Часть 1. «Итак, вы хотите устроить революцию»

Глава 1. Доверительные протоколы

Похоже, что снова кто-то выпустил из бутылки технологического джинна. Неясно, кто и зачем его призвал в наше нестабильное время, но джинн снова к нашим услугам и готов вступить в игру — трансформировать экономическую энергосистему и изменить к лучшему прежний порядок человеческой жизни. Если мы того пожелаем.

Попробуем объяснить.

Первые четыре десятилетия существования Интернета дали нам электронную почту, Всемирную паутину, доткомы, социальные сети, мобильный Интернет, большие данные, облачные вычисления и начало эпохи Интернета вещей. Все это позволило сократить стоимость поиска информации, совместной работы и обмена информацией. Снизились барьеры для выхода на рынок новых медиа и развлечений, новых форм торговли и организации труда, инновационных цифровых предприятий. Благодаря сенсорной технологии стали «умными» наши бумажники, одежда, автомобили, дома, города, даже наши тела. Окружающая среда настолько насыщена всем этим, что скоро мы перестанем «выходить в сеть», а будем просто жить и работать, постоянно погруженные во всепроникающую технологию.

Все восклицают как один: «Вот оно — великое открытие, которого мы ждали!

В целом Интернет привел к большому числу положительных изменений — для тех, у кого есть доступ к сети, — но возможности коммерческой и экономической деятельности в сети значительно ограниченны. «Нью-Йоркер» может сегодня перепечатать без изменений комикс Питера Стайнера 1993 года, где одна собака говорит другой: «В Интернете никто не знает, что я пес». В сети мы по-прежнему не имеем возможности безошибочно установить личность другого человека и доверять друг другу, чтобы переводить и обменивать деньги без подтверждения от третьей стороны — банка или государства. Эти же посредники ради собственной выгоды и национальной безопасности собирают наши личные данные и наблюдают за нашей частной жизнью. Даже в эпоху Интернета их ценовая структура исключает из всемирной финансовой системы около 2,5 миллиарда человек. Несмотря на перспективы равноправного мира, экономические и политические выгоды распределяются несимметрично: новые полномочия и деньги получают те, кто уже ими обладает, даже если перестали что-либо для этого делать. Деньги сейчас зарабатывают больше денег, чем многие люди.

Технологические достижения сами по себе не приносят денег, так же как и не уничтожают частной жизни. Однако в цифровую эпоху технология оказывается в центре любых изменений, как к лучшему, так и к худшему. Она позволяет нам уважать и нарушать права друг друга множеством новых способов. Бум сетевого общения и онлайн-торговли создает новые возможности для киберпреступности. Закон Мура, который гласит, что каждый год мощность вычислений удваивается, удваивает и возможности фальсификаторов и воров («преступников Мура»[1]), не говоря уже о спамерах, похитителях личной информации, фишерах, шпионах, зомби-фермерах, хакерах, киберзапугивателях, вымогателях (берут данные в заложники и с помощью специального программного обеспечения требуют выкуп) и так далее, и так далее.

В поисках доверительного протокола

Еще в 1981 году изобретатели пытались решить проблемы Интернета, связанные с защитой частной жизни, безопасностью и взаимовключенностью, с помощью шифрования. Но, как ни менялась конструкция процесса, возможность утечек всегда оставалась, поскольку в нем участвовали третьи стороны. Оплата карточкой через Интернет была ненадежной: пользователям приходилось предоставлять слишком много личной информации, а стоимость транзакций была слишком высока для небольших платежей.

В 1993 году выдающийся математик по имени Дэвид Чаум предложил eCash — систему цифровых платежей, «технически совершенный продукт, который позволил безопасно и анонимно проводить оплату через Интернет… Она идеально подходила для того, чтобы переводить по сети электронную мелкую монету»[2]. Система оказалась настолько хороша, что Microsoft и другие компании предполагали встроить eCash в собственное программное обеспечение[3]. Однако покупателей в сети тогда не волновала безопасность данных и транзакций. Нидерландская компания Чаума DigiCash обанкротилась в 1998 году.

Примерно в это же время один из коллег Чаума, Ник Сабо, написал небольшую статью под названием «Протокол Бога», обыгрывая словосочетание «частица Бога», предложенное нобелевским лауреатом Леоном Лендерманом для описания важности бозона Хиггса в современной физике. Сабо размышлял о создании всеобъемлющего технологического протокола, в котором Бог выступал бы надежной третьей стороной в любой транзакции: «Все стороны отправляют свои исходящие данные Богу. Бог достоверно определяет результаты и возвращает сторонам входящую информацию. Поскольку Бог всегда

хранит тайну исповеди, ни одна из сторон не узнает об исходящих данных других сторон больше, чем способна понять из собственных исходящих и входящих данных»[4]. С ним трудно не согласиться: бизнес в Интернете требует веры. Так как инфраструктура не обладает необходимым уровнем безопасности, у нас зачастую не остается выбора, за исключением того, чтобы положиться на посредников, как на богов.

Десять лет спустя, в 2008 году, рухнула мировая финансовая система. Возможно, как раз кстати некто под псевдонимом «Сатоси Накамото» описал новый протокол для системы прямых электронных расчетов с помощью криптовалюты под названием «биткойн». Криптовалюта (или цифровая валюта) отличается от традиционных валют, поскольку не создается и не контролируется ни одним государством. Этот протокол установил ряд правил — в виде распределенных вычислений, — которые обеспечивали *целостность* информации, передаваемой между миллиардами устройств напрямую, *без обращения к надежной третьей стороне*. Это незначительное на первый взгляд нововведение стало искрой, взбудоражившей и перепугавшей весь мир информационных технологий и покорившей его воображение. Из этой искры разгорелся пожар в коммерческом секторе и госуправлении; повсюду о ней заспорили защитники частной жизни, активисты социального развития, теоретики медиа и журналисты и многие другие.

«Все восклицают как один: «Вот оно — великое открытие, которого мы ждали! — говорит Марк Андреессен, один из создателей первого коммерческого веб-браузера Netscape и венчурный инвестор в области технологий. — Он решил все проблемы, дайте ему Нобелевскую премию, это гений!» Вот оно — распределенная сеть, основанная на доверии, которой так долго не хватало Интернету»[5].

Сегодня дальновидные специалисты по всему миру размышляют, к чему ведет нас новый протокол, который позволяет простым смертным верить друг другу благодаря продуманному коду. История не знает ничего подобного: надежные транзакции напрямую между двумя и более сторонами, проверяемые и подтверждаемые общими усилиями массы участников и управляемые личными интересами всего коллектива, а не контролируемые крупными корпорациями, которые гонятся за прибылью.

Возможно, этот протокол не назвать Всемогущим, но надежная глобальная платформа для наших транзакций — это нечто грандиозное. Мы называем ее Доверительный протокол.

Этот протокол лежит в основе всевозрастающего числа всемирных распределенных регистров, так называемых блокчейнов (или цепочек блоков), крупнейшим среди которых является биткойн. За сложной

технологией и неблагозвучным словом стоит, однако, простая идея. Блокчейны позволяют нам пересылать деньги безопасно и напрямую от меня к вам, минуя банк, эмитента кредитных карт или PayPal.

Это уже не Интернет информации, но Интернет ценностей или Интернет денег. А еще это платформа, позволяющая всем и каждому знать правду — по крайней мере в том, что касается структурированной фиксированной информации. Говоря совсем упрощенно, это открытый исходный код: любой может свободно его загрузить и использовать, а также разработать на его основе новые инструменты для управления сетевыми транзакциями. Таким образом, в нем заключен потенциал для создания бесчисленных новых приложений и нераскрытых пока возможностей, которые способны изменить очень и очень многое.

Как работает этот глобальный регистр

Крупные банки и некоторые государственные структуры пользуются «блокчейном» или даже просто «блокчейн» как распределенными регистрами, чтобы радикально изменить способ хранения информации и осуществления транзакций. Они преследуют похвальные цели: повышение скорости и безопасности, снижение стоимости, уменьшение числа ошибок, устранение центральных точек уязвимости и отказа. Эти модели не обязательно применяют криптовалюты для осуществления платежей.

Однако наиболее значимые и перспективные блокчейны основаны на модели биткойна Сатоси. Как же они работают?

Биткойн, как и любая другая цифровая валюта, не хранится где-либо в файле; он представлен транзакциями, записанными в блокчейне, подобно некому всемирному гроссбуху или таблице, где ресурсы большой одноранговой сети биткойна используются для подтверждения и одобрения каждой транзакции с использованием биткойна. Любой блокчейн, использует ли он биткойн или нет, является *распределенным*: он работает на компьютерах добровольцев по всему миру, так что у него нет центральной базы данных, которую можно было бы взломать. Блокчейн *публичен*: любой может просматривать его в любой момент, так как он расположен в сети, а не в какой-либо организации, которая занимается аудитом транзакций и их учетом. Блокчейн *зашифрован*: в нем используется мощная система шифрования, применяющая публичные и частные ключи (нечто вроде системы двух ключей для банковской ячейки) для обеспечения виртуальной безопасности. Не нужно беспокоиться о слабых брандмауэрах огромной сети супермаркетов или недобросовестном сотруднике финансовой корпорации или госучреждения.

Каждые десять минут в сети биткойна бьется пульс: все проведенные транзакции проверяются, получают одобрение и сохраняются в блоке, соединенном с предыдущим, образуя таким

образом цепь. Каждый блок действителен только тогда, когда соотнесен с предыдущим. Эта структура ставит перманентный отпечаток времени на каждый обмен ценностями и сохраняет информацию о нем, что не позволяет никому внести изменения в регистр. Чтобы украсть один биткойн, придется в открытую, у всех на глазах, переписать всю его историю в блокчейне. А это практически невозможно. Таким образом, блокчейн — это распределенный регистр, в котором отражено общее представление сети о каждой транзакции, когда-либо осуществленной. Подобно Всемирной паутине информации, этот Всемирный регистр ценностей — распределенный регистр, который любой может загрузить и запустить у себя на компьютере.

Некоторые ученые утверждают, что изобретение двойной бухгалтерии обусловило становление капитализма и национальных государств. Новый цифровой регистр экономических транзакций можно запрограммировать на сохранение практически любой ценной и важной для человечества информации: свидетельств о рождении, браке и смерти, прав собственности, дипломов о высшем образовании, финансовых отчетов, медицинских карт, обращений за страховыми выплатами, голосов на выборах, происхождения продуктов — любых сведений, которые могут быть представлены в виде кода.

Новая платформа позволяет в реальном времени объединить цифровые сведения практически обо всем на свете. Более того, в ближайшем будущем миллиарды умных устройств в материальном мире будут воспринимать и передавать изменения, реагировать на них, покупать электроэнергию для обеспечения своих нужд и распространять важную информацию и полностью возьмут на себя самые разные задачи: от охраны окружающей среды до заботы о нашем здоровье. Этому «Интернету всего» нужен «регистр всего». Бизнесу, торговле и экономике требуется цифровое счисление.

Как это относится лично к вам? Мы убеждены, что правда *способна* освободить нас и что распределенное доверие окажет значительное влияние на человека во всех сферах жизни. Может быть, вы меломан, который хочет помочь музыкантам зарабатывать на своем творчестве. Ответственный потребитель, который хочет узнать, откуда на самом деле поступило мясо для его бифштекса. Иммигрант, которому надоело переплачивать за денежные переводы семье на далекую родину. Женщина из Саудовской Аравии, которая мечтает издавать собственный модный журнал. Гуманитарный работник, которому нужно определить собственников земельных владений, чтобы восстановить дома, разрушенные землетрясением. Гражданин, который хочет, чтобы деятельность политиков стала прозрачна и подотчетна. Пользователь социальной сети, который ценит свою частную жизнь и считает, что вся информация, которую он генерирует, может принести материальную выгоду — ему самому. В эту самую

минуту новаторы создают приложения на основе блокчейна именно для этих целей. И это только начало.

Рациональный энтузиазм по поводу блокчейна

Конечно, технология блокчейна влечет за собой глубокие изменения во многих институтах общества. Этим объясняется повышенный интерес к ней со стороны многих интеллектуальных и влиятельных людей. Бен Лоски покинул пост суперинтендента финансовой службы штата Нью-Йорк, чтобы открыть собственную компанию в этой сфере. Он говорит: «Через пять-десять лет финансовая система может измениться до неузнаваемости… и я хочу быть в центре этих изменений»[6]. Блайт Мастерс, бывший директор по финансам и руководитель сырьевого центра в инвестиционном банке JPMorgan, основала стартап в области технологий, ориентированных на блокчейн, чтобы изменить всю отрасль. На обложке журнала Bloomberg Markets за октябрь 2015 года поместили фотографию Мастерса с заголовком «За блокчейном будущее». Журнал The Economist в том же месяце опубликовал редакционную статью «Машина доверия», в которой утверждалось, что «технология биткойна способна изменить принципы функционирования экономики»[7].

По мнению авторов, технология блокчейна — это «гигантская цепь уверенности во всем». Банки по всему миру для исследования новых возможностей собирают команды высококлассных специалистов (в том числе легендарных техно-гиков). Банкиров привлекает идея надежных и моментальных транзакций без издержек, но при этом пугают открытость, децентрализация и новые виды валюты. Отрасль финансовых услуг уже переименовала и присвоила технологию блокчейна, окрестив ее *технологией распределенного регистра*, пытаясь объединить преимущества биткойна — надежность, скорость и экономичность — с полностью замкнутой системой, которая требует разрешения банка или финансовой организации. Для них блокчейны — это всего лишь более надежные базы данных, которые позволят ключевым заинтересованным лицам (покупателям, продавцам, ответственным хранителям ценностей, регулирующим госорганам) вести общие нестираемые записи, тем самым снижая затраты, расчетные риски и устраняя центральные проблемные точки.

Начинается инвестирование в блокчейн-стартапы, как в свое время (в 1990-е) в доткомы, впрочем, об энтузиазме нынешних венчурных инвесторов доткомы девяностых не могли и мечтать. Только за 2014 и 2015 годы венчурный капитал направил более 1 млрд. долларов США в развивающуюся экосистему блокчейна, и с каждым годом объем инвестиций увеличивается почти вдвое[8]. «Мы вполне убеждены, —

сказал Марк Андреессен в интервью «Уошингтон пост», — что через 20 лет мы здесь будем говорить о [технологии блокчейна] так же, как сейчас говорим об Интернете»[9].

Регулирующие госорганы также активизировались, исследуя перспективы и саму возможность законодательного регулирования этой технологии. Авторитарные режимы, как в России, запрещают или строго ограничивают применение биткойна, как и некоторые демократические государства (например, Аргентина), которым следовало бы обратить внимание на эту технологию, учитывая исторические кризисы национальной валюты. Более дальновидные западные правительства прилагают значительные усилия к тому, чтобы понять, как новая технология способна изменить не только централизованную банковскую систему и природу денег, но и государственное управление и саму природу демократии. Кэролин Уилкинс, первый заместитель управляющего Банком Канады, считает, что мировым центробанкам пора серьезно исследовать возможность перехода национальных валютных систем на цифровые деньги. Ведущий экономист Банка Англии Эндрю Холдейн предлагает ввести в Великобритании национальную цифровую валюту[10].

Времена кружат голову. Конечно, среди растущего числа энтузиастов немало оппортунистов, спекулянтов и преступников. Первое, что многие слышат о цифровых валютах, — это история банкротства биржи Mt Gox или дело Росса Уильяма Улбрихта, основателя черного сетевого рынка «Шелковый путь», где осуществлялся оборот наркотиков, детской порнографии и оружия, а в качестве платежной системы использовался биткойновый блокчейн. Стоимость биткойна подвержена резким колебаниям, и владение биткойнами по-прежнему сконцентрировано. Исследование 2013 года показало, что половиной мирового запаса биткойнов владеет 937 человек, хотя к настоящему времени наблюдаются иные тенденции[11].

Как же перейти от порнографии и финансовых пирамид к всеобщему благоденствию?

Для начала нужно отметить, что предмет этой книги — не биткойн (этот актив, пока что довольно спорный, должен вас интересовать, только если вы играете на бирже), а нечто гораздо большее: возможности и потенциал стоящей за ним технологической платформы.

Это не означает, что биткойн и криптовалюты сами по себе не имеют значения, как предполагают те, кто стремится разорвать всякие связи своих проектов с прежними скандальными предприятиями. Эти валюты критически значимы для блокчейн-революции, которая прежде

всего строится на прямом обмене ценностями, в особенности деньгами.

Как доверять в цифровую эпоху

Доверие в бизнесе — это ожидание, что другая сторона будет действовать в соответствии с четырьмя принципами деловой этики: честностью, взаимным учетом интересов, ответственностью и прозрачностью [12].

Честность — уже не только этическая характеристика, но и экономическая. Чтобы выстроить доверительные отношения с сотрудниками, партнерами, клиентами, акционерами и общественностью, общение организации с ними должно быть правдивым, точным и полным: никакой лжи через умолчание, никакой маскировки истины усложнением.

Взаимный учет интересов в бизнесе часто означает честный обмен благами и невыгодами, который стороны осуществляют сознательно. Но доверительные отношения предполагают также искреннее уважение к чужим интересам, пожеланиям и чувствам и благожелательность обеих сторон.

Ответственность означает взятие на себя четких обязательств перед участниками и их выполнение. Как частные предприниматели, так и компании должны ясно показать, что выполняют свои обязательства и берут на себя ответственность за нарушенные обещания, и желательно показать это таким образом, чтобы это могли проверить сами участники или независимые внешние эксперты. Никакого перевода стрелок и поиска виноватых.

Прозрачность — это деятельность в открытую. Когда появляется вопрос «Что они скрывают?», это значит, что прозрачности нет, и тогда возн икает недоверие. Конечно, у компаний есть законное право хранить коммерческую тайну и другую закрытую информацию, но, когда речь идет о сведениях, важных для клиентов, акционеров, сотрудников и других заинтересованных лиц, в обеспечении доверия главную роль играет активная открытость. Успех определяется не нарядами, а их отсутствием.

Доверие в бизнесе и других общественных институтах почти везде сейчас достигло исторического минимума. Составленный компанией по связям с общественностью Edelman «Барометр доверия» за 2015 год показывает, что доверительность отношений в общественных институтах, особенно в корпорациях, снизилась до уровня экономического кризиса 2008 года. Эдельман отмечает, что даже безупречные когда-то высокие технологии — сектор экономики, до сих пор пользующийся самым большим доверием — в ряде стран впервые показали негативную тенденцию. В целом по миру генеральные директора компаний и высшие государственные чиновники

пользуются наименьшим доверием как источники информации, и далеко позади научных деятелей и отраслевых экспертов [13].

Опрос о доверии различным общественным институтам, проведенный Gallup в США в 2015 году, показал, что «бизнес» находится на предпоследнем месте в списке из 15 типов институтов; менее 20 % респондентов отметили, что оказывают значительное доверие бизнесу. Хуже результат только у Конгресса США[14].

В мире до блокчейна доверие в транзакциях определялось тем, что частные лица, посредники или другие организации действовали этично. Поскольку зачастую мы не знаем лично другую сторону сделки, не говоря уже о возможности судить о ее благонадежности, мы привыкли, что некая третья сторона не только поручается за неизвестных нам участников сделки, но и берет на себя записи транзакции, бизнес-логику и логику транзакций, которыми определяется онлайн-торговля. Эти мощные посредники — банки, государственные учреждения, PayPal, Visa, Uber, Apple, Google и другие цифровые конгломераты — и получают львиную долю выгод (или выгоды).

В новом мире блокчейна доверие определяется сетью и даже отдельными ее элементами. Карлос Морейра из компании криптобезопасности WISeKey отмечает, что новые технологии фактически делегируют доверие, в том числе к неживым материальным объектам. «Если предмет, будь то сенсор на вышке сотовой связи, электрическая лампочка или пульсомер, не пользуется доверием — то есть его качество работы или то, что он оплатит услугу, не гарантируется, — он будет автоматически отвергнут другими элементами сети»[15].

Сам регистр становится залогом доверия[16].

Необходимо прояснить, что «доверие» в данном контексте касается покупки и продажи товаров и услуг и целостности и безопасности информации, а не доверия в широком смысле во всех бизнес-процессах. Однако из данной книги вы узнаете, как глобальный регистр достоверной информации способен обеспечить соблюдение честности (либо этических принципов) всеми нашими общественными институтами и помочь нам создать более безопасный и заслуживающий доверия мир. На наш взгляд, компании, которые осуществляют некоторые или все свои транзакции на блокчейн, пользуются большим доверием, что скажется на стоимости их акций. Акционеры и граждане скоро будут ждать от всех компаний, публично размещающих акции, и учреждений, финансируемых из налоговых сборов, что в блокчейне будет по меньшей мере их казначейство. С ростом прозрачности инвесторы смогут увидеть, заслуживает ли гендиректор своего огромного бонуса. Смарт-контракты,

обеспеченные с помощью блокчейнов, обяжут участников исполнять взятые на себя обязательства, а избиратели смогут оценить, честны ли народные избранники и как расходуют средства.

Возвращение Интернета

Первая эпоха Интернета началась с энергией и энтузиазмом юного Люка Скайуокера — с убежденностью в том, что любой мальчишка с пустынной планеты на окраине Галактики способен повергнуть злую империю и положить начало новой цивилизации, основав свой дотком. Конечно, это наивная позиция, но многие, включая авторов, надеялись, что Интернет, воплощенный во Всемирной паутине, изменит индустриальный мир, где власть держалась в цепких руках меньшинства; во властные структуры было трудно проникнуть и еще труднее их опрокинуть. В отличие от старых средств массовой информации — централизованных и жестко контролируемых сверху, с инертными пользователями, — новые медиа оказались распределенными и нейтральными, и каждый мог стать активным участником, а не только пассивным потребителем. Низкая стоимость и массовая прямая коммуникация посредством Интернета должны были подкосить традиционные иерархии и помочь жителям развивающихся стран включиться в глобальную экономику. Ценность и репутация должны были создаваться качеством вклада человека в дело, а не его статусом. Перед умным и трудолюбивым человеком из индийской глубинки открывался весь мир — более «плоский», гибкий, переменчивый. А главное, новая технология должна была позволить каждому достичь благосостояния, а не умножить богатства небольшой верхушки.

Кое-что из этого осуществилось. Появились такие проекты, как Wikipedia, Linux, Galaxy Zoo, созданные массовыми усилиями. Аутсорсинг и сетевые бизнес-модели позволили жителям развивающихся стран активнее участвовать в глобальной экономике. Два миллиарда людей сегодня сотрудничают на равных. Мы получаем новые, беспрецедентные способы доступа к информации.

Но Империя нанесла ответный удар. Очевидно, что власть, сосредоточенная в бизнесе и госуправлении, подчинила своей воле исходную, демократическую архитектуру Интернета.

Огромные учреждения теперь держат в собственности и контролируют эти новые средства производства и социального взаимодействия — структуру в основе Интернета, богатейшие и все увеличивающиеся залежи информации, алгоритмы, которые все больше управляют бизнесом и повседневной жизнью, мир приложений, необыкновенные возможности, такие как машинное обучение и самоуправляемые автомобили. От Кремниевой долины и Уолл-стрит до Шанхая и Сейла эта новая аристократия пользуется своими преимуществами собственника, чтобы с помощью

удивительнейшей технологии, призванной обеспечить экономическое равенство, скопить огромные личные состояния и укрепить свою власть над экономикой и обществом.

Многие мрачные прогнозы первых пионеров цифрового века сбылись[17]. Рост ВВП не сопровождается ростом занятости в большинстве развитых стран. Вместе с увеличением производства благ увеличивается и социальное неравенство. Флагманы технологии перевели большую часть своей деятельности из открытого, распределенного, уравновешивающего пространства Всемирной паутины в закрытые и надежно огражденные сетевые «садики» или приложения в собственном формате, открытые «только для чтения», где невозможен, в частности, диалог. Корпоративные силы захватили множество замечательных открытых, демократических технологий прямого общения и пользуются ими, чтобы извлекать несоразмерные доли прибыли.

Результат, если о нем вообще можно говорить, состоит в том, что экономическая мощь стала более концентрированной, более сосредоточенной и изолированной. Информация, вместо того чтобы распространяться без ограничений, накапливается и эксплуатируется все меньшим числом заинтересованных лиц, которые пользуются ею, чтобы контролировать и приобретать еще больше власти. Накопление информации и сопутствующей ей власти позволяет еще более укрепить свое положение, производя знания «в собственном формате». А эта привилегия настолько выгодна, что можно и закрыть глаза на ее происхождение.

Мощные «цифровые конгломераты», такие как Amazon, Google, Apple и Facebook (сами когда-то начинавшие как интернет-стартапы), захватывают золотые жилы информации, которую генерируют население и организации в изолированных информационных хранилищах, а не во Всемирной паутине. Хотя эти организации создают огромную ценность для потребителей, в результате данные становятся активом нового класса, который, возможно, превзойдет все другие типы активов. Другое последствие — разрушение традиционных концепций частной жизни и автономности каждой личности.

Все государства пользуются Интернетом, чтобы лучше функционировать и совершенствовать свои услуги, но теперь также обращаются к технологиям, чтобы следить за гражданами и даже манипулировать ими. Во многих демократических странах государство пользуется информацией и технологиями коммуникации, чтобы шпионить за населением, влиять на общественное мнение, продвигать собственные интересы, ограничивать права и свободы и в целом оставаться у власти как можно дольше. Репрессивные режимы —

например, в Китае и Иране — ограничивают Интернет и пользуются им, чтобы бороться с инакомыслием и мобилизовать население на достижение государственных целей.

Однако это не означает, что Всемирной паутине пришел конец, как утверждают некоторые. Веб критически важен для будущего цифрового мира, и мы должны поддерживать глобальные инициативы по его защите, такие как Глобальный Интернет-Фонд, который борется за то, чтобы Интернет оставался открытым, нейтральным и постоянно развивался.

Репрессивные режимы — например, в Китае и Иране — ограничивают Интернет и пользуются им, чтобы бороться с инакомыслием и мобилизовать население на достижение государственных целей.

Теперь технология блокчейна открыла целый спектр новых возможностей, способных обратить вспять все эти негативные тенденции. Появилась настоящая платформа без посредников, которая позволяет реализовать множество увлекательных вещей, о которых мы рассказываем в этой книге. Каждый может быть собственником своих персональных данных. Каждый может осуществлять транзакции, создавать и передавать ценности без участия посредников, которые берут на себя определение цен и информации. Миллиарды людей, остающихся вне мировой экономики, скоро смогут в нее войти. Мы способны защитить свою частную жизнь и монетизировать собственную информацию. Мы можем обеспечить создателям интеллектуальной собственности достойное вознаграждение. Вместо того чтобы пытаться решить проблему растущего социального неравенства перераспределением благ, мы можем изменить сам способ их распределения, причем с самого момента создания этих благ: люди по всему миру, от музыкантов до фермеров, смогут априори более полноценно участвовать в делении благ, которые создают. Здесь мы ничем не ограничены.

Это больше похоже на мастера Йоду, нежели на Бога. Однако этот новый протокол, пусть он и не божествен, позволяет сотрудничать на основе взаимного доверия в мире, где это необходимо. А это немалый уже для радости повод.

Ваш аватар и «черный ящик» идентичности

На протяжении истории человечества каждая новая форма передачи информации помогала нам преодолевать время, пространство и смертность. Эта, с позволения сказать, божественная способность неизбежно приводит вновь к экзистенциальному вопросу идентичности: кто мы? Что значит быть человеком? Как мы себя концептуализируем? Как отмечал Маршалл Маклюэн, со временем средство передачи информации само превращается в сообщение. Люди формируют медиа и сами в свою очередь ими формируются.

Адаптируется наш мозг. Адаптируются наши институты. Адаптируется общество.

«Сегодня, чтобы получить идентифицирующий документ, будь то банковская карта, кредитка или дисконтная карта авиакомпании, вам нужна уполномоченная организация»[18], -говорит Карлос Морейра из WISeKey. Родители дают вам имя, сертифицированный акушер фиксирует ваш рост и вес, наконец, оформляется свидетельство о рождении, где указаны место и время вашего появления на свет. Теперь этот документ можно загрузить в блокчейн, привязать к нему специальный счет для оплаты высшего образования и разослать оповещения о прибавлении в семействе. Друзья и родные смогут перевести на него биткойны, чтобы финансировать ваше обучение. Начинается ваш поток информации.

В первые дни Интернета Том Питерс писал: «Вы — это ваши проекты»[19], имея в виду, что корпоративная принадлежность и должность уже не определяют человека. Сейчас точно так же можно утверждать: «Вы — это ваши данные». Проблема в том, что, как говорит Морейра, «идентичность теперь принадлежит вам, однако данными, которые создаются в ходе ее взаимодействия с миром, владеете не вы»[20]. Так вас видят большинство корпораций и институтов — по инверсионному следу ваших данных в Интернете. Они агрегируют информацию в некое виртуальное представление человека и затем предоставляют этому «виртуальному я» необыкновенные новые преимущества, о которых поколение его родителей не могло и мечтать[21]. Но за это удобство нужно платить — неприкосновенностью частной жизни. Неправы те, кто говорят: «С частной жизнью покончено, смиритесь с этим»[22]. Частная жизнь — это основа свободного общества.

«Многие воспринимают самоидентификацию очень упрощенно [23]", — говорит блокчейн-теоретик Андреас Антонопулос. Словами «идентичность», «личность», «персона» мы описываем себя, проекцию своей личности в мир и все параметры, связанные с личностью и ее проекциями. Одними мы наделены от природы, другие присваивают нам государство и различные организации. У каждого из нас одна или несколько ролей, каждой из которых соответствует набор параметров, причем роли могут меняться. Подумайте о своей работе. Менялась ли ваша роль органично, когда менялись выполняемые задачи или когда уточнялась ваша должностная инструкция?

Представьте теперь, что ваше «виртуальное я» фактически принадлежит вам, являясь чем-то вроде личного аватара, и «обитает» в закрытом от постороннего вмешательства «черном ящике» вашей

идентичности, так что вы способны монетизировать свой поток данных и обнародовать только ту информацию о себе, которая требуется для осуществления того или иного права. Зачем на вашем водительском удостоверении указывать какие-либо сведения помимо того, что вы сдали экзамен и продемонстрировали умение управлять автомобилем? Вообразите себе новую эпоху Интернета, где ваш личный аватар управляет содержимым вашего «черного ящика» и охраняет его. Ваш верный программный слуга выдает только необходимые данные в установленном объеме для каждой ситуации и одновременно подбирает за вами крошки информации, которые остаются на вашем пути в цифровом мире.

Может показаться, что это научная фантастика наподобие «Матрицы» или «Аватара». Однако сегодня технологии блокчейна делают это реальностью. Джо Лубин, генеральный директор Consensus Systems, называет эту концепцию «постоянным цифровым удостоверением личности и электронной персоной» в блокчейне. «Университетским друзьям я демонстрирую вовсе не ту часть своей личности, что Федеральному резерву, — говорит он. — В сетевой цифровой экономике я буду представлен несколькими сторонами своей личности. Я буду действовать в этом мире посредством разных электронных персон». Лубин отмечает, что ему потребуется «юридическая персона», которая будет платить налоги, получать займы, оформлять страховку. «Вероятно, у меня будет бизнес-персона и домашняя персона, чтобы разграничить аспекты, которые я решу связать со своей юридической персоной. Возможно, у меня будет персона-геймер, которую я предпочел бы изолировать от бизнес-персоны. Или даже персона в темной сети, у которой никогда не будет связей с другими моими персонами»[24].

В вашем черном ящике будут храниться удостоверение личности гражданина, номер социального страхования, медицинские сведения, номера банковских счетов, документы об образовании, история трудоустройства и другие официальные данные — и личная информация (например, сексуальные предпочтения или хронические заболевания), которую вы не обнародуете, но желаете монетизировать ее ценность, допустим, в исследованиях или опросах. Вы сможете лицензировать использование этих данных для конкретных целей, конкретными лицами и в конкретный период. Окулисту вы будете посылать один набор сведений, инвестиционному фонду — другой. При этом аватар сможет, не раскрывая вашей личности, отвечать на закрытые вопросы: «Есть ли вам 21 год?», «Ваш ежегодный доход за

последние три года превышает 100 000 долларов?», «Ваш индекс массы тела в норме?»[25]

Может показаться, что это научная фантастика наподобие «Матрицы» или «Аватара». Однако сегодня блокчейн делает это реальностью.

В материальном мире ваша репутация ограничена территориально: у работодателя, у продавца в местном магазине, у друзей есть определенное мнение о вас. В цифровой экономике репутация всех электронных персон в вашем аватаре станет мобильной. Мобильность позволит любому, независимо от места жительства, стать участником цифровой экономики. Житель Африки с цифровым бумажником и аватаром сможет заслужить себе репутацию, чтобы, к примеру, взять займ на открытие своего дела. «Видите, все эти люди меня знают и готовы за меня поручиться. Я финансово надежен. Я обладающий политическими правами гражданин всемирной цифровой экономики».

Идентичность — лишь малая часть этой концепции. Остальное — это облако, облако идентичности, состоящее из элементов информации, прочно или гибко привязанных к вашей электронной персоне. Если мы попытаемся все это записать в блокчейн, в наш неизменяемый регистр, мы лишимся не только тонкостей социального взаимодействия, но и права на забвение. Нельзя человека судить по худшим его проявлениям.

План всеобщего благополучия

В этой книге вы встретите десятки историй об инициативах, которые сделал возможным доверительный протокол, создающий новые возможности для благополучия в мире. Благополучие — это прежде всего хороший уровень жизни. Чтобы достичь его, человеку нужны средства и возможности для создания материальных благ и экономического процветания. Но для нас это означает гораздо больше: это личная безопасность, здоровье, образование, состояние окружающей среды, возможность формировать и контролировать свою судьбу и участвовать в экономической и общественной жизни. Чтобы преуспевать, человеку нужны как минимум доступ к базовым финансовым услугам в той или иной форме, чтобы надежно хранить и перемещать ценности, возможность передачи информации, средства осуществления транзакций, чтобы войти во всемирную экономику, безопасность и защита прав собственности на землю и другие материальные активы[26]. Все это и многое другое нам может дать блокчейн. Истории в этой книге покажут вам будущее, где благополучие доступно каждому, а не только уже обладающим богатством и властью и стремящимся их приумножить. В этом будущем, возможно, мы будем владеть собственными данными и

защищать нашу частную жизнь и личную безопасность. Это будет открытый мир, где любой сможет внести свой вклад в общую технологическую инфраструктуру, а не обнесенные стеной «плантации» крупных компаний, разрабатывающих пр иложения в собственном формате. Это будет мир, где миллиарды людей получат возможность участвовать в мировой экономике и пользоваться ее преимуществами. Что предстоит для этого сделать?

Создать настоящую прямую («Peer-to-Peer» или «без посредников») экономику совместного потребления

Современные теоретики часто называют Airbnb, Uber, Lyft, TaskRabbit и т. д. платформами для «экономики совместного потребления». Это красивая идея: участники на равных создают ценности и пользуются ими. Но эти компании не имеют отношения к совместной работе. Более того, они успешны именно потому, что не работают совместно с поставщиками товаров и услуг — они только агрегируют их деятельность. Uber — корпорация с капиталом в 65 млрд долларов, которая агрегирует услуги водителей. Airbnb — любимое дитя Кремниевой долины с капиталом в 25 млрд долларов — агрегирует арендуемое жилье. Другие агрегируют оборудование и работников через централизованную закрытую платформу и затем перепродают их услуги. При этом они собирают данные для коммерческого использования. Этих компаний не существовало десять лет назад, потому что не было технических условий для этого: повсеместного распространения смартфонов, надежного GPS, сложных систем оплаты. Теперь, в эпоху блокчейна, появилась технология, которая позволит заново перестроить эти отрасли. Прорывным компаниям традиционного рынка самим грозит разрушение.

Представьте себе, что на смену централизованной компании Airbnb приходит распределенное приложение — пусть будет блокчейн-Airbnb, или bAirbnb, — которое по сути является кооперативом, принадлежащим всем его участникам. Когда арендатор ищет помещение, программное обеспечение bAirbnb просматривает содержимое блокчейна, находит все предложения и демонстрирует пользователю те, что соответствуют заданному фильтру. Так как сеть записывает информацию о транзакции в блокчейн, положительный отзыв пользователя повышает репутацию и арендатора, и арендодателя и устанавливает их личности — но теперь без посредника. Виталик Бутерин, основатель блокчейна Ethereum, говорит: «В то время как большинство технологий направлены на автоматизацию повседневной деятельности второстепенных (или вспомогательных) работников, блокчейн автоматизирует и делает ненужным суть сложившихся

вещей. Вместо того чтобы вытеснить с рынка водителя такси, блокчейн вытесняет Uber и позволяет таксисту взаимодействовать напрямую с клиентом»[27].

Преобразовать финансовую систему, сделав ее более быстродействующей и взаимовключающей

Отрасль финансовых услуг движет всемирную экономику, но сегодняшняя система источена проблемами. Во-первых, это, по некоторым данным, наиболее централизованная отрасль во всем мире и наиболее консервативная по отношению к технологическим инновациям. Бастионы старого финансового порядка, такие как банки, всеми силами стараются защищать монополии и нередко препятствуют революционным технологическим изменениям. Финансовая система работает по устаревшим технологиям и по правилам девятнадцатого столетия. Она изобилует противоречиями и неравномерно развита, а потому иногда бывает медленна, часто ненадежна и по большей части непрозрачна для многих заинтересованных лиц.

Технология распределенного регистра способна освободить многие финансовые услуги от оков старых институтов, стимулировать конкуренцию и обновление. Это выгодно конечному пользователю. Даже соединение со старым Интернетом не позволяет миллиардам людей включиться в экономику по той простой причине, что финансовые институты не предоставляют им банковских и иных услуг. Для институтов это клиенты, не приносящие большой выгоды, обслуживание которых связано с большими рисками. Блокчейн даст таким людям не только возможность связываться друг с другом, но и, что более важно, — интегрироваться в финансовую деятельность: покупать, продавать, брать займы и в целом пользоваться возможностями преуспеть.

Давно зарекомендовавшие себя институты смогут модернизироваться с помощью технологии блокчейна, если в них найдутся лидеры, способные этим заняться. Эта технология обладает огромным потенциалом радикально изменить к лучшему всю отрасль — от банков до бирж, от страховых компаний до аудиторских фирм, маклеров, микрозаемщиков, кредитных систем, риелторов и так далее. Когда все пользуются одним и тем же распределенным регистром, урегулирование сделки осуществляется не за несколько дней, а мгновенно, у всех на виду. От этого выиграют миллиарды людей, и такое изменение даст свободу действий и полномочия предпринимателям по всему миру.

Защищать экономические права по всему миру

Право собственности настолько неразрывно связано с системой капиталистической демократии, что в первой версии Декларации

независимости США Томас Джефферсон указал как неотчуждаемые права человека на жизнь, свободу и стремление к собственности (а не к счастью)[28]. Хотя эти вдохновляющие принципы заложили основу современной экономики и общества, которой пользуется почти весь развитый мир, ее преимущества до сих пор недоступны немалой части мирового населения. Определенные успехи достигнуты в области жизни и свободы, но большинство собственников рискуют потерять свои дома или землю по злой воле коррумпированных чиновников — достаточно нажать кнопку в централизованной государственной базе данных о собственности. Не имея возможности подтвердить свои права на недвижимость, собственник не может получить кредит, разрешение на строительство или продать землю, а также рискует вовсе ее лишиться — все это серьезно препятствует процветанию.

Перуанский экономист и президент Института свободы и демократии Эрнандо де Сото, один из ведущих экономических мыслителей в мире, считает, что до пяти миллиардов человек в мире не имеют возможности полноценно приобщиться к ценностям, создаваемым глобализацией, поскольку обладают неподтвержденными правами собственности на недвижимость. Блокчейн, утверждает он, способен изменить положение. «Центральная идея блокчейна — возможность транзакций с правами на блага, будь то финансовые средства, материальные объекты или идеи. Задача не в том, чтобы просто зафиксировать участок земли, а в том, чтобы зафиксировать соответствующие права их обладателя, чтобы они не могли быть нарушены»[29]. Единая система прав собственности способна заложить основу для новой программы всемирного правосудия, экономического роста, благосостояния и мира. В этой новой парадигме права собственника защищают не солдаты, ополченцы или партизаны, а технология. «Блокчейн приведет к миру, который управляется реальными вещами, а не фикциями. И я считаю, что это хорошо» [30], - говорит де Сото. И этот мир децентрализован. Никакая центральная власть его не контролирует, все в курсе, что происходит, и все сохраняется в памяти навечно.

Положить конец поборам на денежные переводы

Практически любая статья, доклад или книга о преимуществах криптовалют освещает их возможности для денежных переводов. И не случайно. Самый большой приток денег в развивающиеся страны дают вовсе не гуманитарная помощь или иностранные инвестиции. Это переводы, отправляемые на родину от иностранных диаспор за рубежом. Это длительный процесс, медленный и не всегда

безопасный; однако каждую неделю миллионы людей отправляются в офисы компаний, занимающихся переводами (не всегда в благополучных районах), всякий раз заполняют одни и те же бумаги и платят комиссию в 7 %. Есть другой способ.

Abra и другие компании создают сети платежей на основе блокчейна. Цель Abra в том, чтобы каждый пользователь сам выполнял функции банковского служащего. Весь процесс — от отправки денег из одной страны до их поступления в другую — занимает час, а не неделю, и комиссия составляет 2 % вместо 7. Abra рассчитывает, что число пользователей ее сети платежей скоро превзойдет количество банкоматов во всем мире. Western Union понадобилось 150 лет, чтобы довести численность своих банковских служащих по всему миру до 500 тысяч. Abra охватит столько же человек за первый год своего существования.

Искоренить бюрократию и коррупцию в международной экономической помощи

Может ли блокчейн решить проблемы международной экономической помощи? Землетрясение в Гаити в 2010 году стало одним из наиболее разрушительных природных катаклизмов в истории. Погибли, по разным оценкам, от 100 000 до 300 000 человек. Руководство страны в итоге не справилось со своими обязанностями в этой ситуации. Всемирное сообщество пожертвовало более 500 млн долларов Красному Кресту — известной международной организации. Расследование выявило, что средства были израсходованы не по назначению или вовсе пропали.

Блокчейн способен усовершенствовать оказание международной помощи, устранив посредников, у которых оседают средства по пути. Во-вторых, будучи неизменяемым регистром, фиксирующим перемещение средств, блокчейн сделает институты подотчетными рядовому пользователю. Представьте, что вы можете проследить каждый доллар, который вы пожертвовали в Красный Крест, от начальной точки (на вашем смартфоне) до конечной — конкретного человека, которому помогли ваши деньги. Вы могли бы условно депонировать свои средства, чтобы новые суммы автоматически переводились, когда Красный Крест выполняет каждую из оговоренных задач, на которые собираются деньги.

В первую очередь платить создателям ценностей

Первое поколение Интернета не позволило многим создателям интеллектуальной собственности получить соответствующее вознаграждение. Прежде всего это коснулось композиторов и исполнителей, работавших со звукозаписывающими компаниями, руководители которых не представляли, как Интернет повлияет на музыкальную индустрию. Им не удалось воспользоваться преимуществами цифровой эпохи и перестроить свои бизнес-модели, и они постепенно уступили инновационным сетевым дистрибьюторам.

Представьте, что вы можете проследить каждый доллар, который вы пожертвовали в Красный Крест, от начальной точки (на вашем

смартфоне) до конечной — конкретного человека, которому помогли ваши деньги.

Вспомним, как крупные лейблы отреагировали на появление Napster — платформы децентрализованного обмена музыкальными файлами, запущенной в 1999 году. Лидеры музыкальной индустрии подали совместный иск против новой платформы, ее основателей и *восемнадцати тысяч пользователей*. В результате к июлю 2001 года платформа прекратила свое существование. Алекс Уинтер, режиссер документального фильма о Napster, отмечал в интервью «Гардиан»: «Я против черно-белого мышления, когда речь идет о масштабных культурных изменениях. Что касается Napster, там было множество оттенков серого между позициями «Я могу делиться всем, за что заплатил» и «Поделиться хотя бы одним купленным файлом — уже преступление»[31].

Мы согласны. Создавать нечто совместно с потребителями — обычно более жизнеспособная бизнес-модель, чем судиться с ними. История с Napster обратила внимание всего мира на музыкальную индустрию, обнажив ее устаревшие рыночные механизмы, огромную неэффективность дистрибуции и правила, ущемлявшие, как сочли некоторые, права музыкантов.

С тех пор мало что изменилось. Но теперь мы видим, как на основе блокчейна зарождается новая музыкальная экосистема, возглавляемая британской исполнительницей и автором песен Имоджен Хип, виолончелисткой Зоэ Китинг и многочисленными разработчиками и предпринимателями. Все направления культуры ждет переворот, который должен принести создателям культурных ценностей достойное и полное вознаграждение.

Трансформировать корпорацию в двигатель капитализма

С развитием глобальной пиринговой платформы, которая позволяет идентифицировать пользователя, устанавливать доверительные отношения, отслеживать репутацию и проводить транзакции, мы наконец сможем перестроить глубинную суть фирмы, чтобы обеспечить инновации, совместную деятельность и, возможно, даже общее благополучие, а не просто обогащение немногих. Речь не идет о фирмах с небольшим капиталом и незначительным влиянием на рынок. Напротив, мы имеем в виду компании двадцать первого века, в том числе с огромными прибылями, доминирующие на своих рынках. Мы убеждены, что предприятия будущего станут больше походить на сети, чем на вертикально интегрированные иерархии индустриальной эпохи. Таким образом, появится возможность распределять (а не перераспределять) прибыль более демократично.

Мы предлагаем задуматься и о многих других поразительных инновациях: о смарт-контрактах, новых независимых экономических посредниках и о так называемых распределенных автономных предприятиях, где умное программное обеспечение берет на себя функции управления и распределения ресурсов и возможностей, быть может, приходя на смену корпорациям. Смарт-контракты позволят создать то, что мы называем открытыми сетевыми предприятиями, основанными на новых бизнес-моделях (или же на старых, но с поправкой на блокчейн).

«Оживить» предметы и заставить их работать

Инженеры и фантасты давно предсказывали мир, в котором бесшовная глобальная сеть сенсоров, соединенных с Интернетом, сможет фиксировать любое событие, действие и изменение на планете. Технология блокчейн позволит предметам сотрудничать, обмениваться единицами ценностей — энергией, временем, деньгами — и перестраивать логистические цепочки и производственные процессы в соответствии с доступной им информацией о потребностях и возможностях всех элементов цепи. Уже сейчас умным устройствам можно присваивать метаданные и программировать их так, чтобы они распознавали другие предметы по их метаданным или определенным образом реагировали на заданные обстоятельства, причем без риска ошибки или постороннего вмешательства.

Материальный мир оживает, и это открывает каждому путь к успеху: от фермера в австралийской глубинке, которому нужно электричество для трудовой деятельности, до домовладельцев по всему миру, которые могут стать частью распределенной блокчейн-энергосети.

Воспитать блокчейн-предпринимателя

Предпринимательство жизненно важно для развития экономики и процветания общества. Интернет должен был освободить предпринимателей, предоставив им средства и возможности крупных компаний, но не их проблемы, такие как унаследованная культура, окостенелые рабочие процессы и тяжелый балласт прошлого. Однако громкие успехи доткомов, сделавших своих владельцев миллиардерами, маскируют неприятную истину: во многих развитых экономиках предпринимательство и появление новых компаний в последние тридцать лет переживают спад[32]. В развивающихся странах Интернет почти не снизил барьеры для потенциальных предпринимателей, которые вынуждены бороться с убийственными государственными бюрократиями. Интернет не дал и миллиардам людей доступа к финансовым инструментам, необходимым для начала

собственного дела. Конечно, не каждому суждено стать предпринимателем, но даже среднестатистическому человеку, пытающемуся достойно зарабатывать, мешают отсутствие финансовых инструментов и засилье государственных ограничений.

Это сложная проблема, но блокчейн во многом способен дать мощный заряд энергии предпринимательству и, соответственно, преуспеванию. Теперь, чтобы приобрести значимость и возможность вести деловую активность за пределами своего сообщества, среднему гражданину развивающейся страны необходимо только устройство, подключенное к Интернету. Доступ к глобальной экономике означает большую доступность источников кредитования и финансирования, поставщиков, партнеров и возможностей для инвестирования. Любой талант, любой ресурс, даже самый скромный, можно монетизировать на блокчейне.

Реализовать власть народа для народа

Готовьтесь к большим переменам и в госуправлении. Технология блокчейна уже радикально трансформирует механизмы государственного управления и дает возможность сделать их высокопроизводительными — более совершенными и дешевыми. Она также создает новые возможности для изменений в самой демократии, позволяя госуправлению стать более открытой, освободиться от лоббистского контроля и действовать в соответствии с четырьмя параметрами деловой этики. Уже сейчас видно, как технологии блокчейна могут изменить роль гражданина и его участие в политическом процессе: от голосования и доступа к социальным услугам до решения застарелых проблем общества и обеспечения ответственности избираемых политиков за их предвыборные обещания.

Что обещает и чем опасна новая платформа

Если в среднестатистическом городе шесть миллионов жителей[33], значит, существует шесть миллионов препятствий к тому, чтобы эта технология реализовала свой потенциал. Более того, есть целый ряд проблем, внушающих опасения. Одни говорят, что технология не готова к широкому внедрению, что она еще трудна в использовании и что она будет применяться во вред обществу. Другие критики указывают, что для достижения консенсуса в одной только сети биткойна требуется огромное количество энергии — а что же произойдет, когда тысячи, даже миллионы взаимосвязанных блокчейнов станут обрабатывать по миллиарду транзакций в день? Хватит ли положительной мотивации для того, чтобы люди участвовали в процессе и постоянно действовали безопасно, а не пытались обрушить сеть? Не приведет ли технология блокчейна к

самой крупной в истории потере рабочих мест наемными работниками?

Но это вопросы лидерства и управления, а не технологии. Первой эпохе Интернета положили начало стратегическое видение и общие интересы главных заинтересованных лиц — правительств, институтов гражданского общества, разработчиков и простых людей. Блокчейну нужны такие же убежденные лидеры. Далее мы подробно рассмотрим, почему лидерам новой распределенной парадигмы придется застолбить свои участки и инициировать волну экономических и институциональных инноваций, чтобы в этот раз добиться цели. Мы приглашаем вас войти в число этих лидеров.

Эта книга стала результатом исследовательской программы Global Solutions Network в Ротмановской школе менеджмента университета Торонто. Финансирование программы (4 млн долларов) поступило преимущественно от крупных технологических корпораций, фонда Рокфеллера, фонда Сколла, Госдепартамента США и Industry Canada. Эта инициатива исследовала новые подходы к решению мировых проблем и управлению. Мы оба участвовали в программе (Дон ее основал, Алекс возглавлял проект по криптовалютам). В 2014 году мы запустили годовую инициативу по исследованию блокчейн-революции и ее последствиях для бизнеса и общества; результатом стала эта книга, в которой мы постарались всесторонне осветить возможности и риски новой платформы.

Если бизнес, госуправление и новаторы гражданского общества справятся с задачей, мы перейдем от Интернета, мотивированного преимущественно снижением цен на поиск, координацию и сбор информации и принятие решений (где в центре внимания мониторинг, посредничество и монетизация информации и транзакций в сети), к Интернету, мотивированному снижением стоимости выработки, регулирования и осуществления общественных и коммерческих соглашений, где в центре внимания будут этичность, безопасность, сотрудничество, неприкосновенность личных данных во всех транзакциях и в создании и распределении ценностей. Это разворот стратегии на 180 градусов. Результатом может стать экономика равноправных участников с институтами, которые будут по-настоящему распределенными, безбарьерными и дающими новые возможности — и потому легитимными. Новая платформа фундаментально переопределяет, что и как мы можем делать онлайн и кто в этом участвует, и таким образом даже способна создать технологические условия для разрешения самых наболевших социальных и экономических проблем.

Если с этой задачей справиться не удастся, многообещающая технология блокчейна будет ограничена или вовсе уничтожена. Хуже того, она может превратиться в орудие мощных институтов, с

помощью которого они будут охранять свое состояние, или, если к ней получат доступ правительства, в платформу для нового общества тотальной слежки. Тесно связанные технологии распределенного программного обеспечения, шифрования, автономных агентов и даже искусственного интеллекта могут выйти из-под контроля и обратиться против своих создателей.

Возможно, эта новая технология замедлится на начальном этапе, не найдет достойного применения или будет обращена во вред. Блокчейн и криптовалюты, в частности биткойн, уже набирают обороты, но мы не беремся предсказать, ждет ли их успех, и если да, то как скоро[34]. Прогнозы — это всегда большой риск. Теоретик технологии Дэвид Тиколл поясняет: «Многим из нас не удалось предсказать всей полноты влияния Интернета. Мы упустили из виду многие опасные явления вроде ИГИЛ, а ряд больших оптимистических прогнозов не оправдались». Он добавляет: «Если блокчейн настолько же грандиозен и универсален, как Сеть, мы, скорее всего, так же плохо сможем спрогнозировать его преимущества и недостатки»[35].

Поэтому не будем предсказывать, что будущее за блокчейном. Мы просто выступаем за него. Мы утверждаем, что блокчейн необходим, потому что он поможет нам начать новую эпоху процветания. Мы считаем, что экономика лучше всего работает, когда работает для всех, а эта новая платформа позволяет победить экономическую дискриминацию. Она значительно снижает стоимость перевода денежных средств. Она заметно снижает барьеры для открытия банковского счета, получения кредита, инвестирования. Она способствует предпринимательству и участию в глобальной торговле. Она выступает катализатором распределения капитала, а не только его перераспределения.

Не нужно бороться с этой инновацией — куда лучше присоединиться к ней и ее усовершенствовать. Вместе мы можем добиться того, чтобы эта огромная сила послужила не кратковременной выгоде меньшинства, а долговременному успеху большинства.

Нас обоих вдохновляет потенциал этой новой ступени в развитии Интернета. Мы исполнены энтузиазма по поводу грандиозной волны инноваций, которая накатывается на мир, и ее потенциала для процветания и совершенствования мира. В этой книге собраны наши доводы в пользу технологии блокчейна, призванные заинтересовать вас и помочь вам понять эту новую тенденцию и сделать все от вас зависящее, чтобы она себя оправдала.

Пристегнитесь покрепче и читайте дальше! Мы проходим одну из критических развилок в истории человечества.

Глава 2. Будущее с нуля: семь конструктивных принципов экономики на блокчейне

«Неприкосновенность частной жизни — основа свободы, — говорит Энн Кавукян, исполнительный директор Института информационной безопасности и больших данных Университета Райерсона. — Впервые я об этом услышала тридцать лет назад, когда стала посещать конференции в Германии. Не случайно сегодня Германия — мировой лидер в области защиты личных данных и информации. Эта страна пережила ужасы Третьего рейха и полное уничтожение гражданских свобод, которое началось с устранения неприкосновенности частной жизни. Когда этот период остался позади, немцы решили: это не повторится»[36].

Поэтому парадоксально — или же совершенно естественно, — что одна из первых децентрализованных пиринговых (платформа без посредников) вычислительных платформ, гарантирующих неприкосновенность частной жизни пользователей, называется Enigma, как и машина, разработанная немецким инженером Артуром Шербиусом для дешифровки информации. Шербиус создал свою «Энигму» для коммерческого применения: благодаря его устройству предприятия по всему миру могли быстро и безопасно обмениваться коммерческими тайнами, биржевыми прогнозами и другой инсайдерской информацией. Но уже через несколько лет вооруженные силы Германии стали изготавливать собственные версии «Энигмы», чтобы передавать по радио шифрованные сообщения войскам. Во время войны нацисты пользовались «Энигмой», чтобы распространять стратегические планы, сведения о целях и планировать атаки. Машина стала орудием притеснения и уничтожения людей.

Enigma наших дней служит обеспечению свободы и благосостояния. Эта разработка Гая Зюскинда и Оза Натана из медиалаборатории Массачусетского технологического института сочетает преимущества открытого регистра блокчейна, прозрачность которого «сильно мотивирует на честное поведение», с так называемыми *гомоморфным шифрованием* и *надежными многосторонними вычислениями*[37]. Проще говоря, «Enigma берет вашу информацию — любую информацию — и разделяет ее на фрагменты, которые зашифровываются в элементы данных, случайным образом распределенные по узлам сети. Информация не существует в одной точке (месте?), — объясняет Кавукян. — Enigma применяет технологию блокчейна, чтобы встроить данные и отследить

все фрагменты информации»[38]. Информацию можно передавать третьим лицам, и они смогут использовать ее в вычислениях, даже не дешифровывая [39]. Если этот метод себя оправдает, может измениться наш подход к собственной идентичности в сети. Представьте, что ваша личная информация надежно хранится в «черном ящике», доступ к которому имеете только вы.

Но как бы привлекательно это ни звучало, осваивать недавно открытые территории криптографии следует с осторожностью. На то есть несколько причин. Во-первых, потребуется большая сеть участников. Во-вторых, «шифрование — это область, где опасно гнаться за самыми новыми и современными тенденциями, потому что не раз случалось, что алгоритм, который все считали надежным, выходил на рынок, а через четыре-пять лет какой-нибудь вдохновенный ученый вдруг заявлял, что в нем есть уязвимость, и все рушилось, — рассказывает Остин Хилл из Blockstream. — Поэтому мы обычно предпочитаем консервативные, хорошо изученные, давно известные алгоритмы. Они достойно прошли проверку временем, и разработка биткойна это учитывает»[40].

Все же к этой концепции следует отнестись серьезно — она способна значительно повлиять на неприкосновенность, безопасность и поддержание личных данных. «Enigma предлагает гарантии неприкосновенности частной жизни, — говорит Кавукян. — Это смелое утверждение, но оно обещает нам то, что особенно необходимо становится в современном связанном и взаимосвязанном мире»[41].

В ходе нашего исследования мы рассматривали целый ряд проектов на основе технологий блокчейна, разработчики которых точно так же стремятся содействовать осуществлению базовых прав человека — не только на частную жизнь и безопасность, но и на собственность, на юридическое признание, на участие в политической, культурной и экономической жизни общества. Вообразите себе технологию, которая защищает нашу свободу выбирать будущее для себя и своих близких и определять собственную судьбу независимо от того, где мы родились или живем. Какие новые средства и новые рабочие места можно создать с этими возможностями? Какие новые предприятия и услуги? Какие изменения в мировоззрении? Ответы оказались прямо перед нами — их дает Сатоси Накамото.

Семь конструктивных принципов

Мы убеждены, что новая эпоха не за горами, если вдохновляться картиной, нарисованной Сатоси Накамото, и заложенными, пусть и несформулированными, в ней принципами; воплотить ее в жизнь позволит совместная работа многочисленных талантливых и увлеченных членов сообщества.

Новаторство Накамото касалось только денег и не преследовало амбициозной цели создать Интернет второго поколения. Он не говорил о преобразовании коммерческих компаний, трансформации социальных институтов или изменении всей цивилизации к лучшему. И все же стратегическое видение Сатоси оказалось поразительно в своей простоте, оригинальности и понимании человечества. Всем читателям его доклада 2008 года стало понятно, что мы стоим на пороге новой эры цифровой экономики. Если первая эпоха цифровой экономики стала возможна благодаря слиянию вычислительных и коммуникационнных технологий, то в основе второй будет продуманное сочетание компьютерной техники, математики, шифрования и экономики поведения.

Вспоминаются строки фолк-певца Гордона Лайтфута: «Если б ты могла читать мои мысли, дорогая, какую историю они бы тебе поведали!» Сатоси с 2011 года не выходит на связь (хотя время от времени его имя всплывает на некоторых форумах), но мы убеждены, что созданный им доверительный протокол позволяет сформулировать принципы преобразования институтов и экономики.

Все, с кем мы общались, с радостью делились своими идеями по поводу технологии блокчейна. Каждая беседа, каждая статья, каждая ветка форума дала нам целый ряд тем, на основе которых мы составили конструктивные принципы — принципы для создания программного обеспечения, услуг, бизнес-моделей, рынков, организаций, даже правительств в блокчейне. Сатоси никогда не формулировал этих принципов, но они следуют из запущенной им технологической платформы. Мы видим в них принципы построения новой эпохи цифровой экономики — и эпохи возвращения доверия.

Если вы далеки от этой темы, надеемся, что эти принципы помогут вам понять суть блокчейн-революции. Если вы убежденный скептик биткойна и блокчейна, они пригодятся вам в размышлениях о своем будущем предпринимателя, изобретателя, инженера, художника, стремящегося к творческому сотрудничеству с единомышленниками, собственника или инвестора, менеджера, который хотел бы переоценить свою роль в зарождающейся экономике блокчейна.

1. Деловая этика в сети

Принцип. Доверие — не внешний, а внутренний элемент процесса. Соблюдение норм этики кодируется на каждом этапе и распределяется между всеми участниками, а не контролируется кем-то одним. Прямой обмен ценностями осуществляется исходя из ожидания, что другая сторона будет действовать этично. Таким образом, ценности деловой этики — честность в словах и делах, учет чужих интересов, ответственность за последствия своих решений и действий, прозрачность принятия решений и действия — закодированы в правах на принятие решений, структурах стимулирования и самих операциях,

так что нарушение этики либо невозможно, либо требует больших затрат времени, денег, энергии и репутации.

Проблема. Осуществлять транзакции или вести бизнес напрямую в Интернете до сих пор было невозможно по той простой причине, что деньги отличаются по своей природе от других информационных товаров и интеллектуальной собственности как таковой. Можно разослать всем друзьям одно и то же селфи, но нельзя отправить другу доллар, который уже уплачен кому-то другому. Деньги должны быть списаны с вашего счета и зачислены на счет вашего друга. Они не могут существовать одновременно в двух местах, не говоря уже о большем их количестве. Есть риск дважды потратить единицу цифровой валюты в разных местах — тогда одна из них не принимается к оплате, как необеспеченный чек. Это называется *проблемой двойного расходования*. Это хорошо для мошенников, которые дважды тратят свои деньги, но плохо для адресата средств, который не получает платежа, и для вашей репутации в сети. По традиции, совершая платеж онлайн, мы решаем проблему двойного расхода, проводя каждую транзакцию через центральные базы данных одной или нескольких третьих сторон: службы денежных переводов (Western Union), коммерческого банка (Citi), госучреждения (Государственный банк Австралии), эмитента кредитных карт (Visa) или платформы онлайн-платежей (PayPal). Проведение платежа может занять несколько дней, а в некоторых регионах и несколько недель.

Прорывное решение . Сатоси сочетал существующую распределенную одноранговую сеть и элементы сложного шифрования, чтобы создать *механизм консенсуса*, который справляется с проблемой двойного расхода так же, как надежная третья сторона, если не лучше. В биткойновом блокчейне сеть ставит отметку времени на первую транзакцию, когда владелец тратит конкретный биткойн, и препятствует повторному расходу этого биткойна, таким образом устраняя возможность двойного расходования. Участники сети, управляющие полнофункциональными узлами биткойна, так называемые майнеры, собирают сведения о недавних транзакциях и сохраняют их в виде блока данных каждые десять минут. Каждый блок действителен только при наличии связи с предыдущим. В протоколы также включен метод регенерации дискового пространства, чтобы каждый узел хранил блокчейн целиком. Наконец, блокчейн публичен: всем видно, как проходят транзакции. Скрыть транзакцию невозможно таким образом, биткойн отследить проще, чем обычные деньги.

Сатоси стремился не только обойтись без посредников в виде центрального банка и надзорных органов, но и устранить возможность расхождений в толковании фактов: пусть код говорит сам за себя, пусть алгоритм сети позволяет ей достичь консенсуса относительно факта и зафиксировать его в блокчейне в зашифрованном виде.

Механизм достижения консенсуса критически важен. «Консенсус — это социальный процесс, — пишет в своем блоге Виталик Бутерин, пионер блокчейна Ethereum. — Людям неплохо удается достигать консенсуса… и без всяких алгоритмов». Далее он объясняет: как только вычислительные мощности системы превосходят человеческие, человек обращается к программному обеспечению. Алгоритм консенсуса в сетях без посредников распределяет права обновлять статус сети, то есть голосовать за то, что участник считает правдой. Алгоритм присваивает это право кругу участников, которые составляют экономическую группу, обладающую личной заинтересованностью. Как отмечает Бутерин, самое важное в этом экономическом наборе то, что его участники надежно распределены: ни один человек или синдикат не сможет победить большинство, даже если будет иметь такие средства и желание[42].

Для достижения консенсуса сеть биткойна применяет так называемый механизм *доказательства выполненной работы* (proof of work, PoW). За сложным названием стоит очень простая идея. Поскольку невозможно выбирать, кто из майнеров будет создавать следующий блок, основываясь на их личности, вместо этого создается головоломка, которую сложно решить (то есть требуется *выполнить работу*), но легко проверить (любой может быстро убедиться, что ответ точен). Участники договариваются, что тот, кто первым решит задачу, и будет создавать новый блок. Майнерам приходится тратить ресурсы (вычислительные мощности и электричество), чтобы решить задачу, найдя правильный хеш — нечто вроде уникального «отпечатка пальца» для текста или файла с данными. За каждый найденный блок майнеры получают биткойны. Головоломка математически устроена так, что быстрого или обходного решения не существует. Поэтому, когда остальные участники сети видят ответ, то полагают, что для его нахождения была выполнена некоторая работа. Решение задач происходит непрерывно — по словам Дино Марка Ангаритиса, «в районе 500 тысяч триллионов хешей в секунду». Майнеры «ищут хеш, соответствующий условию. По статистике, это должно происходить каждые 10 минут. Это процесс Пуассона, так что иногда требуется всего одна минута, а иногда один час, но в среднем это десять минут». Ангаритис объясняет принцип работы: «Майнеры собирают все ожидающие одобрения транзакции, какие находят в сети, и пропускают информацию через функцию криптографического дайджеста — так называемый надежный хеш-алгоритм (SHA-256), который выдает 32-байтовое значение *хеша*. Если хеш не превышает

определенного целевого значения (установленного сетью и уточняемого каждые 2016 блоков), то майнеру удалось найти ответ головоломки и «решить» блок. К несчастью для майнера, найти правильный хеш очень сложно. Если полученное значение неверно, майнер немного меняет исходные данные и предпринимает новую попытку. Каждая попытка дает совершенно другой хеш. Майнерам приходится решать задачу много раз, пока не найдется правильный ответ. По данным на ноябрь 2015 года, среднее число попыток для каждой задачи — 350 квинтиллионов (3,5 * 1020). Это громадная работа!»[43]

Возможно, вам доводилось слышать и о других механизмах консенсуса. Первая версия блокчейна Ethereum — Frontier — также использовала доказательство выполненной работы, но в Ethereum 1.1 предполагается заменить его механизмом *доказательства долей в собственности*. Этот механизм требует от участников инвестировать и поддерживать некий запас ценности (например, в собственной валюте блокчейна, такой как пиркойн, NXT и т. д.), чтобы при голосовании не расходовать электроэнергию. Другие блокчейны, в частности Ripple и Stellar, обеспечивают консенсус с помощью социальных сетей; от новых участников (то есть новых узлов) требуется составить *уникальный список* как минимум 100 узлов, голосованию которых этот пользователь доверяет. Такое доказательство не является непредубежденным — новому участнику нужно обладать социальным интеллектом и репутацией. Еще один механизм — *доказательство активности*. В нем сочетаются доказательство выполненной работой и доказательство долями в собственности: определенное случайным образом количество майнеров должно подписать блок с помощью криптоключа, и только тогда блок станет официальным [44]. *Доказательство емкости* требует, чтобы майнер отводил значительный объем своего жесткого диска на майнинг. Еще одна похожая концепция — *доказательство хранения* — требует приобрести и раскрыть для совместного использования дисковое пространство в распределенном облаке.

Хранение действительно немаловажно. Между данными в блокчейне и данными в Интернете есть одно важное отличие: в Интернете большая часть информации поддается изменению и эфемерна, а точное время ее публикации не имеет критического значения для предыдущей или последующей информации. В блокчейне же движение биткойна по сети сопровождается перманентным отпечатком времени начиная с момента его создания. Чтобы биткойн оставался действителен, он должен ссылаться и на

собственную историю, и на историю всей цепочки. Таким образом, блокчейн необходимо хранить целиком.

Процессы майнинга — сборка блока транзакций, расход ресурса, решение задачи (головоломки, сказать лучше, чтобы быть последовательным), достижение консенсуса, поддержание копии всего регистра — настолько важны, что некоторые называют биткойновый блокчейн таким же полезным, как и Интернет, и призывают к публичной его поддержке. Пол Броуди из Ernst & Young считает, что все технические устройства должны предоставлять свои вычислительные мощности для поддержания блокчейна: «В вашу газонокосилку или посудомойку встроен центральный процессор, мощность которого в тысячу раз превышает реальные потребности устройства. Так пусть он майнит. Не для того, чтобы приносить вам деньги, а для поддержания вашей части блокчейна»[45]. Независимо от выбранного механизма консенсуса, блокчейн обеспечивает соблюдение норм этики благодаря хорошо продуманному коду, а не полагается только на то, что люди будут действовать честно.

Что это значит для экономики блокчейна . Вместо того чтобы доверять крупным компаниям и госучреждениям подтверждать личность людей и поручаться за их репутацию, доверим эти функции сети. *Впервые в истории нам доступна платформа, которая обеспечивает доверие к транзакциям и большей части записанной информации независимо от действий другой стороны.*

Это очень много значит для различных аспектов социальной, политической и экономической деятельности. Речь не только о том, кто с кем вступает в брак, за кого голосует, кому платит, — дело касается любых процессов, которые требуют достоверных записей и подтвержденных транзакций. Кто чем владеет? Кому какие права принадлежат на эту интеллектуальную собственность? Кто закончил мединститут? Кто купил ружье? Кто изготовил эти кроссовки Nike, это устройство Apple, эту детскую смесь? Где и как добыты эти бриллианты? Доверие — это необходимое условие цифровой экономики, а платформа для надежного и достоверного массового сотрудничества открывает много возможностей для нового типа организации и общества.

2. Распределенная сила

Принцип. Система распределяет власть по одноранговой сети, у которой нет единого центра контроля. Ни одна сторона не способна обрушить систему. Если некоему органу власти удастся отключить или изолировать участника или группу участников, система продолжит существовать. Если крупная часть сети попытается захватить над ней контроль, все увидят, что происходит.

Проблема. В начале Интернета ни один крупный институт с большой базой пользователей, будь то сотрудники, граждане, клиенты или другие организации, не задумывался о своих социальных обязательствах. Раз за разом органы централизованной власти показывали, что готовы и способны действовать вопреки мнению пользователей, собирать и анализировать их данные, выдавать информацию по требованию государства, не оповещая об этом пользователей, и внедрять масштабные изменения без согласия пользователей.

Прорывное решение. Затраты на попытку контролировать биткойновый блокчейн значительно превышают возможные финансовые выгоды. Сатоси внедрил метод доказательства работы, который требует от пользователей расходовать большие вычислительные мощности (а значит, много электроэнергии), чтобы защищать сеть и производить новые биткойны. Его вдохновило решение криптографа Адама Бэка Hashcash, которое снижает риск спама и отказа в обслуживании. Метод Бэка требует доказательства выполненной работы при отправке электронного письма — фактически это штамп «повышенная важность» на сообщении, который показывает важность письма для отправителя. «Это письмо настолько важно, что я затратил столько-то энергии, чтобы вам его отправить». Это повышает расходы на рассылку спама, вредоносных программ и программ-вымогателей.

Любой может бесплатно загрузить протокол биткойна и хранить копию блокчейна. При этом используется бутстреппинг, или самонастройка, — желающий загружает программу на компьютер или мобильное устройство, выполняя ряд простых инструкций, которые запускают остальную часть программы. Оно целиком распространяется через бесплатные сети типа BitTorrent, открытой совместной базы данных интеллектуальной собственности, которая хранится на десятках тысяч компьютеров по всему миру.

Конечно, это ограждает сеть от влияния государства, что в зависимости от ситуации может быть как благом, так и злом, например, позволяя диссидентке бороться за права женщин при тоталитарном режиме, а преступнику в демократической стране заниматься вымогательством. Тоталитарные страны не смогут замораживать банковские счета или конфисковать средства политических активистов. Государство не сможет бесконтрольно захватывать активы на блокчейне, как в свое время поступила администрация Ф. Д. Рузвельта с указом 6102, который обязывал население сдавать «золотые монеты, слитки и сертификаты» под угрозой штрафа или тюремного заключения[46]. Джош Фейрфилд из Университета Вашингтона — Ли кратко сформулировал это так:

«Теперь не осталось посредника, которого можно прижать»[47]. Блокчейн повсюду. Добровольцы поддерживают его, храня свои копии блокчейна в актуальном состоянии и отводя свободные вычислительные ресурсы своих компьютеров для майнинга. Никаких тайных сделок: любое действие, любая транзакция транслируется на всю сеть и получает верификацию и подтверждение. Ничто не проходит через единую третью сторону, ничто не хранится на центральном сервере.

Сатоси сделал распределенной и «чеканку» валюты, привязав появление биткойнов к созданию новых блоков в регистре и таким образом передав права на выпуск валюты всем в пиринговой сети. Любой майнер, решивший задачу и подтвердивший свою работу первым, получает новенькие биткойны. Нет ни Федерального резерва, ни центробанка, ни казначейства, контролирующего денежные потоки. Более того, каждый биткойн содержит прямые связи с блоком его происхождения и всеми последующими транзакциями.

Поэтому отпадает необходимость в посредниках. Функционирование блокчейна — это массовое сотрудничество в лучшем своем проявлении. Каждый властен над своей информацией, над своей собственностью и над уровнем своего участия. Распределенные вычислительные мощности делают возможной распределенную коллективную власть людей.

Что это значит для экономики блокчейна. Возможно, такая платформа откроет путь новым распределенным моделям создания благ. Возможно, новые способы прямого децентрализованного сотрудничества позволят решить назревшие проблемы общества. Возможно, удастся ликвидировать кризис уверенности и даже легитимности в сегодняшних институтах, вместо пиар-ходов передав реальную власть населению, которое действительно, а не на словах получит возможность преуспевать и участвовать в общественной жизни.

3. Ценность как стимул

Принцип. Система уравновешивает мотивацию всех заинтересованных лиц. Биткойн или иной токен, отражающий ценность, — неотъемлемая часть этого соотношения, связанная с репутацией. Сатоси программно обусловил вознаграждение тех, кто работает в системе, и передал власть над ней тем, кто владеет и пользуется токенами, чтобы все заботились о ее сохранности. Блокчейн — нечто вроде финального тамагочи, глобально распределенное яйцо в гнезде[48].

Проблема. В эпоху первого поколения Интернета концентрация власти в корпорациях, их размеры, сложность и непрозрачность

позволили им извлекать непропорционально большую прибыль из тех самых сетей, что предоставили им новые возможности. Крупные банки своей деятельностью довели финансовую систему до предела прочности, потому что «система поощрения большинства топ-менеджеров и ряда специалистов в этих банках разработана так, что способствует недальновидному и чрезмерно рискованному поведению», — отмечает экономист Джозеф Стиглиц. В частности, речь идет о «притеснении беднейших граждан». Он так подытоживает проблему: «Если поощряется дурное, люди и совершают дурные поступки, так что они себя вели именно так, как следовало ожидать»[49].

Крупные доткомы заманивали пользователей бесплатными услугами в области торговли, поиска информации и социальных медиа в обмен на их данные. Как показало исследование Ernst& Young, почти две трети опрошенных менеджеров собирали данные пользователей в бизнес-целях, а почти 80 % говорят, что этот майнинг данных позволил увеличить их доходы. Но если фирма становится жертвой хакерской атаки, разбираться с последствиями утечки информации о банковских счетах и кредитных картах приходится пользователям. Неудивительно, что в том же самом опросе почти половина пользователей отметила, что ограничит доступ к своим личным данным в ближайшие пять лет, а более половины сказали, что уже предоставляют организациям меньше информации, в том числе осторожнее высказываются в социальных сетях, чем пять лет назад [50].

Прорывное решение. Сатоси ожидал, что участники системы будут действовать в личных интересах. Он хорошо понимал теорию игр. Он знал, что сети без контроллеров уязвимы для атак типа Sybil, когда узлы формируют множественные фальшивые электронные сущности, размывающие возможности и обесценивающие репутацию [51]. Благонадежность одноранговой сети и репутация ее участников снижаются, если невозможно определить, имеете вы дело с тремя разными сторонами или одной стороной, пользующейся тремя персонами. Поэтому Сатоси составил исходный код так, что, независимо от эгоистических целей участников, любые их действия приносят пользу всей сети и наращивают их репутацию, как бы те ни позиционировали себя в сети. Требования консенсуса к ресурсам в сочетании с биткойном в качестве поощрения могли мотивировать участников поступать правильно и тем самым делать их заслуживаю

щими доверия — а именно предсказуемыми. Атаки типа Sybil становятся экономически невыгодными.

Сатоси пишет: «По умолчанию, первая транзакция в блоке — это особая транзакция, которая создает новый койн, принадлежащий создателю блока. Это мотивирует узлы поддерживать сеть»[52]. Биткойн мотивирует майнеров участвовать в создании блока и соединении его с предшествую щим. Тот, кто первым завершает блок, получает вознаграждение в виде некоторого количества биткойнов. Протокол Сатоси щедро вознаграждал первых активистов: в первые четыре года майнер получал 50 биткойнов за каждый блок. Затем каждые четыре года вознаграждение за блок уменьшалось вдвое: 25 биткойнов, 12,5 биткойна и так далее. Пользователи, уже накопившие запас биткойнов, мотивированы обеспечивать долгосрочный успех платформы и покупают лучшее оборудование, чтобы вести майнинг, наиболее эффективно расходовать энергию и поддерживать регистр. Биткойн — это право собственности на блокчейн, не просто как мотивация участвовать в майнинге и транзакциях, но как владение самой платформой. Распределенные учетные данные пользователей — базовый элемент инфраструктуры зашифрованной сети. Владея и распоряжаясь биткойнами, пользователь финансирует развитие блокчейна.

Сатоси определил экономической группой *владельцев вычислительных мощностей*. Чтобы участвовать в системе поощрения, эти майнеры должны потреблять ресурс, являю щийся внешним по отношению к сети, в частности электроэнергию. Время от времени два разных майнера находят два равноценных блока одного размера, и остальным майнерам требуется решить, на каком из них строить дальше. Обычно они выбирают тот, у которого, на их взгляд, больше вероятность победы, а не строят на обоих, потому что тогда пришлось бы распределить вычислительную мощность между двумя ветвями, а это приводит к снижению ценности. Чем длиннее цепь, тем больше работы в нее вложено, и поэтому участники выбирают ее как каноническое состояние блокчейна. С другой стороны, Ethereum в качестве экономической группы выбрал *владельцев валюты*. A Ripple и Stellar пользуются социальной сетью.

Парадокс схем достижения консенсуса в том, что каждый, действуя в личных интересах, служит пиринговой сети, а это, в свою очередь, влияет на его репутацию как члена экономической группы. До появления технологии блокчейна извлекать выгоду из сетевой репутации было трудно, и не только из-за атак типа Sybil, когда один компьютер может исполнять несколько разных ролей. Личность многогранна, тонка и эфемерна. Мало кто видит все стороны одной

персоны, не говоря уже о тонкостях и полном объеме нашей личности. В разных контекстах мы должны предоставить тот или иной документ, чтобы удостоверить определенную часть нашей личности. Те, у кого «нет бумаг», ограничены взаимодействовать в своем социальном круге. В таком блокчейне, как Stellar, это прекрасное начало — средство создания постоянного цифрового присутствия и установления репутации, которая выходит далеко за пределы географического сообщества человека.

Еще одно прорывное решение, сохраняющее ценность, — это денежная политика, закодированная в программном обеспечении. «Все деньги, которыми когда-либо пользовалось человечество, так или иначе ненадежны, — говорит Ник Сабо. — Эта ненадежность находит много выражений, от фальшивомонетничества до воровства, но самое, пожалуй, пагубное — это инфляция»[53]. Сатоси установил верхнюю границу мирового запаса биткойнов в 21 млн, чтобы избежать неконтролируемой инфляции. Учитывая, что каждые четыре года количество биткойнов, намайненных на блок, и нынешнюю скорость майнинга (шесть блоков в час), эти 21 млн целиком войдут в обращение к 2140 году. Никакой гиперинфляции или обесценивания валюты, вызванных некомпетентной или коррумпированной бюрократией.

Валюта — не единственный актив, которым можно торговать в блокчейне. «Это лишь самое начало возможностей, — говорит Хилл из Blockstream. — Мы недалеко ушли от 1994 года в плане приложений и протоколов, которые действительно пользуются возможностями сети и показывают миру: «Вот какие потрясающие вещи можно сделать!»[54]. Хилл ожидает увидеть появление различных финансовых инструментов — от удостоверяющих право на актив до доказывающих право собственности. Он рассчитывает, что биткойн найдет применение в виртуальном мире — в Метавселенной биткойны можно будет конвертировать в конгбаксы и нанять Хиро Протагониста, чтобы нахакать ценных данных [55], а в OASIS, разыскав реальное «пасхальное яйцо» и унаследовав состояние Хэллидея, продать Google права на виртуальное позиционирование OASIS и купить себе машину без водителя, чтобы кататься на ней по Торонто.

Все деньги, которыми когда-либо пользовалось человечество, так или иначе ненадежны. Эта ненадежность находит много выражений, от фальшивомонетничества до воровства, но самое, пожалуй, пагубное — это инфляция.

И, конечно, есть еще и Интернет вещей, где мы регистрируем свои устройства, присваиваем им электронные индификаторы (Intel уже

этим занимается) и координируем между ними оплату через биткойны, а не разнообразные физические валюты. «Можно описать любые новые бизнес-кейсы, совместить их в сети и пользоваться ее инфраструктурой, не создавая специально для своих нужд новый блокчейн с нуля»[56], -говорит Хилл.

В отличие от физических валют, биткойн раскладывается на доли до восьми десятичных разрядов (то есть сумма в биткойнах может иметь до восьми знаков после запятой). Это позволяет объединять и делить суммы в течение долгого времени в рамках одной транзакции: получение некоторой суммы и все исходящие платежи, финансируемые из этой суммы, могут рассматриваться как единая транзакция, что значительно удобнее серии транзакций. Заключив смарт-контракт для учета пользования услугой, можно автоматически ее оплачивать малыми долями через регулярные интервалы времени.

Что это значит для экономики блокчейна. В первом поколении Интернета ничего из этого не было доступно. Теперь в нашем распоряжении платформа, где люди и даже предметы обладают должной финансовой мотивацией, чтобы эффективно сотрудничать и создавать практически что угодно. Представьте себе онлайн-дискуссию, участники которой стремятся упрочить свою репутацию отчасти и потому, что некорректное поведение будет стоить им реальных денег. Тролли остаются за воротами. Представьте одноранговую сеть солнечных батарей, где домовладельцы получают в реальном времени компенсацию в блокчейне за производство чистой энергии. Представьте программное обеспечение с открытым исходным кодом, где сообщество разработчиков вознаграждает внешних исполнителей за хороший код. Представьте себе мир без границ. Это нетрудно [57].

4. Безопасность

Принцип. Меры безопасности внедрены в сеть так, что не возникает единой точки отказа, и обеспечивают не только конфиденциальность, но и аутентификацию и неотменяемость любого действия. Каждый, кто хочет участвовать в системе, должен пользоваться шифрованием — это не обсуждается, — и последствия неразумных действий испытывает на себе только тот, кто их совершает.

Проблема. Хакерские атаки, кража личных данных, мошенничество, киберзапугивание, фишинг, спам, вредоносные программы, вирусы-вымогатели — все это угрожает безопасности человека в обществе. Первая эпоха Интернета, вместо того чтобы сделать многие процессы прозрачными и затруднить нарушения прав

человека, почти не повысила безопасность частных лиц, институтов и экономической активности. Среднему интернет-пользователю часто приходится полагаться на то, что его электронную почту и учетные записи защитят простые пароли, потому что провайдеры или работодатели не настаивают на более надежных. Представьте себе типового финансового посредника: он не стремится разработать безопасные технологии, он специализируется на финансовых инновациях. В год, когда Сатоси опубликовал свой доклад, на нарушения безопасности в таких финансовых компаниях, как BNY Mellon, Countrywide и GE Money, пришлось более 50 % всех известных похищений личных данных (по сведениям Identity Theft Resource Center)[58]. К 2014 году доля финансового сектора в общем числе нарушений упала до 5,5 %, однако нарушения безопасности в медицине и здравоохранении подскочили до 42 % от общего количества. IBM сообщила, что средняя стоимость одного нарушения безопасности -3,8 млн долларов; соответственно, эти нарушения за последние два года обошлись в 1,5 млрд долларов [59]. Все более распространенное мошенничество с медицинским страховым полисом обходится среднестатистическому гражданину в 13,5 тыс. долларов. Потребитель не знает, какой аспект его жизни следующим подвергнется нападению[60]. Если следующий этап цифровой революции предполагает передачу денег напрямую между сторонами, связь между ними должна быть неуязвима для хакеров.

Прорывное решение. Чтобы обеспечить надежность платформы, Сатоси потребовал от участников применять инфраструктуру открытых ключей (ИОК). Это продвинутая форма «асимметричной» криптографии, где пользователи получают по два ключа, которые выполняют разные функции: один для шифрования, другой для дешифровки. Таким образом, они асимметричны. Биткойновый блокчейн в настоящее время — самый крупный гражданский образец ИОК в мире, уступающий только системе общего доступа Департамента обороны США[61].

Асимметричная криптография, начало которой было положено в 1970-е[62], получила развитие в форме бесплатного программного обеспечения для шифрования электронной почты, в частности Pretty Good Privacy (PGP). Программа PGP обеспечивает хороший уровень безопасности, но трудна в применении: ею должны пользоваться все в выбранной сети, и при этом необходимо следить не только за собственными двумя ключами, но и за общественными ключами всех остальных участников. Отсутствует функция переустановки пароля —