая лаборатории крупнейших компаний мира.

В числе лидеров разработки такие стартапы, как Mooti, Civic, Procivis, Tradle и BanQu; все они ищут способ перевести сертификационные услуги банков и прочих посредников в мобильный цифровой формат. Первые четыре компании работают с разными сегментами рынка, а BanQu предлагает пакеты услуг для малоимущих и социально незащищенных слоев населения, включая беженцев, потерявших свои документы.

В данный момент активно разрабатывается концепция *бюро идентичности* (если проводить параллель с финансовой сферой, то в основе идеи лежит принцип «знай своего клиента», но по отношению к частным лицам), которое должно функционировать подобно кредитному: если гражданин получил некий документ или сертификат за подписью инстанции, уполномоченной подтверждать идентичность и репутацию, этот документ может быть использован для получения доступа к услугам третьих сторон. Отчасти это напоминает технологию единого входа, описанную в начале главы. Однако

блокчейн-платформы предлагают систему авторизации, которая не зависит от централизованных структур типа Facebook. Поэтому такая форма подтверждения идентичности может приниматься различными системами, следовательно, доказательство становится мобильным. Гражданин может предъявить его где угодно, и оно всякий раз будет распознаваться как достоверное. Группа банков, в которую входят BBVA, CIBC, ING, Société Générale и UBS, уже разработала подобное доказательство кредитоспособности на базе блокчейн-платформы, предложенной лабораториями R3 CEV.

Теоретически такие системы могут избавить нас от канцелярской работы, а также от затяжных процедур согласования и подтверждения, проводимых разного рода инстанциями. Это, в свою очередь, понизило бы себестоимость операций и вероятность сбоев, а в идеале расширило бы доступ к денежным средствам. Но те же механизмы могут служить и более масштабным общественным целям, например помочь финансовой инклюзии. Скажем, недокументированные мигранты в США могли бы использовать посольство своей страны как «бюро идентичности». Посольство предоставляло бы доказуемое цифровое удостоверение личности, которое затем предъявлялось бы при переводе денег за рубеж вместо всех остальных документов. Если привязать посольские идентификаторы к прозрачным биткоин-транзакциям, финансовые институты смогут осуществлять полностью легальные переводы средств, но при этом сохранят набор инструментов, позволяющих распознать отмывание денег и прочие незаконные операции.

Блокчейн как механизм идентификации привлекает не только молодые компании. Серьезный интерес к нему проявляют и корпорации Microsoft, IBM и Intel. Руководство Microsoft ищет универсальные решения и сотрудничает с разработчиками открытого ПО из всех стран мира, а также лидерами в сфере разработки инфраструктур для Биткоина и Эфириума: Blockstack и ConsenSys соответственно. Глобальная цель, как объясняет главный блокчейн-стратег Microsoft Йорк Роудс, заключается в создании «открытой, независимой системы идентификации на базе блокчейна, которая позволит пользователям, продуктам, приложениям и сервисам взаимодействовать друг с другом, с организациями и провайдерами облачных хранилищ» [12]. Идея весьма амбициозна, и, если выработать стандартную, универсальную архитектуру, с помощью которой пользователь может накапливать и хранить

личные данные на блокчейн-адресе, подконтрольном только ему, этот адрес мог бы стать ядром распределенной идентичности, открывая «цифровые двери» блокчейн-экосистем и реестров. Это позволило бы инноваторам начать разработку новых мощных приложений, обслуживающих цифровую идентичность и прокладывающих нам путь в мир децентрализованной коммерции.

Легко не будет

Важно прояснить некоторые свойства ныне преобладающей модели управления идентичностью на основе блокчейна. Концепция, которую сейчас развивают такие крупные игроки, как ConsenSys, Blockstack и Microsoft, не предполагает непосредственного внесения данных, подтверждающих идентичность, в блокчейн-транзакции. Это очень быстро исчерпало бы ограниченные накопительные возможности распределенного реестра, по крайней мере в системе Биткоин. Следовательно, данные должны храниться *вне сети*, там, где предпочтет пользователь: на компьютере, смартфоне или другом локальном устройстве, или же в облачном хранилище, предоставленном IBM, Microsoft или Amazon Web Service. Конечно, все эти варианты требуют определенного уровня доверия к провайдеру. Поэтому интересно, что часть новых децентрализованных систем для хранения данных в интернете (Maidsafe, Storj, IPFS или Sia) также рекламируются как инструменты для управления личными данными в целях идентификации. Эти хостинговые системы не контролируются отдельно взятыми компаниями.

Тем не менее есть принципиально важные виды данных, которые должны храниться в блокчейне. Во-первых, информация о ключевых парах — открытой и тайной части криптографической подписи, о которой мы уже говорили. Впрочем, здесь речь идет о том, как именно мы используем личный ключ, когда делимся идентифицирующей информацией, а не о подписи официальных заверителей. Частное лицо или организация подписывается с помощью открытого ключа, который очевидным образом прикреплен к имени или названию, означающему нечто в реальном мире, например PaulVigna1,

MichaelCasey9342, AcmeCorp, theageofcryptocurrency.com. Таким образом пользователь демонстрирует компьютерам — валидаторам блокчейна, а значит, и всему миру, что он и только он владеет правами на это имя и может законным образом привязывать его к данным, хранимым вне сети.

Чтобы понять, как работает эта модель, представим, что Майкл ищет работу. Итак, ему нужно доказать потенциальному работодателю, что он окончил Университет Западной Австралии. Для этого он должен 1) использовать личный ключ, чтобы подписать открытый блокчейн-адрес MichaelCasey9342; 2) с помощью того же ключа предъявить цифровую запись, или хеш, своего диплома, который, в свою очередь, криптографически подписан университетом и хранится вне сети. Такая последовательность действий создает неизменяемое подтверждение одного из атрибутов Майкла, а именно его статуса выпускника австралийского университета. Благодаря временны́м меткам блокчейн-транзакции могут подтвердить, что вся последовательность доступа к данным должным образом контролировалась правообладателем, то есть Майклом.

Процесс показался вам сложным? Что ж, так оно и есть. Потому многие скептики и сомневаются, что технология блокчейн может решить проблему идентификации. Процедуры подтверждения влекут за собой риск нарушения конфиденциальности. Кроме того, как мы отмечали в прошлой главе в связи с регистрацией права собственности, для подтверждения почти всегда требуется свидетельство доверенной третьей стороны, что возвращает нас к давней проблеме посредничества. Во многих случаях вам все равно понадобится поручительство банка (чтобы доказать, что ваш счет не связан ни с какими махинациями), или, скажем, университета (чтобы подтвердить подлинность диплома), или почтового провайдера (чтобы доказать, что вы добросовестный корреспондент, а не спам-бот).

Блокчейн-скептики не всегда принадлежат к лагерю любителей «официальных бумаг». В их числе немало влиятельных поклонников цифровой идентификации, таких как Стив Уилсон, давний и убежденный сторонник перехода от устаревшей модели статической идентичности к предъявлению криптографически доказуемых атрибутов. «Открытые и общедоступные блокчейны гордо отвергают любых посредников, однако в большинстве случаев наши заявления ничего

не стоят без свидетельства третьей стороны, которая ручается за нас тем или иным образом, — поясняет Уилсон. — Блокчейн прекрасно подходит для выполнения многих задач, но это все же не волшебная универсальная платформа. Он разрабатывался вовсе не для управления идентичностью» [13].

Но что если мы действительно можем окончательно избавиться от уполномоченных посредников? Если мы хотим выстроить такую блокчейн-модель, которая докажет нашу благонадежность и платежеспособность, не лучше ли собрать и подтвердить все те богатые цифровые данные, которые мы пассивно накапливаем в ходе своей онлайн-жизни, чем полагаться на свидетельства третьих сторон, фиксирующих важные для нас события: рождение, защиту диплома, первую работу и пр.? При наличии надежных криптографических инструментов, позволяющих скрыть конфиденциальную информацию, наши «цифровые следы» помогут, например, использовать аккаунт в соцсетях, чтобы показать, что мы общаемся не с недоучками, а с обладателями университетских дипломов. Он же может предоставить полезные сведения об истории платежей и поездок, распорядке дня и, конечно, посещаемых сайтах. Если владельцы соцсетей и прочих интернет-площадок согласятся на открытые стандарты в сфере метаданных, можно будет создать куда более тонкие и грамотные инструменты идентификации, чем, скажем, у таких бюро кредитных историй, как Equifax. Именно поэтому в наши дни появляются компании, занятые алгоритмическим кредитным скорингом, и многочисленные стартапы, работающие с «большими данными». Блокчейн-система, основанная на математических доказательствах, могла бы помочь нам достигнуть взаимного доверия и расширить рамки социально-экономического обмена.

Однако она же может стать механизмом дискриминации. Алгоритмический подход к интерпретации нашего поведения имеет очень серьезную социальную подоплеку. Один неверный шаг — и мы почти наверняка получим шкалу предвзятых оценок, которая существенно ущемит права тех, кто в силу неблагоприятных обстоятельств, культурных различий или личных факторов не впишется в доминирующую систему ценностей. Если я часто просматриваю республиканские сайты, мой кредитный рейтинг должен быть выше или ниже? Опасный вопрос. Как выразился журналист Хуан Гальт — сторонник

псевдонимной криптовалюты, — «всемирная сеть доверия может превратиться в оруэлловскую сеть позора» [14].

Влиятельный криптоэксперт Андреас Антонопулос полагает: «Корень проблемы в том, что мы вообще взялись за идентификацию, которая противоречит принципам открытой, общедоступной архитектуры Биткоина» [15]. Разработчики блокчейн-платформ, которые создают инструменты для подтверждения идентичности/репутации, «закрепляют пережитки традиционной финансовой системы». Устаревшие структуры и институты, например банки, используют репутацию как «страховочный механизм, который помогает оценить степень риска, связанного с тем или иным именем», и делают это из-за неспособности успешно справиться с риском. По мнению Антонопулоса, мы зря играем в судью и присяжных, используя прошлое «подсудимого», чтобы сделать вывод о его поведении в будущем. Вместо этого стоило бы встроить системы, которые лучше амортизируют риск, в портфолио самих кредиторов. С его точки зрения, Биткоин обладает всем необходимым набором инструментов. У этой технологии множество уровней защиты: смарт-контракты; контролеры мультиподписи, которые гарантируют, что ни одна из сторон не получит доступа к фондам без подписи другой стороны; автоматизированные депозитные соглашения; наконец, полная прозрачность и децентрализованность данных в открытом реестре. Иными словами, в распоряжении инвесторов уже есть целый арсенал средств, защищающих от убытков. Так ли важна прошлая жизнь и репутация контрагента?

Можем ли мы *не* заниматься идентификацией?

Андреас Антонопулос предлагает весьма заманчивую либертарианскую картину мира, где конфиденциальность рассматривается как главная ценность, которую нужно защищать во имя экономического прогресса. Но насколько она реалистична? Основополагающий принцип нашей экономики можно назвать «именным финансированием»; эта модель — неотъемлемая часть архитектуры доверия, которая позволяет функционировать обществу. Подтверждение

личности — будь то с помощью устаревших аналоговых документов, или новомодных цифровых следов, или путем личного опроса — всегда будет требоваться при взаимодействии с частными лицами и организациями.

Поэтому, даже если у вас уже голова идет кругом от бесконечных за и против, несомненно одно: налицо большая проблема. Нынешнюю модель идентификации и защиты личных данных действительно нужно перестраивать, чтобы подготовить к наступлению цифровой эпохи. Самое главное — нужно, чтобы люди взяли управление данными в свои руки, приблизились к идеалу суверенной идентичности. Выяснить, как этого добиться, — задача номер один на сегодняшний день.

Прежде всего необходимо сделать так, чтобы пользователи не боялись утратить личный ключ, без которого невозможно ни расплатиться, ни предъявить информацию о себе. Если забываешь пароль от рабочего компьютера, всегда можно попросить системного администратора назначить новый. Однако у блокчейн-реестра администраторов нет. Биометрическое решение кажется очевидным, но у него есть серьезные подводные камни. Оставляя за скобками те вопросы конфиденциальности, которые мы обсуждали в связи с индийской программой Aadhaar, следует отметить, что в случае взлома биометрические параметры невозможно установить заново (вы же не заведете себе новые пальцы или сетчатку?!). А хакеры уже продемонстрировали нам, как легко использовать воск или мастику, чтобы снять отпечаток пальца с бокала и взломать систему Apple iPhone's Touch ID или же обмануть систему распознавания лиц с помощью фотографий [16].

Кроме того, будем откровенны: несмотря на философию самостоятельности и независимости (например, от банков), исповедуемую адептами биткоина, большинство людей все-таки предпочтут нанять профессионала, который позаботится об их счетах и активах, а не брать риск и хлопоты на себя. Многих пользователей утомляет необходимость работать с паролями от сайтов и почтовых ящиков, что уж говорить об управлении ключами к цифровой идентичности или криптовалютному счету! Фактически большинство биткоин-кошельков, включая крупнейший — Coinbase, предлагают именно посреднические услуги. Вы поручаете сервису выполнить биткоин-транзакцию от вашего имени, а не совершаете ее самостоятельно.

Чтобы не вернуться в недобрые старые времена тотальной зависимости от банков, блокчейн-сообщество вкладывает огромные усилия в разработку решений, которые не позволят посредникам и попечителям украсть или потерять ваши активы. Неплохой компромиссный вариант предлагает технология мультиподписи. Она присваивает набор взаимосвязанных криптографических ключей всем вовлеченным сторонам — потребителю и одному или нескольким посредникам, что исключает вероятность совершить транзакцию в одностороннем порядке: необходимо участие определенного количества обладателей ключа. Система может включать в себя «холодные», или внесетевые, ключи для потребителя на случай утраты активного («горячего») ключа, а также позволяет потребителю отменить транзакцию посредника, объединив все запасные ключи. Этот вариант хорош тем, что, несмотря на необходимость доверить активы посреднику, клиент может контролировать его действия.

Тем же, кто считает, что неизбежная зависимость от внешнего подтверждения делает блокчейн-идентификацию ненадежной, можно дать хлесткий философский ответ: мы уже давно позволили всем этим внешним организациям давать нам характеристику, и если статус блокчейна как универсальной «машины правды» предоставит нам возможность собирать сертификаты и свидетельства, сортировать их удобным образом, предъявлять при первой необходимости и пользоваться расширенным спектром услуг, то почему бы нет? Это определенно лучше, чем нынешняя система. Если мы сможем создать цифровую идентичность с помощью цифровых и виртуальных следов, которые предоставляют намного больше данных и точнее нас характеризуют, уменьшая вероятность ошибки или мошенничества, то кому от этого станет хуже?

Как мы уже говорили, будущее технологии блокчейн зависит от нашей способности применить ее (не до конца раскрытый) потенциал в качестве «бесконтрольного» хронологического реестра транзакций к моделям доверия, преобладающим в реальном, нецифровом мире. Решения, сочетающие в себе разные подходы к ведению учета, явно возымеют больший эффект, чем те, которые опираются только на блокчейн-инструменты. Реестры, хранящие информацию о внешнем мире, должны *укреплять* структуры доверия, а не подменять их собой.

Полный контроль над собственными идентификаторами — весьма достойная цель. Она сулит нам мир, в котором сами граждане (а не централизованные институты, к чьим услугам приходится прибегать) определяют, кто они и что хотят рассказать ему о себе. Однако сложно представить, как осуществить эту мечту без блокчейн-реестра, который защитил бы все стороны от махинаций и подтасовки данных. Если у нас на руках будет лишь криптографически подписанный сертификат какого-либо учреждения, мы, конечно, получим заверенный документ, но учреждение всегда сможет отозвать свою подпись в одностороннем порядке. Фактически именно это сделал президент Трамп, отменив указы своих предшественников, в частности о правах военнослужащих-трансгендеров. Тому же риску подвержены документы с цифровой подписью, если они не хранятся в неизменяемом реестре.

Если свидетельства об идентификации помещены в неуязвимую блокчейн-среду, их невозможно аннулировать без согласия всех причастных сторон. Именно на этом настаивают приверженцы суверенной идентичности. Вот почему, например, в компании Learning Machine разрабатывается платформа Blockcerts, которая позволяет подтверждать дипломы и сертификаты, а в лабораториях Массачусетского технологического института пишут открытое ПО для хеширования и нотариального заверения документов о высшем образовании, которые заносятся в блокчейн-реестр. Что примечательно, с этой целью выбран самый надежный из открытых реестров — Биткоин. Закрытый блокчейн признан непригодным, потому что в нем тоже есть контролирующая инстанция, которая при желании может отменить цифровую подпись выпускника и отозвать диплом. Только общедоступный реестр предоставит выпускникам реальный контроль над документами и возможность предъявлять их при любом требовании. Как отмечает глава компании Learning Machine Крис Джейгерс, «суверенное право не бывает автоматическим, его нужно специально встраивать в любую инфраструктуру на основе блокчейна» [17].

Почему же именно вопросами контроля и собственности столь одержимы разработчики? Вот что сказал Крис Аллен, научный сотрудник компании Blockstream и один из лидеров в сфере разработки цифровой идентичности на базе блокчейна, по этому поводу:

> Идентичность, «я», — явление, присущее исключительно человеку. За ним стоит самосознание личности — понятие, близкое любому жителю Земли, общее для всех культур и цивилизаций. Как сказал Рене Декарт, *cogito ergo sum* — «я мыслю, следовательно, я существую». Однако современное общество исказило эту концепцию. В наши дни государства и корпорации сводят человеческое «я» к набору официальных документов: паспорт, водительские права, полис социального страхования и т. д. Это очень плохо, ведь если государство по какой-то причине аннулирует документы или человек просто приедет в страну, где они не считаются валидными, то он словно бы утратит личность. Я мыслю, но меня нет [18].

К сожалению, панацеи не существует. И впереди немало проблем. Реализация описанных нами идей пока находится в зачаточной стадии. Но она крайне важна, ведь речь идет о фундаментальных принципах и механизмах бытия. Будь то с помощью блокчейна как машины правды или другой децентрализующей, освободительной технологии, мы должны хотя бы попытаться вернуть элемент человечности в повседневную жизнь.

Глава

9

Каждый из нас — творец

Вспомните первую главу книги, где говорилось о системе тройной записи. А теперь давайте подумаем, что это означает для сферы, которая полностью построена на традиционной системе *двойной* записи, — бухгалтерского учета? «Большая четверка» бухгалтерских фирм — Deloitte, Price Waterhouse, Ernst&Young и KPMG — похоже, решила действовать по принципу «если не можешь победить, присоединяйся». В середине 2017 года только в лабораториях компании Deloitte 250 сотрудников занимались распределенными реестрами, остальные три компании демонстрировали не меньшее рвение. Конечно, на поддержку лабораторий уходит крохотная часть бюджета этих гигантов, однако интенсивность исследований говорит о том, насколько серьезно их руководство воспринимает технологию блокчейн. Если неизменяемые цифровые реестры войдут в нашу жизнь, отделы аудита и бухгалтерских услуг со временем прекратят существование — со всеми вытекающими последствиями. В данный момент они приносят компаниям около 40 процентов от их совокупной выручки в 127 миллиардов долларов. В них непосредственно занято около 300 тысяч сотрудников.

Поэтому сейчас компании пытаются понять, как новая революционная технология скажется на их отношениях с клиентами. Очевидно одно: бухгалтерское дело в привычном представлении — с ежеквартальными сессиями, на которых большие команды специалистов изучают отчеты и проверяют легитимность

транзакций, — скоро уйдет в прошлое. И отделы аудита «большой четверки» — всего лишь верхушка айсберга. В зону риска попадают не только они, но и все аудиторы вообще, включая штатных аудиторов разных учреждений. Фактически, как только системы учета полностью автоматизируются и надобность в ручном контроле отпадет, без работы окажутся и те, кто сейчас ведет отчетность, и те, кто ее проверяет. Машины будут сами вносить финансовые данные, анализировать их и оценивать их легитимность — и все в течение нескольких минут, если не секунд. На данный момент в одних только США работает около 1,3 миллиона бухгалтеров и аудиторов (по данным Бюро трудовой статистики).

Резкое сокращение кадров коснется не только бухгалтеров. Весь инвестиционный бизнес, который опирается на отложенный выпуск официальных результатов аудита, тоже окажется под прицелом. Инвестиционный цикл Уолл-стрит определяется релизами данных: аналитики прогнозируют размер ежеквартальной прибыли компании с проданных акций, рынок делает ставки, а затем при появлении очередных цифр инвесторы корректируют цену акций в большую или меньшую сторону. Вся жизнь рынка ценных бумаг вращается вокруг квартальных отчетов. То же верно и для управления активами взаимных фондов, пенсионных фондов и хедж-фондов, чья прибыль зависит от того, насколько успешно в каждом квартале торговались бумаги из их портфеля по сравнению с остальными предложениями на рынке. Даже торговля правительственными бондами подчинена тем же квартальным ритмам: в этом случае ключевую роль играет публикация экономических индикаторов — предварительных оценок инфляции, безработицы, роста ВВП. Что произойдет с этой сферой, когда все финансовые и экономические данные будут автоматически и неопровержимо обновляться в режиме реального времени? Что будет с людьми, которые потеряют работу? А с профессиональной культурой?

Если прогнозы, сделанные в этой книге, оправдаются, нас ждут самые серьезные кадровые потрясения за всю историю человечества. Причем на этот раз в наиболее уязвимой позиции окажутся вовсе не рабочие, продавцы или чиновники нижнего звена, а бухгалтеры, банкиры, нотариусы, страховые и депозитные агенты, поверенные — и даже юристы. Конечно, расхожее утверждение, что юристов заменят смарт-контракты, не совсем верно, ведь условия самого контракта все

равно будут обсуждаться между людьми. Тем не менее правовую индустрию тоже ждет серьезная встряска. Юристы, которые мало разбираются в новых технологиях, скорее всего, будут менее востребованы, чем «компьютерно грамотные». (Одной из наиболее популярных междисциплинарных профессий станет «юрист с навыками программирования».) В общем, основная перспектива ясна: среднему классу надо готовиться к потрясениям.

Похоже, многие наши политики абсолютно к этому не готовы и вообще не понимают, о чем речь. В США Дональд Трамп призывает «покупать американское» (употребляя лозунги, от которых веет фашизмом), а заодно угрожает поднять тарифы, разорвать торговые соглашения, выдворить из страны нелегальных мигрантов и «навести порядок в Америке». Все это ничтожно по сравнению с революцией, которую произведут распределенные платформы и приложения. Узлы «интернета вещей» и 3D-принтеры, соединенные через блокчейн и управляемые смарт-контрактами, окончательно лишат смысла любую президентскую попытку надавить на компанию, чтобы сохранить сотню рабочих мест на производстве.

Обществу придется взглянуть в глаза грядущим переменам, иначе нам не справиться с травмой от потери доходов и не обуздать вполне вероятные вспышки враждебности к мигрантам, которым часто отводится роль козла отпущения, и прочим маргинализированным группам. В прошлом технологический прогресс обычно стимулировал развитие американской экономики, создавая новые рабочие места, которые приносили больше дохода, чем утраченные архаичные профессии. Фермеры становились рабочими, а рабочие — офисными служащими. Однако переход к системе распределенного доверия вкупе со всеми прочими новшествами — беспилотными автомобилями, автоматизированными клиниками, одноранговыми кредитами, 3D-печатью, искусственным интеллектом — будет слишком масштабным, чтобы за ним угнаться. Не исключено, что офисные башни Нью-Йорка и Чикаго опустеют на долгие годы. «Компьютерные программы пожирают мир», — как любит говорить Марк Андриссен [1].

Однако опасность кроется не только в потере рабочих мест. Есть и более глобальная проблема — передача алгоритмам власти над нашей повседневностью. Приоритеты, предпочтения и принципы разработчиков неизбежно находят отражение в коде, будь то программа,

которая определяет, каких пассажиров повезет водитель Uber, или модель поощрений в протоколе Биткоин. Вспомним о мучительных (и не слишком успешных) разбирательствах сервиса Airbnb с клиентскими жалобами на требование сопровождать каждое объявление фотографиями, приведшее к тому, что домовладельцы начали отказывать цветным квартиросъемщикам. Подобные платформы скоро придут в каждую сферу нашей жизнедеятельности, и, если мы не справимся со встроенными в них механизмами дискриминации, они начнут разъедать саму ткань социума. «Если мы не изучим и не выясним, как новые технологии влияют на основные формы социального взаимодействия, включая иерархические структуры и проявления неравенства, понятия демократии и гражданских свобод перестанут быть фундаментом нашего общества», — уверена Шейла Джасанофф, профессор факультета высоких технологий Гарвардского университета [2].

Решение всех этих проблем нельзя оставлять на усмотрение технических специалистов. И конечно, недостаточно просто заявить: «Все должны научиться программировать». Здесь на сцену должны выйти не виртуальные, а вполне реальные учреждения — политические, правовые, благотворительные. Без них структуры общества рассыпятся, и весь огромный освободительный потенциал распределенных моделей пропадет понапрасну.

Среди некоторых политиков и экономистов все большей поддержкой пользуется концепция универсального базового дохода, или УБД. Эту идею выдвинула лейбористская партия Великобритании, и частично ее уже опробовали правительства скандинавских стран. Ее суть — ежемесячная выплата базового прожиточного минимума каждому совершеннолетнему гражданину страны. Идея не нова: впервые ее высказал Томас Пейн в XVIII веке. Левые круги вспомнили о ней, когда стало очевидно, что робототехника, искусственный интеллект и прочие новшества скоро ударят по рабочему классу, например по водителям грузовиков. Однако популярность такого решения может вырасти еще больше, когда децентрализованные блокчейн-платформы начнут отнимать рабочие места у среднего класса. Несмотря на извечные опасения экономистов-прагматиков, что универсальный базовый доход, как и любая государственная субсидия, лишит население мотивации к труду, эта идея вызывает

определенные симпатии и среди политиков правого толка. Одна из причин — более простой и менее бюрократизированный процесс реализации таких выплат, чем нынешние программы социальной помощи. Да и что означает «утрата мотивации к труду», если трудиться будет уже не нужно?

Высказываются также опасения, что универсальный базовый доход усугубит неравенство в статусе, если не в уровне обеспеченности. Зависимость от государства подорвет социальные структуры. Владельцы капитала и активов продолжают накапливать богатства, тогда как основная масса населения будет вынуждена обходиться прожиточным минимумом. Поэтому в качестве альтернативы УБД иногда предлагают «универсальный базовый актив» — личную, доступную для инвестиций долю в социально-экономической инфраструктуре. Что если все городские жители получат акции распределенной энергосети своего города, отображенные в форме криптоактива? Захотят ли они вложить этот актив в бизнес, требующий новых энергозатрат? Ранее мы обсуждали репутационные токены и персональные бренды — концепции, в рамках которых индивидуальные навыки и опыт работы рассматриваются скорее как инструменты для создания капитала, чем пакеты готовых услуг. Возможно, такой подход стимулирует работу на благо общества. Не исключено, что со временем каждый из нас будет владеть долей в общественном благосостоянии.

Призывы помочь тем, кто попадет под удар в результате новой технической революции, носят одновременно и моральный, и прагматический характер. Ведь под вопросом может оказаться само понятие человеческого достоинства — осознание того, что каждый из нас имеет право сделать из своей жизни нечто осмысленное и плодотворное. По мере того как машины начнут занимать места «синих», а затем и «белых воротничков», нам придется заново задуматься о цели и смысле бытия. Пожалуй, самым конструктивным было бы стремление перейти к постиндустриальному образу существования, при котором всячески поощряется творческая деятельность — даже если она и не вознаграждается финансово. В рамках подобного мировоззрения каждый из нас, а не только «звезды» бизнеса вроде Илона Маска или популярные деятели культуры вроде Джеффа Кунса, Бейонсе и Джоан Роулинг ценен своей способностью к созиданию.

Идея, конечно, не нова. На рубеже XIX и XX веков многие социалисты мечтали о политико-экономическом строе, при котором общедоступная техника освободила бы человечество от тягот повседневного труда и позволила бы каждому раскрыть свой творческий потенциал. В 1891 году в статье под названием «Душа человека при социализме» Оскар Уайльд утверждал, что «социализм избавит нас от презренной необходимости жить для других» [3]. В прекрасном и светлом будущем техника освободит нас от работы и позволит увидеть «истинную человеческую личность. <...> Она будет необыкновенна. Она станет развиваться просто и естественно, как распускается цветок или растет дерево». Уайльд не сомневался, что «в нормальных условиях техника должна служить человеку. <...> Именно таково будущее техники, и если известно, что хозяин спит, а сад растет, значит, и Человечество сможет предаваться приятным занятиям или наслаждаться возвышенным досугом... создавать произведения искусства, читать прекрасные книги или просто созерцать мир с восхищением и восторгом, а машины будут вершить всю необходимую и неприятную работу».

Хотя и не столь витиевато, мы все же обсуждали нечто подобное в книге «Эпоха криптовалют», когда рассказывали об идее одного из создателей биткоина Майка Хирна — беспилотном автомобиле общего пользования. Проект, конечно, не совсем социалистический, но его результатом должна стать именно машина, работающая на благо общества. По сути, автомобиль будет программироваться на основе смарт-контрактов и взаимодействовать с прочими системами, устройствами и онлайн-рынками. Это позволит добиваться оптимального соотношения тарифов: заправляться топливом по наиболее выгодной цене и принимать решения о выезде или невыезде на дороги в зависимости от количества запросов на рынке. Почему обществу нужна такая система? По той же причине, что и совместные проекты вроде The DAO (которые мы обсуждали в главе 8), где нет места для личной выгоды, отвлекающей от максимизации общего блага. Перед нами современная версия общественной инфраструктуры, которая станет возможна вследствие повышения эффективности «интернета вещей» за счет автоматизированных систем распределенного доверия на основе блокчейна. Таким образом, технология могла бы освободить нас от работы и при этом повысить общий уровень жизни, затратив минимум ресурсов.

А как же насчет романтического пророчества Уайльда, согласно которому благодаря освободительницам-машинам каждый из нас найдет в себе художника или поэта и тем самым достигнет внутренней гармонии? (То, что сам Уайльд назвал свое видение «новым индивидуализмом», свидетельствует о том, насколько неортодоксальна его анархическая трактовка идей социализма.) Великий драматург, словно опережая критиков, признал, что его мечта «непрактична и противоречит человеческой природе». Однако именно поэтому, уверял Уайльд, «ее и стоило осуществить». Что ж, давайте посмотрим, как ведет себя человечество в эпоху социальных сетей. Каждый пользователь Twitter, похоже, мечтает о собственной трибуне. И хотя селфи сложно назвать высоким искусством, нельзя отрицать, что в постоянном позировании для Instagram есть некий элемент перформанса. Возможно, каждый из нас и впрямь мечтает раскрыть свой творческий потенциал. Интересно, что благодаря новым технологиям творчество все чаще превращается в коллективный процесс. Даже юмор отчасти перешел на рельсы «краудсорсинга»: вспомните, как стремительно обрастают новыми шутками всевозможные мемы и хештеги, причем каждая вариация как бы надстраивается над предыдущими. Музыка, брендинг и субкультура фактически слились воедино благодаря коллективным творческим проектам. Хацунэ Мику — вечно юная японская виртуальная певица, или «вокалоид» (компьютерная программа, синтезирующая пение на основе банка голоса, плюс голограмма и сопровождение «живых» музыкантов), — может похвастаться репертуаром в 100 тысяч песен, созданных и раскрученных ее поклонниками; количество видеоклипов на YouTube с ее участием превысило 170 тысяч, а общее число посвященных ей интернет-произведений уже перевалило за миллион.

Если вам кажется, что все это массовое искусство не заслуживает серьезного внимания, позвольте напомнить: аналогичный принцип коллективного созидания в наши дни движет миром науки и инноваций. Это особенно заметно в области открытых программных разработок, самые яркие примеры которых, конечно же, Биткоин и Эфириум. Однако по мере появления вычислительных мощностей не только у компьютеров импульс совместного, безграничного творчества распространяется дальше. Один из примеров — вероятно, опередивший свое время проект Pink Army Cooperative, запущенный биотехнологом Эндрю Хесселом в 2009 году. Хессел сформировал открытое сообщество

биоинженеров для коллективной разработки программ, редактирующих геном, в частности искусственного онколитического вируса, который выявлял и убивал бы раковые клетки в молочной железе. Ожидалось, что глобальное сообщество экспертов вложит в поиск спасительного решения намного больше творческой энергии, причем почти даром, чем фармацевтические компании с чисто коммерческой мотивацией. С тех пор Хессел прибег к помощи компании Human Genomics, чтобы собрать деньги для финансирования проекта. Однако принцип открытой коллективной разработки остался незыблемым.

Наверное, наивно полагать, что бескорыстное коллективное производство идей и контента послужит на благо общества безо всяких осложнений. Одна из главных проблем — сложность с установлением авторства (а стало быть, принадлежности), что приводит к не всегда справедливому распределению дивидендов, которые оно приносит. В первую очередь проблема касается художественного или текстового контента, ведь блоги, агрегаторы и платформы социальных сетей забирают бóльшую часть выручки от рекламы, которую генерирует этот контент. Но это также относится и к профессиональным авторам и художникам, чей доход от материалов, выложенных на YouTube и прочих сервисах, распределяется по непрозрачным, плохо прописанным схемам. Здесь тоже может помочь технология блокчейн. Многие инноваторы разрабатывают децентрализованные модели публикации, которые дадут авторам больше власти над судьбой их произведений. Подобно тому как блокчейны создают уникальные цифровые активы из криптовалютных токенов и хешированных документов, можно придать те же свойства контенту. Механизмы защиты от двойного расходования, успешно работающие в Биткоине, в один прекрасный день можно было бы применить, скажем, к цифровым фотографиям. Тогда, вероятно, система оплаты творческого труда стала бы гораздо справедливее.

Вернем власть художникам

Прежде чем рассматривать предлагаемые решения, давайте поговорим об одном из самых злостных нарушителей авторского и потребительского права — сети Facebook, число пользователей которой превысило

два миллиарда человек. Как сказал легендарный эксперт по кибербезопасности Брюс Шнайер, «вы думаете, что вы потребитель Facebook? Не обольщайтесь. Вы не потребитель, вы — товар». Facebook берет наши посты, комментарии, ресурсы, которыми мы делимся, и (что самое главное) группы подписки, которые мы создаем, и предоставляет все это рекламным агентствам в качестве готовой, заботливо сегментированной аудитории.

Новостная лента Facebook — это не хронологическая последовательность публикаций, как у Twitter, а продукт особого алгоритма. «Умная», максимизирующая прибыль машина производит анализ и решает, кому и что захочется почитать. Публикации сортируются и предлагаются различным пользовательским сегментам. Сами маркетологи Facebook с некоторой тревогой называют эти сегменты «аудиториями близнецов». Именно так создаются и закрепляются пресловутые «эхо-камеры» социальных сетей — группы единомышленников, с которыми мы подсознательно объединяемся и чьи ленты новостей никогда не включают в себя мнение другой стороны. Без нашего ведома нам скармливают информацию, которая подтверждает наши политические взгляды. Wall Street Journal даже опубликовал статью под названием «Красная и синяя лента новостей». В ней показано, насколько разными стали подборки постов и ссылок, которые Facebook предлагает республиканцам и демократам [4].

С точки зрения политики это крайне опасно, поскольку лишает нас возможности выслушать мнение другой стороны, прийти к консенсусу и выйти на новую ступень развития общества. Однако для рекламных агентств здесь просто золотое дно. Теперь они могут работать с соответствующей аудиторией и пожинать плоды сетевого эффекта, возникающего за счет многочисленных лайков и репостов. Публикации, которые должны выйти в топ (собрать максимальное количество пользовательских реакций), можно сделать буквально из ничего, поместить в нужную «эхо-камеру» и использовать для привлечения драгоценного внимания к исходному сайту в обмен на размещение рекламы или часть выручки от Google Ad. Давайте подумаем, что это означает для серьезных изданий вроде The New York Times или The Wall Street Journal, которые тоже хотят использовать мощнейшую платформу Facebook, чтобы привлечь публику к собственным сайтам и заработать на рекламе. Эти издания вкладывают миллионы в работу корреспондентов,

редколлегий, юристов — словом, в ту инфраструктуру, которая обеспечивает должное качество информации. Однако им приходится конкурировать (причем имея меньше возможностей создать «аудиторию близнецов») с авторами фейков вроде тех македонских подростков, которые успешно скормили консервативной публике новость о папе Франциске, который якобы «запретил католикам голосовать за Клинтон» [5].

Другие социальные сети тоже используют алгоритмы отбора информации, однако версия Facebook особенно навязчива, что, конечно же, радует акционеров компании. Этот пример прекрасно подчеркивает опасность централизации в медийной среде. И та аудитория, которая видит наши публикации в Facebook, и тот контент, который видим мы, определяются тайным алгоритмом платформы. А кто получает дивиденды от нашего невольного участия в этом социальном эксперименте? Уж точно не мы. Не производители контента. Всю прибыль забирают себе акционеры Facebook.

Нам давно пора создать децентрализованную модель публикаций. Коль мы не можем вернуться к централизованной, строго иерархичной системе традиционных СМИ, необходимо переосмыслить устройство медийных платформ. Производство и распространение информации должно стать открытой, демократичной сферой, куда любой пользователь может войти на равных. Но как?

Для начала следовало бы заняться защитой контента, который генерируют пользователи. Если вы выкладываете в интернет фотографию или, скажем, собственную музыку, записанную не на крупной студии, кто угодно может скопировать и распространить ваш материал. Теоретически, конечно, можно отслеживать случаи воспроизведения, заявлять об авторских правах и, если удастся установить конкретных нарушителей, подавать на них в суд. На практике же, учитывая огромные расходы на юридические услуги, такое могут себе позволить только крупные медиакомпании. Да и тем не хватает ресурсов для борьбы с каждым мелким нарушением.

Впрочем, и запрет на свободное использование контента не совсем в ваших интересах. Одно из главных достоинств открытой, щедрой природы интернета — возможность создавать ценности, формируя аудитории и каналы связи между ними. Всемирная сеть — это открытое пространство коммуникации, единый общий ресурс, который

генерирует символический капитал, доступный каждому. Художники, писатели, музыканты и поэты не берут денег за доступ к произведениям, размещенным на этой площадке, но тем не менее получают отдачу в виде высокого рейтинга, репутации, влияния и авторитета. Все это можно монетизировать по-разному: музыканты привлекают публику на свои концерты, художники получают заказы, писатели завязывают контакты с издателями. Или как среднестатистические пользователи соцсетей мы просто зарабатываем социальный капитал благодаря подписчикам на наши обновления, лайкам и репостам. И все же, учитывая, что гигантский доход от рекламы на подобных платформах перетекает в карманы их владельцев, нельзя сказать, что процесс коллективного создания ценностей устроен справедливо. По большей части это объясняется тем, что авторам сложно связать свое имя с судьбой своих произведений. У них есть определенная возможность отследить, как их контент порождает социальный капитал в рамках отдельно взятой платформы (например, сколько лайков он получает на Facebook), но, как только этот контент копируется и размещается на другом ресурсе, связь разрывается.

На данный момент существует довольно удачное решение — интернет-лицензия Creative Commons. Она помогает хотя бы частично навести порядок в сфере воспроизведения авторского контента и фотографий, создавая правовую структуру, которая разрешает различные формы свободного использования при соблюдении оговоренных правил и условий. Исходя из ряда категорий и параметров, эти условия определяют, например, нужна ли ссылка на источник при перепечатке, можно ли использовать произведение в коммерческих целях и т. п. На сегодняшний день лицензировано более миллиарда произведений, которые в основном размещены на таких платформах, как Flickr и Wikimedia [6]. Однако нам предстоит еще многое сделать для поддержки авторов и урегулирования их отношений с аудиторией. Во всех сферах творчества, и особенно в музыке, отсутствие четко определенных авторских прав приводит к гегемонии посредников, которые берут на себя дистрибуцию и продвижение творческого материала, а в уплату требуют эксклюзивных прав на него. Наша общая площадка пока далека от идеальной, демократичной питательной среды для творческого самовыражения, о которой мечтает гарвардский профессор Лоуренс Лессиг и другие лидеры движения «за свободу культуры».

Чем же технология блокчейн и родственные ей криптографические системы распределенной информации могут помочь в борьбе с несправедливостью?

В главе 4 мы уже рассказывали о попытке компании Brave переформатировать индустрию контекстной рекламы с помощью токена Basic Attention, который должен вознаградить потребителей творческого контента за уделенное время и помочь рекламодателям точнее измерить эффективность пользовательского внимания. Судя по количеству конкурентов, появившихся у Brave, многие разработчики полагают, что подобные технологии смогут оптимизировать индустрию творческого контента. На платформе Эфириум работает сервис AdChain, чья задача — создать блокчейн-реестр данных, используемых в контекстной рекламе [7]. В то же время консорциум медиагигантов, куда входят Comcast, Disney, NBCUniversal, Cox Communications, Mediaset Italia, Channel 4 и TF1, запустил платформу Blockchain Insights, которая должна перевести покупку рекламных объявлений на принципиально новые рельсы. Но куда более сложная задача — выяснить, каким образом лучше всего использовать блокчейн для оценки и оплаты творческого контента, особенно если учесть, что в эпоху социальных сетей *каждый* причастен к его производству. Как же отследить это все?

Невзирая на сложность задачи, неофициальный альянс технологов, предпринимателей, художников, музыкантов и уставших от пиратства музыкальных продюсеров сейчас исследует потенциал применения блокчейна ко всей сфере человеческого самовыражения. Основная идея состоит в том, что в результате присоединения к цифровому произведению метаданных о названии, авторе, дате создания и прочих деталях и их последующем внесении в неизменяемый блокчейн-реестр можно превратить фактически бесхозный, легко воспроизводимый ресурс в уникальный продукт, чьи перемещения в интернете легко отслеживать и контролировать. Хотелось бы надеяться, что это наделит новыми правами и свободами как создателей творческого контента, так и его потребителей.

Нам удалось провести один из первых экспериментов в этой области: 2 февраля 2015 года мы взяли хеш нашей первой книги «Эпоха криптовалют» и внесли эту информацию в блок № 341705 на блокчейне Биткоина. Дэн Ардл, научный директор Совета по цифровым валютам, чьи блокчейн-инструменты мы использовали для транзакции, пояснил

ее важность так: «Этот хеш — уникальная функция книги, следовательно, он не мог быть создан раньше, чем ее текст [8]. Если хеш фигурирует в биткоин-транзакции, он неоспоримо подтверждает существование книги в конкретный момент осуществления транзакции. Это доказательство вписано в самый надежный и прозрачный реестр, когда-либо созданный человечеством». В каком-то смысле мы проделали усложненную версию старого трюка, к которому раньше прибегали писатели, чтобы подтвердить авторство: они отправляли копию рукописи сами себе, чтобы штемпель с датой на конверте послужил доказательством их права на интеллектуальную собственность.

По правде говоря, мы нисколько не сомневаемся, что американский суд защитит наше авторское право, и занесли книгу в блокчейн-реестр исключительно в экспериментальных целях. Кроме того, большинство ее экземпляров продано в бумажном виде, то есть их невозможно скопировать, но нельзя и отследить, и блокчейн здесь тоже бессилен. Его потенциал главным образом применим к цифровым произведениям (в частности, музыкальным), которые сейчас бесконтрольно распространяются в интернете. Есть надежда, что блокчейн сможет выполнять ту же функцию, что теги и подписи на фотоснимках, — превращать воспроизводимый контент в уникальный актив, в данном случае цифровой.

Британская певица, лауреат премии «Грэмми» Имоджен Хип в числе первых музыкантов опробовала блокчейн-сервисы. С помощью компании Ujo — одного из детищ лаборатории ConsenSys — Хип занесла в блокчейн Эфириума песню «Маленький человек» (Tiny Human), посвященную дочери. За 60 центов любой пользователь может скачать трек, зная, что средства автоматически распределятся по смарт-контракту и поступят на счета создателей песни, включая не только саму Имоджен Хип, но и звукооператора, музыкантов и т. п. За 45 долларов другие музыканты, занятые некоммерческими проектами, могут скачать различные «элементы» песни — вокал, партию ударных, струнных или басов, чтобы семплировать их и использовать в своей работе. Впрочем, пока этот маркетинговый ход не принес особой прибыли.

С точки зрения Имоджен Хип, главное — не доход от прямых продаж музыкального произведения, а полнота и богатство сведений, которые мы получим, когда музыкальный файл будет неразрывно связан

с именем своего создателя. Певица рассматривает эту информацию не как инструмент конкурентной борьбы с другими исполнителями или ревностной защиты авторского права, а скорее как возможность открытия, сотрудничества и инновации. «В мире миллионы исполнителей, о которых мы ничего не знаем. Мы никогда не слышали их музыки и понятия не имеем, на что они способны, что умеют, — говорит Хип. — Этих людей надо как-то поддерживать и выводить в свет, чтобы не только крошечный процент музыкантов мог прилично зарабатывать, но и у каждого была возможность найти свою публику. <...> Мне кажется, в музыкальной индустрии давно назрели перемены, и это хорошо. Я чувствую, что прямо сейчас начнется что-то важное» [9].

В наши дни монополия на сведения об исполнителях и композициях принадлежит студиям звукозаписи. Нередко они злоупотребляют этим с помощью правовой системы контроля, известной как «технические средства защиты авторских прав» (ТСЗАП), которая разработана для борьбы с пиратством в эпоху интернета. Претензии к этой системе высказывают как создатели, так и потребители творческого контента, поскольку она налагает жесткие ограничения на творчество. Например, документалистам приходится останавливать съемку, если где-то фоном звучит музыка, иначе можно нарваться на иск от студии, которой принадлежат права на композицию. Исполнители тоже жалуются, так как им достается лишь небольшая часть выручки. «Уж лучше бы наши поклонники свободно слушали музыку и делились ею из любви к искусству, чем сидели и боялись, что на них подадут в суд», — считает Имоджен Хип [10].

Конечно, не стоит забывать, что система ТСЗАП создавалась для борьбы с бесконтрольным распространением цифровых файлов, однако, похоже, решение этой проблемы уже найдено. Раньше считалось, что, в отличие от материальных объектов вроде книги или видеокассеты, цифровой файл нельзя рассматривать как отдельный уникальный актив, так как его в любой момент можно скопировать, причем практически бесплатно. Но с ТСЗАП вся творческая индустрия превратилась в площадку, где взаимный обмен между создателями не поощряется, а постоянно ограничивается. Кроме того, наши возможности как потребителей тоже сузились. По мере того как потоковое вещание, или стриминг, становится основным способом потребления (и монетизации) музыки и фильмов, заметно ухудшается качество

воспроизведения (ведь для совместимости с любыми проигрывателями и устройствами нужны «легкие» форматы файлов). В этом не было бы ничего страшного, если бы потребитель мог доплатить за доступ к высококачественному контенту на другой платформе, но выбора у нас как раз нет. (Этим фактором, а не только ностальгией и модой на хипстерское движение отчасти и объясняется проснувшаяся любовь к винилу.)

Однако технология блокчейн помогла бы нам вспомнить забытое чувство уникальности каждого произведения искусства. По мнению Лэнса Кунса, юриста компании Davis Wright Tremaine, блокчейн предлагает цифровую версию «доктрины первой продажи», которую проще всего объяснить на примере книжных магазинов [11]. При продаже книги происходит передача не только права собственности на объект, но и самого объекта. Поэтому вторичные продажи книг — например, с рук или в букинистических магазинах — никем не контролируются, ведь торговец не может одновременно и продать книгу, и оставить ее себе (разве что проделает трудоемкий и долгий процесс копирования, но тогда у него останется не книга, а ее жалкая копия). Но в отношении электронных книг и прочих цифровых файлов возникает та же проблема, которая преследовала криптовалюты до появления биткоина, — двойное расходование. Скопировать текстовый, музыкальный или видеофайл — пара пустяков. Но, как говорит Лэнс Кунс, благодаря блокчейн-платформам «на наших глазах появляются системы, которые могут гарантировать, что лишь одно цифровое "издание" будет законным образом продаваться или передаваться другому владельцу». Вспомним главу 3, где мы объясняли, каким образом блокчейн сделал возможным понятие *цифрового актива*.

Предстоит пройти еще немалый путь, прежде чем сформируется полноценный рынок невоспроизводимых цифровых активов. Технологии копирования никуда не исчезнут, даже если покупатель № 1 будет приобретать файл непосредственно у автора, зарегистрировавшего право собственности в блокчейне. Выгодополучатели, которые зарабатывают в рамках нынешней системы, тоже так просто не сдадут позиции. Тем не менее уже само наличие метаданных в неизменяемом реестре позволит авторам управлять своими творческими активами, не прибегая к услугам посредников вроде студий, руководствующихся ТСЗАП. В действительности пользователи медийных продуктов чаще

всего хотят точно знать имя их создателя. Блокчейн поможет им отдать должное авторам.

Ujo — отнюдь не единственный стартап, который изучает, как блокчейны могут помочь создателям творческого контента. В том же русле движется компания Monegraph, предоставляющая авторам уникальные лицензии, где право интеллектуальной собственности подтверждено записью в блокчейн-реестре. Компания Stem использует смарт-контракты и соглашения о сотрудничестве с временны́ми метками, позволяющие музыкантам и прочим авторам треков автоматически получать роялти от YouTube и других платформ. Следует отметить и проект DotBlockchain Music, в рамках которого планируется разработать уникальный кодек с расширением .bc, предназначенный для записи метаданных музыкальной композиции.

Но, несмотря на все усилия и совместные разработки, придется сделать поправку на медленную реакцию тяжеловесов творческой и развлекательной индустрии, без которых нам пока не обойтись. Впрочем, некоторые из них уже исследуют возможности новой технологии. Среди 170 участников некоммерческого проекта Open Music Initiative под эгидой Музыкального колледжа Беркли такие гиганты, как Sony Music Entertainment, Universal Music Group и Warner Music Group, а также лидеры потокового вещания компании Spotify, Napster и Netflix. Цель проекта — убедить крупнейших игроков согласиться на новые правила и условия, однако успех будет зависеть от способности разработчиков предложить «открытый протокол для стандартной идентификации правообладателей и авторов музыкальных произведений». Конечно, не стоит ждать, что крупные компании с восторгом воспримут все перемены. Open Music Initiative вполне может стать формальным мероприятием, которое медиагиганты будут использовать, чтобы затянуть процесс и сохранить свои права на бесчисленные старые записи.

Следовательно, большинство принимаемых мер будут направлены на новые фильмы, тексты и музыкальные композиции, а не на огромный массив уже продаваемых произведений, с которого кормятся издательства, киностудии и студии звукозаписи. Тем не менее стоило бы разобраться и с залежами опубликованного контента: создать инфраструктуру достоверных данных о каждом произведении, его истории и авторах. Причем это касается и непрофессионального (или полупрофессионального) контента, размещенного на таких площадках,

как Facebook, Instagram, YouTube, Flickr и Pinterest. Не будем забывать, что наше коллективное творчество приносит немалый доход корпо-
[266] рациям (владельцам этих платформ), но почти ничего не дает нам, его создателям.

Банк метаданных

Идентификация контента — необходимый первый шаг, если мы хотим изменить нынешнее отношение к творчеству и механизмы его оценки. (Обратите внимание: снова встает вопрос об идентификации — на сей раз цифровых художественных артефактов.) Это масштабная задача, и на пути ее реализации нас на каждом шагу будут подстерегать ловушки субъективности. Например, что делает один фотоснимок ценнее, чем другой? Какая степень уверенности нужна для заявления об авторских правах? Какой механизм лучше использовать для улаживания разногласий?

Тем не менее с чего-то нужно начинать. Нью-Йоркская компания Mediachain уже прикрепляет метаданные художников — имя, название произведения, дату создания — к существующим цифровым изображениям в интернете, причем таким образом, чтобы сведения можно было хранить, регистрировать и подтверждать в системе децентрализованного доверия. Разработчики Mediachain создали открытую распределенную базу данных из более чем 125 миллионов изображений с поиском по самым разным параметрам, включая описания, сгенерированные программой распознавания образов. В основном они взяты из гигантского хранилища произведений с лицензией Creative Commons в надежде сделать эту систему более привлекательной для авторов. «Сейчас весь набор данных Creative Commons разбит, раздроблен и хранится в изолированных базах данных на разных платформах, — говорит сооснователь Mediachain Джесс Уолден. — Когда ваше произведение выходит из такого хранилища в широкий мир, вы не испытываете никакого удовлетворения от того, что кто-то оценил вашу работу и захотел поделиться ею с другими, поскольку не получаете об этом никакого уведомления» [12]. Чтобы исправить это упущение, разработчики Mediachain создали распределенную структуру, которая

должна работать на разных платформах, делая метаданные каждого изображения доступными и читаемыми для всех.

Однако в системе Mediachain не используется блокчейн-реестр — по крайней мере, его ключевые компоненты. Причина в том, что ограничения, налагаемые нынешней пропускной способностью на открытые публичные блокчейны вроде Биткоина и Эфириума, особенно чувствительны к данным такого рода. Их вполне достаточно, чтобы заполнить блок емкостью в 1 мегабайт на десятилетия вперед, а у авторов нет ни малейшей возможности заплатить сотни миллионов долларов майнерам за включение их информации в блоки и ее подтверждение. Однако учитывая гигантский объем и хаотичное состояние творческого контента в сети с сотнями миллионов художников, разбросанных по всему миру, рано или поздно придется выстроить открытую децентрализованную систему, в которой данные не будут подвержены контролю и манипуляции со стороны крупных институтов вроде студий звукозаписи.

Как и многие другие инноваторы, разрабатывающие неуязвимые децентрализованные хранилища для нефинансовой информации, специалисты компании Mediachain нашли «внесетевое» решение проблемы. Они используют иерархическую структуру подтверждаемых криптографических ссылок, которые упорядочивают информацию весьма эффективным и прозрачным способом, а затем хранят ее в интернете с помощью межпланетной файловой системы (IPFS), распределяющей файлы между многочисленными компьютерами-участниками. Затем Mediachain предоставляет бесплатное открытое ПО, позволяющее пользователям осуществлять поиск по базе данных, а разработчикам — создавать новые приложения. Криптографическая защита делает базу неуязвимой для взлома и вполне надежной — настолько, насколько можно верить утверждениям об авторстве (что, впрочем, касается почти всех претензий на право интеллектуальной собственности). Алгоритм консенсуса, подобный используемому в блокчейнах, нужен лишь при передаче цифровых активов или прав на них от одного владельца другому.

Конечная цель — разорвать «порочный круг» и гарантировать, что ценности, порожденные общим для всех ресурсом, не присвоят медиаплатформы вроде Facebook или профессиональные сайты типа BuzzFeed. Все эти сервисы монополизируют и, следовательно,

монетизируют данные о поведении пользователей на своих закрытых и огороженных площадках. Поскольку бóльшая часть изображений в коллекции Mediachain имеет свободную лицензию Creative Commons, едва ли стоит в рамках борьбы с монополиями требовать непосредственных выплат от пользователя автору. Скорее всего, такое решение вызовет недовольство пользователей и уничтожит саму идею общего ресурса. Поэтому следует поискать более приемлемое решение.

Одна из концепций, предложенных командой Mediachain, называется CC Gratitude license, или «лицензия пользовательской благодарности». Она разработана при участии юриста Лэнса Кунса на основе базовой лицензии Creative Commons. По ее условиям, пользователь должен уведомлять автора о месте размещения его произведения. Таким образом сбылась бы мечта певицы Имоджен Хип, поскольку артисты напрямую получали бы информацию о поведении публики. Однако руководство Creative Commons поначалу восприняло идею скептически, высказав опасения, что новая лицензия добавит лишней работы либо конечным потребителям, либо администраторам платформ, которым придется встраивать в них новую функцию, из-за чего естественный рост общего ресурса будет ограничен. Такие препятствия, вероятно, можно было бы преодолеть, если бы платформы типа Flickr брали с авторов небольшую одноразовую плату за подключение сервиса. Но в целом, как говорит сооснователь Mediachain Джесс Уолден, крупные менеджеры «не хотят помещать данные в открытую общедоступную базу, несмотря на то что речь идет о лицензиях Creative Commons... Эта идея слишком революционная, чтобы платформы согласились добровольно взвалить на себя такую нагрузку» [13]. В этом смысле Flickr мало чем отличается от других централизованных провайдеров в сети. Он стремится удержать пользователей в рамках сайта, а не перенаправлять их по интернету туда, куда укажет Mediachain. Таким образом платформа генерирует данные, которые можно продать рекламным агентам и другим пользователям. Иными словами, ей самой угрожают децентрализованные решения на основе блокчейна.

Наверное, можно ускорить реформы с помощью идеи, которую уже озвучило, но пока не успело опробовать руководство Mediachain. В какой-то момент компания была готова присоединиться к распродажам токенов и даже составила план выпуска собственной криптовалюты под названием CCcoin. «Коины» должны были перечисляться

правообладателям контента с лицензией Creative Commons, если они загрузят свои произведения в систему Mediachain и получат одобрительные голоса других пользователей [14]. Представьте себе рейтинговую систему групповой модерации вроде практикуемой на платформе Reddit, с той лишь разницей, что здесь фигурирует криптовалюта. «Проект CCcoin можно назвать экспериментом с "доказательством творческой работы"», — говорит Уолден. Он рассчитан на будущий мир, в котором каждый творец получает некий «пакет акций» в зависимости от своего вклада в общий ресурс, тогда как те, кто приобретает и использует токены, становятся своего рода меценатами. Примерно из тех же соображений некоторые пользователи сейчас добровольно переводят средства в фонд Creative Commons.

К сожалению, проект CCcoin так никуда и не продвинулся с весны 2017 года. Основная причина — в резком изменении статуса компании Mediachain. Ее выкупила корпорация Spotify — лидер в сфере потокового аудио [15]. В итоге команда Уолдена была переброшена в нью-йоркский офис корпорации. Для сделки была как минимум одна веская причина: в 2016 году Spotify пришлось выложить около 20 миллионов долларов правообладателям по иску о невыплаченных авторских отчислениях [16]. Похоже, Spotify купила Mediachain именно из соображений получить более надежный механизм отслеживания авторских прав и роялти. В каком-то смысле это, безусловно, повышает востребованность и престиж проектов Mediachain. Однако в результате частная корпорация может завладеть технологией, которая должна широко использоваться на благо общества и поставить ее вместе с другими новаторскими решениями себе на службу. Остается надеяться, что этого не произойдет.

Благодаря подобным проектам мы теперь хотя бы представляем, как подступиться к реформе системы, которая защищает права создателей творческого контента в интернете. Однако если мы действительно хотим снова сделать интернет общим ресурсом для всех, то есть для огромной массы пользователей, всевозможными способами генерирующих информацию, идеи и развлечения, нам необходимо задуматься и об управлении самой Всемирной паутиной.

Концепции, лежащие в основе блокчейна, вынуждают нас взяться за эту задачу, поскольку сама технология, по сути, и есть система

управления. А это по умолчанию придает ей политический аспект — не в том смысле, что традиционные политические институты определяют курс развития технологии (хотя действия Конгресса и регуляторов, конечно, играют свою роль), а в том, что все участники процесса влияют на работу программы, которая управляет их жизнью. Вопрос о том, кто составляет алгоритмы, и дебаты о внешних стандартах, которые могут ограничить развитие технологии, и есть политика. Крайне важно, чтобы представители всех заинтересованных сторон высказались по поводу устройства блокчейн-систем и приложений. Поиск компромисса — основная политическая задача.

Глава

10

Новая конституция для цифрового века

Идеи, которые легли в основу Конституции США, включая ее знаменитое начало («Мы исходим из той самоочевидной истины, что все люди созданы равными»), не возникли в одночасье, а вырабатывались поколениями. За сто с лишним лет до Американской революции, в 1647 году, английские левеллеры — группа религиозно-политических диссидентов — ратовали за так называемое Народное соглашение. Оно содержало призывы к религиозной терпимости, всеобщему избирательному праву и равенству всех граждан перед законом. Впрочем, задолго до левеллеров те же принципы провозглашали древние римляне. В «законах XII таблиц», принятых около 450 года до н. э., прописано равенство правящего класса и рядовых граждан в глазах правосудия. Конечно, древнеримскому законоуложению, согласно которому женщины находились в подчинении у мужчин, а смертной казнью каралось большинство преступлений, было далеко до современных идеалов. Однако и здесь уже очевидно стремление выработать единый свод правил, скрепляющих гражданское общество. Биткоин с его новой моделью децентрализованного управления цифровой экономикой тоже не возник на пустом месте. Некоторые элементы этой модели, например криптография, зародились тысячи лет назад. Другие — скажем, идея электронных денег — насчитывают уже десятилетия. И, как видно хотя бы из дебатов по поводу размера блоков, Биткоин еще находится в стадии становления. Оптимальную конфигурацию составных частей, которая позволит миру применить эту новую технологию, еще только предстоит найти.

По мере развития и взросления технологии блокчейн нам все чаще приходится обращаться к истории важных политических решений. Конституция США, которая функционирует более 200 лет, вполне подходит на роль образца, ведь отцам-основателям нации доводилось улаживать примерно такие же политико-экономические конфликты, как и те, что сейчас сотрясают Биткоин и Эфириум. Однако следует отметить, что актуальность главных документов западной демократии — включая Конституцию США — постоянно оказывается под вопросом в переменчивом мире, опутанном сетью цифровых коммуникаций.

Глобализация, авиасообщение и всеобщая компьютеризация размывают границы, внутри которых правительства могут осуществлять полномочия, предоставленные им прежде веским общественным договором. Бессилие властей породило ощущение утраченного суверенитета и страх вмешательства внешних сил, что сейчас нередко проявляется в политике ксенофобии и протекционизма. Деятели вроде Дональда Трампа пытаются воскресить былую силу национализма, сворачивая соглашения о свободной торговле, используя риторику доморощенного капитализма, выдворяя мигрантов и подпитывая межэтнические конфликты.

Тем не менее профессиональный анализ экономических, технологических и демократических тенденций недвусмысленно показывает, что остановить перемены такими действиями невозможно. В конце концов, любая компания может просто перебраться в офшоры с более благоприятным законодательным климатом. Единственное, что национализм может сделать с ходом технологической революции, — это гарантировать максимально несправедливое распределение прибылей и убытков от грядущих перемен. Общее недовольство, приведшее к власти Дональда Трампа, требует совершенно иного подхода. И мы полагаем, что для начала следовало бы понять, как приспособить законы и правила, которые сейчас регулируют экономический обмен, к децентрализующим силам, порожденным новыми информационными технологиями.

Это не означает, что привычные формы управления вот-вот отомрут — скорее, наоборот. Уже сейчас, когда новые онлайн-технологии позволяют международным сообществам функционировать без надзора традиционных локальных правительств, они же дают

и правительствам новые инструменты для усиления власти. Биткоин и прочие системы, управляемые алгоритмом распределенного консенсуса, создавались именно с целью избежать центральной «точки контроля» и не сосредоточивать всю власть в руках одной инстанции. Однако другие системы далеко не столь демократичны. Информация, обнародованная Сноуденом, ясно показала, что спецслужбы и правительственные структуры США весьма охотно используют новые устройства, которые сохраняют и накапливают наши цифровые следы, чтобы вторгнуться в частную жизнь граждан. Однако правительства — по крайней мере, на данном этапе — могут сыграть и ключевую роль в защите нашего личного пространства. Например, недавно принятый в Европе «Общий регламент по защите данных» опирается на принципы индивидуальной свободы. Американцам же, увы, приходится на горьком опыте узнавать, что бывает, когда правительство пренебрегает этими принципами. В 2017 году Конгресс отменил установленные администрацией Обамы правила, согласно которым провайдеры онлайн-сервисов не имели права разглашать или продавать данные пользователей без их ведома и согласия.

Полномочия государства небезграничны, да и не должны таковыми быть, но оно не может и не должно оставаться в стороне, пока всемогущие корпорации диктуют, как применять новые технологии. Уж точно это недопустимо в ситуации, когда ежедневно сокращаются рабочие места, а социально-политическое напряжение растет. Нам необходима система, которая позволит справедливо разделить блага, генерируемые техническим прогрессом. Разумеется, мы не призываем вновь обратиться к коммунистической утопии; тем не менее нужно гарантировать, что те, у кого сейчас есть доступ к новым технологиям, не станут эксплуатировать остальных и что новаторские идеи получат максимально широкое распространение.

Наше будущее во многом зависит от трех главных «центров силы»: технологической отрасли, финансового мира и правительственных структур. На карте Америки им условно соответствуют Кремниевая долина, Нью-Йорк и Вашингтон, однако сама триада во всем мире примерно одинакова. Более того, по нашим ощущениям, каждый из этих центров силы стремится подчинить будущее собственным интересам. Банкиры не слишком разбираются в высоких технологиях, инженеры

не рвутся изучать экономику, а политические деятели заняты исключительно политикой. Если мы действительно хотим поставить новые технологии на службу человечеству, предстоит разрушить немало барьеров, причем речь идет не о привычном разделении на правых и левых, консерваторов и либералов и даже не о культурной границе между Западом и Востоком. Нет, мы говорим о пропасти между централизованными и децентрализованными системами. Необходимо понять, как лучше всего использовать вторую, чтобы исправить недочеты и перекосы первой. А для этого понадобится как можно больше специалистов, которые одновременно разбираются хотя бы в азах технологии, экономики и политики. По правде говоря, не помешала бы и паратройка философов.

Хотя основная задача книги — рассказать о возможностях, которые предоставляет Биткоин и прочие ответвления технологии блокчейн, мы первыми готовы признать, что на данный момент они дают мало готовых ответов. Пока история самого Биткоина — это опыт накопления средств первыми пользователями и небольшой группой из трех или четырех майнинговых пулов, которые захватили львиную долю вычислительных мощностей сети. Прежде чем пропускная способность Биткоина, Эфириума и других блокчейн-систем позволит достичь идеала децентрализации, предстоит проделать огромную работу. Но, как мы старались подчеркнуть, основной вклад Биткоина и технологии блокчейн в дискуссию об управлении интернет-средой состоит в том, что они заставили нас по-другому взглянуть на проблемы общества. Биткоин и блокчейн помогли наметить новый подход к их решению. Главное — это та волна инноваций, которая в наши дни благодаря концепту блокчейна захватила не только программистов и предпринимателей, но и политологов и экономистов. Что касается всех остальных, то необходима социальная и политическая атмосфера, в которой свободный творческий поиск может породить открытые, общедоступные системы. В любом случае, независимо от того, какая платформа или система ПО окажется самой жизнеспособной, наша общая социальная задача должна заключаться в децентрализации доверительных отношений и сокращении роли посредников. Учитывая, сколько творческой энергии и фантазии сейчас вкладывается в разработку этих идей, пожалуй, не так уж наивно ожидать от них радикального обновления мира.

Конечно, децентрализация не ответ на все вопросы. Она должна быть не самоцелью, а скорее средством достижения других целей — равенства возможностей, широкой инклюзии, общего процветания и т. п. В тех сферах, где децентрализация действительно помогает приблизиться к идеалу, ее нужно всячески поощрять. Но во многих случаях — особенно там, где организации-посреднику можно доверять, — централизованная структура окажется намного эффективнее при обработке информации.

Предприниматели, изучающие новые технологии, часто задают вопрос: «А мне для работы нужен блокчейн?» Наш ответ таков: «Если централизованный механизм доверия в вашей сфере обходится дороже, чем установка компьютеров и внедрение децентрализованной структуры, то да. Если нет, блокчейн вам ни к чему». Поскольку для подтверждения транзакций в блокчейн-реестре сообщество должно затратить серьезные ресурсы, такая система учета имеет смысл там, где высокая степень взаимного недоверия ведет к непомерно большим расходам при исполнении контрактов. (Эти расходы могут принимать разные формы: выплата комиссий посредникам, задержки при проведении платежей и зачислении средств или невозможность полноценно осуществить некоторые рабочие процессы, скажем, распространить информацию в цепи поставок.) В случае, когда банк отказывает в ипотеке законопослушному и платежеспособному собственнику жилья или же дает заем только под заоблачные проценты, потому что не доверяет информации кредитных бюро, можно утверждать, что цена доверия чересчур высока и блокчейн-реестр будет удачным решением проблемы.

Что касается децентрализации целых отраслей, то здесь нужно задаться вопросом: изменит ли это расстановку сил, уравняет ли возможности игроков? Может быть, нынешняя централизованная структура налагает непомерную дань на участников и не позволяет инноваторам претворять в жизнь ценные идеи? Вспомним об антимонопольном законе, подписанном Теодором Рузвельтом в начале XX века, согласно которому национальные интересы США требуют, чтобы правительство обеспечивало честную конкуренцию на рынке. Мы до сих пор придерживаемся этого принципа, однако проблема в том, что определение монополии, выработанное в индустриальную

эпоху, плохо применимо к миру программных продуктов и информационных сетей, где потребительская ценность напрямую зависит от масштаба сети, а расплачивается потребитель не долларами, а ценными личными данными. Ведущие игроки, которые уверяют, что улучшенные версии продукта и «бесплатные» сервисы появляются в результате их заботы о клиентах, скрывают хищническую природу своих бизнес-моделей. В действительности же они используют тайные алгоритмы и престиж крупных, «раскрученных» сетей, чтобы ограничить конкурентам свободу маневра и обезопасить свое господствующее положение на рынке.

Все это, похоже, ускользает от внимания антимонопольных регуляторов вроде Федеральной торговой комиссии США, чьи устаревшие стандарты честной конкуренции не позволяют заметить, как централизованные инстанции злоупотребляют властью в эпоху интернета. Иными словами, нынешние борцы с монополиями не осознают, что мы не потребители Facebook, а его товар. В эпоху, когда каждый из нас творец и предлагает себя как «бренд», необходим новый манифест гражданских прав на рынке информации. Децентрализация должна быть его частью. И принципы, на которых основана технология блокчейн, могли бы стать неплохой отправной точкой.

Каждая централизованная система должна быть открыта для переоценки, даже правительства и политический процесс. Такие стартапы, как Procivis, уже работают над системами онлайн-голосования, которые возложат задачу подсчета голосов на механизмы на основе блокчейна. Некоторые правительства готовы взять эту идею на вооружение. Лидирует Эстония: в стране уже опробована программа для голосования акционеров, созданная на базе блокчейн-сервиса биржи Nasdaq. Есть надежда, что блокчейн предотвратит двойной учет голосов, так же как предотвращает двойное расходование биткоинов, и позволит гражданам изъявлять свою волю с помощью смартфонов. Это бы устранило дискриминацию тех, кто не может попасть на избирательный участок в установленное время, а главное — создало бы более прозрачную электоральную систему, открытую для независимого аудита и вызывающую доверие граждан.

А как насчет функций самого правительства? Не нужно ли избавить его от посреднических операций? В некоторых случаях да. Мы уже говорили о том, как можно регистрировать право собственности

на жилье в неизменяемом блокчейн-реестре. Некоторые криптолибертарианцы задаются и более высокой целью — заменить устаревшую и неудачную с их точки зрения модель национального правительства. К примеру, стартап BitNation предлагает идею «мирового гражданства», а также «посольств», «наций» и «союзников» для онлайн-сообществ с новыми принципами самоуправления. На сайте компании сказано: «Блокчейн Биткоина позволяет нам самим выбирать форму правления, наиболее соответствующую нашему образу жизни: одноранговую, более локальную и в то же время более глобальную» [1]. Наивно полагать, что такие идеи получат широкий отклик в обозримом будущем. Во-первых, они игнорируют важнейшую роль национального законодательства, которую оно традиционно играет в нашем представлении о справедливости. Закон — весьма сложное понятие, укоренившееся в нашем коллективном сознании благодаря тысячелетиям человеческой эволюции. Большинство людей не разделяют утверждения «код есть закон» и не захотят отказаться от богатого элемента нашей культурной ткани ради непонятного им программного продукта. Безусловно, некоторые составляющие государственной власти действительно отмирают в эпоху цифровой глобальной экономики. Однако время формального роспуска национальных правительств пока не пришло. В любом случае у нас и без того хватает важных задач!

Редецентрализация сети

Первая задача, которую мы должны немедленно решить, — восстановить здоровый баланс сил в интернете. На наших глазах предпринимаются многочисленные попытки «редецентрализовать» Всемирную паутину, то есть изменить иерархические принципы хранения файлов и обмена информацией так, чтобы создателям сайтов было легче контролировать, что и где публикуется. Эта тенденция подается как возвращение к изначальной идее сети как открытого форума, где каждый может свободно высказываться и где нет места централизованным контролерам и хозяевам вроде Google и Facebook. «Если мы не избавимся от их диктата и не добьемся полной совместимости всех интернет-платформ, — говорят сторонники движения, — нам никогда

не приблизиться к идеалу открытых данных и не получить богатой аналитической информации о жизни нашей планеты, которая была бы доступна в свободном цифровом пространстве».

В достижение этой цели вкладывается немало интеллектуальных и научных ресурсов. Предлагается несколько решений на основе блокчейна, которые должны, к примеру, избавить от посредников индустрию аутсорсингового хранения и вычисления. Это позволило бы сократить неоправданные издержки и ущерб для окружающей среды, с которыми сопряжена работа корпоративных дата-центров. Такие новые платформы, как Storj, Sia и Maidsafe, вознаградят вас токенами за предоставление места на жестком диске другим пользователям общей глобальной сети. Можно сказать, что эти сервисы гораздо ближе к изначальной идее «облака», чем предоставляемые Amazon, Google, Dropbox, IBM, Oracle, Microsoft и Apple — провайдерами, с которыми у большинства людей ассоциируется название этой технологии.

Однако обсуждаются и более радикальные перемены, в том числе и полная смена архитектуры сети. Разработан, к примеру, новый протокол для хранения данных Solid (или Social Linked Data), возвращающий пользователю контроль над своей информацией путем помещения данных в персональные онлайн-хранилища (Pods) и их распространения с помощью приложений, доступ к которым определяем мы, пользователи. Solid — детище Тима Бернерса-Ли, того самого кибернетика, который усовершенствовал протокол HTTP и подарил нам интернет. Бурный энтузиазм вызывает и система IFS, разработанная Хуаном Бенетом. Ее устройство напоминает популярную систему файлообмена BitTorrent, которую так и не удалось закрыть в рамках борьбы с пиратством. IFS тоже распределяет файлы по сети независимых компьютеров, чтобы они не лежали на одном сервере, а были словно разбросаны то тут, то там на жестких дисках обычных пользователей с многочисленными копиями в качестве бекапа. Таким образом веб-хостинг превращается в коллективный процесс обмена ресурсами в интернете.

Еще более радикальные решения предлагает группа ECSA — Economic Space Agency, или «Агентство экономического пространства». Ее проекты в значительной степени вдохновлены криптотокенами, системами распределенного доверия и смарт-контрактами,

однако данный подход к децентрализации экономики и расширению прав и возможностей индивида заметно отличается от программ Биткоина и Эфириума. Вместо того чтобы проводить каждую транзакцию или инструкцию смарт-контракта через всю сеть единого блокчейна, ECSA подходит к децентрализации с другого конца. Группа разработала набор программных инструментов под названием Gravity, взяв за основу давний проект шифропанка Марка Миллера. Gravity позволяет компьютерам в локальной сети безопасно работать с общими смарт-контрактами. Кроме того, по мнению разработчиков ECSA, у сообщества должна быть возможность автономно выбирать собственную модель управления. Главная цель, к которой стремится пестрая команда из технологов, экономистов, политологов и антропологов, — предоставить пользователям возможность строить новые «экономические пространства», где их сообщества сами смогут выпускать и распределять криптотокены, вознаграждая сотрудничество и взаимопомощь. В отличие от Эфириума, их транзакции не нужно будет подтверждать в мощной глобальной блокчейн-сети. Тем не менее, обеспечивая торговлю и взаимодействие между отдельными группами без вмешательства доверенной третьей стороны, протокол Gravity в дальнейшем должен способствовать строительству децентрализованной глобальной экономики, начиная с низов.

Если проект окажется успешным, метод ECSA может не только помочь в решении извечных проблем Биткоина и Эфириума — малой пропускной способности, чрезмерного потребления мощностей и административных сложностей, но и избавить нас от куда более серьезной опасности — риска стать «рабами алгоритма», о чем предупреждает Люсиан Тарновски, основатель открытой образовательно-поисковой платформы Brave New. Сосредоточившись на монолитных решениях вроде Биткоина и Эфириума, мы можем подвергнуться диктату их программного кода и, соответственно, узкой группы разработчиков, которые будут этот код писать. Конечно, использование открытых лицензий для большинства блокчейн-моделей должно расширить круг идей, которые лягут в их основу. Но на практике правила кода могут стать довольно-таки жесткими, а возможность изменить их будет только у небольшой группы узких специалистов.

Впрочем, здесь нужно сделать все ту же оговорку: все эти решения находятся на стадии эксперимента и сейчас невозможно предсказать,

какие из них сработают. Что касается денег, вливающихся в эти проекты с помощью ICO и других инструментов фандрайзинга, то, скорее всего, бóльшая их часть будет израсходована на пробы и поиски. Однако мы хотели бы еще раз подчеркнуть, что сам факт реализации этих проектов в одно и то же время, на общей площадке, в условиях практически свободного обмена идеями и данными многократно повышает шансы на успех. Нельзя рассматривать каждую концепцию по отдельности. Все они результат бурного инновационного движения, в которое вовлечены лучшие умы технического мира. «Коллективный разум» запускает плодотворный цикл творческих поисков и научного прогресса. Сложно предсказать, к чему мы в итоге придем, — точно так же создатели интернета представить себе не могли, что на основе их изобретения возникнет потоковое вещание, IP-телефония и электронная коммерция, — но уже сейчас с уверенностью можно заявить, что интернет и вся связанная с ним экономика через несколько лет заметно изменятся и станут гораздо менее централизованными.

Зеленый свет в коридорах власти

В ходе президентской кампании 2016 года Хиллари Клинтон изрядно озадачила избирателей, когда объявила о поддержке «блокчейн-платформ общественного значения». Клинтон произнесла эти слова с подачи Брайана Форда, советника президента Обамы по вопросам высоких технологий и бывшего директора инициативы по цифровым валютам медиалаборатории Массачусетского технологического института, который в декабре 2017 года решил баллотироваться в Конгресс. Впоследствии Форд описывал попытки убедить команду Клинтон в пользе блокчейна как «непростые» [2]. И хотя Клинтон и постаралась сделать акцент на потенциальной пользе технологии блокчейн для общества (а не на необходимости ее жестко регулировать), стоит отметить, что больше слово «блокчейн» в ее предвыборной агитации ни разу не звучало.

И все же в некоторых коридорах власти понемногу загораются зеленые огоньки. Мы уже упоминали об исследованиях, проводимых десятками центробанков. То и дело приходится слышать о пилотных

проектах и запуске блокчейн-приложений от правительственных структур, причем не только в крупнейших экономиках мира — США, ЕС, Китае и Японии, но и в таких разных странах, как ОАЭ, Грузия, Швеция, Эстония, Мексика, Сингапур и Люксембург. В Японии, например, Агентство финансовых услуг классифицировало биткоин и другие цифровые валюты как платежные системы, предъявив биткоин-биржам ряд требований по борьбе с отмыванием нелегальных средств. Тем самым агентство фактически кодифицировало криптовалюты, придав им официальный статус на традиционном рынке капитала. Эффект не заставил себя долго ждать: торговля биткоином в Японии возросла в разы, что в значительной степени обусловило резкое подорожание валюты в 2017 году, а многочисленные японские компании начали использовать и принимать биткоин. Тем временем блокчейн-стартап Neocapita начал работу в Папуа — Новой Гвинее и Афганистане, занося расходы правительственных структур в распределенный реестр, чтобы повысить прозрачность, восстановить доверие иностранных спонсоров и разблокировать замороженные благотворительные средства [3]. На международном уровне технологию блокчейн изучают МВФ и Всемирный банк. К ней с большим интересом относится Межамериканский банк развития, а ООН, под чьей эгидой сейчас работает команда блокчейн-разработчиков, как мы уже упоминали, провела конференцию по вопросам суверенной идентичности.

Даже на Капитолийском холме наблюдается некоторая активность законодателей [4]. В феврале 2017 года двое конгрессменов — демократ Джаред Полис и республиканец Дэвид Швайкерт — объявили о созыве «совещания по вопросам блокчейна», на котором предстояло выработать «осмысленную единую политику по отношению к технологии блокчейн и криптовалютам». На уровне отдельных штатов тоже происходят заметные подвижки. Власти штата Делавэр работают с компанией Symbiont над переводом корпоративного реестра и системы управления сертификатами на акции на блокчейн-платформу [5]. В марте 2017 года администрация штата Иллинойс объявила о сотрудничестве с лабораториями R3 и запуске проекта, который должен объединить ряд официальных структур с помощью блокчейн-реестра [6].

Учитывая такой всплеск активности, неудивительно, что новые идеи относительно регуляторных технологий возникают едва

ли не каждый день. Блокчейн — лишь одно из подмножества, однако уже сейчас международные правоохранительные органы вроде Europol прибегают к услугам блокчейн-аналитиков (например, компании Chainanalysis), чтобы разметить мировые финансовые потоки [7]. А в таких странах, как Эстония, которая фактически превратилась в лабораторию гражданских технологий, правительство понемногу свыкается с мыслью об использовании блокчейна как платформы для нотариальных услуг, благодаря которой официальные документы станут намного доступнее для любых служб. Вскоре все виды правительственной документации будут перенесены в неизменяемые реестры. А чем больше у граждан появится возможностей самостоятельно контролировать эти данные вместо их отправки в закрытые изолированные хранилища, против которых не раз высказывался Тим Бернерс-Ли, тем быстрее мы приблизимся к великим вычислительным мощностям столь заманчивого века открытых данных.

Увы, несмотря на отдельные инициативы, общую готовность регуляторов к переменам можно считать нулевой. И одна из проблем состоит в том, что, прежде чем учить юристов и регуляторов разбираться в блокчейнах, им нужно объяснить все процессы, которые протекают в цифровом мире, то есть тот сдвиг, который вот-вот произойдет в экономике благодаря искусственному интеллекту, 3D-печати, «интернету вещей» и сетевой аналитике. На одной из конференций в Вашингтоне два года назад сенатор Кори Брукнер сказал: «Невозможно сформулировать позицию демократов или республиканцев по вопросам высоких технологий, потому что ни у тех ни у других никакой позиции нет».

Именно поэтому нам приходится сталкиваться с совершенно неадекватными правилами. Борьба с отмыванием денег и требование «знать своего клиента» налагают массу ограничений на международные транзакции, например на перевод денег мигрантами. Уже появились надежные инструменты цифровой идентичности, которые в сочетании с блокчейн-анализом могли бы помочь малообеспеченным гражданам делиться средствами, а регуляторам — отслеживать нелегальные денежные потоки. Тем не менее инспекторы финансового надзора G20 упорно настаивают на том, что единственный способ борьбы с отмыванием денег и терроризмом — дальнейшее ужесточение правил традиционной, «бумажной» идентификации. Отсутствие решений

заставляет финансовых посредников отказывать все большему числу клиентов, в результате население беднейших стран теряет источники дохода, что, в свою очередь, создает весьма комфортную среду для террористов и вынуждает жителей прибегать к услугам подпольных синдикатов. По словам Хуана Льяноса, эксперта по техусловиям платежных систем, «наши регуляторы не готовы даже к цифровому веку, не говоря уже о веке блокчейна».

Однако, как мы с вами убедились, блокчейн-продукты разрабатываются повсеместно — с правительственной поддержкой и без. Перемены все же грядут. И нам необходимо подготовить к ним законодательную и регуляторную базу. Кстати, это не означает, что непременно нужны новые правила. Стремление регулировать все и вся, пожалуй, самый верный способ задушить инновации. Скорее, здесь нужна хорошо продуманная, понятная и логичная стратегия, даже если она пока сводится к выжидательной позиции.

Вот одна из причин: технология блокчейн, как и многие другие цифровые идеи, по своей природе глобальна. Это означает, что использующие ее стартапы будут перебираться в страны с самым дружественным законодательством. Уже сейчас в швейцарском местечке Цуг появилась своя «Криптодолина», которую облюбовали разработчики Эфириума и компании, специализирующиеся на смарт-контрактах, криптовалютах и блокчейн-платформах. Место выбрано неслучайно, поскольку швейцарское законодательство упрощает процедуры, которые необходимы для проведения ICO и выпуска цифровых токенов. Британское управление по финансовому регулированию и надзору тоже предлагает стратегию, в рамках которой стартапы с относительной легкостью могут разрабатывать и тестировать новые экономические инструменты, что весьма по душе инноваторам со всего мира [8]. Польза для британской экономики тоже налицо: после Brexit Лондону нужно сохранить за собой статус крупнейшего финансового центра и не проиграть Нью-Йорку, а также европейским «центрам силы». Под руководством предыдущего премьер-министра Дэвида Кэмерона правительство Соединенного Королевства даже выделило 10 миллионов фунтов на исследования в области криптовалютных технологий. Остается вопрос: что должно произойти, чтобы законодатели США начали беспокоиться о том, чтобы финансовые и технологические центры страны не проиграли конкурентную борьбу иностранцам?

Программы «без доверия» и сообщества доверия

Доверие — неотъемлемая часть любой транзакции, в том числе и в биткоинах. Пересылая друг другу биткоины, мы должны быть уверены, что взамен получим обещанные товары или услуги. Кроме того, мы должны быть уверены, что компьютер или смартфон, с помощью которого мы отправляем средства, а также Wi-Fi-сеть и оборудование интернет-провайдера работают должным образом и не взломаны злоумышленниками.

Мы не случайно возвращаемся к этой теме. Ведь для создания полностью интегрированной системы распределенных реестров и блокчейнов для очень сложно устроенной глобальной экономики необходимо понимание того, как поставить децентрализованные реестры на службу доверенным лицам или структурам, вовлеченным в наши транзакции. Чтобы принять правильное решение, нужно прежде всего выяснить, каким образом доверие определяет нашу сущность и формирует отношения взаимной поддержки, лежащие в основе любого сообщества.

Возьмем для примера французскую Депозитно-ссудную кассу (Caisse des Dépôts et Consignations). История этого учреждения насчитывает более двухсот лет. Эта государственная организация с почти неограниченными полномочиями функционирует под контролем парламента, а не как агент исполнительной власти. Депозитно-ссудная касса играет ключевую роль в координации инвестиций в государственные проекты. Она же регистрирует права собственности на недвижимость, инвестирует в государственную инфраструктуру, занимается социальными накоплениями и пенсионными планами, при этом она же гарантирует финансовую поддержку судебной системы и правоохранительных органов, а также государственных университетов и научно-исследовательских проектов, причем вне зависимости от политических факторов. Если бы такая структура работала в менее здоровом политическом климате, она могла бы стать рассадником коррупции и мощным инструментом давления, утратив всякое доверие народа. Но для французов большая честь работать в Депозитно-ссудной кассе. И эта культура социального престижа порождает глубочайшее доверие граждан.

Отсюда вопрос: даже если Депозитно-ссудную кассу можно заменить алгоритмом, который создает систему распределенного доверия, стоит ли это делать? А вдруг это уничтожит давнюю социокультурную традицию, благодаря которой возникают подобные институты?

Многие структуры, которым западное общество поручает операции обмена и взаимодействия — будь то правительственные учреждения и суды или частные организации вроде нотариальных контор и управляющих компаний, — тоже возникли в результате многовековой работы по формированию гражданского общества, и их функционирование зависит не только от законодательных и управленческих систем, которые мы создали для надзора за ними, но и от ряда культурных норм. Благодаря этим нормам мы охотно доверяемся уполномоченным посредникам, а они, в свою очередь, обязуются оправдать наше доверие. Здесь проявляется то же чувство гражданской ответственности, которое побуждает нас ждать своей очереди, придерживать дверь перед идущим сзади или просто говорить «спасибо» и «пожалуйста». Институционализированное доверие — своего рода общественная добродетель, вид социального капитала, запасы которого в мире не так уж велики. Так нужно ли избавляться от него там, где оно есть? Когда доверие заслуживается и культивируется веками, его ценность для общества намного выше, чем практическая ценность отдельно взятого учреждения.

Среди любителей криптографии популярна поговорка «Не доверяй, а проверяй». Это мудрый совет для тех, кто отвечает за безопасность важных транзакций в вычислительной системе, подверженной риску кибератак. И правильный подход в случае, когда нужно позаботиться о сохранности своих денег, особенно при сделке с незнакомцем. Но если взглянуть шире, этот постулат принижает ценность ключевого элемента, скрепляющего человеческое общество. Мы не зря привыкли воспринимать доверие как нечто положительное, поэтому неудивительно, что изначальное описание Биткоина как системы «без доверия» не понравилось никому, кроме ярых адептов криптографии. Нам стоило бы рассматривать архитектуру распределенного доверия, которую предлагает блокчейн, как способ скрепить узы доверия в обществе, а не подменить их собой.

Если хотите, доверие играет роль «социального клея». Благодаря ему мы можем вступать в отношения обмена, ежедневно заключать и выполнять небольшие договоренности, не имеющие никакой

юридической силы, но все же налагающие на нас некие обязательства. Например, соблюдать очередь перед билетной кассой; подносить билет к валидатору, когда заходим в автобус; твердо рассчитывать, что автобус и его водитель доставят нас в нужное место в обозримый промежуток времени и что пассажиры на остановке дадут нам спокойно выйти из автобуса, а не кинутся тут же его штурмовать. Культурные, социологические и психологические факторы, которые позволили нам создать все эти узы доверия, должны рассматриваться как жизненно важные компоненты любой системы децентрализованного управления, какую мы решим построить для бурно развивающегося цифрового общества. Они помогут образовать соединительную ткань между пространством сетевых, автоматизированных транзакций и миром человеческого взаимодействия, в котором мы живем.

Одна из главных причин, по которой необходимо встроить человеческий элемент в новые системы, связана с уже упомянутым «больным местом» ранних блокчейнов — низкой пропускной способностью. В своем нынешнем виде Биткоин и Эфириум сложны в управлении и обходятся довольно-таки дорого, поскольку все компьютеры должны участвовать в каждой вычислительной операции, совместно подтверждать одну и ту же транзакцию, перевод активов, смарт-контракт. Несмотря на то что алгоритмы консенсуса, механизмы поощрения и различные протоколы придают каждой системе свои технические плюсы и минусы, Биткоин и Эфириум, как и большинство открытых общедоступных блокчейнов, по мере роста пожирают все больше вычислительных мощностей и энергии.

Опять же, хорошая новость в том, что в решение этих проблем вкладываются очень серьезные финансовые и интеллектуальные ресурсы. Вспомним идеи, которые мы с вами обсуждали: протокол Lightning Network добавляет к системе Биткоина новый уровень платежных каналов, которые помогут облегчить транзакции; EOS — открытый блокчейн, который, по утверждению стартапа block.one, сможет обрабатывать миллионы транзакций в секунду; Tezos предлагает новые способы управления, чтобы выстроить более гибкую и демократичную систему оптимизации протоколов; наконец, Zcash и Monero стремятся решить проблемы конфиденциальности. Также стоит отметить проект Джеймса Лавджоя Cryptokernel и приложение K320, которое может со временем избавить Биткоин от двух напастей — накопления валюты пользователями

и технического диктата мощных интегральных схем для майнинга (ASIC). Добавьте к этому проект Algorand — новое и весьма интересное предложение от команды Массачусетского технологического института, куда входит и лауреат премии Тьюринга профессор Сильвио Микали, представляющее собой комплексное блокчейн-решение, которое может исправить несколько недочетов сразу [9]. Если представить, что хотя бы один из этих проектов однажды превзойдет пропускную способность Биткоина и Эфириума и как минимум сравняется с Биткоином по уровню безопасности (или же что два крупнейших блокчейна возьмут на вооружение ряд этих находок), то весь поисковый процесс начинает внушать большие надежды. Вместе взятые, эти новинки существенно повышают вероятность того, что глобальная цифровая экономика будет управляться архитектурой распределенного доверия — открытой, общедоступной, динамичной, но при этом более маневренной, надежной и безопасной для окружающей среды.

Однако чтобы достичь этого идеала, крайне необходимы новые технические таланты. Сложность задачи и потребность в надежных механизмах киберзащиты на глобальном уровне означают, что сегодня над блокчейн-системами чаще всего работают узкопрофильные специалисты. Без их работы — поддержки, обновления и исправления базовых программных протоколов — не сможет функционировать ни одна блокчейн-среда. В своем нынешнем виде блокчейны объединяют в себе самые разнородные черты и элементы — от криптографии до алгоритмов консенсуса, а также сложные инструменты защиты. Все это делает их громоздкими, запутанными и трудоемкими. Работать с ними может лишь программист определенной направленности.

Такие сервисы, как EOS, предназначены для создания более удобных пользовательских инструментов, чтобы каждая организация могла выстроить собственную блокчейн-систему. Это отчасти сняло бы проблему кадрового голода. Тем не менее, если мы хотим, чтобы общество решало, как будет развиваться новая система экономического управления, нужно существенно расширить круг разработчиков. Более того, таланты необходимо искать повсюду, стремясь к гендерному, этническому и культурному разнообразию. Только тогда ценности и установки, которые неизбежно просачиваются в программный код, будут отображать запросы всего общества, а не одной его узкой прослойки. Отсюда вывод: необходимо вкладываться в общедоступное техническое образование.

Гражданин поднимает голову

За процессом децентрализации кроется нечто более фундаментальное, чем мечта о финансовой стабильности. Это «нечто» связано с принципом гражданских свобод. Мы уже не раз говорили о том, как разные группы граждан могут впервые в истории осуществить право на свободу торговли, самовыражения, творческой мысли и в то же время получить в свое распоряжение собственность, которая по праву должна им принадлежать. В наши дни само понятие гражданства, определяемое этими фундаментальными правами, неразрывно связано с вопросом контроля над информацией. Границы нашей свободы зависят от того, кто и как ею распоряжается, устанавливает параметры доступа к ней и т. п. Вот почему идея сверхнадежной машины правды, которую никто не может взломать, выглядит столь заманчиво.

Это не только наше мнение. Вот что сказано в отчете британской правительственной комиссии по науке за январь 2016 года, посвященном технологии блокчейн: «Эта технология, вероятно, смогла бы привнести новый тип доверительных отношений в самый широкий спектр услуг». Во вступлении к отчету члены британского парламента Мэтью Хэнкок и Эд Вейзи утверждают: «Мы уже видели, как системы открытых данных произвели переворот в отношениях граждан с государством. Точно так же прозрачность новой технологии может преобразить финансовые рынки, цепи поставок, потребительские и деловые услуги, а также государственные реестры» [10]. Далее в разделе, озаглавленном «Применение в сфере госуправления», профессор лондонского Imperial College Кэтрин Маллиган пишет: «Итоговое влияние [технологий цифрового реестра] на британское общество может быть сопоставимо с принятием Великой хартии вольностей». Именно так. Великой хартии вольностей.

Почему же этот способ ведения учета столь важен с точки зрения прав и свобод? Как мы уже говорили, блокчейн может дать человечеству систему, позволяющую вести непрерывную хронологическую запись. Кроме того, она могла бы покончить с тысячелетней моделью общественного устройства, в которой власть проистекает из контроля над информацией. Для американцев это сейчас особенно важно, если учесть, что в Белом доме сидит президент, который полагает, что лишь он имеет право решать, где «фейковая новость», а где «альтернативный

факт» [11]. В этом контексте сама возможность создать машину правды — будь то на основе блокчейна или протокола Gravity — вызывает бурный энтузиазм. Есть что-то весьма вдохновляющее в том, чтобы позволить независимому индивиду вносить данные в коллективно заверяемый архив, не спрашивая ничьего дозволения. Допустим, вы создали нечто ценное, например популярное произведение цифрового искусства или идею, которая может лечь в основу прибыльного начинания. Вам будет намного легче добиться успеха, если вы сможете заявить о праве собственности, не прибегая к услугам регистратора брендов или другой официальной инстанции. Особенно это касается граждан тех стран, где подобные инстанции должным образом не работают, а то и вовсе отсутствуют. Если добавить тот факт, что такую запись невозможно уничтожить, перед нами открываются поистине безграничные возможности. Постоянство информации — залог демократии.

Я здесь был. Я человек

Если вы сомневаетесь, что нечто столь утилитарное, как реестр, составленный из буквенно-цифровых кодов, поможет сохранить нашу человеческую сущность со всеми ее парадоксами, безумием и очарованием, приглашаем вас рассмотреть малоизвестный аспект системы Биткоин — феномен блок-граффити. Пользователи Биткоина нередко добавляют к переведенным монетам сообщение, следуя традиции, которая восходит к самой первой транзакции, когда Сатоши Накамото взял заголовок из газеты Times за тот день — 3 января 2009 года — и ввел его в поле данных. С тех пор пользователи рассматривают блокчейн-реестр как неизменяемый, хронологически размеченный дневник, куда можно записать сведения, которые они по тем или иным причинам хотели бы сохранить на долгое время.

Рассмотрев биткоин-граффити, которые за несколько месяцев накопились на сайте CryptoGraffiti.info, мы обнаружили удивительно разнообразные послания. Среди них было множество любовных записок, например вот эта, от 20 марта 2017 года, которая пришла с адреса 1GRtrEG KPwXJTqS3jp8JbZDkLNpZjagCCb (она обошлась автору в 0,00055039 BTC, то есть 0,57 доллара по тогдашнему курсу) и запечатлелась в блоке #458160:

Моя любовь ко всем созданиям этого мира безгранична. Моя любовь к одному созданию выходит за пределы этого мира. Яна Седлачкова, ты для меня все. Петр.

Кроме того, на сайте CryptoGraffiti.info, если не в самом блокчейне, можно просмотреть фотографии, включая знаменитый снимок 1989 года, запечатлевший человека, застывшего перед танком на площади Тяньаньмэнь. Фотография также была выложена на сайт в марте 2017 года и предварена текстовым сообщением — сначала на китайском, а потом на английском языке — с призывом к китайскому президенту Си Цзиньпиню «рассказать правду о площади Тяньаньмэнь» к грядущей годовщине событий. Обнаружилось одно фото молодой пары с любовным стихотворением на испанском языке. Нашлась и такая надпись: «Светлой памяти Жоржа Френонта (16.01.1946 — 19.02.2017). Ты был прекрасным мужем, отцом и другом. Мы будем очень скучать по тебе».

Прокручивая ленту сайта с транзакциями, мы читали надписи на разных языках с выражением самых разных чувств и пожеланий вперемешку с объявлениями о продаже авто, курсе акций, сообщениями о протестах против строительства нефтепровода в городке Стэндинг-Рок, прощальной запиской некоему Тобиасу от коллектива «Блокчейн в Беркли», конспирологическими заметками и, что неудивительно, комментариями о путешествиях во времени. Затем мы добрались до октября 2016 года, когда правительственная армия Сирии осаждала Алеппо, — спустя год после того, как наша знакомая Наджа Салех аль-Меймед, с которой вы встречались во вступлении к книге, бежала в Иорданию. Жители Алеппо были почти отрезаны от окружающего мира, и лишь несколько оставшихся в городе блогеров, пользуясь ненадежным интернет-соединением, иногда вывешивали посты о жизни местного населения. Нам попались три сообщения за тот месяц:

Нужно 30 биткоинов. Пожалуйста! Хочу уехать из Сирии.

http://syria.mil.ru/syria/livecam.htm

Помогите выбраться из Сирии. Живу в Алеппо. Мне 14 лет. Это не обман. Пожалуйста, помогите!!!

На этой стадии от чтения граффити стало несколько неуютно. Нам вспомнилось другое место и время, когда изолированное сообщество пыталось достучаться до окружающего мира — Берлинская стена в эпоху холодной войны. Там тоже были граффити — в основном на стороне Западной Германии — с призывами уважать права человека, любовными признаниями, словами о мире и надежде, а также с простой констатацией того, что «Здесь был некий Х» — доказательством бытия и человеческой сущности. Однако если граффити времен холодной войны прочитывались как акт протеста против стены, которой пытались разделить людей с их живыми отношениями, то на мониторе компьютера, в этой странной цифровой учетной системе, послания обретали особую силу именно потому, что это НЕ стена. Никакое правительство, никакая корпорация не в силах обложить блокчейн Биткоина кирпичами или замазать надпись, внесенную в реестр. Выключить машину правды невозможно, именно поэтому она особенно ценна для записи человеческого опыта, будь то признание в любви или мольба о помощи. Вот почему блокчейн так нужен человечеству!

Введение

1. Интервью проведено сотрудниками ВПП. Отправлено Майклу Кейси по электронной почте 7 августа 2017 года.
2. Интервью взято Майклом Кейси по телефону 20 июля 2017 года.
3. Подробнее об этом см: Kashmir Hill, "'God View': Uber Allegedly Stalked Users For Party-Goers' Viewing Pleasure," *Forbes*, October 3, 2014, https://www.forbes.com/sites/kashmirhill/2014/10/03/god-view-uber-allegedly-stalked-users-for-party-goers-viewing-pleasure/#2aa731af3141.
4. Подробное объяснение архитектуры Internet 3.0 см. в: Jeff Hussey, "Internet 3.0: Welcome to the Future of Secure Networking," *Tempered Networks*, https://www.temperednetworks.com/blog/internet-3-0-welcome-to-the-future-of-secure-networking/.
5. *См.* об этом: Jonathan Shieber, "Blockchain Consortium R3 Raises $107 Million," *TechCrunch*, May 23, 2017, https://techcrunch.com/2017/05/23/blockchain-consortium-r3-raises-107-million/.
6. Цифры предоставлены Майклу Кейси порталом CoinDesk. Получены по электронной почте 22 августа 2017 года.
7. *См.* Chris Burniske and Jack Tatar, *Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond* (McGraw Hill, 2017).
8. Термин «интернет ценностей» был введен в обиход командой Ripple Labs, которая занимается разработкой протокола для одноранговых платежей и транзакций. Первое упоминание см. в: Stefan Thomas, "The Internet's Missing Link," *TechCrunch,* September 27, 2014, https://techcrunch.com/2014/09/27/the-internets-missing-link/.

Глава 1

1. *См.*: Douglas Garbutt, "The Significance of Ancient Mesopotamia in Accounting History," Accounting Information 11, no. 1 (1984), http://www.accountingin.com/accounting-historians-journal/volume-11-number-1/the-significance-of-ancient-mesopotamia-in-accounting-history/.
2. *См.*: Lehman Brothers Holdings, Inc., "Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 for the Fiscal Year Ended November 30, 2007," United States Securities and Exchange Commission, https://www.sec.gov/Archives/edgar/data/806085/000110465908005476/a08-3530_110k.htm.
3. *См.*: Pew Research Center, "Public Trust in Government: 1958–2017," May 3, 2017, http://www.people-press.org/2017/05/03/public-trust-in-government-1958-2017/.
4. *См.*: Gallup, "Confidence in Institutions," http://www.gallup.com/poll/1597/confidence-institutions.aspx.
5. Подробнее о механизме использования «РЕПО 105 в деле Lehman Brothers *см*: Jacob Goldstein, "Repo 105: Lehman's 'Accounting Gimmick' Explained," *NPR Planet Money*, March 12, 2010, http://www.npr.org/sections/money/2010/03/repo_105_lehmans_accounting_gi.html.
6. *См.*: Mary Poovey, *A History of the Modern Fact* (University of Chicago Press, 1998).
7. *См.*: Mary Poovey, *A History of the Modern Fact* (University of Chicago Press, 1998).
8. *См.*: L. E. Sigler, *Fibonacci's Liber Abaci: A Translation into Modern English of Leonardo Pisano's Book of Calculation* (Springer, 2003).
9. *См.*: Jeremy Cripps, *Particularis de Computis et Scripturis, a Contemporary Interpretation* (Pacioli Society, 1994).
10. *См.*: ibid., p. 2.
11. *См.*: James Aho, *Confession and Bookkeeping: The Religious, Moral, and Rhetorical Roots of Modern Accounting* (State University of New York Press, 2006).
12. *См.*: James Aho, *Confession and Bookkeeping: The Religious, Moral, and Rhetorical Roots of Modern Accounting* (State University of New York Press, 2006).

13. Цит. по: Jeremy Cripps, *Particularis de Computis et Scripturis: A Contemporary Interpretation* (Pacioli Society, 1994).
14. *См.*: Matt Levine, "Bank of America Made $168 Million Last Quarter, More or Less," *Bloomberg View*, October 15, 2014, https://www.bloomberg.com/view/articles/2014-10-15/bank-of-america-made-168-million-last-quarter-more-or-less.
15. *См.*: Satoshi Nakamoto, ibid.
16. *См.*: "Triple Entry Accounting," 2005, http://iang.org/papers/triple_entry.html.
17. *См.*: Nick Szabo, "The God Protocols," http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/msc.html.
18. Комментарий сделан во время саммита по вопросам технологии блокчейн на Британских Виргинских островах в июле 2017 года.
19. *См.*: Yuval Noah Harari, *Sapiens: A Brief History of Humankind* (Harper, 2015).

Глава 2

1. Полный отчет о происшествии *см.* в блоге Питера Симза: Peter Sims, "Can We Trust Uber?" *Silicon Guild*, September 6, 2014, https://thoughts.siliconguild.com/can-we-trust-uber-c0e793deda36.
2. *См.*: Johana Bhuiyan and Charlie Warzel, " 'God View': Uber Investigates Its Top New York Executive For Privacy Violations," BuzzFeed, November 18, 2014, https://www.buzzfeed.com/johanabhuiyan/uber-is-investigating-its-top-new-york-executive-for-privacy.
3. *См.*: Kaja White-house, "Uber Settles 'God View' Allegations," USA *Today*, January 6, 2016, http://www.usatoday.com/story/tech/2016/01/06/uber-settles-god-view-allegations/78383276/.
4. *См.*: Craig Silverman and Duping Trump Supporters with Fake News," BuzzFeed, November 3, 2016, https://www.buzzfeed.com/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo.
5. *См.*, например, высказывания Брюса Шнайера, приведенные в статье: Barton Gellman, "Facebook: You're Not the Customer, You're the

Product," October 15, 2010, *TIME*, http://techland.time.com/2010/10/15/facebook-youre-not-the-customer-youre-the-product/, или статью в журнале *The Economist* "The world's most valuable resource is no longer oil, but data," *Economist*, May 6, 2017, https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource.

6. Подробный анализ этого судебного диспута можно найти здесь: Arash Khamooshi, "Breaking Down Apple's iPhone Fight with the U.S. Government," *The New York Times*, March 21, 2016, https://www.nytimes.com/interactive/2016/03/03/technology/apple-iphone-fbi-fight-explained.html.
7. *См.*: "Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach $75.4 Billion in 2015," Gartner, September 23, 2015, http://www.gartner.com/newsroom/id/3135617.
8. *См.*: Stephen Gandel, "Lloyd's CEO: Cyber Attacks Cost Companies $400 Billion Every Year," Fortune, January 23, 2015, http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/.
9. *См.*: Juniper Research, "Cyber-crime Will Cost Businesses over $2 Trillion by 2019," *Juniper*, May 12, 2015, https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion.
10. По оценкам Всемирного банка: "Global Economic Prospects: A Fragile Recovery," World Bank Group, June 2017, https://www.worldbank.org/content/dam/Worldbank/GEP/GEP2015a/pdfs/GEP15a_web_full.pdf.
11. Подробный анализ кибератаки можно найти здесь: Peter Tran, "The Dyn Attack—How Iot Can Take Down the "Global Information Grid" Back Bone (Part I)," RSA, October 25, 2016, https://www.rsa.com/en-us/blog/2016-10/the-dyn-attack-how-iot-can-take-down-the-global-information-grid-back-bone-part-i.
12. *См.*: Ralph Jacobsen, "2.5 Quintillion Bytes of Data Created Every Day. How Does CPG & Retail Manage It?" IBM, April 14, 2013, https://www.ibm.com/blogs/insights-on-business/consumer-products/2-5-quintillion-bytes-of-data-created-every-day-how-does-cpg-retail-manage-it/.
13. *См.*: "Identity Theft: The Aftermath 2013," Identity Theft Resource Center, http://www.idtheftcenter.org/images/surveys_studies/Aftermath2013.pdf.

14. Вскоре после авиакатастрофы появились сообщения о том, что хакерская группа Naikon взломала официальный сайт правительства Малайзии. См.: Elsie Viebeck, "Cyberattacks Followed Malaysia Airlines Flight Disappearance," *The Hill*, April 21, 2015, http://thehill.com/policy/cybersecurity/239529-cyberattacks-followed-malaysia-airlines-flight-disappearance.
15. *См.*: Brendan I. Koerner, "Inside the Cyberattack That Shocked the US Government," *Wired*, October 23, 2016, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.
16. А. Лудвин выступал на симпозиуме DTCC 29 марта 2016 года.
17. *См.*: John Crossman: "The 'Shared Secret' Identity Model Is Finished," *Medium*, February 24, 2016, https://medium.com/@john_17722/the-shared-secret-identity-model-is-finished-59bd30e1da6a и "The Device Identity Model," *Medium*, February 26, 2016, https://medium.com/@john_17722/the-device-identity-model-6444ca6328f9.
18. *См.*: Anna Wilde Mathews, "Anthem: Hacked Database Included 78.8 Million People," *The Wall Street Journal*, February 24, 2015, https://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364.
19. *См.*: Ian Scherr, "WannaCry Ransomware: Everything You Need to Know," *CNET*, May 19, 2017, https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/.
20. *См.*: Ariel Ekblaw and Asaf Azaria, "MedRec: Medical Data Management on the Blockchain," *PubPub*, September 19, 2016, https://www.pubpub.org/pub/medrec.
21. *См.*: Thomas Friedman, *The World Is Flat: A Brief History of the Twenty-first Century* (Farrar, Straus and Giroux, 2005).
22. *См.*: Paul Vigna and Michael J. Casey, *The Age of Cryptocurrency* (St. Martin's Press, 2015), pp. 57–60.
23. *См.*: Timothy C. May, "The Crypto Anarchist Manifesto," https://www.activism.net/cypherpunk/crypto-anarchy.html.
24. Подробный анализ проекта Xanadu и причин его краха можно найти здесь: "The Curse of Xanadu," *Wired*, June 1, 2015, https://www.wired.com/1995/06/xanadu/.
25. *См.*: Don Tapscott and Alex Tapscott, *Blockchain Revolution: How the Technology behind Bitcoin Is Changing Money, Business and the World* (Portfolio, 2016), p. 5.

26. *См.*: Lawrence Lessig, "Code Is Law: On Liberty in Cyberspace," *Harvard Magazine*, January 1, 2000, http://harvardmagazine.com/2000/01/code-is-law-html.
27. *См.*: C. G. Jung, *The Structure and Dynamics of the Psyche (Collected Works of C. G. Jung, Vol. 8)* (Princeton University Press, 1970, 2nd edition), p. 325.
28. *См.*: Emin Gun Sirer, "Caution: The DAO Can Turn Into a Naturally-Arising Ponzi," *Hacking, Distributed*, June 13, 2016, http://hackingdistributed.com/2016/06/13/the-dao-can-turn-into-a-naturally-arising-ponzi/ и Drew Hinkes, "A Legal Analysis of the DAO Exploit and Possible Investor Rights," *Bitcoin Magazine*, June 21, 2016, https://bitcoinmagazine.com/articles/a-legal-analysis-of-the-dao-exploit-and-possible-investor-rights-1466524659/.
29. Онлайн-версия документов была удалена, однако основные положения можно прочесть здесь: https://www.reddit.com/r/ethereum/comments/4oo0ql/the_dao_terms_and_conditions/.
30. *См.*: Emin Gun Sirer, "Thoughts on The DAO Hack," *Hacking, Distributed*, June 17, 2016, http://hackingdistributed.com/2016/06/17/thoughts-on-the-dao-hack/.
31. *См.*: Preston Byrne, "#THEDAO: Broken, but worth fixing," May 17, 2016, https://prestonbyrne.com/2016/05/17/thedao-dont-walk-away-restructure/.
32. *См.*: "SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities," U.S. Securities and Exchange Commission, July 25, 2017, https://www.sec.gov/news/press-release/2017-131.

Глава 3

1. Подробную техническую информацию об устройстве сети Биткоин можно найти здесь: Andreas M. Antonopoulos, *Mastering Bitcoin: Un-locking Digital Cryptocurrencies* (O'Reilly Media, 2014).
2. *См.*: "Visa Inc. Over view," Visa, April 2017, https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/visa-net-fact-sheet.pdf.

3. *См.*: Paul Vigna, "Why You Won't Be Buying a Coffee with Bitcoin Anytime Soon," *The Wall Street Journal*, July 2, 2017, https://www.wsj.com/articles/why-you-wont-be-buying-a-coffee-with-bitcoin-anytime-soon-1498996800*.
4. В интервью Майклу Кейси, Нью-Йорк, сентябрь 2016 года.
5. Первые разработки и исходный код можно найти по адресу: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki.
6. *См.*: Joseph Poon and Thaddeus Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," January 14, 2016, https://lightning.network/lightning-network-paper.pdf.
7. *См.*: Laura Shin, "Is This Massive Power Struggle About to Blow Up Bitcoin?" *Forbes*, March 21, 2017, https://www.forbes.com/sites/laurashin/2017/03/21/is-this-massive-power-struggle-about-to-blow-up-bitcoin/*9872e4873250.
8. *См.*: "Bitcoin Scaling Agreement at Consensus 2017," Digital Currency Group, *Medium*, May 23, 2017, https://medium.com/@DCGco/bitcoin-scaling-agreement-at-consensus-2017-133521fe9a77.
9. *См.*: Vitalik Buterin, "Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform," http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.
10. *См.*: "An Ode to the Ethereum Community," *Steemit*, October 2016, https://steemit.com/ethereum/@owaisted/an-ode-to-the-ethereum-community.
11. В интервью Майклу Кейси, Майами, 26 января 2014 года.
12. *См.*: "$30 Million: Ether Reported Stolen Due to Parity Wallet Breach," CoinDesk, July 19, 2017, https://www.coindesk.com/30-million-ether-reported-stolen-parity-wallet-breach/.
13. *См.*: "The History of Ethereum," http://www.ethdocs.org/en/latest/introduction/history-of-ethereum.html*the-ethereum-foundation-and-the-ether-presale.
14. *См.*: Joseph Poon and Vitalik Buterin, "Plasma: Scalable Autonomous Smart Contracts," August 11, 2017, http://plasma.io/plasma.pdf.
15. Презентация, записанная группой Triangle Bitcoin & Business Meetup, 4 апреля 2017 года, доступна на YouTube по адресу https://www.youtube.com/watch?v=OZu4u_5L0l8.

16. Комментаторы на одном из форумов подметили, что «чистые» монеты торговались примерно на 3,5 процента дороже остальных. *См.*: "US Marshalls to Auction off 29,656 bitcoins" at https://texags.com/forums/16/topics/2488176.
17. *См.*: Robert Hackett, "Big Business Giants from Microsoft to J.P. Morgan Are Getting behind Ethereum," *Fortune*, February 27, 2017, http://fortune.com/2017/02/28/ethereum-jpmorgan-microsoft-alliance/.
18. *См.*: James Mosher, "Initial Coin Offerings Going Way beyond Small Change," American Institute for Economic Research, July 26, 2017, https://www.aier.org/research/initial-coin-offerings-going-way-beyond-small-change.
19. *См.* интервью с Йеном Григгом: "Millions of Transactions Per Second on EOS.IO Blockchain | Interview Ian Grigg of Block.One," https://www.youtube.com/watch?v=UC6RYwYPnpU.
20. Интервью CEO Tezos Кэтлин Брейтман и CTO Артура Брейтмана Майклу Кейси, 29 июня 2017 года.

Глава 4

1. Некоторые части этой главы взяты из отчета, написанного Майклом Кейси для научно-исследовательского института Blockchain Research Ins Institute (BRI) в сентябре 2017 года. Все фрагменты текста приводятся с разрешения правообладателя.
2. *См.*: Jon Russell, "Former Mozilla CEO Raises $35M in under 30 Seconds for His Browser Startup Brave," *TechCrunch*, June 1, 2017, https://techcrunch.com/2017/06/01/brave-ico-35-million-30-seconds-brendan-eich/.
3. По данным портала Coindesk: https://www.coindesk.com/ico-tracker/.
4. *См.*: Rob Leathern, "Carriers Are Making More from Mobile Ads Than Publishers Are," *Medium*, October 4, 2015, https://medium.com/@robleathern/carriers-are-making-more-from-mobile-ads-than-publishers-are-d5d3c0827b39.
5. *См.*: Margaret Boland, "Cyber Criminals Are Stealing Billions from the Ad Industry Each Year," *Business Insider*, May 28, 2016, http://www.businessinsider.com/the-ad-fraud-report-bot-traffic-2016-3.

6. Данные приводятся по: "Basic Asset Token (BAT): Blockchain Based Digital Advertising," May 29, 2017, p. 9, https://basicattentiontoken.org/BasicAttentionTokenWhitePaper-4.pdf.
7. ibid.
8. *См.*: Garrett Hardin, "The Tragedy of the Commons," Science, December 13, 1968, 162 (3859): pp. 1243–1248.
9. *См.*: "The World's Most Valuable Resource Is No Longer Oil, But Data," *The Economist*, May 6, 2017, https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource.
10. *См.*: Steven D. Levitt and Stephen J. Dubner, *Freakonomics: A Rogue Economist Explores the Hidden Side of Everything* (William Morrow, 2005).
11. Согласно данным, опубликованным на сайте компании: https://gamecredits.com/.
12. Телефонное интервью Майклу Кейси, 29 июня 2017 года.
13. В число критиков входил и основатель Эфириума Виталик Бутерин: https://twitter.com/VitalikButerin/status/869972830191984641.
14. *См.*, например: Dustin Byington, "Why We Need a Cap on Every ICO—Looking at You Tezos," *Medium*, May 7, 2017, https://medium.com/@dustin_byington/why-we-need-a-cap-on-every-ico-looking-at-you-tezos-90d412f34b88.
15. *См.*: Michael del Castillo, "Why Brave's $35 Million ICO May Not Be Enough for a High-Tech Hiring Spree," *CoinDesk*, July 12, 2017, https://www.coindesk.com/braves-35-million-ico-may-not-enough-high-tech-hiring-spree/.
16. *См.*: Pete Rizzo, "Ethereum: Bitcoin Price Decline Created $9 Million Funding Shortfall," *CoinDesk*, September 28, 2015, https://www.coindesk.com/ethereum-bitcoin-decline-9-million-funding-shortfall/.
17. *См.*: Paul Vigna, "Chiefless Company Rakes in More Than $100 Million," *The Wall Street Journal*, May 16, 2016, https://www.wsj.com/articles/chiefless-company-rakes-in-more-than-100-million-1463399393.
18. *См.*: Roger Aitken, "Fintech Golem's 'Airbnb' For Computing Crowdsale Scores $8.6M in Minutes," *Forbes*, November 12, 2016, https://www.forbes.com/sites/rogeraitken/2016/11/12/fintech-golems-airbnb-for-computing-crowdsale-scores-8-6m-in-minutes/#324579c73583.

19. *См.*: Alyssa Hertig, "ICO Insanity? $300 Million Gnosis Valuation Sparks Market Reaction," *CoinDesk*, April 25, 2017, https://www.coindesk.com/ethereum-ico-irrationality-300-million-gnosis-valuation-sparks-market-concerns/.
20. Телефонное интервью Полу Винья, 29 июня 2017 года.
21. *См.*: https://www.coindesk.com/ico-tracker/.
22. *См.*: Paul Vigna, "How a Bitcoin Clone Helped a Company Raise $12 Million in 12 Minutes," *The Wall Street Journal*, May 17, 2017, https://www.wsj.com/articles/how-a-bitcoin-clone-helped-a-company-raise-12-million-in-12-minutes-1495018802?tesla=y&mod=e2tw.
23. Телефонное интервью Майклу Кейси, 22 июня 2017 года.
24. *См.*: Laura Shin, "Crypto Boom: 15 New Hedge Funds Want In on 84,000 % Returns," *Forbes*, July 12, 2017, https://www.forbes.com/sites/laurashin/2017/07/12/crypto-boom-15-new-hedge-funds-want-in-on-84000-returns/#40c3d1aa416a.
25. *См.*: Stan Higgins, Alex Sunnarborg, and Pete Rizzo, "$150 Million: Tim Draper-Backed Bancor Completes Largest-Ever ICO," *CoinDesk*, June 12, 2017, https://www.coindesk.com/150-million-tim-draper-backed-bancor-completes-largest-ever-ico/.
26. *См.*: Paul Vigna, "Forget an IPO, Coin Offerings Are New Road to Startup Riches," *The Wall Street Journal*, July 7, 2017, https://www.wsj.com/articles/forget-an-ipo-coin-offerings-are-new-road-to-startup-riches-1499425200.
27. *См.*: Arthur Breitman, "The Path Forward: A letter from Arthur & Kathleen Breitman to the Tezos community," *Medium*, October 18, 2017, https://medium.com/@arthurb/the-path-forward-eb2e6f63be67.
28. *См.*: Anna Irrera, Steve Stecklow and Brenna Hughes Neghaiwi, "Special Report: Backroom battle imperils $230 million cryptocurrency venture," *Reuters*, October 18, 2017, https://www.reuters.com/article/us-bitcoin-funding-tezos-specialreport/special-report-backroom-battle-imperils-230-million-cryptocurrency-venture-idUSKBN1CN35K; Paul Vigna, "Tezos Raised $232 Million in a Hot Coin Offering, Then a Fight Broke Out," *The Wall Street Journal*, October 19, 2017; https://www.wsj.com/articles/tezos-raised-232-million-in-a-hot-coin-offering-then-a-fight-broke-out-1508354704; Jeff John Roberts, "Tezos Rebuffs Rumors of SEC Probe Into $232

Million Crypto ICO," *Fortune*, October 28, 2017, http://fortune.com/2017/10/28/tezos-sec/; Chloe Cornish, "Acrimony over $232m ICO set to intensify regulatory scrutiny," *Financial Times*, October 26, 2017, https://www.ft.com/content/fcb16026-b45a-11e7-aa26-bb002965bce8.

29. ibid.
30. *См.*: Stan Higgins, "China's Crypto Ex-changes Yank Token Listings amid ICO Ban Fallout," *CoinDesk*, September 6, 2017, https://www.coindesk.com/chinas-exchanges-yank-token-listings-ico-crackdown/.
31. *См.*: "SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities," U.S. Securities and Exchange Commission, July 25, 2017, https://www.sec.gov/news/press-release/2017-131.
32. Телефонное интервью Майклу Кейси, 26 июня 2017 года.
33. *См.*: Stan Higgins, "$200 Million in 60 Minutes: Filecoin ICO Rockets to Record Amid Tech Issues," CoinDesk, August 10, 2017, https://www.coindesk.com/200-million-60-minutes-filecoin-ico-rockets-record-amid-tech-issues/.
34. *См.*: Fred Wilson, "The Golden Age of Open Protcols," AVC, July 21, 2016, http://avc.com/2016/07/the-golden-age-of-open-protocols/.
35. В интервью Майклу Кейси, 23 марта 2017 года.
36. *См.*: https://interledger.org/.
37. *См.*: Jae Kwon and Ethan Buchman, "Cosmos: A Net work of Distributed Ledgers," https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md.
38. Интервью Майклу Кейси, Гейдельберг, Германия, 19 июня 2016 года.
39. *См.*: https://tokenstars.com/.
40. *См.*: Cade Metz, "Forget Bitcoin. The Blockchain Could Reveal What's True Today and Tomorrow," *Wired*, March 22, 2017, https://www.wired.com/2017/03/forget-bitcoin-blockchain-reveal-whats-true-today-tomorrow/.
41. Брошюра с проектом была показана Майклу Кейси 8 августа 2017 года.

Глава 5

[304]

1. *См.*: Klaus Schwab, The Fourth Industrial Revolution (Crown, 2017).
2. *См.*: Bruce Schneier, "The Internet of Things Will Turn Large-Scale Hacks into Real World Disasters," Mother-board, July 25, 2016, https://motherboard.vice.com/en_us/article/qkjzwp/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster.
3. *См.*: Veena Pureswaran and Paul Brody, "Device Democracy: Saving the Future of the Internet of Things," September 2014, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03620USEN.
4. *См.*: Andy Greenberg, "This 'Demonically Clever' Backdoor Hides in a Tiny Slice of a Computer Chip," *Wired*, June 1, 2016, https://www.wired.com/2016/06/demonically-clever-backdoor-hides-inside-computer-chip/.
5. *См.*: "Trusted Computing: Promise and Risk," Electronic Frontier Foundation, October 1, 2003. https://www.eff.org/wp/trusted-computing-promise-and-risk.
6. Подробнее об этом *см.*: "Hyperledger Sawtooth documentation," https://intelledger.github.io/.
7. Daniel Palmer, "Broken Hash Crash? IOTA's Price Keeps Dropping on Tech Critique," CoinDesk, September 8, 2017, https://www.coindesk.com/broken-hash-function-iota-price-drops-on-tech-critique/.
8. *См.* образцы комментариев здесь: https://www.reddit.com/r/Iota/comments/6z87sw/all_of_this_fud_is_a_good_sign/?st=j8ks3khu&sh=8be3c663.
9. Limo, "Competitors and Amy Castor: A Tale on Reputation Usage and a Campaign to Discredit IOTA," *The Tangler*, September 13, 2017, http://www.tangleblog.com/2017/09/13/competitors-amy-castor-tale-reputation-usage-discredit-campaign/.
10. Misty Wind, "IOTA Cofounder Sergey Ivancheglo aka Come-from-Beyond's Responses to the Ongoing FUD about So Called 'Vulnerabilities' in IOTA Code Which Never Really Existed," *Medium*, September 10, 2017, https://medium.com/@misty-wind/iota-cofounder-sergey-ivancheglo-aka-come-from-beyonds-responses-to-the-ongoing-fud-about-so-ea3afd51a79b.

11. См.: https://www.trusted-iot.org/
12. Jamie Redman, "Dept of Homeland Security Awards $200K to Factom for ID System," *Bitcoin*, June 18, 2016, https://news.bitcoin.com/dhs-awards-200k-factom/.
13. G. Ananthakrishnan, "Modi Asks Rich Nations to Cut Emissions, Share Carbon Space with Poor," *The Hindu*, December 1, 2015, http://www.thehindu.com/sci-tech/energy-and-environment/cop21-paris-climate-conference-narendra-modi-cautions-against-unilateral-steps-in-combating-climate-change/article7933873.ece.
14. Katie Fehrenbacher, "A Jaw-Dropping World Record Solar Price Was Just Bid in Abu Dhabi," *Fortune*, September 19, 2016, http://fortune.com/2016/09/19/world-record-solar-price-abu-dhabi/.
15. Jeff St. John, "How Microgrids Helped Weather Hurricane Sandy," *Greentech Media*, November 20, 2012, https://www.greentechmedia.com/articles/read/how-microgrids-helped-weather-hurricane-sandy.
16. Набросок плана был показан Майклу Кейси.
17. "Energy Companies Join Forces with Rocky Mountain Institute and Grid Singularity to Launch Global Blockchain Initiative for Energy," March 8, 2017, Rocky Mountain Institute, https://www.rmi.org/about/news-and-press/press-release-energy-web-foundation-launch/.
18. Katie Little, "One Year after Chipotle's E. coli crisis, Chain Still Struggling," CNBC.com, October 31, 2016 https://www.cnbc.com/2016/10/31/one-year-after-chipotles-e-coli-crisis-chain-still-struggling.html.
19. www.provenance.org
20. Robert Hackett, "Walmart and IBM Are Partnering to Put Chinese Pork on a Blockchain," *Fortune*, October 19, 2016, http://fortune.com/2016/10/19/walmart-ibm-blockchain-china-pork/.
21. Pete Rizzo, "World's Largest Mining Company to Use Blockchain for Supply Chain," *CoinDesk*, September 23, 2016, https://www.coindesk.com/bhp-billiton-blockchain-mining-company-supply-chain/.
22. Gian Volpicelli, "How the Blockchain Is Helping Stop the Spread of Conflict Diamonds," *Wired UK*, February 15, 2017, http://www.wired.co.uk/article/blockchain-conflict-diamonds-everledger.

23. В электронном письме Майклу Кейси, 2 марта 2017 года.
24. Lockheed Martin Contracts Guardtime Federal for Innovative Cyber Technology," *Lockheed Martin*, April 27, 2017, http://news.lockheedmartin.com/2017-04-27-Lockheed-Martin-Contracts-Guardtime-Federal-for-Innovative-Cyber-Technology.
25. По итогам встречи авторов книги с главами компании 22 марта 2017 года.
26. "Reinventing Construction: A Route to Higher Productivity," McKinsey Global Institute, February 2017, https://www.mckinsey.com/~/media/McKinsey/Industries/Capital%20Projects%20and%20Infrastructure/Our%20Insights/Reinventing%20construction%20through%20a%20productivity%20revolution/MGI-Reinventing-Construction-Executive-summary.ashx.
27. Kim S. Nash and Rachael King, "IBM Set to Launch One of the Largest Blockchain Implementations to Date," *The Wall Street Journal*, July 29, 2016, https://blogs.wsj.com/cio/2016/07/29/ibm-set-to-launch-one-of-the-largest-blockchain-implementations-to-date/.
28. "Standard Chartered Pilots Blockchain Trade Finance Tool," PYMNTS.com, April 3, 2017, https://www.pymnts.com/news/b2b-payments/2017/standard-chartered-hong-kong-blockchain-distributed-ledger-trade-finance-banking-pilot-blockchain-hong-kong/.
29. Andrew Sawers, "Foxconn Uses Blockchain for New SCF Platform after $6.5m Pilot," http://www.scfbriefing.com/foxconn-launches-scf-blockchain-platform/.
30. Michael J. Casey and Pindar Wong, "Global Supply Chains Are About to Get Better, Thanks to Blockchain," *Harvard Business Review*, March 13, 2017, https://hbr.org/2017/03/global-supply-chains-are-about-to-get-better-thanks-to-blockchain.
31. https://www.beltandroadblockchain.org/.
32. "China's One Belt, One Road: Will It Reshape Global Trade?" Podcast Transcript, July 2016, McKinsey.com, https://www.mckinsey.com/global-themes/china/chinas-one-belt-one-road-will-it-reshape-global-trade.

Глава 6

1. "Bitcoin Open Source Imple-mentation of P2P currency," P2P Foundation, February 11, 2009, http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.
2. Karen Weise, "Tallying the Full Cost of the Financial Crisis," *Bloomberg*, September 14, 2012, https://www.bloomberg.com/news/articles/2012-09-14/tallying-the-full-cost-of-the-financial-crisis.
3. http://www.dtcc.com/charts/daily-total-us-treasury-trade-fails.
4. Mike Hearn, "The Resolution of the Bitcoin Experiment," *Medium*, January 14, 2016, https://blog.plan99.net/the-resolution-of-the-bitcoin-experiment-dabb30201f7.
5. Michael Lewis, *The Big Short: Inside the Doomsday Machine* (Norton, 2010).
6. Lawrence Lewitinn, "How Buffett Used 'Financial Weapons of Mass Destruction' to Make Billions of Dollars," Yahoo! Finance, https://finance.yahoo.com/news/how-buffett-used-financial-weapons-of-mass-destruction-to-make-billions-of-dollars-175922498.html.
7. В электронном письме Майклу Кейси, 18 сентября 2016 года.
8. Tim Swanson, "Settlement Risks Involving Public Blockchains," Tabbforum.com, December 30, 2016, http://tabbforum.com/opinions/settlement-risks-involving-public-blockchains.
9. "Blockchain and Central Banks: A Tour de Table Part II," *Finextra*, January 9, 2017. https://www.finextra.com/blogposting/13532/blockchain-and-central-banks-a-tour-de-table-part-ii.
10. В электронном письме Майклу Кейси, 1 сентября 2017 года.
11. John Barrdear and Michael Kumhoff, "Staff Working Paper No. 605: The Macroeconomics of Central Bank Issued Digital Currencies," Bank of England, July 2016, http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf.
12. http://hyperledger.org/about.
13. На конференции в Массачусетском технологическом институте 18 апреля 2017 года.
14. В кулуарах офисов DTCC, 28 января 2016 года.
15. "IBM Delivers Blockchain-As-A-Service for Developers; Commits to Making Blockchain Ready for Business," IBM, February 16, 2016, https://www-03.ibm.com/press/us/en/pressrelease/49029.wss.

Глава 7

1. Jorge Salomón, "El barrio Charrúa, una pequeña Bolivia en el sur de Buenos Aires," *El País*, February 12, 2016, http://www.elpaisonline.com/index.php/2013-01-15-14-16-26/sociedad/item/204708-el-barrio-charrua-una-pequena-bolivia-en-el-sur-de-buenos-aires.
2. Hernando de Soto, *The Mystery of Capital: Why Capitalism Triumphs in the West and Fails Everywhere Else* (Basic Books, 2000).
3. Lori London, "The Top 10 Un-banked and Underbanked Cities," goEBT, March 29, 2017, https://blog.goebt.com/the-top-10-unbanked-and-underbanked-cities.
4. Global Findex Database, World Bank, 2014, http://www.worldbank.org/en/programs/globalfindex.
5. Sustainable Development Goals, United Nations, http://www.un.org/sustainabledevelopment/poverty/.
6. Consultative Group to Assist the Poor, "2014 Saw $31 Billion in International Funding for Financial Inclusion," CGAP, January 19, 2016, http://www.cgap.org/news/2014-saw-31-billion-international-funding-financial-inclusion.
7. Joshua J. Mark, "Cylinder Seals in An-cient Mesopotamia—Their History and Significance," *Ancient History Encyclopedia*, December 2, 2015, http://www.ancient.eu/article/846/.
8. David Roodman, "Grameen Bank, Which Pioneered Loans for the Poor, Has Hit a Repayment Snag," Center for Global Development, February 9, 2010, https://www.cgdev.org/blog/grameen-bank-which-pioneered-loans-poor-has-hit-repayment-snag.
9. Michael J. Casey, "Could the Blockchain Empower the Poor and Unlock Global Growth?" Techonomy, March 7, 2016, http://techonomy.com/2016/03/blockchain-global-growth/.
10. Laura Shin, Forbes, April 21, 2016, "Republic of Georgia to Pilot Land Titling on Blockchain with Economist Hernando De Soto, BitFury," https://www.forbes.com/sites/laurashin/2016/04/21/republic-of-georgia-to-pilot-land-titling-on-blockchain-with-economist-hernando-de-soto-bitfury/#3c381e6144da.
11. "Ubitquity, the Blockchain-Secured Platform for Real Estate Transactions, Partners with US-Based 'Rising Barn' for Property

Recording," Ubitquity.io, October 17, 2016, https://www.ubitquity.io/blog/ubitquity_llc_partners_prioritytitle_blockchain_10_17_2016.html.

12. Land Governance Assessment Framework, Draft Final Report, World Bank, September 2015, http://siteresources.worldbank.org/INTLGA/Resources/Sierra_Leone_Final_Draft_Report_Oct12_v2.pdf; Sierra Leone Ministry of Lands, Country Planning and the Environment, "Draft National Land Policy of Sierra Leone," United Nations Development Programme, August 1, 2015, http://www.sl.undp.org/content/dam/sierraleone/docs/projectdocuments/environment/Land%20Policy%20SL%20151214%20FINAL.pdf.
13. Victoria Louise Lemieux, "Trusting Records: Is Blockchain Technology the Answer?" *Records Management Journal* 26, no. 2 (2016): 110–139, doi: 10.1108/RMJ-12-2015-0042.
14. "Unleashing the Wealth of Nations," http://wealthofnations.media.mit.edu/node/2.
15. Детали проекта *см.* на сайте института: https://www.media.mit.edu/.
16. GSMA's Mobile Money Deployment Tracker: http://www.gsma.com/mobilefordevelopment/m4d-tracker/mobile-money-deployment-tracker.
17. Carol Realini, "Unbanked Consumers Strive for Better Banking Services," www.carolrealini.com, February 7, 2015, http://www.carolrealini.com/unbanked-consumers-better-banking-services/: Rob Jillo, "Airtel Presses for Share of Safaricom's M-PESA Platform," *Capital Business*, July 3, 2015, http://www.capitalfm.co.ke/business/2015/07/airtel-presses-for-share-of-safaricoms-m-pesa-platform/.
18. https://remittanceprices.worldbank.org/en/corridor/United-States/Jamaica.
19. Laura Shin, "Bitcoin Payments Firm BitPesa Secures Greycroft as Lead Investor for $10 Million Total Funding," *Forbes*, August 30, 2017, https://www.forbes.com/sites/laurashin/2017/08/30/bitcoin-payments-firm-bitpesa-secures-greycroft-as-lead-investor-for-10-million-total-funding/#4dfaefb66066.
20. Luke Parker, "Bitcoin Remittances '20 percent' of South Korea-Philippines Corridor," *Brave New Coin*, September 14, 2016, https://

bravenewcoin.com/news/bitcoin-remittances-20-percent-of-south-korea-philippines-corridor/.

21. New York State Department of Financial Services, New York Codes, Rules, and Regulations, Title 23, Chapter 1, Part 200: Virtual Currencies, http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf.
22. Maria Konnikova, "The Limits of Friendship," *New Yorker*, October 7, 2014, https://www.newyorker.com/science/maria-konnikova/social-media-affect-math-dunbar-number-friendships.

Глава 8

1. Mariana Dahan and Alan Gelb, "The Identity Target in the Post-2015 Development Agenda," World Bank, September 17, 2015. http://www.worldbank.org/en/topic/ict/brief/the-identity-target-in-the-post-2015-development-agenda-connections-note-19.
2. "Trafficking and HIV/AIDS Project," UNESCO, July 4, 2017, https://bangkok.unesco.org/content/trafficking-and-hivaids-project.
3. Joon Ian Wong, "Microsoft Thinks Blockchain Tech Could Solve One of the Internet's Toughest Problems: Digital Identities," *Quartz*, June 1, 2017, https://qz.com/989761/microsoft-msft-thinks-blockchain-tech-could-solve-one-of-the-internets-toughest-problems-digital-identities/.
4. Jeanette Rodrigues, "India ID Program Wins World Bank Praise Despite 'Big Brother' Fears," *Bloomberg*, March 15, 2017, https://www.bloomberg.com/news/articles/2017-03-15/india-id-program-wins-world-bank-praise-amid-big-brother-fears.
5. Sandeep Phuken, "Aadhaar Pay: New App Does Away with Transaction Fee, Debit, Credit Cards," NDTV, March 8, 2017, http://www.ndtv.com/india-news/aadhaar-pay-new-app-does-away-with-transaction-fee-debit-credit-cards-1667254.
6. Shaun Waterman, "Nasdaq Says Estonia Evoting Pilot Successful," *CyberScoop*, January 25, 2017, https://www.cyberscoop.com/nasdaq-estonia-evoting-pilot/.

7. Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. Alex Halderman, "Security Analysis of the Estonian Internet Voting System," ACM CCS 2014—21st ACM Conference on Com-puter and Communications Security, November 3–7, 2014, http://dx.doi.org/10.1145/2660267.2660315.
8. При встрече с Майклом Кейси в Нью-Йорке, июнь 2015 года.
9. David Birch, *Identity Is the New Money* (London Publishing Partnership, 2004).
10. "A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity," World Economic Forum, August 2016, http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf.
11. "Towards an Internet of Trusted Data: A New Framework for Identity and Data Sharing," August 2016, MIT Connection Science, https://www.nist.gov/sites/default/files/documents/2016/09/16/mit_rfi_response.pdf.
12. Yorke Rhodes III, "What Does Identity Mean in Today's Physical and Digital World?" Microsoft.com, https://azure.microsoft.com/en-us/blog/what-does-identity-mean-in-today-s-physical-and-digital-world/.
13. Ron Miller, "The Promise of Managing Identity on the Blockchain," *TechCrunch*, September 10, 2017, https://techcrunch.com/2017/09/10/the-promise-of-managing-identity-on-the-blockchain/.
14. Juan Galt, "Andreas Antonopoulos: The Case Against Reputation and Identity Systems," *Bitcoin Magazine*, December 19, 2015, https://news.bitcoin.com/andreas-antonopoulos-case-reputation-identity-systems/.
15. Там же.
16. Russell Brandon, "Your phone's biggest vulnerability is your fingerprint," The Verge, May 2, 2016, http://www.theverge.com/2016/5/2/11540962/iphone-samsung-fingerprint-duplicate-hack-security.
17. Chris Jagers, "Digital Identity and the Blockchain," Learning Machine Blog, July 16, 2017, https://medium.com/learning-machine-blog/digital-identity-and-the-blockchain-10de0e7d7734.
18. Chris Allen, "The Path to Self-Sovereign Identity," Life with Alacrity blog, April 25, 2016, http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

Глава 9

[312]

1. Marc Andreessen, "Why Software Is Eating the World," *The Wall Street Journal*, August 20, 2011, https://www.wsj.com/articles/SB10001424053111903480904576512250915629460.
2. S. Jasanoff, *The Ethics of Invention: Technology and the Human Future* (W. W. Norton, 2016).
3. Oscar Wilde, "The Soul of Man under Socialism," First publication in *Fortnightly Review*, February 1891, p. 292.
4. "Blue Feed, Red Feed: See Liberal Facebook and Conser vative Facebook, Side by Side," *The Wall Street Journal*, http://graphics.wsj.com/blue-feed-red-feed/.
5. Craig Silverman and Lawrence Alexander, "How Teens in the Balkans Are Duping Trump Supporters with Fake News," *BuzzFeed*, November 3, 2016, https://www.buzzfeed.com/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo.
6. "State of the Commons," https://stateof.creativecommons.org/2015/.
7. Robert Hof, "How MetaX Plans to Use Blockchain to Stop Ad Fraud," *Forbes*, March 21, 2017, https://www.forbes.com/sites/roberthof/2017/03/21/how-metax-plans-to-use-blockchain-to-stop-ad-fraud/#2e417d0e59da.
8. "*Age of Cryptocurrency*, Recorded on the Bitcoin Blockchain," CoinDesk, February 3, 2015, https://www.coindesk.com/age-of-cryptocurrency-bitcoin-blockchain/.
9. В интервью Майклу Кейси, 28 июля 2017 года.
10. "Imogen Heap— Future Music—PART 1/2, London Real," YouTube channel, December 27, 2015, https://www.youtube.com/watch?v=IkLrdRx0F6w.
11. Lance Koonce, "Copyright's 'Double Spend' Problem: Digital First Sales," *Medium*, April 27, 2016, https://medium.com/creativeblockchain/copyrights-double-spend-problem-digital-first-sales-f18c586612b9.
12. В телефонном интервью с Майклом Кейси, 25 марта 2017 г.
13. Там же.
14. Tim Gosselin, "A New Cryptocurrency to Reward Creative Commons Creators," mediachain.io, March 9, 2017, https://blog.mediachain.

io/a-new-cryptocurrency-to-reward-creative-commons-creators-e41e1791c4c0.

15. Sarah Perez, "Spotify Acquires Blockchain Startup Mediachain to Solve Music's Attribution Problem," *TechCrunch*, April 26, 2017, https://techcrunch.com/2017/04/26/spotify-acquires-blockchain-startup-mediacha in-to-solve-musics-attribution-problem/.
16. Todd Spangler, "Spotify to Pay More Than $20 Million to Music Publishers in Roya lty Pact for 'Un-matched ' Songs," *Variety*, March 17, 2016, http://variety.com/2016/digital/news/spotify-nmpa-music-publishers-royalties-1201732879/.

Глава 10

1. https://bitnation.co/.
2. Brian Forde, "Hillary Clinton and the Blockchain," TechCrunch, July 7, 2016, https://techcrunch.com/2016/07/07/hillary-clinton-and-the-blockchain/.
3. Diana Ngo, "Governments, NGOs Consider Neocapita's Blockchain Pilots for E-Governance," *Bitcoin Magazine*, March 31, 2017, https://bitcoinmagazine.com/articles/governments-ngos-consider-neocapitas-blockchain-pilots-e-governance/.
4. Ali Breland, "Lawmakers Introduce the Blockchain Caucus," *The Hill*, February 9, 2017, http://thehill.com/policy/technology/318845-lawmakers-introduce-the-blockchain-caucus.
5. Jeff John Roberts, "Companies Can Put Shareholders on a Blockchain Starting Today," Fortune, August 1, 2017, http://fortune.com/2017/08/01/blockchain-shareholders-law/.
6. Anna Irrera, "Illinois Watchdog First U.S. Regulator to Join Blockchain Consortium R3," Reuters, March 16, 2017, https://www.reuters.com/article/us-blockchain-illinois/illinois-watchdog-first-u-s-regulator-to-join-blockchain-consortium-r3-idUSKBN16N2FN.
7. The Traderman, "Chainanalysis Partners with Europol's European Cybercrime Centre," *The Merkle*, February 22, 2016, https://themerkle.com/chainanalysis-partners-with-europols-european-cybercrime-centre/.

8. Similarly, the UK Financial Conduct Authority's "sandbox" strategy: Regulatory sandbox details at FCA Innovate: https://www.fca.org.uk/firms/regulatory-sandbox.
9. Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich, "Algorand: Scaling Byzantine Agreements for Cry ptocurrencies," MIT CSAIL, https://people.csail.mit.edu/nickolai/papers/gilad-algorand-eprint.pdf.
10. "Distributed Ledger Technology: Beyond block chain [sic]," UK Government Office for Science, January 19, 2016.
11. "Conway: Press Secretary Gave 'Alternative Facts'," per KellyAnne Conway's interview with Chuck Todd of NBC News, NBC News, January 22, 2017, https://www.nbcnews.com/meet-the-press/video/conway-press-secretary-gave-alternative-facts-860142147643.

Благодарности

Крайне сложно угнаться за теми невероятными темпами, которыми развиваются технология блокчейн и сфера криптографии, а тем более когда пишешь об этом книгу. Темп жизни в блокчейн-сообществе многократно превышает размеренный ритм издательского дела. Поэтому авторам никак не обойтись без команды помощников, которые при необходимости идут навстречу и готовы потерпеть, когда усталость и напряжение начинают давать о себе знать. В нашем случае работу осложняло еще и то, что каждый из нас параллельно писал другую, собственную книгу. Поэтому мы хотели бы выразить признательность всем, кто помог нам довести дело до конца. Как обычно, их слишком много, чтобы называть каждого по имени.

Среди тех, кого обязательно нужно упомянуть, лидирует Джиллиан Маккензи — наш литературный агент и неутомимый соратник. Спасибо за веру в нас и за бесценные советы! Джиллиан стала для нас не только партнером и коллегой, но и близким другом.

Наш редактор Тим Бартлетт — действительно один из лучших в своей области. Его требовательность и настойчивость заставили нас многократно переработать текст и прояснить все, что могло бы показаться чересчур сложным неподготовленному читателю. Благодаря ему книга стала несравненно лучше. Хочется отметить, с каким пониманием и тактом Тим относится к нашему сложному рабочему графику. Отдельную благодарность выражаем команде издательства St. Martin's, без которой нам едва ли удалось бы собраться с силами и уложиться в срок. Помощница Тима Элис Пфайфер оказала неоценимую поддержку при подготовке рукописи к печати. Благодарим выпускающего редактора Алана Брэдшоу за то, что следил за соблюдением графика,

а корректора Дженнифер Симингтон — за тщательную, добросовестную работу. Издатель Лора Кларк уже второй раз помогает нам с публикацией. Без содействия специалиста по связям с общественностью Кэти Бассел и маркетолога Джейсона Принса наш путь к читателю был бы намного сложнее.

Майкл Кейси

Для меня мои коллеги из Массачусетского технологического института — неизменный источник вдохновения. Вряд ли они представляют, какую огромную роль сыграли в работе над книгой. Особой благодарности заслуживают директор медийной лаборатории Джой Ито, руководитель проекта по исследованию криптовалют Неха Нарула, а также Саймон Джонсон, Роблех Али, Марк Вебер, Тадж Дрийя, Челси Барабас, Према Шрикришна, Алин Драгош, Джеймс Лавджой, Сэнди Пентланд, Дазза Гринвуд, Харви Майклз, Давид Бернбах и Кристиан Каталини. Отдельный теплый привет Брайану Форду, первому руководителю проекта по исследованию криптовалют, который сейчас знакомит Конгресс США с технологией блокчейн и убедил меня оставить журналистику и посвятить себя научной работе. Также выражаю благодарность команде портала CoinDesk: Кевину Уорту, Марку Хохштайну, Питу Риццо и всем остальным. Спасибо за предоставленную новую платформу для публикаций. Приятно было снова заняться журналистикой, даже по совместительству.

Среди остальных друзей и помощников хочу отметить Рика Уилларда, Нии Локко, Лэнса Кунса, Патрика Мурка, Хуана Льяноса, Мариану Дахан, Майю Вуйнович, Кайла Берджесса, Джо Коланджело, Йорка Роудза, Баладжи Сринивасан, Джэля Телпнера и Дона Тапскотта. Отдельная благодарность друзьям по Блокчейн-саммиту: Валерию Вавилову, Георгу Киквадзе, Биллу Таи, Джейми Смит, Томике Тиллеман, Данте Диспарте, Винни Лингему, Эрнандо де Сото, Габриэлю Абеду, Имоджен Хип, Эрику Миллеру, Хайди Пиз, Лори Шин, Джиму Ньюсому, Ройе Мабуб, Еве Кайли, Суне Саид, Бет Мозес, Джоби Виксу, Джен Моррис и многим другим.

И в заключение хочу сказать сердечное спасибо самым важным и близким людям, без которых эта книга не появилась бы на свет. Зуи, Лия и, конечно же, моя дорогая жена Алисия! Спасибо, что вы всегда рядом и поддерживаете меня в любых начинаниях.

Пол Винья

Как всегда, огромную и неоценимую помощь мне оказали коллеги из редакции The Wall Street Journal. Выражаю самую теплую признательность Стивену Гросеру и Эрику Холму, Аарону Луккетти и Дэвиду Рейли, Нилу Липшутцу, Карен Пенсьеро и главному редактору Джерарду Бейкеру.

Моя семья была и остается для меня главным источником вдохновения в жизни. Без их поддержки и одобрения я не смог бы довести дело до конца. Спасибо вам, дорогие Элизабет и Роберт. Бесконечно люблю вас обоих.

Научно-популярное издание

Винья Пол, **Кейси** Майкл

Машина правды

Блокчейн и будущее человечества

Книга издана при поддержке Университета Иннополис

Руководитель редакции *Артем Степанов*
Шеф-редактор *Ренат Шагабутдинов*
Ответственный редактор *Наталья Шульпина*
Литературный редактор *Татьяна Сковородникова*
Арт-директор *Алексей Богомолов*
Дизайнер *Оксана Зварич*
Верстка *Вадим Мартыновский*
Корректоры *Елена Попова, Лидия Киселева*

Подписано в печать 7.08.2018
Формат 70×100 1/16. Гарнитура Гарамонд
Бумага офсетная. Печать офсетная
Усл. печ. л. 25,93. Тираж 4000 экз.
Заказ № 7979.

ООО «Манн, Иванов и Фербер»
www.mann-ivanov-ferber.ru
www.facebook.com/mifbooks
www.vk.com/mifbooks

Отпечатано в АО «Первая Образцовая типография»,
филиал «УЛЬЯНОВСКИЙ ДОМ ПЕЧАТИ»,
432980, г. Ульяновск, ул. Гончарова, д. 14
http://www.uldp.ru

В новой книге авторов бестселлера «Эпоха криптовалют» рассказывается о технологии блокчейн и ее потенциальном влиянии на разные сферы бизнеса и жизни.

В условиях современной экономики миром правит тот, кто контролирует потоки информации, что хорошо видно на примере информационно-технологических гигантов вроде Google и Facebook.

В XXI веке само понятие власти определяет тот, кто имеет полномочия собирать, хранить и публиковать данные. Сейчас эти полномочия централизованы и разделены между несколькими гигантскими корпорациями, при этом наблюдается резкое уменьшение доверия к общественным институтам из-за обилия фейковых новостей и применения двойных стандартов. Технология блокчейн позволяет решить проблему доверия и устранить назойливое вмешательство и контроль посреднических организаций.

Потенциал блокчейна огромен и способен обеспечить нам:

— *неуязвимые реестры собственности;*

— *мгновенные, прямые, защищенные межбанковские операции;*

— *децентрализованные вычислительные системы и хранилища данных;*

— *децентрализованный «интернет вещей»;*

— *децентрализацию СМИ и контента;*

— *мгновенное получение цифровых удостоверений личности.*

И это не весь список. О том, что уже сделано и что еще предстоит сделать на этом пути, вы узнаете из этой книги.

Издано при поддержке
INNOPOLIS UNIVERSITY

ISBN 978-5-00117-660-2

издательство
МАНН, ИВАНОВ И ФЕРБЕР

Like facebook.com/**mifbooks**
vk.com/**mifbooks**
instagram.com/**mifbooks**

Максимально полезные книги на сайте **mann-ivanov-ferber.ru**