

ГЛАВА

5

Четвертая промышленная революция

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

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

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

[147]

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

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

[148]

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

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

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

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

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

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

[149]

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

Спасти «интернет вещей» от самого себя

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

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

[150]

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

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

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

[151]

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

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

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

[152]

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

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

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

«Доверенные» вычисления

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

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

[153]

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

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

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

[154]

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

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

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

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

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

[155]

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

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

[156]

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

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

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

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

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

[158]

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

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

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

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

[159]

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

Энергетика блокчейна

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

[160]

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

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

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

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

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

Преимущества децентрализованных энергосетей очевидны. Если [161] любое местное сообщество будет само производить и распределять энергию, например, через микросети, объединяющие солнечные панели на каждом доме, то это значительно сократит ее потери при передаче на большие расстояния (а они иногда доходят до 30 процентов). Децентрализованные микросети менее уязвимы для кибератак, поскольку последовательный взлом каждого узла обойдется хакерам гораздо дороже, чем взлом главного сервера в централизованной региональной сети. Кроме того, децентрализованная сеть позволяет подстраховаться на случай стихийного бедствия. (Найдите в интернете фотографии ночного Манхэттена после урагана «Сэнди»: весь район ниже 34-й улицы — сплошная черная дыра, кроме одного светлого пятнышка вокруг Вашингтон-сквера. Там находится Нью-Йоркский университет, корпуса которого объединены в децентрализованную энергосеть [15].) Есть и еще один плюс: хотя полностью искоренить коррупцию очень сложно, маленькие локализованные инициативы будут не столь лакомым куском для продажных чиновников и теневых банкиров, как гигантские энергетические проекты. Без тридцатилетних контрактов, навязанных нам крупными международными банками и политическими силами, можно будет значительно сократить лишние издержки и снизить цены на энергию для рядовых граждан.

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

[162]

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

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

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

[163]

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

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

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

[164]

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

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

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

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

[165]

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

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

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

[166]

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

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

Отслеживаем товары

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

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

[167]

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

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

[168]

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

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

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

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

[169]

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

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

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

[170]

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

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

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

[171]

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

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

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

[172]

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

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

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

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

[173]

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

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

[174]

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

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

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

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

[175]

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

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

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

ГЛАВА

6

Новый мундир старой гвардии
