Глава 4
Блокчейны

Если большинство технологий автоматизируют работу людей на периферии, тех, кто выполняет «черную» работу, то блокчейны автоматизируют центр. Вместо того чтобы лишать работы таксиста, блокчейн лишает работы Uber, позволяя водителям такси связываться с клиентом напрямую, без посредника.

Виталик Бутерин, сооснователь сети Ethereum [109]

В чем особенность компьютеров: цикл обратной связи «платформа — приложение»

Во второй части фильма «Назад в будущее» (1989 года) главный герой путешествует в 2015 год. На экране мы постоянно видим летающие автомобили, но люди по-прежнему пользуются телефонными будками. Никаких тебе смартфонов.

Это типично для научной фантастики доинтернетовской эпохи: почти ни одно произведение не предсказало потрясающего успеха компьютеров и интернета. Почему же писатели-фантасты вечно прокалываются в своих прогнозах? Почему портативные суперкомпьютеры, подключенные

к интернету, появились раньше летающих автомобилей? Почему компьютеры и интернет развиваются быстрее, чем все остальное?

Это отчасти объясняется чисто технологическими причинами. Законы физики позволяют нам уменьшить транзисторы — мельчайший компонент вычислительной техники — и, следовательно, втискивать во все меньшие объемы все больше вычислительной мощности. Темпы этого процесса описывает закон Мура. Он назван в честь Гордона Мура, основателя компании Intel, специализирующейся на производстве чипов [110]. Закон Мура гласит, что количество транзисторов, которые могут поместиться на чипах, примерно удваивается каждые два года. История это правило подтверждает: в современном iPhone более 15 млрд транзисторов — сравните с настольным ПК 1993 года выпуска, в котором их было около 3,5 млн. Очень немногие технологии могут похвастаться улучшениями более чем в тысячу раз за такой короткий период. Физические ограничения в других технологических сферах преодолеть гораздо труднее.

Но не все объясняется технологическим аспектом. Не следует забывать и об экономическом феномене: о взаимоотношениях между компьютерными приложениями и платформами, на которых они работают. В современном iPhone гораздо больше транзисторов и других компонентов, чем в первой его модели, но у него есть и множество других приложений. И они намного более полезные и продвинутые, чем те, что были в самом начале. Новые приложения помогают продавать больше телефонов, что приводит к увеличению реинвестирования в этот продукт и, в свою очередь, в дальнейшую разработку приложений. Это и есть цикл обратной связи «платформа — приложение». Платформы, такие как

iPhone, создают условия для создания новых приложений. Они повышают ценность и полезность платформ. В результате создается цикл позитивной обратной связи накопления улучшений и усовершенствований.

Благодаря техническому прогрессу и циклу обратной связи «платформа — приложение» компьютеры становятся все быстрее, миниатюрнее, дешевле и функциональнее. И эти силы действуют на протяжении всей истории вычислений. Предприниматели создали текстовые процессоры, программы графического дизайна и электронные таблицы для ПК. Разработчики оснастили интернет поисковыми системами, механизмами для электронной торговли и соцсетями. Технари перенесли сервисы для обмена сообщениями и фотографиями и сервисы доставки по требованию на мобильные телефоны. И в каждом случае инвестиции переходили от платформ к приложениям и обратно, способствуя быстрому многолетнему росту и тех и других.

Цикл обратной связи «платформа — приложение» применим как к платформам, принадлежащим сообществу, так и к корпоративным. В первом случае от него выиграли и сети с протоколами, такие как Веб и электронная почта, и операционная система с открытым исходным кодом Linux. С корпоративной стороны эти циклы стали истинным благом для Microsoft в 1990-х, когда разработчики создавали приложения для компьютеров с Windows. Теми же преимуществами пользуются сегодня разработчики приложений для мобильных операционных систем Apple и Google.

Иногда несколько тенденций налагаются друг на друга и взаимно усиливаются, как своего рода конструктивная интерференция перекрывающихся волн. Социальные сети стали для мобильных телефонов «убойным» приложением; они помогли сделать эти устройства популярными. А облачные

вычисления предложили гибкую инфраструктуру, которую стартапы смогли использовать для быстрого масштабирования своих приложений, таких как социальные сети, что позволило им обеспечить связью миллиарды пользователей. Мобильные телефоны, в свою очередь, сделали все доступным и недорогим. А все вместе эти тенденции привели к появлению волшебных портативных суперкомпьютеров, которые сегодня повсеместно распространены, но которые в не таком уж далеком прошлом не могли себе представить большинство писателей-фантастов.

Крупные циклы в сфере вычислений обычно случаются каждые десять — пятнадцать лет [111]. Мэйнфреймы доминировали в 1950–1960-х. Мини-компьютеры царствовали в 1970-х. Затем, в 1980-х, появились ПК, а в 1990-х «взлетел» интернет. И уже совсем недавно, начиная с 2007 года, когда на рынок вышел iPhone, повсеместно распространились мобильные телефоны. Четкого правила, по которому эта модель должна развиваться далее, не существует, но определенная логика все же просматривается. Закон Мура гласит, что для увеличения вычислительной мощности в сто раз требуется примерно десять — пятнадцать лет. Примерно столько же времени нужно для «вызревания» многих исследовательских проектов. Если принять, что этот паттерн сохраняется, можно сказать, что мы с вами сейчас примерно в середине очередного цикла.

Этот следующий цикл будет определяться целым рядом тенденций. Одна из них — искусственный интеллект (ИИ). Сложность ИИ-моделей растет с экспоненциальной скоростью и зависит от количества параметров в нейронных сетях, которые лежат в их основе. Сегодняшние темпы усовершенствований позволяют предположить, что будущие модели станут гораздо мощнее, чем уже весьма впечатляющие

варианты, имеющиеся на рынке сегодня. Еще одним прорывом станут новые аппаратные устройства, такие как беспилотные автомобили и гарнитуры виртуальной реальности. Эти технологии стремительно развиваются благодаря неуклонному улучшению датчиков, процессоров и других компонентов. Все крупные компании, в том числе Apple, Meta♦ и Google, щедро инвестируют в эти сферы [112]. Это консенсусные ставки — традиционный вариант — на то, что нас ждет в сфере вычислений. Почти все сходятся на том, что это будет иметь огромное значение.

С блокчейнами же ситуация совсем иная. Тут речь не о консенсусе. Многие люди, в том числе ваш покорный слуга, осознают их великий потенциал, но значительная часть истеблишмента игнорирует их. По сути, согласно преобладающей в сфере высоких технологий точке зрения, единственными важными векторами улучшений оказывается то, на чем уже сфокусированы действующие игроки отрасли: более масштабные базы данных, более быстрые процессоры, более крупные нейронные сети, более миниатюрные устройства. Но это близорукий подход. Он излишне опирается на технологии, созданные на базе устоявшихся институтов, практически игнорируя при этом те, что приходят из других мест, из длиннющего «хвоста» сторонних разработчиков.

Два пути к принятию технологий: «изнутри наружу» и «снаружи внутрь»

Новые технологии всегда пробивают себе путь либо «изнутри наружу», либо «снаружи внутрь» [113]. В первом случае они зарождаются в недрах пятерки крупнейших технологических компаний. Они намного заметнее технологий второго типа, поскольку выходят «на сцену» уже полностью готовыми;

появляются из стабильных, устоявшихся институтов и совершенствуются темпами, на которые способны корпоративные сотрудники, штатные исследователи и прочие специалисты, получающие за это зарплату. Они, как правило, нуждаются в значительном капитале и формальном обучении, что повышает барьеры для входа.

Большинство людей признают ценность технологий, идущих по пути «изнутри наружу», еще до их появления. Несложно представить, что карманные суперкомпьютеры с подключением к интернету станут суперпопулярными. Доказано Apple с ее iPhone. Или что люди с радостью примут машины, способные научиться действовать разумно и самостоятельно выполнять всевозможные задачи; доказано университетскими и корпоративными исследовательскими лабораториями, работающими в сфере ИИ. Старожилы индустрии выбирают эти технологии, поэтому их потенциал очевиден.

А вот технологии, идущие по пути «снаружи внутрь», зарождаются на периферии. Любители, энтузиасты, open source* — разработчики и основатели стартапов «высиживают» и «вынашивают» их вне мейнстрима. Работа над ними обычно требует меньшего капитала и формального обучения, что помогает уравновесить условия со старожилами. А еще из-за такой относительно низкой планки крупные компании менее серьезно относятся к этим технологиям и их поклонникам.

Потенциал технологий «снаружи внутрь» рассмотреть гораздо труднее, поэтому их постоянно недооценивают. Над

* Open Source — это программное обеспечение, которое поставляется для конечного пользователя с открытым исходным кодом. То есть приложение можно доработать под свои задачи без нарушения авторских прав разработчиков исходного ПО. *Прим. науч. ред.*

ними работают в гаражах, подвалах, комнатах студенческих общежитий и в основном не в официальные рабочие часы: по их окончании, во время перерывов, в выходные. Людей мотивируют особая философия и культура, которые, скорее всего, покажутся посторонним довольно странными. Другим этого не понять. К тому же эти новички выводят свой продукт на рынок недоделанным и без четкого, понятного способа применения. Большинство сторонних наблюдателей отвергают такие технологии, считая их игрушечными, странными, несерьезными, очень дорогими, а то и попросту опасными.

Мы уже говорили, что программное обеспечение — это, по сути, форма искусства. Вы же не думаете, что все великие романы и картины написаны людьми из авторитетных институтов. Не следует ожидать этого и от великих программ.

Но кто же они, эти новички, о которых мы только что упоминали? Представьте себе двадцать-с-чем-то-летнего Стива Джобса, фаната контркультуры и завсегдатая компьютерного клуба Homebrew, приюта для одержимых идеей микрокомпьютера ботаников, который в 1970-е ежемесячно организовывал собрания в Калифорнии [114]. Вспомните Линуса Торвальдса образца 1991 года, студента Хельсинкского университета, работавшего над персональным проектом, которому было суждено стать одноименной операционной системой Linux [115]. Или представьте, как Ларри Пейдж и Сергей Брин, бросив в 1998 году Стэнфордский университет, переезжают в гараж в Менло-Парке и через какое-то время превращают свой проект каталогизации веб-ссылок под названием BackRub в гигант Google [116].

Ценность и польза технологий «снаружи внутрь» зачастую неясны не только до их появления, но и на протяжении многих лет после этого. Веб, детище Тима Бернерса-Ли, зародившаяся в швейцарской физической лаборатории, явилась

в этот мир в 1989 году «недоношенной», но потом она росла в геометрической прогрессии, поскольку многие разработчики и предприниматели быстро увидели ее потенциал. Как шутит мой друг-технарь Сеп Камвар, если бы вы спросили тогда людей, что им нужно для лучшей жизни, они вряд ли сказали бы, что остро нуждаются в децентрализованной сети информационных узлов, связанных друг с другом с помощью гипертекста. И все же, если оглянуться назад, им, судя по всему, нужно было именно это.

Отрасли часто зарождаются из хобби. Программное обеспечение с открытым исходным кодом, прежде чем стать мейнстримом, возникло как нишевое движение против авторских прав. Социальные сети зародились как развлечение в среде идеалистов-энтузиастов блогерства, и только потом эту идею принял мир. То, что энтузиасты в футболках и шлепанцах зачинают крупные отрасли, может казаться забавной причудой и свидетельством эксцентричности индустрии высоких технологий, но хобби тут действительно играет огромную роль. Бизнесмены голосуют своими кошельками: они нацелены преимущественно на создание краткосрочной финансовой отдачи. А инженеры голосуют своим временем: они обычно мечтают изобрести что-то новое и действительно интересное.

Хобби — то, на что расходуют свое время самые умные люди, когда не ограничиваются краткосрочными финансовыми целями. То, что умнейшие из умнейших делают сегодня по выходным, через десять лет будут делать все остальные в рабочее время.

Эти два режима развития технологий: «изнутри наружу» и «снаружи внутрь» — часто дополняют и усиливают друг друга. Пример — комбинация тенденций, способствовавших развитию и росту вычислительной техники в последнее

десятилетие. Как упоминалось ранее, мобильные устройства — технология «изнутри наружу», пионерами которой были Apple, Google и другие, — сделали компьютеры доступными миллиардам людей. Технология социальных сетей — «снаружи внутрь», детище хакеров вроде Марка Цукерберга, бросившего Гарвардский университет, — стимулировала их использование и монетизацию. Облачная технология, тоже типа «изнутри наружу», разработанная Amazon, позволила масштабировать серверную часть веб-сервисов [117]. Когда два режима совпадают, это позволяет высвободить огромную мощь, примерно как при ядерной реакции.

Блокчейны представляют собой классическую технологию «снаружи внутрь». Как уже говорилось, большинство старожилов индустрии высоких технологий ее игнорируют, а некоторые сотрудники этих компаний даже принижают и высмеивают. Многие пренебрегают блокчейнами и вовсе не считают их компьютерами. Развитием блокчейнов занимаются стартапы и независимые группы разработчиков с открытым кодом. Иначе говоря, возглавляют это новое компьютерное движение энтузиасты отрасли — так же как первые сети с протоколами, например Веб, и ПО с открытым исходным кодом, такие как Linux.

Блокчейны — новый вид компьютера

В опубликованной в 2008 году статье Сатоши Накамото — это псевдоним изобретателя или коллектива изобретателей (точно до сих пор никому не известно) — представил миру первый блокчейн [118]. Накамото не называл свое изобретение так — он использовал термины block (блок) и chain (цепочка) отдельно, — но сообщество, сложившееся вокруг его идей, со временем «склеило» два слова в одно. В той статье

новый вид цифровых денег, биткойн, описывался как «электронная платежная система, основанная на криптографическом доказательстве, а не доверии, что позволяет любым двум сторонам заключать сделки напрямую друг с другом без потребности в доверенной третьей стороне». Чтобы удалить из процесса доверенную третью сторону, Накамото нужен был инструмент, позволяющий системе выполнять вычисления независимо. Для этого он и предлагал использовать новый тип компьютера, блокчейн.

Компьютер — концепция абстрактная, определяемая скорее тем, что он делает, чем тем, из чего он сделан. Первоначально так называли людей, занимавшихся вычислениями. В XIX и XX столетиях это слово стало относиться к машинам, способным производить вычисления. В знаменитой работе, написанной в 1936 году и посвященной математической логике, британский математик Алан Тьюринг исследует природу и пределы применения алгоритмов и предлагает более четкое обоснование этого явления [119]. Автор дал определение того, что сегодня ученые-компьютерщики называют конечным автоматом, а все остальные — просто компьютером.

Конечный автомат состоит из двух частей: 1) места для хранения информации и 2) средств изменения этой информации. Хранящаяся в автомате информация — эквивалент компьютерной памяти. Наборы инструкций, называемые программами, определяют, как принять начальное состояние, входные данные, и вывести новое состояние, результат. Поскольку в мире гораздо больше людей, которые умеют читать и писать, чем тех, кто умеет программировать, я люблю описывать вычисления с использованием лингвистической терминологии. Представьте, что *существительные* представляют собой состояние или память — то, чем мы можем

манипулировать, *глаголы* — код или программы: действия, посредством которых осуществляется это манипулирование. Я еще не раз повторю: все, что вы способны нарисовать в своем воображении, можно закодировать. Именно поэтому я сравниваю кодирование с творческой деятельностью, такой, например, как написание художественной литературы. В этом смысле компьютеры крайне разнообразны и разносторонни.

Конечный автомат — самый четкий способ представления о компьютере. Блокчейн Накамото — не физический компьютер, такой как ПК, ноутбук, телефон или сервер, а виртуальный: компьютер по функциям, а не материальному воплощению. Блокчейны — программная абстракция, которая накладывается поверх физических устройств. Это конечные автоматы. Когда-то слово «компьютер» стало вместо людей обозначать машины; теперь этот термин охватывает не только аппаратное обеспечение, но и программное.

Компьютеры на базе ПО, или «виртуальные машины», существуют с тех пор, как IBM в конце 1960-х разработала первый компьютер и в начале 1970-х вывела его на рынок [120]. Позже, в конце 1990-х, ИТ-гигант VMware сделал эту технологию массовой и популярной. Сегодня любой может запустить виртуальную машину, загрузив на свой ПК так называемую программу-гипервизор. Компании обычно используют такие машины для оптимизации управления корпоративными центрами обработки данных, и они играют ключевую роль в работе провайдеров облачных услуг. Блокчейны расширяют модель программных вычислений на новый контекст. Компьютеры могут быть построены разными способами; они определяются своими функциональными свойствами, а не внешним видом.

Как работают блокчейны

Блокчейны изначально, по своей конструкции, устойчивы к манипуляциям [121]. Они строятся на базе сети физических компьютеров, к которой может подключиться каждый, но которую чрезвычайно трудно контролировать кому-то одному. Эти физические компьютеры поддерживают нужное состояние компьютера виртуального и контролируют его переходы в новые состояния. В сети Bitcoin эти физические компьютеры называют майнерами, но сегодня больше распространен другой термин, «валидаторы»: они и правда выполняют именно функцию валидации (переходов, или смены) состояния.

Если концепция перехода состояния кажется вам излишне абстрактной, попробуйте воспользоваться аналогией. Думайте о биткойне как о странной электронной таблице или бухгалтерской книге с двумя столбцами. (Все, конечно, гораздо сложнее, но уж потерпите.) Каждая строка первого столбца имеет уникальный адрес. В каждой строке второго столбца указано количество биткойнов, хранящихся по этому адресу. Переходы состояния обновляют строки во втором столбце, отражая все переводы биткойнов, выполненные в последнем блоке транзакций. В этом вся суть.

Но как же виртуальный компьютер обеспечивает единый источник истины о его состоянии, если к сети может присоединиться любой желающий? Проще говоря, если электронная таблица открыта и доступна всем, как можно доверять числам, которые видишь в ее ячейках? Ответ: посредством математических гарантий, в частности криптографии (наука о безопасности коммуникаций) и теории игр (наука о принятии стратегических решений).

Рассмотрим, как некое предложенное состояние становится следующим состоянием компьютера. Во время каждого перехода состояния валидаторы запускают процесс для достижения консенсуса по следующему состоянию сети. Во-первых, они делают то, что следует из их названия: осуществляют валидацию, проверяя, что каждая транзакция подтверждена надежной цифровой подписью. Затем сеть случайным образом выбирает одного валидатора, который объединяет проверенные транзакции вместе для перехода к следующему состоянию сети. Другие валидаторы проверяют, что новое состояние отвечает требованиям сети, как и все транзакции в блоке, и что главные обязательства блокчейн-компьютера выполнены (например, если говорить конкретно о биткойнах, что их число никогда не будет превышать 21 млн). Валидаторы фактически «голосуют» за новое состояние, опираясь на него при переходе в следующие состояния.

Этот процесс по определению гарантирует, что все работают на базе одной и той же проверенной версии истории — чтобы достичь *консенсуса.* Если какой-либо валидатор (или некое их подмножество) попытается смошенничать, остальные имеют все возможности уличить его во лжи и проголосовать против него. Правила этого процесса установлены так, что он не сработает, кроме только того случая, когда большинство валидаторов вступит в преступный сговор.

Если вернуться к нашему упрощенному примеру с электронной таблицей, новой мастер-копией будет таблица, предложенная выигравшим валидатором. Конечно, в реальности никакой таблицы нет. Есть только переходы состояний — суть вычислений. Каждый переход состояния называется блоком, и все блоки соединены в цепочку, в результате чего каждый может, просмотрев их, верифицировать полную

историю данного компьютера. Отсюда и название: блокчейн — цепочка блоков.

Переходы состояний могут содержать не только числа, отображающие простые балансы счетов, но и наборы вложенных компьютерных программ. Биткойн идет в паре с языком Bitcoin Script, который можно использовать для написания программ, модифицирующих переходы состояний. Однако этот язык изначально ограничен, по задумке. Он в основном позволяет людям переводить средства с одной учетной записи на другую или создавать учетные записи, контролируемые многочисленными пользователями. Более новые блокчейны — например, Ethereum, первый блокчейн общего назначения, дебютировавший в 2015 году, — позволяют программировать, используя гораздо более экспрессивные языки [122].

Добавление в блокчейны продвинутых языков программирования — прорыв поистине революционный. В итоге мы получили что-то вроде магазина приложений Apple для iPhone (только они модерируются, а блокчейны доступны всем и не требуют разрешений). Любой разработчик в мире может написать и запустить на базе блокчейнов вроде Ethereum приложение, начиная от торговых площадок и заканчивая метавселенными. Это чрезвычайно мощное свойство. Оно делает блокчейны неизмеримо более экспрессивными и универсальными, чем вышеупомянутая бухгалтерская книга из нашего примера. Конечно, блокчейны — не просто гроссбухи для табулирования данных. Это не базы данных, а полноценные компьютеры.

Однако, как известно, для запуска приложений на компьютерах нужны ресурсы. И блокчейны, созданные под конкретные приложения, такие как Bitcoin, и универсальные, например Ethereum, нуждаются в людях, которые платят за

вычислительные мощности, расходуемые на валидацию переходов состояний, а значит, они должны давать людям повод для инвестирования в них. Накамото предложил для этого отличный прием: цифровая валюта системы — в блокчейне Bitcoin это биткойн — сама по себе становится источником финансирования компьютеров, которые ее используют. Впоследствии эту схему скопировали другие блокчейны.

У каждого блокчейна есть собственный набор внутренних стимулов для привлечения людей. В большинстве систем валидатор получает небольшое вознаграждение за каждый новый блок или переход состояния. (Заметьте, что термин «валидатор» может относиться к компьютерам, которые голосуют за переходы состояний, или к физическим лицам либо группам людей, этими компьютерами управляющим.) Вознаграждаются только честные валидаторы — те, которые добросовестно проверяют цифровые подписи и предлагают только проверенные изменения в блокчейне. Этот финансовый стимул побуждает валидаторов продолжать поддерживать сеть и вести себя честно. (А еще деньги в блокчейны поступают за счет платы, взимаемой с пользователей; подробнее о том, как это работает, и о токенах мы поговорим в главе 10.)

Как уже говорилось, блокчейны не требуют разрешений; использовать эту сеть может каждый, у кого есть подключение к интернету. Накамото создал первый блокчейн, Bitcoin, именно таким потому, что считал все существовавшие на тот момент финансовые системы элитарными, отдающими явное предпочтение привилегированным посредникам, например банкам. А он хотел поставить всех в равные условия. Включение в схему требования подачи заявки или проверки кандидатов привело бы к появлению новых привилегированных посредников и непременно воссоздало бы проблемы

существовавшей тогда системы, которые Накамото хотел решить. Но и эта схема была чревата одной весьма серьезной проблемой: если любой компьютер сможет голосовать без ограничений, сеть наверняка наводнят спам и злоумышленники.

Решение этой проблемы, предложенное Накамото, заключалось в том, чтобы взимать «плату» за участие. Чтобы проголосовать за следующее состояние, майнеру нужно выполнить вычислительную работу, требующую затрат энергии, и представить доказательства того, что она проделана. Эта система, остроумно названная «доказательством работы» (PoW — proof of work), сделала возможным открытое голосование без разрешений, обеспечив при этом фильтрацию спама и других нечестных схем. Другие блокчейны, в том числе Ethereum, используют более новую систему, которую назвали «доказательством доли (владения)» (PoS — proof of stake). Вместо того чтобы требовать от валидаторов тратиться на электроэнергию, согласно этому механизму, они должны вносить залог, рискуя своими деньгами (так называемый стейкинг). Если валидатор работает честно, он получает небольшое денежное вознаграждение. Если же его поймают на лжи — например, на голосовании за неправильное состояние или одновременном предложении нескольких конфликтующих переходов состояний, — залог «урезается» либо конфискуется вовсе.

Одно из основных критических замечаний в адрес сети Bitcoin заключается в том, что ее работа требует потребления огромных объемов энергии, а это может нанести вред окружающей среде. Безусловно, негативные экологические последствия системы PoW помог бы смягчить переход на «чистые» источники энергии, скажем, на возобновляемую энергию плотин и ветряных турбин, но, думаю, более

эффективным подходом была бы ее полная замена менее энергоемкими системами, такими как PoS, которые полностью сняли бы возражения экологического характера против блокчейнов [123].

Доказательство доли не менее, а то и более надежно, чем доказательство работы, а также дешевле, быстрее и гораздо энергоэффективнее. Ethereum завершила переход на эту систему осенью 2022 года, и с весьма, надо признать, впечатляющими результатами. Ниже представлен график, отображающий энергопотребление Ethereum, которая использует доказательство доли, по сравнению с другими популярными системами.

Сравнение годового потребления энергии (Твт/ч) разных компаний с потреблением PoS Ethereum [124]

Банковская система	239	92 000 x
Глобальные центры обработки данных	190	73 000 x
Bitcoin	136	52 000 x
Золотодобывающие компании	131	50 000 x
Вся игровая индустрия США	34	13 000 x
PoW Ethereum	21	8100 x
Google	19	7300 x
Netflix	0,457	176 x
PayPal	0,26	100 x
Airbnb	0,02	8 x
PoS Ethereum	0,026	1 x

Многие блокчейны, упомянутые в этой книге, — за одним существенным исключением, Bitcoin, — используют доказательство доли. По моим ожиданиям, в будущем все популярнейшие блокчейны будут использовать эту систему. Так что тревоги по поводу чрезмерного потребления энергии ни

в коем случае не должны удерживать нас от принятия этой мощной новой технологии.

Как и весьма распространенное ныне заблуждение: что блокчейны изначально сопутствуют секретности и анонимности. Слово «крипто» несет в себе коннотацию приемов политического управления и интриг, но буквально оно означает «закодированный» или «скрытый». Из-за того, что это слово используется для обозначения криптоиндустрии, многие ошибочно полагают, что блокчейны скрывают информацию и, следовательно, идеально подходят для неправомерных и мошеннических действий. Подобная трактовка часто встречается, например, в теле- и кинофильмах, где преступники постоянно используют криптовалюту для тайных переводов незаконно заработанных денег. Это тоже не имеет ни малейшего отношения к действительности.

Фактически все, что происходит в популярных блокчейнах, таких как Bitcoin и Ethereum, напротив, общедоступно и может быть отслежено. Как и в случае с электронной почтой, в них можно создать фейковую учетную запись, но сегодня существуют компании, специализирующиеся на деанонимизации, и правоохранительные органы без особого труда распознают подлог [125]. Блокчейны *настолько* открыты и общедоступны по умолчанию, что их врожденная прозрачность, возможно, препятствует их принятию. Вам может показаться, что это противоречит здравому смыслу, особенно учитывая ошибочное восприятие обществом криптовалюты как своего рода «черного ящика», но это действительно так. Люди могут не захотеть использовать блокчейны для определенных действий, опасаясь, что это приведет к раскрытию конфиденциальной информации: данных о зарплате и банковских счетах, медицинских сведений и т. д. Сегодня реализуется ряд проектов, призванных решить эту проблему;

в их рамках пользователям напрямую предоставляют возможность сделать транзакции конфиденциальными. В самых передовых проектах подобного рода используется новейшая продвинутая криптография, — в частности, такие инновации, как «доказательства с нулевым разглашением» [126], — что позволяет проводить аудит зашифрованных данных, соответственно, снижает риск неправомерной деятельности и удовлетворяет потребность общества в четком соблюдении требований закона [127].

Блокчейны «крипто» не потому, что они обеспечивают анонимность (они ее вовсе не обеспечивают), а потому, что они основаны на революционном математическом открытии 1970-х, криптографии с открытым ключом [128]. Главное, что нужно знать об этой технологии: она позволяет нескольким сторонам, которые никогда раньше не общались, выполнять криптографические операции друг с другом. Две самые распространенные операции такого типа: 1) *шифрование* (кодирование информации, которую сможет расшифровать только конкретный получатель) и 2) *аутентификация* (позволяет человеку или компьютеру подписывать информацию, подтверждая ее подлинность и то, что она гарантированно исходит из конкретного источника). Так вот, когда блокчейны описывают как криптотехнологию, этот термин используется во втором смысле: они не «зашифрованные», а «аутентифицированные».

Фундамент безопасности блокчейна — пары открытых (публичных) и закрытых (секретных) криптографических ключей. Люди используют закрытые ключи — числа, которые хранятся в секрете, — для создания транзакций в сети. А открытые ключи, напротив, идентифицируют публичные адреса, по которым проводятся транзакции. Характер математической связи, соединяющей пару ключей, таков, что

извлечь открытый ключ из закрытого не составляет труда, но извлечение закрытого ключа из открытого потребует неимоверных усилий и огромных объемов вычислительной мощности. Это позволяет пользователю блокчейна отправить деньги другому человеку, зафиксировав подписью транзакцию, которая, по сути, означает следующее: «Я даю тебе эти деньги». Эта подпись, по существу, аналогична таковой на банковском чеке или юридическом документе в офлайн-мире, просто для предотвращения подделок в ней вместо уникального почерка используется математика.

Цифровые подписи широко, но негласно используются в сфере компьютерных вычислений для верификации подлинности и достоверности данных. Браузеры проверяют их, чтобы убедиться в законности сайтов. Серверы и клиенты электронной почты используют такие подписи в качестве гарантии, что сообщения не подделываются и ими не манипулируют при передаче. Большинство компьютерных систем путем верификации подписей проверяют, что ПО загружается из нужного источника и оно не подделано.

Блокчейны тоже используют цифровые подписи — для обеспечения функционирования децентрализованных сетей «без доверия». Согласен, фраза «без доверия» может сбивать с толку своей двусмысленностью, но в контексте блокчейна она всегда означает только одно: что для надзора над транзакциями ему не нужны никакие высшие авторитеты, ни посредники, ни центральные корпорации. Благодаря процессам достижения консенсуса блокчейны способны самостоятельно и весьма надежно верифицировать отправляющую сторону транзакции, и никакой компьютер не обладает властью изменять эти правила.

Грамотно спроектированные блокчейны используют стимулы, побуждающие валидаторов к честности. А некоторые,

например Ethereum, еще и наказывают их за неправомерное поведение. Основой гарантий безопасности блокчейнов, опять же, становятся системы консенсуса. Если затраты на атаку на блокчейн достаточно высоки, а большинство валидаторов действуют честно, в соответствии со своими материальными интересами (и именно так обстоят дела в большинстве популярных блокчейнов), система безопасна. Но в случае крайне маловероятной успешной атаки участники сети могут «расщепить» ее, сделав «хардфорк» (блокчейн «расщепляется» на два отдельных блокчейна, работающих параллельно), и откатить блокчейн к предыдущей верной точке. Это создает для злоумышленников дополнительные препятствия.

Даже если некоторые нечестные и особо азартные пользователи пытаются использовать блокчейн ради наживы, эта система обеспечивает честность всех и каждого. В этом ее гениальность — в наборе структур стимулов, позволяющем ей контролировать себя. Благодаря тщательно продуманным материальным вознаграждениям блокчейны побуждают пользователей к взаимному контролю. В результате, даже если пользователи не верят друг другу, они могут полностью доверять децентрализованному виртуальному компьютеру, безопасность и защищенность которого они сами коллективно обеспечивают.

На практике система «без доверия» позволяет людям создавать сети, работающие совсем не так, как традиционные онлайн-системы. Большинство интернет-сервисов, такие как онлайн-банки или соцсети, требуют от человека, желающего получить доступ к своим данным и деньгам, войти в систему, залогиниться. Эти компании хранят наши персональные и учетные данные для входа в своих базах, которые могут быть взломаны или неправомерно использованы. В некоторых корпоративных сетях уже используется криптография, но

в основном интернет-сервисы полагаются на так называемую охрану периметра — подход, включающий использование разных технологий вроде файрволов и систем обнаружения вторжений, которые предназначены для защиты внутренних данных от посторонних и неавторизованных сторон. Эта модель сродни тому, чтобы возвести вокруг крепости, набитой золотом, высоченные стены и стараться защитить только их. Она явно не работает. Утечки данных сегодня стали явлением настолько распространенным, что уже никого особо не удивляют. Более того, модель охраны периметра во многом благоприятствует злоумышленникам, ведь им достаточно одной щелки, чтобы проникнуть внутрь.

А вот блокчейны позволяют вам хранить свои данные и деньги, но вы не можете залогиниться, войти в это хранилище, поскольку *входить некуда*. Вместо этого, решив перевести кому-то деньги, вы отправляете подписанные транзакции в блокчейн. При этом сохраняете конфиденциальность своих персональных данных; вам не нужно делиться ими ни с одним сервисом, с которым вам взаимодействовать не хочется [129]. В отличие от корпоративных сетей, в блокчейнах отсутствует единая точка отказа. Здесь попросту нет привычных для интернет-сервисов внутренних серверов, куда можно «вломиться». Это открытые, общедоступные сети. Для «взлома» одной из них — если это вообще можно так назвать — потребуется захватить «большинство» узлов сети, а это крайне дорогостоящий и совершенно непрактичный план.

Ключевая концепция любой системы безопасности — «поверхность атаки». Этим термином описываются все места, в которых злоумышленник может найти уязвимости. Философия обеспечения безопасности блокчейнов заключается в использовании криптографии для минимизации

поверхности атаки. В модели просто нет золота, которое может быть украдено из крепости. Все данные, которые должны оставаться конфиденциальными, зашифрованы, и ключи имеются только у пользователей (и у всех, кого они авторизовали). Эти ключи, конечно, должны быть надежно защищены, и пользователи могут привлечь для выполнения этой задачи сторонних операторов ПО (кастодианов, или «хранителей»). Разница в том, что в блокчейне эти «хранители» будут сфокусированы исключительно на безопасности. В корпоративной модели хранить данные и управлять ими поручают разным случайным компаниям, зачастую без должного опыта в сфере безопасности. Больница сама обеспечивает сохранность медицинской документации, автодилер — своей финансовой отчетности и т. д. и т. п. Блокчейны же четко отделяют функцию безопасности от бизнес-функций и позволяют кастодианам делать то, что у них получается лучше всего.

Когда вы слышите о предполагаемых взломах блокчейна, речь почти всегда идет об атаках на институты, использующие криптографию, либо о старомодных фишинговых атаках на физических лиц. Ко взломам самих блокчейнов это обычно никакого отношения не имеет. В крайне редких случаях, когда они действительно подвергаются взлому, речь почти всегда идет о небольших, малоизвестных и плохо защищенных сетях. Успешная атака прерывает процесс обработки транзакций или позволяет злоумышленникам осуществить «двойные траты», потратив одни и те же деньги в нескольких местах. Такие атаки также известны под названием «атаки 51%»: чтобы добиться успеха, необходимо заполучить контроль над более чем половиной валидаторов системы [130]. Жертвами таких атак становились слабые системы, например Ethereum Classic и Bitcoin SV. Но для успешного нападения

на крупные блокчейны, такие как Bitcoin или Ethereum, потребуются настолько огромные средства и ресурсы, что эта задача практически неосуществима.

Впрочем, данный факт не останавливает людей от попыток это сделать. Многие пробовали атаковать популярные блокчейны, в частности Bitcoin и Ethereum, но ни одну из этих попыток и близко не назовешь успешной. Так что, можно сказать, эта технология проверена в боях. Блокчейны — по сути, крупнейшая в мире программа вознаграждения за ошибки. Их взлом мог бы стать для злоумышленников настоящим сокровищем, ведь это позволило бы им перевести себе огромные суммы, сотни миллиардов долларов. Но пока такого ни разу не было. Гарантии безопасности блокчейнов с продуманным дизайном до сих пор отлично работали не только в теории, но и на практике.

Почему блокчейны важны

Но что же побуждает человека писать программы, работающие на базе блокчейнов, а не на традиционных компьютерах, таких как веб-серверы или мобильные телефоны? Мы подробнее ответим на этот вопрос в части III, но тут предлагаю кратко пробежаться по принципиально новым для нашего мира свойствам и характеристикам блокчейнов.

Во-первых, они демократичны. Они доступны каждому. Они унаследовали дух и идеалы раннего интернета и так же, как он, предоставляют равные возможности для участия. Любой, у кого есть подключение к интернету, может загрузить и выполнять любой код по собственному желанию. Ни один пользователь не имеет привилегий перед другими, и сеть трактует и обрабатывает коды и все остальные данные одинаково. Согласитесь, это куда более справедливая система,

чем статус-кво сегодняшней индустрии высоких технологий с ее преградами.

Во-вторых, блокчейны прозрачны. Полная история их кодов и данных общедоступна; ее в любой момент может проверить любой желающий. Будь код и данные доступны только избранным, другие участники были бы поставлены в невыгодное положение, а это идет вразрез с эгалитарным обещанием этой технологии. Любой желающий может проверить историю блокчейна и удостовериться, что текущее состояние системы сгенерировано действительным, правомерным процессом. Даже если вы не проверяете код и данные лично, вы знаете, что другие могут это сделать и, скорее всего, делают. Прозрачность порождает доверие.

В-третьих и в-главных, блокчейны способны брать на себя твердые обязательства относительно своего поведения в будущем: что любой код, ими запускаемый, всегда будет работать так, как это изначально предполагалось. Традиционным компьютерам подобных обязательств не выполнить. Ими управляют люди или группы людей — либо напрямую, как в случае с персональными компьютерами, либо косвенно, как в случае с компьютерами корпоративными. А обязательствам людей, как известно, особо верить не стоит. Блокчейны же переворачивают эти отношения с ног на голову, в результате вся ответственность ложится на код. Вышеописанный механизм консенсуса и неизменность ПО блокчейнов делают их устойчивыми к вмешательству человека. Тут вам не нужно доверять обещаниям людей или компаний.

Инженеры таких компаний, как Google, Meta♦ и Apple, видят в компьютерах машины, которые они могут заставить выполнять свои приказы. Кто контролирует компьютер, тот контролирует и ПО, на котором оно работает. Единственные гарантии для пользователей относительно дальнейшей

работы их компьютеров — длиннющие юридические соглашения под заголовком «Условия обслуживания», составленные провайдерами ПО. Эти документы несут мало смысла, и почти никто не удосуживается их прочесть, не говоря уже о том, чтобы оспорить. (Не зря же говорят: «Облако — это просто чужой компьютер».)

С блокчейнами все иначе. Они замечательны не только тем, что могут, но и тем, чего не могут. Блокчейн устойчив к манипуляциям, и это, судя по всему, способствует ошибочному представлению, что он скорее сродни базе данных, чем компьютеру. Да, ПО блокчейна работает на чужих компьютерах, но — и это главное — весь контроль лежит на софте. Человек или компания, конечно, могут попытаться им манипулировать, но он будет сопротивляться любому несанкционированному вмешательству. Этот виртуальный компьютер продолжит работать, как изначально предполагалось, несмотря на попытки подорвать его функции.

Такая устойчивость к несанкционированному вмешательству характерна не только для блокчейнов, но и для ПО, работающего на их базе. Приложения, основанные на программируемых блокчейнах, таких как Ethereum, наследуют гарантии безопасности этой платформы. Это означает, что приложения: социальные сети, торговые площадки, игры и многое другое — тоже могут брать на себя твердые обязательства относительно своего поведения в будущем. Это касается всего технологического стека: и самих блокчейнов, и того, что создано на их основе.

У критиков, не сумевших оценить мощь технологии блокчейнов, как правило, иные приоритеты. Многих людей, в том числе из пятерки крупнейших технологических компаний, заботит улучшение компьютеров по давно знакомым параметрам, таким, например, как память и вычислительная

мощность. И они рассматривают возможности блокчейнов как ограничения — скорее в негативном, чем в позитивном ключе. Им, привыкшим к безраздельной власти, трудно осознать, что компьютеры могут улучшить какой-то параметр, отчасти призванный несколько ослабить их полномочия.

Революционные технологические прорывы за рамками нормы часто игнорируются по той же причине, по которой для ранних стадий развития новой технологии намного чаще характерно скевоморфное, а не нативное мышление. Предвзятость берет инновации в заложники.

Но вы, возможно, все еще недоумеваете: в чем же важность компьютеров и приложений, способных брать на себя максимально твердые обязательства относительно своего поведения в будущем? Как продемонстрировал Накамото, одна из главных причин в том, что это позволяет создать цифровую валюту. Обязательное требование любой успешной финансовой системы — доверие к ее долгосрочным обязательствам. В случае, например, с биткойном это обязательство, что в мире никогда не будет создано более 21 млн монет; оно делает эту валюту безусловно и очевидно дефицитной. А еще биткойн гарантирует, что люди не смогут мошенничать, например использовать такой прием, как «двойные траты»: тратить одни и те же деньги в двух разных местах сразу. Эти обязательства — необходимые, но недостаточные условия ценности такой цифровой валюты, как биткойн. (Вдобавок к этому она должна иметь стабильные источники спроса, о чем мы подробно поговорим далее.)

В случае с традиционными компьютерами никакие обязательства особого веса не имеют, ведь люди или организации, которые их контролируют, могут просто передумать. Если бы Google воспользовалась стандартными серверами в своих центрах обработки данных для выпуска монет GoogleCoins

и заявила, что их будет только 21 млн, и ни монетой больше, ничто не заставило бы компанию в будущем выполнить это обязательство. Руководство может в одностороннем порядке и когда заблагорассудится изменить правила и ПО.

Корпоративные обязательства ненадежны. Даже если бы Google включила соответствующие пункты в свои условия обслуживания, она в любой момент могла бы их нарушить, пересмотрев соглашения, начав их обходить или вовсе заблокировав сервис (как это на сегодняшний день сделано почти с 300 продуктами) [131]. Мы просто не можем верить компаниям, что они непременно выполнят обещания, которые дают пользователям. Фидуциарные обязательства* превыше всего. Корпоративные обязательства на практике не работают и никогда не работали. Вот почему первая достойная попытка создать цифровые деньги была предпринята на базе блокчейна, а не какой-то компанией. (Теоретически некоммерческая организация имеет возможность брать на себя долгосрочные обязательства перед своими пользователями, но и здесь свои проблемы, о которых я рассказываю далее, в главе 11.)

Цифровые валюты — лишь первое из множества новых приложений, ставших возможными благодаря блокчейнам. Блокчейны, как и любой компьютер, — по сути, чистый холст, который технари могут использовать для инноваций и творчества. Их уникальные свойства открывают путь для целого ряда приложений, которые было бы невозможно создать на базе традиционных компьютеров. Полный их ассортимент нам еще только предстоит увидеть, но многие из них потребуют создания новых сетей, которые улучшат существующие,

* Фидуциарные обязательства — обязательства, принимаемые на себя каким-либо лицом, осуществляющим свою профессиональную деятельность в пользу другого лица. *Прим. науч. ред.*

предложив новые возможности, более низкую стоимость, лучшую совместимость, более справедливое управление и честное распределение материальных плодов.

В качестве примера можно назвать, скажем, финансовые сети, которые берут на себя обязательства по займам, кредитованию и прочим видам деятельности на прозрачных и предсказуемых условиях; социальные сети, которые обязуются улучшить экономический аспект, конфиденциальность данных и прозрачность для пользователей; игровой мир и мир виртуальной реальности, которые обязуются обеспечить открытый доступ и благоприятные экономические условия для создателей и разработчиков; медиасети, которые обещают предложить создателям контента новые способы зарабатывания денег и сотрудничества. И наконец, сети для ведения коллективных переговоров, которые обязуются справедливо вознаграждать авторов и художников, чьи произведения используют ИИ-системы. Обо всех этих и других сетях, а также о том, как они приводят к лучшим результатам, я расскажу дальше (особенно в части V), но сначала мы с вами рассмотрим механизм, с помощью которого блокчейны обеспечивают право собственности.

издательство
МАНН, ИВАНОВ И ФЕРБЕР
Максимально полезные книги