Александр Цихилов
Блокчейн

Текст предоставлен правообладателем
«Блокчейн: Принципы и основы»: Интеллектуальная Литература; Москва; 2019
ISBN 978-5-6042-8813-9

Аннотация

Большая часть информации, представленная на сегодняшний день по блокчейн, страдает отрывочностью, однобокостью или сложностью терминологии. Перед вами – первое систематизированное изложение темы блокчейн на русском языке, в котором автор технологически сложные концепции объясняет понятным языком.

Помимо истории возникновения и описания технологии, в книге рассмотрены наиболее популярные проекты, реализованные на блокчейн, уже существующее и потенциальное применение в различных отраслях, а также проблематика взаимоотношений блокчейн-проектов и государств. Наконец, автор подробно разбирает самые востребованные и популярные темы – инвестиции в криптоактивы, связанные с ними риски и перспективы развития блокчейн. Книга адресована широкому кругу читателей и будет интересна как техническим специалистам, так и аудитории, далекой от финансовых и IT-технологий.

Александр Цихилов
Блокчейн: Принципы и основы

Редактор *Екатерина Закомурная*
Руководитель проекта *М. Пикалова*
Дизайн обложки *М. Грошева*
Корректор *Ю. Николаева*
Компьютерная верстка *Б. Руссо*

* * *

Часть I
Как устроен блокчейн

Предисловие

«Сначала они не замечают тебя, потом они смеются над тобой, затем они начинают войну, желая сжечь тебя, и, наконец, они воздвигают тебе памятники…»

Это цитата из речи американского профсоюзного адвоката Николаса Кляйна, которую, в несколько измененном виде, часто ошибочно приписывают Махатме Ганди. Кляйн произнес эту речь сто лет назад совсем по другому поводу, однако эти слова, как никакие другие, наилучшим образом подходят к ситуации, которая сложилась вокруг некого явления. Оно ворвалось в нашу жизнь недавно, но столь стремительно, что создало вокруг себя вихри полярных суждений: от категорического неприятия у противников до бурных восторгов у апологетов. Сам факт подобного дискурса означает, что явление, вокруг которого ломается столько копий, само по себе неординарно и заслуживает вдумчивого изучения. Это явление – технология блокчейн и построенные на ее основе проекты.

Действительно, блокчейн и, в частности, его практические реализации в виде криптовалют – предмет оживленных дискуссий как в

мире компьютерных технологий, так и в финансовой индустрии. Относительная техническая сложность создает некоторые препятствия для быстрого понимания всех преимуществ и недостатков этой нетривиальной технологии. Те же, кто сумел постичь основные аспекты принципов работы блокчейн-сетей, довольно быстро приходят к мысли, что появление и дальнейшее развитие этой технологии может привести к существенному изменению картины современного мироустройства. Одних эта мысль приводит в восторг, других – повергает в уныние. Для кого-то появление такой технологии – шанс самореализации в новой отрасли, а кто-то всерьез опасается утратить текущие позиции в отраслях, для дальнейшего существования которых блокчейн может представлять угрозу.

Появившийся в 2008 году документ за авторством некоего Сатоши Накамото и последовавшая за ним первая практическая реализация на базе технологии блокчейн – проект Биткоин – прошли в то время совершенно незамеченными для мирового сообщества. Если на этот проект кто-то и обратил тогда внимание, то только специалисты-криптографы, которых в основном интересовали лишь профессиональные аспекты. Позднее, когда информация начала потихоньку распространяться, над проектом начали откровенно посмеиваться – сама идея о том, что есть некая электронная валюта, обеспеченная потребленным на ее эмиссию электричеством, казалась многим забавной. Однако когда стоимость одной монеты биткоин стала исчисляться тысячами долларов, многим стало не до смеха.

По-настоящему массовый интерес к блокчейн-проектам начал проявляться в первой половине 2016 года. И вот тогда, если следовать цитате Кляйна, блокчейн-индустрия перешла на следующий этап своей эволюции – ей начали оказывать противодействие. Проекты на блокчейне стали создавать серьезные угрозы и конфликты интересов для национальных правительств, финансовых регуляторов, традиционных финансовых институтов и крупных посреднических сервисов. Справедливости ради следует отметить, что многие из этих угроз небеспочвенны, и несколько глав этой книги будут посвящены описанию и анализу данной проблематики.

Что касается критики или негативного отношения к технологии в целом, очевидно, что трудно было бы ожидать позитива и поддержки для явления, принципы работы которого сами по себе достаточно непросты для понимания. Задача книги – объяснить технологически сложные концепции понятным, насколько это возможно в данном контексте, языком. Таким, чтобы читатели, даже достаточно далекие от компьютерных или финансовых технологий, смогли бы составить для себя ясное представление о принципах работы технологии блокчейн и построенных на ее базе проектах. Книга не будет содержать сложных математических аппаратов с замысловатыми формулами или чрезмерно подробных описаний алгоритмов. Многие относительно сложные концепции переработаны с целью упрощения их понимания и обрисованы в книге «крупными штрихами». С самого начала хотелось бы отметить, что автор книги – не математик, не физик, не историк, не экономист и уже пару десятков лет как не программист. Автор – предприниматель, криптоэнтузиаст и в какой-то степени даже блокчейн-евангелист, исходя из чего и следует рассматривать изложенные в книге мировоззренческие позиции относительно столь масштабного и захватывающего явления, как блокчейн.

Теперь о структуре книги. После краткого исторического экскурса в историю изобретений, которые в свое время серьезно изменили мир, последует раздел, посвященный подробному описанию технологии блокчейн. Затем будут рассмотрены наиболее популярные проекты, реализованные на блокчейн – в основном речь пойдет о криптовалютах. Следующий раздел посвящен потенциальному применению технологии в различных отраслях: будут описаны как уже существующие проекты, так и еще только планируемые к реализации. О разделе, посвященном описанию проблематики взаимоотношений блокчейн-проектов и государств, уже говорилось выше. Наконец, последует один из наиболее востребованных читателями разделов, связанный с инвестициями в криптоактивы. Многие мечтают извлечь значительный доход от криптоинвестиций, однако не все потенциальные инвесторы достаточно хорошо осведомлены обо всех рисках, связанных с этим процессом, и о том, каким образом необходимо этими рисками управлять. Заключительный раздел книги касается перспектив развития технологии блокчейн.

И, наконец, хотелось бы сказать несколько слов об актуальности информации в книге. Блокчейн-индустрия и события внутри нее развиваются весьма динамично. В связи с этим не исключена ситуация, что на момент прочтения книги определенные факты, в ней изложенные, могут уже стать несколько устаревшими, а недорассказанные истории успеют получить продолжение. Одновременно с этим в книге представлена информация фундаментального характера, которая едва ли существенно изменится со временем. Причем описания подобного рода будут превалировать в представлениях автором различных концептов, составляющих технологию блокчейн. Учитывая вышеизложенное, есть надежда, что даже спустя некоторое время с момента выхода книги ее содержание останется интересным для читателей, желающих познакомиться со столь занимательным предметом, как блокчейн.

Автор выражает искреннюю благодарность друзьям и коллегам за помощь и поддержку, без которой появление этой книги было бы невозможным.

Изобретения, изменившие мир

История человеческой цивилизации насчитывает тысячи лет. За это время человечество прошло длинный путь от примитивных приемов и практик, используемых в древности, до сложнейших современных технологий. За всей эволюцией человеческой цивилизации стоит цепочка важнейших изобретений, каждое из которых в свое время оказало серьезное влияние на жизнь людей и способствовало

переходу на следующую ступень развития. Обычное колесо, появившееся более 6000 лет назад, существенно облегчило задачу перемещения людей и грузов. А произошло это лишь на основании понимаемого на интуитивном уровне факта, что сила трения качения на относительно ровной поверхности существенно меньше, чем сила трения скольжения. В итоге выяснилось, что катить груз на колесах значительно легче, тем тащить его по земле волоком. Примерно тогда же стали появляться первые попытки зафиксировать речевую информацию в форме рисунков и знаков с целью ее дальнейшего сохранения. Так появились ранние зачатки письменности, а вместе с ними – возможность накапливать и распространять начальные элементы человеческого знания. Через какое-то время, по мере появления ранних государственных образований, человечеству потребовалось научиться учитывать и распределять подконтрольные ресурсы – так появились цифры и элементарные арифметические действия над ними.

Начало первого тысячелетия нашей эры было отмечено военным, политическим и культурным доминированием Римской Империи на территории Европы, Северной Африки и Ближнего Востока. Как следствие, римская система счисления получила на этих территориях широкое применение и продолжала использоваться и после падения империи в конце V века. Однако непозиционная система записи чисел была крайне неудобной, особенно в части совершения более сложных арифметических операций, таких, например, как умножение и деление. Развитие точных наук, усложнение их математических аппаратов, да и более затейливые формы учета ресурсов и их движения создали общественный запрос на более прогрессивную систему счисления – позиционную. На рубеже X и XI веков французский ученый (и будущий Папа Римский) Герберт Аврилакский стал одним из первых популяризаторов такой системы, которую он позаимствовал во время своего обучения в Испании, большей частью находившейся в то время под арабским владычеством. Новая система прижилась в Европе не сразу, и только к середине XIII века, благодаря усилиям итальянского ученого Фибоначчи, «арабские цифры» начали получать относительно широкое распространение. Это дало существенный толчок к созданию и развитию индустрии финансовых услуг в Европе и в первую очередь в самой Италии, которая стала финансово-технологическим флагманом позднего Средневековья.

Именно в Италии того периода была наконец в значительной степени решена задача эффективного учета движения товарно-денежных ценностей, а именно – была изобретена двойная бухгалтерская запись. Суть метода двойной записи состоит в балансировании активов и пассивов. Иными словами, изменяя их величины, необходимо поддерживать их в постоянном совокупном равенстве. Возникли первые учетные книги, содержащие бухгалтерские проводки (прообразы транзакций) на базе двойной записи, появились первые балансы и отчеты о прибылях и убытках. Все это позволило заложить основу для более сложных моделей ведения предпринимательской деятельности, а также образовать первые кредитные институты. Считается, что именно в средневековой Италии появились первые банки, в частности – Банк Святого Георгия в 1407 году, в Генуе. Принцип двойной записи, позволяющий сопоставлять источники средств и направления их расходования, способствовал развитию системы банковского кредитования. Банки активно ссужали деньги торговцам, нобилитету и даже европейским суверенам. Взамен банкиры получали не только значительный доход от процентов по кредитам, но и могли добиться существенного политического влияния, как, например, семья Медичи из Флоренции, представители которой в конечном итоге стали герцогами Тосканскими и наследственными правителями целой области.

Очередной революцией в области сохранения и распространения человеческого знания стало изобретение печатного пресса Иоганном Гутенбергом в 1448 году. Строго говоря, принципы печатания текстов на бумаге или ткани были известны и ранее – в Китае, примерно с IX века. Разница состояла лишь в том, что для оттиска на бумаге текст гравировался на специальной деревянной доске полностью, а не набирался отдельными литерами. Однако именно появление наборного шрифта создало необходимую гибкость, свободу и удобство для активного развития книгопечатания. Изобретение печатного станка позволило распространять научные знания с невиданной доселе скоростью, что в конечном итоге привело человечество к научной революции Нового Времени. Унаследованное от предков традиционное видение основных принципов мироустройства подверглось коренному пересмотру такими учеными, как Коперник, Галилей и Ньютон.

С давних времен люди размышляли над тем, каким образом создать механизмы, которые бы не нуждались в приложении мускульной силы человека или животного. Во второй половине I века нашей эры греческий математик и механик Герон Александрийский (более известный как изобретатель «золотого правила механики») создал первую модель парового двигателя. Несмотря на крайнюю примитивность аппарата, Герон создал на его основе такие устройства, как вращаемая водяным паром сфера, механизм автоматического открывания дверей и даже автомат по продаже «святой воды». Из-за весьма низкого уровня распространения знаний в те времена поистине революционное изобретение Герона было забыто почти на семнадцать столетий, если не считать отдельных экспериментов с водяным паром в XVI–XVII веках, проводимых египетскими и итальянскими инженерами. Только в 1781 году шотландский инженер-изобретатель Джеймс Уатт запатентовал свою модель парового двигателя, который, будучи изобретенным заново, фактически положил начало английской промышленной революции. Если бы паровой двигатель Герона не был забыт на столь длительное время, технологическая революция могла бы состояться гораздо раньше, и кто знает, может быть, уже веку к IX, то есть еще в эпоху Карла Великого, человечество смогло бы начать процесс освоения космического пространства. Однако это, увы, не единственное серьезное изобретение, которое было забыто на слишком долгий период человеческой истории.

В 1936 году австрийский археолог Вильгельм Кённинг обнаружил в предместье Багдада странный предмет – небольшой

керамический сосуд высотой около 13 см с залитым смолой горлышком, из которого выступал кончик железного стержня. Находку датировали по стилю керамики и отнесли к эпохе Сасанидской империи (224–651 гг. н. э.). Археолог предположил, что данный сосуд – не что иное, как примитивная форма гальванического элемента, иначе говоря – батареи, предназначенной для выработки электрического тока. Доподлинно неизвестно, применялась ли «багдадская батарейка», как ее назвали, по предполагаемому назначению. Известны мнения ряда скептиков, что это маловероятно – в силу полного отсутствия сопутствующих находок, которые данная «батарея» могла бы питать. Однако некоторые ученые все же считали, что, например, процесс гальванизации (покрытие одного металла тонким слоем другого с помощью электролиза) уже был известен как минимум 2000 лет назад. Так или иначе, еще в Древней Греции люди обратили внимание на странные свойства янтаря, который, если потереть его о шерсть, начинал притягивать легкие предметы. Так, еще неосознанно, человечество столкнулось с явлением, которое потом назовут «электричеством», что, собственно, и означает в прямом переводе «янтарность». Как и в случае с паровым двигателем, системный подход к изучению электричества начал осуществляться только во второй половине XVIII века, а основные научные законы, с ним связанные, появились еще веком позже. Электричество, поставленное на службу человечеству, изменило облик цивилизации. Освещение, отопление, приведение в движение механизмов, передача информации – все это осуществляется при помощи электричества, и современный человек не мыслит свою жизнь без этого ценнейшего научного достижения, которое открыло дорогу еще более важным изобретениям.

Исследования электромагнитного излучения Фарадеем, Максвеллом и Герцем привели к появлению устройств, позволяющих передавать информацию на расстоянии – сначала телеграфом (по проводам), а затем по радио (без проводов). Появились резисторы, конденсаторы, трансформаторы, электрические ключи, вакуумные электронные лампы и прочие электронные компоненты. На их базе создавались и развивались различные электроприборы как промышленного, так и бытового назначения. В 1946 году в США появилась первая электронно-вычислительная машина ENIAC на электронных лампах, весом в 27 тонн и вычислительной мощностью в 5000 операций в секунду. Впоследствии при изготовлении компьютеров от громоздких и капризных в эксплуатации электронных ламп отказались и перешли на полупроводниковые технологии. Компьютеры стали сильно уменьшаться в размерах, одновременно серьезно прибавляя в вычислительной мощности. Изобретение микропроцессора в 1971 году способствовало появлению первых персональных компьютеров уже через несколько лет. Примерно в это же время начались первые эксперименты по практическому созданию глобальной телекоммуникационной сети для обмена электронными почтовыми сообщениями. Впоследствии эти начинания эволюционировали в то, что нам сейчас известно как сеть интернет. Благодаря ей человечество получило уникальную возможность исключительно быстро и в значительных объемах накапливать, распространять и получать информацию во всех областях человеческого знания. В мире произошла очередная технологическая революция, вновь до неузнаваемости изменившая окружающий мир и позволившая человечеству открыть новую страницу в развитии цивилизации.

К середине 90-х годов XX века интернет получил достаточно широкое распространение, а к началу XXI века стал предметом практически первой необходимости для людей, активно его использующих. Подавляющее большинство коммерческих предприятий и государственных служб создали свои представительства в интернете – от простейших «домашних страниц» до масштабных порталов, на которых можно получить необходимую информацию, заказать услугу или приобрести какой-либо продукт. С развитием социальных сетей проникновение интернета в повседневную жизнь многократно усилилось. Начался активный процесс вытеснения традиционных средств массовой информации: печатных изданий, телевидения и радио. Интернет-магазины начали составлять значительную конкуренцию обычным магазинам, а большинство финансовых операций стали проводиться без физического посещения офисов банков – вместо этого стали использоваться банковские интернет-приложения. Телефонные звонки финансовым брокерам сменились операциями через торговые интернет-платформы. Пользователи получили возможность консолидировать и визуализировать всю необходимую информацию для комфортного принятия инвестиционного решения, поскольку теперь у них был доступ к котировкам, графикам финансовых инструментов, аналитическим отчетам и рыночным прогнозам.

Логично предположить, что каждое новое революционное изобретение возникает не на пустом месте – ему предшествуют такие же масштабные и значимые открытия, формирующие непрерывную цепочку, протянутую сквозь века из современного мира в глубокую древность. Каждая технологическая революция становилась своего рода ответом на возникающие запросы цивилизации, формирующиеся под действием исторических обстоятельств. Одна из целей данной книги – донести до читателя мысль, что блокчейн представляет собой не менее значимое явление в человеческой истории, чем любое из вышеописанных изобретений. Появление криптовалют на базе технологии распределенного реестра – это также своеобразная форма ответа цивилизации на ту совокупность обстоятельств, которые сложились в современном финансовом мире, и аргументы, изложенные в последующих главах, преследуют цель убедить читателя в справедливости этих утверждений.

Введение в структуру блокчейн

Сама по себе блокчейн-технология не содержит чего-то принципиально нового или ранее науке неизвестного. Ценность модели функционирования блокчейн-сетей состоит в комбинировании различных инструментов, технологий и принципов, которые, будучи

определенным образом совмещенными, формируют логичную и защищенную структуру для распределенного хранения данных. Что же представляет собой блокчейн? Фактически его можно сравнить с большой бухгалтерской книгой, на страницах которой записываются проводимые между контрагентами финансовые операции. Только книга эта составлена так, что каждая запись, которая в нее попадает, не может быть впоследствии никаким образом изменена или удалена – этому будут препятствовать серьезные криптографические алгоритмы, интегрированные в технологию. Сами же данные хранятся не в каком-то конкретном месте, имеющем статус управляющего центра, а копируются и синхронизируются, или, иначе говоря – реплицируются между всеми участниками системы – узлами сети. Таким образом, даже если кто-то захочет поменять хранимые у себя данные, то другие участники системы просто не примут во внимание эти изменения, поскольку они были проведены вопреки принятым в системе правилам.

Как же устроена такая «бухгалтерская книга»? Ее «страницы» называются блоками. Так же, как и страницы в обычной книге, блоки следуют друг за другом в строгом пронумерованном порядке. Однако если обычную страницу можно из книги изъять или при желании переместить в другое место, а то и вовсе выбросить, то с блоками так обойтись не получится. Все блоки жестко сцеплены между собой специальными криптографическими «замками», взломать которые, даже теоретически, исключительно сложно. Отсюда, собственно, и название технологии – «блок-чейн» – от английского blockchain – «цепочка блоков». Для того чтобы стать надежным хранилищем данных, любая блокчейн-структура должна удовлетворять следующим критериям.

● Иметь децентрализованную технологическую основу, то есть уметь распространять между всеми узлами сети необходимые данные и поддерживать их актуальное состояние через процессы репликации и синхронизации.

● Поддерживать неразрывную связь между блоками данных путем формирования в каждом новом блоке ссылки на предыдущий по отношению к нему блок.

● Уметь эффективно кодировать массивы данных в уникальные информационные блоки стандартного размера, иначе говоря – хешировать данные.

● Применять исключительно стойкие к взлому криптографические алгоритмы, необходимые для защиты записываемых в блоки данных.

● Использовать элементы специального подраздела математики – теории игр – для того, чтобы все узлы системы соблюдали установленные правила и достигали общего консенсуса при создании новых блоков и записи в них данных.

Все вышеперечисленные задачи составляют пять основных «столпов», на которых базируется технология блокчейн. В дальнейшем мы рассмотрим каждый из них достаточно подробно. У читателей может возникнуть вопрос: а где же в блокчейн, собственно, деньги? Как они туда попадают, где хранятся, как их получить и как затем потратить? А главное, каким образом эти деньги защищены от посягательств злоумышленников? У всех на слуху слово «криптовалюта», которое прочно ассоциируется с технологией блокчейн. Более того, сам интерес людей к блокчейн чисто с технологической точки зрения, как правило, вторичен. Однако чтобы попытаться извлечь доход от инвестиций в криптовалюты, необходимо хотя бы на базовом уровне понимать принцип их работы.

На самом деле криптовалюты – это лишь одна из возможных «надстроек» над структурой блокчейн, а точнее – одна из форм его утилитарного использования. Так исторически сложилось, что самый первый проект, реализованный на базе этой технологии, Биткоин, является криптовалютной платежной системой. Причем достаточно небогатой по своим функциональным возможностям, что вполне простительно для генезисного проекта. Несмотря на то что понятия «биткоин» и «блокчейн» появились одновременно, их значения отнюдь не синонимичны, поскольку первое означает криптовалюту, а второе – собственно технологию, на базе которой данная криптовалюта реализована. К слову сказать, термин «криптовалюта» появился на несколько лет позднее, чем сам проект Биткоин – в 2011 году в журнале *Forbes* в статье CryptoCurrency. Сам же автор биткоина Сатоши Накамото называл его e-cash, или «электронная наличность». О Биткоине как о проекте мы еще подробно поговорим в разделе, посвященном практическим реализациям на базе блокчейн-технологии.

Децентрализация управления

Любые системы как совокупности связанных элементов, взаимодействующих между собой, нуждаются в управлении. Причем это касается любых систем – от форм социальной организации различных обществ до аппаратно-программных технологических комплексов. В противном случае их запланированная при проектировании и создании функциональность не гарантирована в силу того, что большинство систем неспособны к эффективной самоорганизации. С этой управленческой проблематикой человеческая цивилизация сталкивалась на протяжении всей своей истории.

Рассматривая различные варианты управления системами, можно в общем виде выделить две его основные формы: централизованную и децентрализованную.

Исторически наиболее ранняя форма управления социумом естественным образом сложилась во времена первобытных людей, когда родовые и племенные группы имели внутри себя строгую управленческую иерархию, но в отношении управления всей популяцией можно было говорить лишь о сугубой децентрализации. Более того, каждая группа в большинстве случаев представляла

собой управленческий изолят, поэтому всю совокупную популяцию вида Homo Sapiens сложно представить единой, хотя и децентрализованной системой. Действительно, управленческие связи между группами отсутствовали, а взаимодействие если и имело место, то носило исключительно деструктивный характер. Обычно оно было направлено на уничтожение или в лучшем случае ассимиляцию слабых групп более сильными. По мере развития социальных взаимоотношений между группами у них начали проявляться устойчивые связи, породившие в конечном итоге более сложные иерархические системы с доминирующими элементами во главе. Как только совокупная численность взаимодействующих внутри иерархии групп стала относительно большой, система стала приобретать черты централизованной модели. Иначе говоря, люди создали понятие «государство», во главе которого встал единоличный правитель, выборный или наследственный. Подобная форма государственного устройства оказалась вполне жизнеспособной, поскольку дожила до наших дней, хотя и претерпев различные модификации.

Таким образом, можно констатировать, что вынужденная форма децентрализованного управления социумом на ранних стадиях его становления эволюционировала в более прогрессивный на тот момент централизованный способ. Централизация породила возможность ресурсной консолидации, которая позволила осуществлять проекты на государственном уровне – вести захватнические войны или заниматься масштабным строительством, хотя, впрочем, одно никогда не исключало другого. История таких древних государств, как Вавилон или Египет, – наглядные тому примеры. На первый взгляд, централизация – единственно верный и наиболее эффективный вариант управления системами. Однако уже в средневековый период нашей истории начали появляться и другие управленческие формы. Речь в данном случае не идет об эволюции управленческих принципов, но в некоторых случаях политические обстоятельства просто не позволяли создавать эффективные централизованные управленческие модели.

Хорошим примером является католическая церковь, которая фактически стала, хотя и не без многовековой борьбы, независимым наднациональным институтом в средневековой Европе. И хотя сама внутренняя структура католической церкви была строго иерархичной, а управление в ней в значительной степени централизованным, непосредственные выборы главы церкви были результатом политического консенсуса между великими европейскими державами. Воспоследовавший в эпоху раннего Нового Времени протестантизм и вовсе привнес чистую децентрализацию в организацию новой конфессиональной структуры. Возникла пресвитерианская форма управления церковными общинами в пику традиционному, централизованному епископальному управлению.

Государства также не отставали от прогресса в части организации своего устройства: в 1291 году на карте средневековой Европы появилось по-настоящему децентрализованное государство – Швейцарская Конфедерация – союз нескольких независимых кантонов с фактическим отсутствием центрального управленческого политического института. Сейчас мы можем оценить это давнее событие по достоинству – Швейцария не только не утратила свой суверенитет за века, но и сумела стать одной из самых социально благополучных стран мира. С другой стороны, история знает немало примеров, когда децентрализация в виде феодальной раздробленности государств приводила к их ослаблению, а подчас и гибели.

Эти примеры говорят о неоднозначности утверждения, что одна из форм управления системами лучше другой. Безусловно, у обеих управленческих форм есть свои плюсы и минусы. Попробуем перенести наш анализ от форм социального устройства к технологическим системам. Схожесть социальной и технологической формы управления базируется на общем принципе, который сводится к приложению совокупности управляющих воздействий субъекта на объект. Рассмотрим в качестве технологического примера управление структурой глобальной компьютерной сети интернет. Когда интернет повсеместно вошел в жизнь людей, его стали активно использовать для организации различных сервисов – коммерческих, государственных, социальных. Интересно, что сам по себе интернет – это децентрализованная структура, хотя и имеющая иерархическую природу, особенно на нижних уровнях использования.

Конечный пользователь подключается к сети через своего провайдера, а тот, в свою очередь, если является небольшой организацией, имеет всего лишь один внешний канал к более крупному оператору. Чем крупнее субъект сети, тем больше связей он имеет с другими крупными субъектами, как посредством прямых соединений, так и через пункты обмена сетевым трафиком. Самые крупные операторы сети имеют свою инфраструктуру магистральных каналов по всему миру и обеспечивают наиболее значительную пропускную способность для передаваемых данных. И тем не менее интернет не имеет единой «точки отказа». То есть отключение одного участника системы, пусть даже достаточно крупного, не приведет к остановке работы сети в целом, за исключением того сегмента, который был полностью «замкнут» на выпавший из сети крупный узел. Впрочем, элементы этого сегмента могут в этом случае переключиться на резервные каналы и таким образом вернуться в онлайн.

Именно отсутствие точки отказа и есть одно из главных преимуществ децентрализованных систем. Вернемся к примеру Швейцарии: известно, что федеральный президент или какой-либо иной политический институт этого государства не имеет права отдавать приказ о капитуляции в условиях внешнего военного вторжения. А если такой приказ и будет отдан, то закон категорически запрещает жителям страны его исполнение. Таким образом, агрессору придется иметь дело чуть ли не с каждым швейцарцем по отдельности. То же самое касается и сети интернет. Даже если какая-то страна своим политическим решением захочет отключить интернет, то с большой вероятностью технологически осуществить это намерение будет возможно лишь на своей территории (за исключением узлов, подключенных к интернету по спутниковой связи, при условии, что спутник принадлежит другому государству). Возможно, пострадают пользователи в других странах, магистральные каналы из которых подключены к транзитным узлам страны,

решившей отключиться от глобальной сети. Но вся остальная сеть в мире сохранит работоспособность.

Фактически для того, чтобы уничтожить интернет, необходимо отключить почти все его узлы, что само по себе представляет организационную и технологическую сложность, граничащую с практической невозможностью исполнения задуманного. То есть мы можем говорить о теоретической неуязвимости сети, построенной на базе распределенной топологии без единого управляющего центра. Но если мы обратимся на уровень сервисов, построенных на базе сети интернет, то мы увидим, что подавляющее их большинство построено на технологии «клиент – сервер», то есть технологии централизованной.

Все мы давно привыкли пользоваться различными интернет-сервисами. Порталы поддержки сервисов электронной почты, системы облачного хранения данных (например, документов или фотографий), доступ в систему «банк – клиент» для управления своими счетами и совершения платежей, бронирование отелей и авиабилетов, торговые платформы для осуществления сделок на финансовых рынках и многое другое – все эти сервисы построены на базе централизованной инфраструктуры. При использовании каждой такой системы, чтобы получить доступ к ресурсам и услугам, необходимо посетить специальный сайт поставщика конкретной услуги, ввести свой логин и пароль и подключиться к центральному серверу, где хранятся данные клиента или его активы. Однако в случае, если центральный сервер поставщика услуг по какой-то причине отключится, мы не сможем воспользоваться данной услугой, и нам придется ждать, пока сервер восстановит свою работоспособность. В данном случае мы сталкиваемся с главной проблемой централизованных систем – наличием «точки отказа». Отказ в обслуживании может быть результатом действия различных факторов: технологических проблем в виде выхода оборудования из строя, ошибок в программном обеспечении, злоупотреблений внутри структуры самого поставщика услуг, различных внешних хакерских атак или действия компьютерных вирусов. Не последнюю роль могут играть также результаты репрессивного воздействия государственных силовых или регулятивных структур на территории юрисдикции, где физически расположен поставщик услуг.

Все эти факторы, результатом влияния которых становится отказ в обслуживании, заставляют задуматься о том, каким образом можно технологически или организационно избежать подобных ситуаций. Ответом на этот вопрос стало возникновение технологии блокчейн, основанной на построении децентрализованной системы для хранения и обмена данными, что исключает все негативные факторы, естественным образом возникающие при централизации сервисов. На смену сетевой топологии «звезда», лучи которой от всех узлов-пользователей в обязательном порядке сходятся к центральной точке – узлу-серверу, пришла форма организации сети, в которой понятие «центральный сервер» отсутствует как таковое, а все взаимодействие осуществляется между узлами-клиентами напрямую между собой. Такие сети еще называют «одноранговыми» или «пиринговыми». Все узлы в подобной сети в большинстве случаев равноправны, и каждый из них может выполнять как клиентские, так и серверные функции. Подобная децентрализованная топология сети устраняет фактор «точки отказа», повышая степень надежности и работоспособности системы до величин, близких к абсолютным.

Однако у читателей может возникнуть вполне резонный вопрос: если серверы в сети как таковые отсутствуют, то каким образом в подобной системе хранятся общие данные, как они распространяются по сети и каким образом они защищены от несанкционированного доступа или модификации? А также каким образом подобные системы обслуживаются и развиваются, если все участники сети имеют равные права? Технология блокчейн обеспечивает решение большинства из этих вопросов. Данные реплицируются (копируются) между всеми узлами системы. Защиту от изменений или от несанкционированного доступа к данным обеспечивают математические алгоритмы асимметричной криптографии. Вся система функционирует на базе заданного набора правил, с которыми соглашаются все участники системы. В случае если необходимо внести значимые изменения, решение принимается общим голосованием участников системы.

Следует отметить, что администрирование децентрализованных систем на порядок сложнее, чем централизованных. Но это стоит рассматривать как плату за те преимущества, которые дает децентрализация. На текущий момент решены далеко не все проблемы, которые могут возникнуть при управлении децентрализованными системами. И мы еще неоднократно вернемся к обсуждению этой проблематики в последующих главах.

Хеширование информации

Инструмент хеширования данных является важной и неотъемлемой частью технологии блокчейн. Хеширование используется для создания адресации в блокчейн-системах, для формирования цифровой электронной подписи сообщений, а также для добычи криптомонет (так называемого «майнинга») в некоторых блокчейн-проектах, базирующихся на принципе «доказательства работы». Прежде чем рассматривать вышеупомянутые элементы блокчейн-систем, нам потребуется разобраться с тем, что же все-таки такое хеширование данных и на основе каких принципов эта процедура работает.

Начнем с определения. Хеширование – это метод преобразования набора данных произвольного размера в стандартизированную строку фиксированной длины при помощи специального алгоритма. То есть если взять какой-то набор данных, например, весь текст этой книги, то можно создать его цифровой отпечаток длиной, скажем, десять символов. При этом мы должны определить точный алгоритм преобразования входных данных и использовать его без изменения для любых других данных произвольного размера, получая на выходе стандартную строку в десять символов. Еще говорят, что в таком случае используется «детерминированный алгоритм»,

потому что он всегда выдает предопределенный результат. Фактически получаемый результат должен стать уникальным отображением преобразуемых входных данных. Для этого мы должны создать такой алгоритм преобразования, который ни при каких обстоятельствах не допустит получения одинакового результата преобразования для разных входящих наборов данных. То есть не создаст так называемых «коллизий». При этом малейшее изменение во входных данных, даже изменение одного их бита, должно видоизменять результирующий хеш на выходе до неузнаваемости. Вот пример работы одного из самых простых алгоритмов хеширования (SHA-1), где прообразами хешей являются два варианта написания английского слова «децентрализация», при этом во втором слове изменена всего лишь одна буква:

Как видно из полученных результатов, второй хеш не имеет ничего общего с первым, хотя разница в исходных прообразах минимальна. Читатель, вероятно, задастся вопросом: а зачем вообще это все нужно? На самом деле хеширование – это исключительно полезная функция, которая довольно широко применяется в компьютерных технологиях.

Представим себе ситуацию, что нам необходимо передать по каналам связи значительный объем данных, в которых при передаче по тем или иным причинам могут возникать помехи и искажения. Как нам проверить, дошли ли до конечного получателя данные в исходном виде? Пока мы не сравним каждый бит исходной информации с полученным, мы не сможем с уверенностью сказать, что передача данных прошла без ошибок. А что, если по пути следования в данные вмешался кто-то посторонний и намеренно исказил информацию? А как быть, если объем информации измеряется гигабайтами? Процесс сравнения двух огромных информационных блоков может занять значительное время. Не проще ли к передаваемому блоку данных приложить короткий уникальный «цифровой отпечаток», созданный на базе общеизвестного алгоритма хеширования? Тогда при получении мы можем еще раз запустить этот же самый алгоритм, подав ему на вход полученные данные, и затем просто сравнить результирующий хеш с тем, который был приложен к передаваемым данным. Если они в точности совпадут, значит, передача прошла без искажений, и мы имеем на руках данные, полностью аналогичные исходным. Таким образом мы проверяем целостность данных. Популярным вариантом использования алгоритма подобной проверки является получение значения так называемой «контрольной суммы», расчет которой базируется на алгоритме хеширования входного блока данных.

Рассуждая логически, мы приходим к пониманию, что совершенно невозможно преобразовать большой блок данных в исключительно малый без потерь исходной информации. И это действительно так. Алгоритм хеширования представляет собой одностороннюю математическую функцию, результат действия которой практически невозможно обратить в исходные данные до преобразования. То есть вычислительно из хеша чрезвычайно сложно получить его прообраз. Теоретически это возможно осуществить только последовательным перебором вариантов – при помощи так называемого метода «грубой силы». Этот метод базируется на принципе «зашифруй и сравни»: некие предполагаемые исходные данные хешируются и сравниваются с имеющимся хешем. Если эти два хеша не совпали, значит, данный предполагаемый прообраз нам не подходит. Меняем его и хешируем снова – и так далее до бесконечности, пока хеши вдруг неожиданно не совпадут. Только тогда мы можем говорить о том, что мы «расшифровали хеш», но количество вариантов, которое нам необходимо перебрать, чтобы добиться такого результата, измеряется, без преувеличения, астрономическими величинами.

Данный метод, кстати, широко используется для защиты хранимых секретных паролей на различных серверах. Размещать пароли пользователей на интернет-серверах в открытом виде явно небезопасно – их могут похитить злоумышленники и затем попытаться нанести системе и ее участникам материальный ущерб. Но если пароли хранятся не в открытом виде, а в виде хешей, то задача несанкционированного доступа значительно усложняется. Если пароль вводит его владелец, то система хеширует пароль и сравнивает с хранимым хешем пароля для данного пользователя. Если они совпали, значит, пароль введен верный, и система открывает пользователю доступ. Если хеши не совпадают – пароль неправильный. А наличие у злоумышленника украденного хеша пароля задачу ему отнюдь не упрощает, поскольку ему необходимо восстановить исходный пароль методом масштабного перебора вариантов. Понятно, что чем длиннее исходный пароль, тем больше максимально возможных вариантов его перебора. Поэтому для получения исходного пароля необходимо задействовать исключительные вычислительные мощности, что в конечном итоге отражается на общей стоимости атаки, которая может обойтись дороже, чем возможная материальная выгода от подбора конкретного пароля.

Еще один популярный способ использования алгоритмов хеширования применяется в так называемых торрент-трекерах. Торренты – это технология обмена файлами, как правило, медийного характера (в подавляющем большинстве – видео). Сама технология имеет гибридную модель, когда торрент-файлы, содержащие техническую информацию, распространяются централизованно через

специальные торрент-трекинговые порталы. При этом непосредственный обмен основными файлами происходит децентрализованно, через организацию прямого соединения между «сидерами» – теми, кто отдает файлы, и «личерами» – теми, кто их получает. В силу объема передаваемой по сети интернет информации (а иные видеофайлы могут иметь объем, измеряемый гигабайтами) их передача осуществляется фрагментами. Задача принимающей стороны – связаться с различными отправителями фрагментов одного и того же файла и получить на свое устройство все его части.

Конечная цель – собрать в правильном порядке из этих кусочков исходный файл большого объема так, чтобы целостность всех данных не пострадала и медийный проигрыватель не выдал ошибку при попытке запустить файл для просмотра. Одна из основных процедур данной технологии – постоянное сравнение значительных блоков данных с целью контроля их целостности и правильной идентификации их фрагментов. Вот здесь на помощь и приходит функционал хеширования. Именно по хешам как целых файлов, так и их фрагментов осуществляется идентификация соответствия блоков данных именно тем, которые были запрошены. И если все хеши совпадают, значит, в итоге мы гарантированно «склеим» нужный нам файл без ошибок. Поэтому именно технология хеширования позволяет быстро и надежно сравнивать различные блоки данных и гарантировать их целостность при передаче.

Наконец, технология хеширования активно используется для ускорения поиска данных. Для этого формируются так называемые «хеш-таблицы», которые содержат хеши различных информационных блоков. Их сортируют в определенном порядке, чтобы при осуществлении поиска можно было быстро найти данные по их хешам, обращаясь сразу в нужный раздел вместо масштабного поиска по всей базе.

Теперь рассмотрим вопрос, какие математические и логические операции используются для вычисления хешей. Алгоритмов хеширования достаточно много – от относительно простых до достаточно затейливых. Обычно при создании математической модели алгоритма преследуются цели усложнения задачи обратного восстановления прообраза из хеша и расширения максимально возможного диапазона получаемых из прообраза хешей. Это необходимо для того, чтобы вероятность появления коллизий, то есть получения одинаковых хешей из двух различных прообразов, составила исключительно малую величину. Понятно, что с увеличением разрядности (размера) хеша вероятность появления коллизий экспоненциально уменьшается. Однако в ряде случаев требуется решить задачу для хешей относительно небольших размеров, поскольку это влияет на совокупный объем хранимой информации и, как следствие, на стоимость этого хранения.

В качестве примера работы алгоритмов хеширования приведем несколько наиболее популярных процедур, в том числе и тех, которые используются в различных проектах, базирующихся на технологии блокчейн – таких, как, например, Bitcoin (SHA-256) или Ethereum (SHA-3). Данные алгоритмы состоят из определенного количества шагов (итераций), на каждом из которых с данными совершаются какие-либо логические операции из следующего набора.

- «Конкатенация» (то есть «сцепление» или «склеивание» двух блоков данных, когда второй становится продолжением первого, например, конкатенация «1111» и «2222» дает результат «11112222»).
- «Сложение» (обычное арифметическое действие для двух и более чисел).
- «Конъюнкция», или «Логическое И», «AND» (результат этой побитовой операции будет истинным (1), если оба бита являются единицами, в противном случае результат будет ложным (0)).
- «Дизъюнкция», или «Логическое ИЛИ», «OR» (результат этой операции будет истинным (1), если хотя бы один из аргументов является истинным (1), в противном случае результат будет ложным (0)).
- «Логическое Исключающее ИЛИ», «XOR» (результат этой операции для двух бит будет истинным (1), только если один из аргументов будет истинным (1), а второй ложным (0), в противном случае результат будет ложным (0)).
- «Логическое отрицание», «NOT» (побитовая инверсия, результат унарной операции, где результирующий бит всегда будет противоположен по значению входящему биту, то есть единицы становятся нулями и наоборот).
- «Побитовые сдвиги» (когда значения битов перемещаются в соседние регистры по направлению сдвига, например, для блока «10100110» результатом логического сдвига влево будет «01001100»).

Побитовые сдвиги могут быть логическими (когда последний бит по направлению сдвига теряется, а первый становится нулем) и циклическими (когда последний бит по направлению становится на место первого). В приведенном выше примере рассматривается именно логический сдвиг, поскольку результат циклического сдвига влево в данном случае представлял бы из себя результат «01001101». Кроме того, внутри каждой итерации могут применяться наборы вспомогательных констант, закрепленные за каждым из

алгоритмов. Эти константы используются в различных операциях, описанных выше. Таким образом, с каждым шагом алгоритма результат все больше отдаляется от исходных данных. Происходит сложное циклическое «перемешивание» данных — возможно, именно поэтому эту процедуру и назвали «хеширование», что в переводе с английского означает «мешанина» и часто относится к блюдам из мелко порубленного мяса или овощей. Ингредиенты подобных блюд, как и результат хеширования, невозможно привести к исходному виду (прообразу). Однако попытки поиска эффективных методов восстановления прообразов для различных хеширующих алгоритмов существовали с самого начала их появления.

Для того чтобы представить себе проблематику, связанную с криптостойкостью самых популярных алгоритмов хеширования, оценим рассчитанные показатели многообразия вариантов хешей и вероятностей нахождения коллизий для них. Соотношение между разрядностью (размером) хеша n и числом возможных выходов (вариантов генераций хеша) равно 2 в степени n. Если средняя длина хеша в основных популярных блокчейн-проектах составляет 256 бит, это означает число выходов, равное 2256 или примерно 1,2 × 1077, то есть значению, сопоставимому с оценкой числа атомов в наблюдаемой Вселенной. Однако чтобы найти коллизию, необязательно перебирать все варианты.

Существует известный алгоритм атаки — так называемая «атака дней рождения», которая базируется на парадоксе, связанном с решением задачи о вероятности совпадений дней рождения хотя бы у двух человек в группе, состоящей из N людей. Парадокс состоит в том, что оценивается не вероятность того, что у какого-то конкретно выбранного человека в группе с кем-то совпадает день рождения (эта вероятность для небольших групп достаточно мала), а вероятность совпадения дней рождения у любой пары людей из данной группы. А это уже совсем другой порядок вероятности. Например, для группы из 23 людей такая вероятность превышает 50%, а для 60 человек и более вероятность становится больше 99%. С коллизиями в алгоритмах хеширования также можно провести аналогию, но базируясь на гораздо больших числовых значениях. Однако общий смысл от этого не меняется: для того, чтобы найти коллизию с какой-то значимой величиной вероятности, нужно перебрать гораздо меньшее число вариантов, чем максимальное число возможных выходов. Для ключа в 256 бит и вероятности нахождения коллизии в 75% это значение составляет 5,7 × 1038, что на 39 порядков меньше максимального математически возможного числа выходов. Как видите, даже подобная существенно меньшая величина вероятности все равно поддерживает сложность задачи перебора вариантов на исключительно высоком вычислительном уровне. Поэтому в блокчейн-технологиях используются алгоритмы хеширования с высокой разрядностью, чтобы защитить хранимые данные от посягательств злоумышленников как минимум до того момента, пока вычислительные мощности не позволят преодолеть эти барьеры сложности.

Мы постарались рассмотреть основные моменты, которые необходимо знать о принципах хеширования. К непосредственным применениям этой процедуры мы еще вернемся в специальных разделах книги, посвященных практическим реализациям блокчейн-проектов.

История криптографии

Рассматривая технологию блокчейн в деталях, совершенно невозможно пройти мимо одного из ее самых важных элементов — криптографической части. Криптография в блокчейн является мощнейшим связующим элементом, на котором базируется основная ценность технологии распределенного реестра в целом. Именно криптография стоит на страже целостности хранения и передачи данных, обеспечивает права владения и защищает активы пользователей системы, в первую очередь — финансовые. Без криптографии технология блокчейн просто не смогла бы существовать — она бы утратила все свои преимущества, и в ее использовании не было бы никакого смысла. Но почему же криптография настолько важна? Давайте попробуем разобраться, что же такое криптография и каким образом она стала фактическим ядром блокчейн-технологии.

История криптографии уходит далеко в глубь тысячелетий. Во все времена у людей существовала необходимость передавать секретную информацию на расстоянии. В первую очередь дело обычно касалось информации, имеющей военное значение. В эпоху отсутствия в мире систем коллективной безопасности более слабые в военном отношении государства постоянно становились добычей агрессивных соседей. Единственным шансом для малых государств сохранить свою свободу и независимость было найти себе сильных союзников. Но для заключения подобных соглашений необходимо было обмениваться информацией, которая ни при каких обстоятельствах не должна была стать известна потенциальному противнику. То же самое касалось и приказов военного командования к своим подразделениям, находящимся вдали от дислокации основных сил: для осуществления постоянной координации нужно было передавать и получать информацию о местоположении, численности, снабжении, а также тактике и стратегии предстоящих боевых действий.

Информация передавалась через специально подготовленных людей (гонцов или шпионов), задачей которых было максимально быстро и незаметно для противника передать послание конечному адресату. Тем не менее существовал немалый риск, что такой посланец будет перехвачен, а информация, которую он несет, станет достоянием врагов. Эти риски постоянно учитывались при составлении сообщений,

поэтому их практически никогда не писали открытым текстом, а пытались определенным образом зашифровать. Подобная практика предполагала, что ключ к расшифровке текстов имеется только у отправителя и у тех, кому данное послание адресовано. А это означает, что до того, как начать обмен сообщениями, необходимо было приложить определенные усилия к распространению шифровальных ключей между центром и его потенциальными адресатами. Что, в свою очередь, влекло за собой риск, что эта информация может быть перехвачена (или перекуплена) и впоследствии использована для чтения сообщений неприятеля. Разумеется, сам отправитель не будет иметь об этом ни малейшего понятия, поскольку факт обладания тайным ключом не будет предан противником гласности.

Принцип, когда сообщения шифруются и дешифруются одним и тем же ключом, которым владеют обе стороны, вступающие в обмен информацией, называется симметричной криптографией, поскольку в данном случае имеет место явная симметрия в шифровальных ключах. Именно этот принцип и использовался почти все время существования человеческой цивилизации — от глубокой древности и вплоть до конца 70-х годов прошлого века. Какие же приемы использовались в те времена для шифрования? Как и у других областей человеческого знания, у криптографических технологий была своя собственная эволюция. Начиналось все с банальной подстановки одних букв послания вместо других. Например, римский полководец Гай Юлий Цезарь кодировал послания своим генералам методом сдвига букв на три позиции в латинском алфавите. То есть буква B становилась буквой E, C — F и так далее. Подобные подстановочные шифры называют еще моноалфавитными. Впоследствии моноалфавитные шифры были вытеснены полиалфавитными, когда к буквам шифруемого текста циклически применялись несколько моноалфавитных шифров. Этот метод с различными вариациями использовался почти 1000 лет, до начала XX века, когда в обиход вошли электромеханические устройства для шифрования сообщений. Наверное, самой известной реализацией подобного способа криптографии является немецкая роторная шифровальная машина «Энигма», шифры которой считались невскрываемыми.

С современной точки зрения шифр «Энигмы» выглядит криптографически слабым. Однако во времена Второй мировой войны эта шифровальная машина сумела доставить изрядные хлопоты противникам Германии. Еще задолго до начала военных действий, в 1932 году, польской разведке удалось на базе сведений от своих германских агентов получить некоторые коды и принципы устройства машины. Это позволило полякам воссоздать машину у себя в лаборатории и попытаться разобраться в алгоритме ее работы. В 1939 году Германия вторглась в Польшу, однако незадолго до этого все наработки по «Энигме» были переданы британской разведке, которая создала специальную группу по дешифровке сообщений и привлекла в нее талантливого математика и криптографа Алана Тьюринга. К 1940 году команда Тьюринга сумела построить около двухсот криптоаналитических машин, работающих с шифром «Энигмы», но исключительное многообразие вариантов перебора для расшифровки очень долго не позволяло взломать код. Тем не менее Тьюрингу удалось выявить повторяющиеся фразы в зашифрованных сообщениях. Одним из таковых оказалось нацистское приветствие, присутствующее почти в каждом тексте, что позволило существенно сузить диапазон перебора вариантов и наконец взломать шифр. Считается, что именно это событие существенно повлияло на поражение Германии, а дата окончания войны, как полагают некоторые специалисты, приблизилась не менее чем на год.

К началу второй половины XX века ученые стали все больше приходить к выводу, что возможностей симметричной криптографии явно недостаточно для решения ряда современных задач. С появлением компьютеров и увеличением их вычислительной мощности взломы даже самых сложных симметричных шифров, используемых в то время, перестали быть серьезной проблемой. Поэтому мир постепенно стал переходить к математической криптографии. Результатом этого перехода стала настоящая революция, которая выразилась в появлении принципиально нового раздела криптографии. Речь идет о криптографии асимметричной, или, как ее еще называют, криптографии с открытым ключом.

В 1976 году два криптографа, Уитфилд Диффи и Мартин Хеллман, опубликовали работу под названием «Новые направления в современной криптографии». Основная идея, изложенная в работе, состояла в методе, при котором, помимо одного секретного ключа, формируется также и второй — открытый, математически связанный с секретным ключом. При этом процесс восстановления секретного ключа из открытого представляет собой исключительно сложную математическую задачу. Конечный результат этой идеи воплотился в возможности распространять секретный ключ по открытым каналам, не рискуя при этом раскрыть его третьим лицам. Для этого сторонам необходимо было лишь обменяться между собой открытыми ключами с добавлением вспомогательной расчетной информации. А затем, при помощи математических операций, восстановить общий секретный ключ на стороне получателя. Этот алгоритм получил название «Диффи–Хеллмана», по имени его создателей, и открыл новую криптографическую эпоху, в которой начали появляться и развиваться исключительно криптостойкие алгоритмы шифрования, использующиеся, в частности, и в технологии блокчейн.

Каким же образом работает шифрование с открытым ключом? На самом деле принцип достаточно прост — каждый пользователь генерирует себе секретный ключ, пусть даже и случайным образом. Затем при помощи математических операций, зависящих от конкретного алгоритма шифрования, он получает из этого секретного ключа второй ключ, который имеет статус публичного. То есть владелец публичного ключа может открыто его распространять: поместить на сайте, в почтовом сообщении или вообще напечатать в

газете. Раскрывать свой публичный ключ необходимо, поскольку он обязательно понадобится тому, кто захочет отправить сообщение владельцу этой пары ключей — для шифрования сообщения. Фокус в том, что расшифровать сообщение, закодированное публичным ключом, можно только лишь при помощи соответствующего ему секретного ключа и никак иначе. Как мы видим, подобная система не в пример удобнее, чем симметричная форма криптографии, где постоянная необходимость распространения общего секретного ключа по незащищенным каналам создает серьезную уязвимость для технологии шифрования в целом.

Однако следует отметить, что и симметричные системы шифрования продолжают использоваться в наше время. Дело в том, что симметричные алгоритмы обладают очень высокой скоростью шифрования и расшифровки. В системах, где этот параметр является критичным, а также при условии, что стороны смогут обеспечить безопасный обмен секретными ключами между собой, применение симметричного шифрования может оказаться вполне оправданным и эффективным. Довольно часто при передаче данных в сети интернет применяется комбинация алгоритмов асимметричной и симметричной криптографии. В частности, при установлении соединения используется передача общего секрета при помощи алгоритма Диффи–Хеллмана, а затем этот общий секрет используется обеими сторонами как ключ для шифрования и дешифрования пакетов данных симметричными алгоритмами. Но все же в распределенных системах с большим количеством пользователей безраздельно властвует асимметричная криптография, и блокчейн-проекты — не исключение. Какие же методы асимметричного шифрования наиболее популярны в настоящее время?

Асимметричная криптография

Алгоритмов асимметричного шифрования достаточно много. Но в этой книге мы остановимся лишь на нескольких из них, переходя от относительно простых к более сложным. Алгоритм Диффи–Хеллмана, появившийся первым среди методов асимметричной криптографии, не решал задачу аутентификации сторон, которые совместно генерировали секретный ключ. Однако уже в 1977 году появился алгоритм, который обеспечивал не только сам процесс шифрования, но и был пригоден для создания аутентификации субъекта системы посредством цифровой электронной подписи. Данный алгоритм базировался на задаче так называемой «факторизации» больших целых чисел и получил название в виде аббревиатуры RSA — по фамилиям ученых, его создавших — Рональда Ривеста, Ади Шамира и Леонарда Адлемана. Факторизацией называется процесс разложения натурального числа на произведение простых множителей. В алгоритме RSA секретный ключ представляет собой два больших простых числа, а публичный ключ — произведение этих двух чисел. Использование этого метода в криптографии обусловлено его свойством, благодаря которому задача перемножения нескольких чисел является достаточно легкой, в том числе и для весьма больших значений. В то же время обратное разложение полученного числа на исходные множители является задачей исключительной вычислительной сложности.

Поясним на примере. Допустим, у нас есть три простых числа — 3, 5 и 7. Простые числа — это те, которые без остатка делятся лишь на себя самих и на единицу. Перемножим эти три числа между собой и получим результат — 105. А теперь представим, что у нас имеется только конечный результат 105 и нам необходимо разложить его обратно на простые множители, то есть получить исходные числа 3, 5 и 7. При решении задачи даже для такого небольшого трехразрядного числа человек столкнется с трудностями. А задача о факторизации чисел, имеющих разрядность в десятки позиций, и для современного компьютера может стать весьма нетривиальной. Безусловно, существуют алгоритмы, которые позволяют осуществлять факторизацию несколько эффективнее, чем простым перебором делителей, но однозначно оптимального алгоритма, позволяющего быстро решить эту задачу для больших чисел, пока не изобрели.

Проблема факторизации чисел занимала умы ученых еще сотни лет назад. Одним из первых, кто занялся этой задачей, стал французский математик Пьер де Ферма. Еще в 1643 году он предложил свой метод факторизации, который используется для криптоанализа шифров RSA и в наши дни. Понятно, что для любого алгоритма шифрования всегда найдутся люди, которые будут искать возможности для эффективной атаки на него. Кто-то в преступных целях, а кто-то в научных — чтобы исследовать криптостойкость алгоритма и защитить проекты, базирующиеся на данном решении. Еще в середине 2000-х гг. стали появляться сообщения о том, что группа ученых того или иного университета взломала сначала 512-битный, а затем и 1024-битный ключ RSA. При этом они не задействовали какую-то исключительную вычислительную мощность, а для решения задачи им потребовалось вполне разумное время. Конечно, ни один, даже самый мощный компьютер, с такой вычислительной нагрузкой в одиночку не справится, поэтому для решения подобных задач компьютеры обычно объединяют в специальные вычислительные кластеры.

За последние десять лет вычислительная мощность компьютеров заметно выросла. Согласно закону Мура, производительность компьютерных процессоров удваивается каждые 18 месяцев, поэтому для поддержания криптостойкости алгоритма RSA в различных технологических решениях необходимо постоянно увеличивать длину открытого ключа. Поскольку до бесконечности этот процесс продолжаться не может, от данного алгоритма стали отказываться и переходить к более прогрессивным решениям, в которых достаточная криптостойкость поддерживается для ключей с разумной разрядностью — в пределах 256–1024 бит. Одним из таких стал алгоритм формирования цифровой подписи DSA, построенный на модели дискретного логарифмирования. В данном алгоритме используется так называемая модульная арифметика, которая представляет собой задачу поиска степени, в которую необходимо

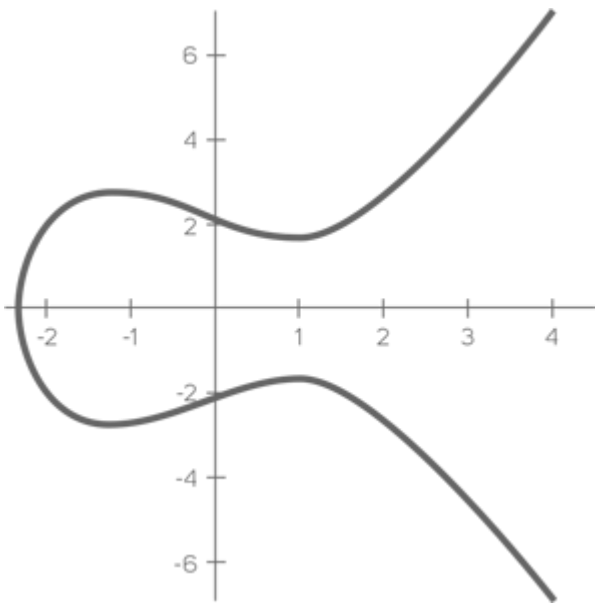
возвести заданное число, чтобы, разделив результат по модулю на другое заданное число, получить желаемый остаток от деления. Чтобы стало понятнее, рассмотрим следующий пример:

$$3^x \bmod 17 = 13$$

Деление по модулю — это обычное деление целых чисел друг на друга с целым остатком. Подобную арифметическую операцию проходят в младших классах школы, непосредственно перед изучением дробей. После чего про деление с остатком благополучно забывают и не вспоминают до университетского курса высшей математики. Где неожиданно выясняется, что деление с остатком на самом деле играет довольно важную роль в теории чисел и алгебре. В нашем примере мы должны определить, в какую степень нам надо возвести тройку, чтобы потом, разделив полученный результат по модулю на 17, получить число 13 в качестве остатка от деления. Правильный ответ: x = 4. То есть 34 = 81, 81/17 = 4 + остаток 13 (проверка: 4 x 17 = 68 + 13 = 81). Довольно просто, не правда ли? Возводя тройку в различные степени x от единицы и более, а затем деля по модулю полученный результат на 17, мы будем каждый раз получать различные остатки от деления. Однако у них будет одно общее свойство — все эти остатки будут находиться в диапазоне от 1 до 16 включительно, но выстраиваться отнюдь не по порядку (по мере последовательного возрастания степени x). Множество этих чисел называется кольцом вычетов. Кольцом, потому что остатки будут постоянно повторяться для разных показателей степени, в которую возводится базовое число. А теперь представим, что мы оперируем не одно-двухразрядными, а очень большими числами. В этих случаях, если степень заданного числа нам заранее неизвестна, то задача ее нахождения для конкретных величин остатков становится очень и очень сложной. Именно эта сложность и лежит в основе алгоритма DSA.

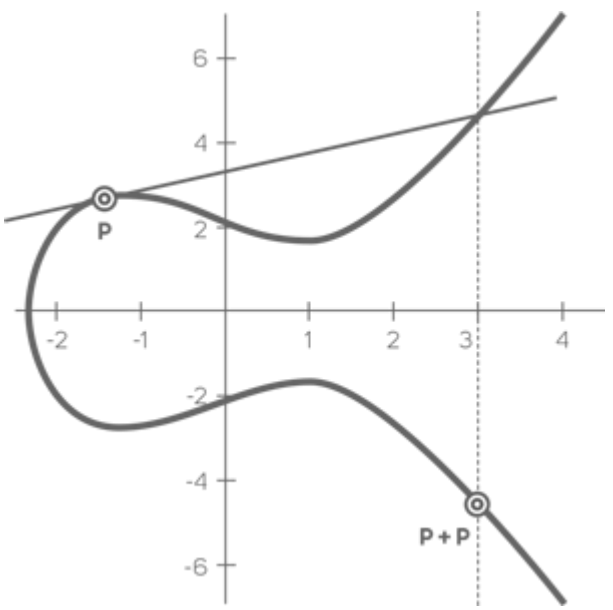
Как уже упоминалось выше, все подобные алгоритмы шифрования построены на принципе, при котором задача в одну сторону решается очень быстро и просто, а в обратную — исключительно сложно. И алгоритм DSA — не исключение. Если мы будем решать задачу для больших чисел путем простого перебора различных значений, то данный метод будет работать очень медленно. Поэтому вместо обычного перебора были разработаны алгоритмы, которые решают эту задачу гораздо эффективнее. Настолько эффективно, что, принимая во внимание постоянное увеличение производительности современных компьютеров, математики вынуждены были задуматься о необходимости повышения сложности алгоритма шифрования. В противном случае они могли бы столкнуться с проблемой массового взлома шифров уже в относительно недалеком будущем.

Чтобы придать задаче существенное усложнение, в 1985 году был разработан алгоритм дискретного логарифмирования на базе эллиптических кривых (алгоритм ECDSA). О чем в данном случае идет речь и что это за кривая? Эллиптическая кривая — это множество точек, описываемое уравнением y2 = x3 + ax + b. То есть, по сравнению с алгоритмом DSA, операции совершаются не над кольцом целых чисел, а над множеством точек эллиптической кривой, что существенно усложняет задачу восстановления закрытого ключа из открытого. Вот пример обычной эллиптической кривой:



На множестве точек эллиптической кривой могут выбираться такие точки, для которых возможно совершить операцию сложения самих с собой и получить результат в виде другой точки на этой же кривой. То есть решить уравнение X = nP, где n = 2 и более, а X и P являются точками на данной кривой с координатами по осям x и y. Умножение на константу n есть не что иное, как операция последовательного сложения n раз. Таким образом, мы начинаем с того, что нам необходимо сложить начальную точку с ней же самой и

получить результат в виде такой же точки, но уже с новыми координатами. Геометрически операция сложения точки эллиптической кривой с самой собой представляет построение касательной к данной точке. Затем мы находим точку пересечения касательной с графиком кривой и строим от нее вертикальную прямую, находя таким образом точку ее пересечения на обратной стороне кривой. Эта точка и будет результатом сложения. Вот как выглядит операция сложения точки с самой собой геометрически:



После чего, уже при следующей итерации, исходной точкой будет являться та, которая была получена в виде результата сложения на предыдущем шаге. Именно от нее мы строим новую касательную, и так далее — n раз. Сложность задачи состоит в обратном поиске n для известных точек X и P, и эта задача не имеет быстрого решения. В данном случае n будет закрытым ключом, а X — открытым. Понятно, что компьютер при расчетах осуществляет операцию сложения не геометрически, а чисто алгебраически, для чего существуют специальные формулы на базе имеющихся координат по осям x и y для каждой из точек.

Отдельно отметим, что далеко не все формы эллиптических кривых подойдут для формирования на их базе криптографических алгоритмов. Существуют довольно «слабые» в этом аспекте эллиптические кривые, которые неустойчивы к различным алгоритмам решения задачи дискретного логарифмирования. Поэтому, чтобы эллиптическая кривая была пригодна для сложных криптографических задач, она должна удовлетворять различным требованиям, которые мы здесь рассматривать не будем, чтобы излишне не усложнять описание общих принципов.

В теории алгоритмов выделяют различные категории сложности решения математических задач: полиномиальную, субэкспоненциальную и экспоненциальную. Сложность алгоритма дискретного логарифмирования на базе эллиптических кривых растет с экспоненциальной скоростью. До сих пор не разработано ни одного решения данной задачи даже за субэкспоненциальное время. То есть за время, пропорциональное функции, которая растет медленнее, чем любая степенная функция. Именно поэтому данный алгоритм получил в наши дни наиболее широкое применение как достаточно криптостойкая модель, использующая ключи с относительно небольшой разрядностью. Если мы сравним вышеописанные алгоритмы между собой, то для случая, когда длина открытого ключа RSA или обычного DSA, например, будет равна 1024 бит, алгоритму, использующему эллиптические кривые для достижения сопоставимой криптостойкости, достаточно будет иметь разрядность всего 160 бит. Разница в эффективности очевидна, поэтому самые популярные блокчейн-проекты, такие как Биткоин или Ethereum (да и многие другие), используют именно криптографию на эллиптических кривых, признанную на текущий момент самой надежной.

Помимо собственно процедуры шифрования данных важнейшим элементом, связанным с шифрованием, в технологии блокчейн является цифровая электронная подпись (ЭЦП). Что это такое и каким образом она используется?

Цифровая электронная подпись

Привычное для нас понятие «подпись» старо как мир — задача проверки подлинности документов стояла перед человечеством с древнейших времен. В качестве элементов, усложняющих подделку документов, использовались уникальные формы начертания имени чиновника, купца, феодала или даже монарха, созданные рукой самого автора. Делалось это подчас в сочетании с сургучными или восковыми печатями с оттиском государственных или родовых гербов подписанта. Считалось, что данная комбинация в большой степени защищает документ от несанкционированного воспроизведения с измененными в пользу фальсификатора данными. В

большинстве случаев эти защитные меры действительно себя оправдывали. Однако не существовало никакой гарантии, что какой-нибудь средневековый злоумышленник, вооруженный специальными для таких случаев приспособлениями, не сможет воссоздать копию документа, достаточно близкую к оригиналу.

С появлением и развитием компьютерных технологий проблема аутентичности информации, передаваемой по телекоммуникационным каналам, встала особенно остро — ведь подделать незащищенный цифровой документ гораздо проще, чем рукописный. Поэтому долгое время компьютерные документы распечатывали, подписывали вручную и в большинстве случаев ставили на них чернильную печать. Затем документ сканировался и передавался как графическое изображение, содержащее как печатные данные, так и рукотворные регалии. Но и в этом случае никаких гарантий от подделок существовать не могло. По крайней мере, до тех пор, пока технологии не перешли на совершенно новый качественный уровень — создание документов с цифровой электронной подписью, сформированной на базе алгоритмов асимметричной криптографии.

Цифровая электронная подпись — это результат работы определенного криптографического алгоритма, на вход которого подается два необходимых элемента: хеш набора данных, подлежащих подписанию, и секретный ключ владельца подписи. Цифровая подпись обладает целым рядом полезных свойств, главным из которых является то, что сформировать подпись может только владелец секретного ключа и никто иной. Точнее, могут иметь место вычислительные попытки восстановить секретный ключ из открытого, но, как мы убедились ранее, сделать это крайне сложно, и вероятность подобного исхода исчезающе мала. Цифровую подпись можно проверить на подлинность, зная открытый ключ владельца подписи. При этом подписанный конкретной подписью документ уже не сможет быть изменен ни в одном своем бите, поскольку подпись в этом случае сразу утратила бы свою валидность. Это произошло бы потому, что изменился бы хеш подписываемого документа, от которого напрямую зависит формирование самой подписи. То есть электронная цифровая подпись не только идентифицирует ее автора, но еще и гарантирует неизменность документа, который ею подписан.

Для формирования цифровой электронной подписи необходимо в первую очередь выбрать достаточно криптостойкий алгоритм асимметричной криптографии. Затем сформировать на его базе пару ключей — секретный и публичный. После чего вычислить хеш подписываемого блока данных, например, какого-то документа, предварительно выбрав подходящий алгоритм хеш-функции. Хеширование преследует две цели: защиту целостности исходных данных и создание их цифрового отпечатка в стандартизированной форме. После чего, имея хеш данных и закрытый ключ, мы запускаем алгоритм формирования ЭЦП и получаем на выходе результат в виде строки данных. Проверка подлинности подписи и целостности подписанных данных в различных алгоритмах шифрования математически отличается друг от друга. Однако общим принципом проверки является вычисление двух результатов, полученных разными способами, при этом для получения одного из них в обязательном порядке используется открытый ключ подписанта. Затем эти результаты сравнивают и в случае их неравенства делают вывод, что подпись подделана либо исходные данные претерпели изменения после подписания.

В качестве примера рассмотрим алгоритм RSA. Здесь сравниваются хеши подписанного блока данных, где первый хеш получается стандартным способом как результат действия хеш-функции над исходными данными, а второй вычисляется при помощи открытого ключа. Затем два полученных хеша сравниваются, после чего можно сделать выводы о подлинности подписи, то есть ее математическом соответствии подписанным данным. Следует еще раз подчеркнуть, что формирование ЭЦП или процедура ее проверки проводятся при помощи математических операций, присущих только конкретному, предварительно выбранному алгоритму шифрования. Как правило, для этого используются алгоритмы факторизации или дискретного логарифмирования, в том числе и на множестве точек эллиптических кривых. Именно последний способ в основном применяется в блокчейн-средах как наиболее криптостойкий. Схема примера подписания и проверки подписи при помощи алгоритма RSA показана на рисунке:

Следует также отметить, что электронная цифровая подпись совершенно не обязательно базируется на алгоритмах асимметричного шифрования. Существуют методики ее использования и для симметричных систем. В этом случае необходим еще один субъект — третье лицо в виде арбитра, которому доверяют обе стороны и который хранит общий секретный ключ. Очевидно, что данная схема используется достаточно редко в силу отсутствия эффективных алгоритмов и необходимости безусловного доверия третьим сторонам. Поэтому в подавляющем большинстве случаев используют алгоритмы асимметричной криптографии, а в блокчейн-проектах их применяют повсеместно.

Помимо стандартной цифровой подписи, в различных реализациях блокчейн-проектов применяются некоторые экзотические ее формы. Например, «слепая подпись», которую еще называют «доказательством с нулевым разглашением». Алгоритм слепой подписи прост: один участник системы шифрует свое сообщение и посылает его другому участнику, который является доверенным узлом (доверенным для некоторого множества других узлов) в системе. Этот доверенный участник ставит свою подпись на зашифрованном сообщении, при этом фактически не имея понятия о его содержимом. После чего подписанное сообщение возвращается его исходному отправителю, который обратно дешифрует его, оставляя только подпись доверенного узла. Это можно было бы сравнить с ситуацией, когда доверенный участник получает заклеенный конверт, внутри которого, помимо листа с сообщением, находится также и копировальный лист. Получатель, не вскрывая конверт, ставит на него свою подпись, которая через копировальный лист автоматически отпечатывается на листе с сообщением. По возвращении конверта отправителю тот изымает из него подписанное сообщение, достигнув таким образом желаемого — получить подпись доверенного узла, не разглашая ему само сообщение. Подобную операцию можно провести и чисто математически, используя протоколы асимметричной криптографии, например, при помощи алгоритма факторизации RSA.

Для чего используются такие замысловатые приемы? На самом деле вариантов предостаточно. В качестве примера приведем систему тайного голосования на выборах. Чтобы получить бюллетень, избиратель должен быть идентифицирован сотрудником избирательной

комиссии, который не должен видеть, каким образом проголосует избиратель. Использование технологии слепой подписи гарантирует, что бюллетени получат только идентифицированные избиратели, имеющие право голоса. В результате можно говорить о доверии к результатам выборов, поскольку в обществе присутствует доверие к сотрудникам избирательных комиссий. По аналогичному принципу работает и система электронного голосования, где проверяющий узел подписывает сообщение от идентифицированного им избирателя (содержащее зашифрованную информацию о его выборе), после чего возвращает ему подписанное сообщение. Подпись в данном случае означает, что факт права участия избирателя в голосовании был проверен доверенным узлом сети. Избиратель, получив подписанное сообщение, отправляет его на адрес специального счетчика, который учитывает его как легитимный голос за одного из кандидатов. Подобные алгоритмы уже используются в ряде стран на выборах в различные органы власти — от муниципальных структур до национальных парламентов. Самой известной страной, использующей интернет-голосование на базе национальных идентификационных карт, является Эстония, которая впервые применила эту процедуру на парламентских выборах 2007 года.

Еще одним интересным способом формирования ЭЦП является так называемая «кольцевая подпись». Еще в XVII столетии британские военные, подавая различные петиции с жалобами своему начальству, подписывали ее вокруг текста самого заявления. Столь необычная форма подписи использовалась для того, чтобы невозможно было выявить первого подписанта, которого командование всегда квалифицировало как главного зачинщика. Впоследствии этот способ переняли и американские военные, в частности, в конце XIX века во время войны с Испанией на Кубе. Когда появились электронные системы, позволяющие подписывать различные блоки данных, одновременно возникла необходимость в некоторых случаях маскировать конкретного подписанта в списке прочих потенциальных кандидатов. Для этого был разработан специальный математический алгоритм, формирующий определенный набор публичных ключей, связанных с различными участниками системы.

Большая часть самих задействованных участников сети обычно даже не подозревает, что их открытый ключ мог быть использован для формирования кольцевой подписи. В полученном таким образом наборе открытых ключей только один из них имеет в паре соответствующий ему секретный ключ, поскольку им оперирует, собственно, сам подписант, пожелавший остаться для всех остальных неизвестным. Сама кольцевая подпись формируется путем подачи на вход алгоритма набора открытых ключей (одного своего и многих чужих), собственного секретного ключа и самого подписываемого сообщения. После чего подписант получает на выходе строку данных кольцевой подписи. Эту подпись любой другой участник системы может проверить специальным алгоритмом, который использует все те же данные, за исключением, разумеется, секретного ключа, поскольку он может быть известен только лишь самому подписанту. Алгоритмы формирования кольцевой подписи обычно применяются в блокчейн-системах для дополнительной анонимизации в случае, если изначальной технологически заложенной секретности ее пользователям недостаточно. Подобные криптовалютные проекты мы еще будем рассматривать в разделе, посвященном проблематике анонимности в блокчейн.

Наконец, существует система консолидации электронных подписей от различных участников, которая называется «мультиподпись». Бывают ситуации, когда возникает необходимость управлять цифровыми активами на базе принятия решения несколькими участниками системы одновременно. Например, имеется некий электронный счет, на котором лежит существенная денежная сумма, принадлежащая группе участников или даже юридическому лицу. Правилами системы задается общее количество управляющих счетом, а также процентное значение веса подписи каждого из них. Как вариант предполагается, что любой перевод с данного счета должен быть подтвержден не менее чем 60% весового участия всех управляющих. В случае трех управляющих с равным весом подписи (у каждого по 33,3%) необходимо не менее двух участников, которые бы поставили свою электронную подпись под транзакцией, пересылающей денежные средства ($33{,}3\% \times 2 = 66{,}6\% > 60\%$ — пороговое условие считается выполненным). Подобная практика в блокчейн-системах обусловлена технологической невозможностью отозвать совершенные транзакции. Поэтому каждое решение по переводу значительных сумм, находящихся в коллективном владении, должно исключать возможность злоупотреблений со стороны какого-то конкретного лица, допущенного к управлению счетом. Мультиподпись может быть реализована в блокчейн-проектах различными математическими методами на базе алгоритмов асимметричной криптографии.

Идентифицирующий и охранительный функционал электронной подписи открывает широчайшие возможности для ее использования в повседневной практике, в первую очередь юридической и деловой. В настоящее время цифровая электронная подпись нашла применение как средство удаленной идентификации контрагентов при заключении различных соглашений — от учреждения новых предприятий до приобретения крупных активов, в том числе объектов недвижимости. В ряде государств цифровая электронная подпись юридически приравнена к обычной. Достаточно часто технология ЭЦП, а точнее, алгоритм мультиподписи используется в так называемых «эскроу-сервисах». Подобные услуги необходимы для заключения важных сделок, к которым привлекается третья арбитражная сторона, гарантирующая своей подписью надлежащее исполнение обязательств контрагентами по сделке. Значительное распространение различные алгоритмы формирования ЭЦП получили именно в блокчейн-средах. Являясь краеугольным камнем всего технологического процесса, цифровые подписи гарантируют пользователям распределенной сети права собственности на криптоактивы,

осуществляя защиту целостности помещаемой в систему информации. Безусловно, вопросы безопасности и неуязвимости к взломам этого метода защиты информации всегда выходят на первый план.

В предыдущей главе отмечалось, что первый предложенный алгоритм шифрования с открытым ключом (алгоритм Диффи–Хеллмана) не имел возможности формирования цифровой подписи. Однако последующие за ним алгоритмы факторизации или дискретного логарифмирования, включая эллиптическую криптографию, как нельзя лучше подходят для этой цели. Тем не менее не следует пребывать в уверенности, что даже столь криптостойкие алгоритмы, как ECDSA, ожидает безоблачное будущее, поскольку ученые готовят для всего криптографического мира сюрприз в виде так называемых квантовых компьютеров. Именно этот тип нетривиальных вычислительных устройств может создать серьезную угрозу всем популярным алгоритмам шифрования. Что же представляет собой такое явление, как квантовый компьютер, и почему криптографическим алгоритмам следует его опасаться?

Квантовые вычисления

Возможности взлома криптографических алгоритмов, а именно — попытки восстановить секретный ключ из открытого, всегда были ограничены вычислительной мощностью компьютеров. Производительность процессоров с годами постоянно росла, но вместе с ней также росла и криптостойкость алгоритмов. Иными словами, задача взлома с каждым днем пропорционально усложнялась, и казалось, что этой гонке не будет конца. Однако за последние годы перед технологами, производящими электронные компоненты на интегральных схемах, в первую очередь микропроцессоры, начали явственно очерчиваться физические пределы дальнейшего уменьшения размера транзистора как базового элемента электронной схемы. По состоянию на 2018 год позднейшие разработки в области полупроводниковых технологий позволяют массово создавать микропроцессоры на базе 10-нанометрового технологического процесса. По крайней мере, компания Samsung уже использует эту технологию в своих смартфонах, в то время как компания Intel все еще продолжает делать процессоры для персональных компьютеров по технологии 14 нм. В любом случае технология изготовления транзистора постепенно приближается к атомным размерностям, при том, что одного атома явно недостаточно, чтобы из него сделать транзистор.

Последние новости из мира науки сообщают, что ученым удалось создать транзистор всего из семи атомов, и уменьшать это число далее уже едва ли возможно. Дело в том, что размер одного атома кремния оценивают в 0,2 нанометра, но одновременно с этим считается, что из-за физических ограничений минимально возможный размер затвора кремниевого транзистора составляет 5 нанометров. О чем это говорит? О том, что небезызвестный закон Мура, согласно которому производительность процессоров удваивается каждые 18 месяцев, практически достиг своего физического предела. Что, в свою очередь, отразится на максимально возможной вычислительной мощности компьютеров, которая также перестанет пропорционально увеличиваться, как это происходило ранее. В результате прогресс во взломе криптостойких алгоритмов шифрования постепенно сойдет на нет, и все текущие проекты, построенные на базе этих алгоритмов, смогут наконец почувствовать себя в безопасности. Однако так ли это на самом деле?

Если классическая технология создания компьютеров упирается в свой предел развития, значит, следует искать решения по дальнейшему увеличению производительности в принципиально новых научно-технологических направлениях. Наиболее перспективной областью в части поиска возможностей для существенного роста производительности вычислений в настоящий момент считаются так называемые квантовые компьютеры.

Квантовые компьютеры — это вычислительные устройства, существенно отличающиеся от привычной для нас архитектуры двоичной логики. В классическом представлении мельчайшая ячейка памяти, называемая битом, может принимать устойчивые значения либо нуля, либо единицы. В квантовом же компьютере биты имеют квантовую природу и называются «кубитами». В роли таких кубитов могут выступать, например, направления спинов субатомных частиц, а также различные состояния внешних электронов или фотонов. Чтобы не углубляться в основы квантовой механики, мы не станем подробно рассматривать физическое устройство квантового компьютера, а отметим лишь некоторые свойства, отличающие его от компьютера классического.

В 1931 году австрийский физик Эрвин Шредингер предложил мысленный эксперимент, в котором он помещал условного кота в стальную камеру, где находилось устройство с радиоактивным атомным ядром, а также колба с ядовитым газом. По условиям эксперимента атомное ядро в течение часа может ожидать распад с вероятностью 50%. Если это происходит, то срабатывает механизм, разбивающий колбу, после чего кот погибает. Но если распад ядра все же не случился, тогда кот остается цел и невредим. Смысл этого эксперимента в том, что внешний наблюдатель никогда точно не знает, распалось ли ядро и жив ли кот, до тех пор, пока не откроет сам ящик, а до этого момента считается, что кот и жив, и мертв одновременно.

Понятно, что ни одна сущность в нашем мире не может находиться в двух разных состояниях в один и тот же момент времени. Поэтому правильнее было бы сказать, что кот находится в так называемом состоянии «суперпозиции», в котором все возможные варианты

состояния принимаются с различной степенью вероятности. При этом сумма вероятностей всех возможных состояний обязательно должна быть равна 100%. То же самое можно отнести и к принципу работы кубита квантового компьютера — он таким же образом может находиться в состоянии суперпозиции, принимая одновременно значения логического нуля и единицы. До момента непосредственного измерения состояния кубита его точное значение наблюдателю неизвестно, а после измерения и получения результата кубит сразу же фиксируется в однозначном состоянии нуля или единицы. Это на первый взгляд странное свойство кубитов оказалось очень полезным в организации параллельных расчетов сложных вычислительных задач, включая криптографические алгоритмы.

Еще одна интересная особенность кубитов состоит в том, что вместе они могут находиться в состоянии так называемой «квантовой запутанности», когда изменение состояния одного кубита автоматически влечет за собой изменение состояния другого, связанного с ним, на противоположное. Однако организовать квантовую запутанность большого числа кубитов между собой технологически очень сложно, поскольку их необходимо тщательно изолировать от любых видов помех в окружающей среде. На текущий момент ведущим производителям квантовых компьютеров, таким, например, как Google, удалось удержать в связанном состоянии целых 72 кубита, что пока является мировым рекордом среди подобных разработок. Много или мало 72 кубита для решения задач взлома хотя бы, например, алгоритма факторизации RSA? Если рассматривать n обычных бит, то из 2n возможных состояний в один момент времени можно выбрать лишь одно, в то время как n кубитов в состоянии суперпозиции будут находиться в 2n состояниях одновременно. Как результат при линейном возрастании количества кубитов количество возможных состояний будет расти экспоненциально. А это, в свою очередь, означает, что квантовый компьютер с большим количеством кубитов будет обладать исключительной вычислительной мощностью. Учитывая новейшие разработки в области квантовых вычислений, специалисты оценивают различия по мощности между квантовым и обычным компьютером не менее чем в миллиарды раз. При этом главное преимущество квантовый компьютер будет иметь именно при решении математических задач, связанных с переборами вариантов.

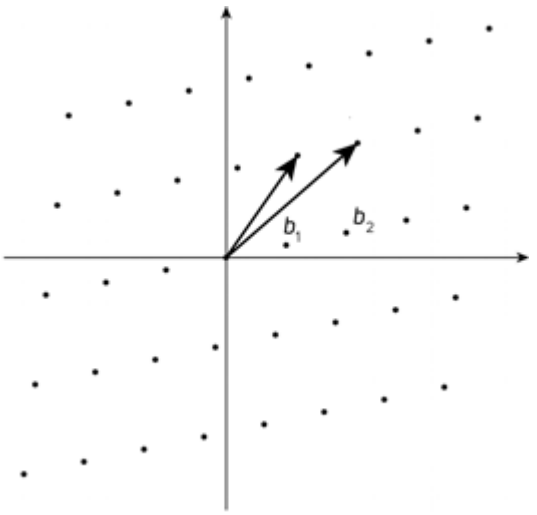
Тем не менее даже такая существенная вычислительная мощность может оказаться недостаточной, чтобы легко взламывать криптоалгоритмы с открытым ключом. Необходимое для этого число кубитов исчисляется гораздо большими величинами: например, для алгоритма факторизации RSA с ключом в 2048 бит потребуется ровно вдвое больше кубитов. Эти данные рассчитаны на базе вычислительных требований гибридного (содержащего как классическую, так и квантовую части) алгоритма, представленного в 1994 году американским ученым, специалистом в области квантовой информатики Питером Шором. Для взлома же эллиптической криптографии необходимое количество кубитов, как ни странно, меньше: для ключей в 256 бит потребуется 1536 кубитов, а для 512 бит — 3072. Учитывая скорость роста производительности квантовых компьютеров (а она на данный момент превышает закон Мура), до момента, когда самые популярные криптоалгоритмы сдадут свои позиции, остались, возможно, считаные годы. И о решении этой потенциальной угрозы специалистам-криптографам необходимо позаботиться уже сейчас.

Все не так страшно, как может показаться на первый взгляд. Уже разработан ряд алгоритмов асимметричной криптографии, которые остаются устойчивыми к квантовому перебору даже с использованием достаточно большого количества кубитов. Такие алгоритмы называют «постквантовыми», и о некоторых из них мы поговорим. В частности, о подписях Лэмпорта, криптографии на решетках и об изогениях эллиптических кривых.

Формирование цифровой электронной подписи на базе алгоритма Лэмпорта представляет собой использование криптографической хеш-функции и генератора случайных чисел. Создается 256 пар случайных чисел длиной по 256 бит каждое. Этот набор данных суммарным объемом 16 килобайт и будет являться секретным ключом. Каждая из 256-битных пар хешируется, и эти 512 хешей представляют собой открытый ключ. Затем на базе секретного ключа формируется электронная подпись для отправляемого сообщения. Как известно, чтобы подписать сообщение электронной подписью, его сначала надо хешировать. А затем составляется электронная подпись, в которой для каждого значения бита хеша сообщения (нуля или единицы) выбирается либо первое, либо второе число из пары секретного ключа, соответствующей порядковому номеру бита в хеше.

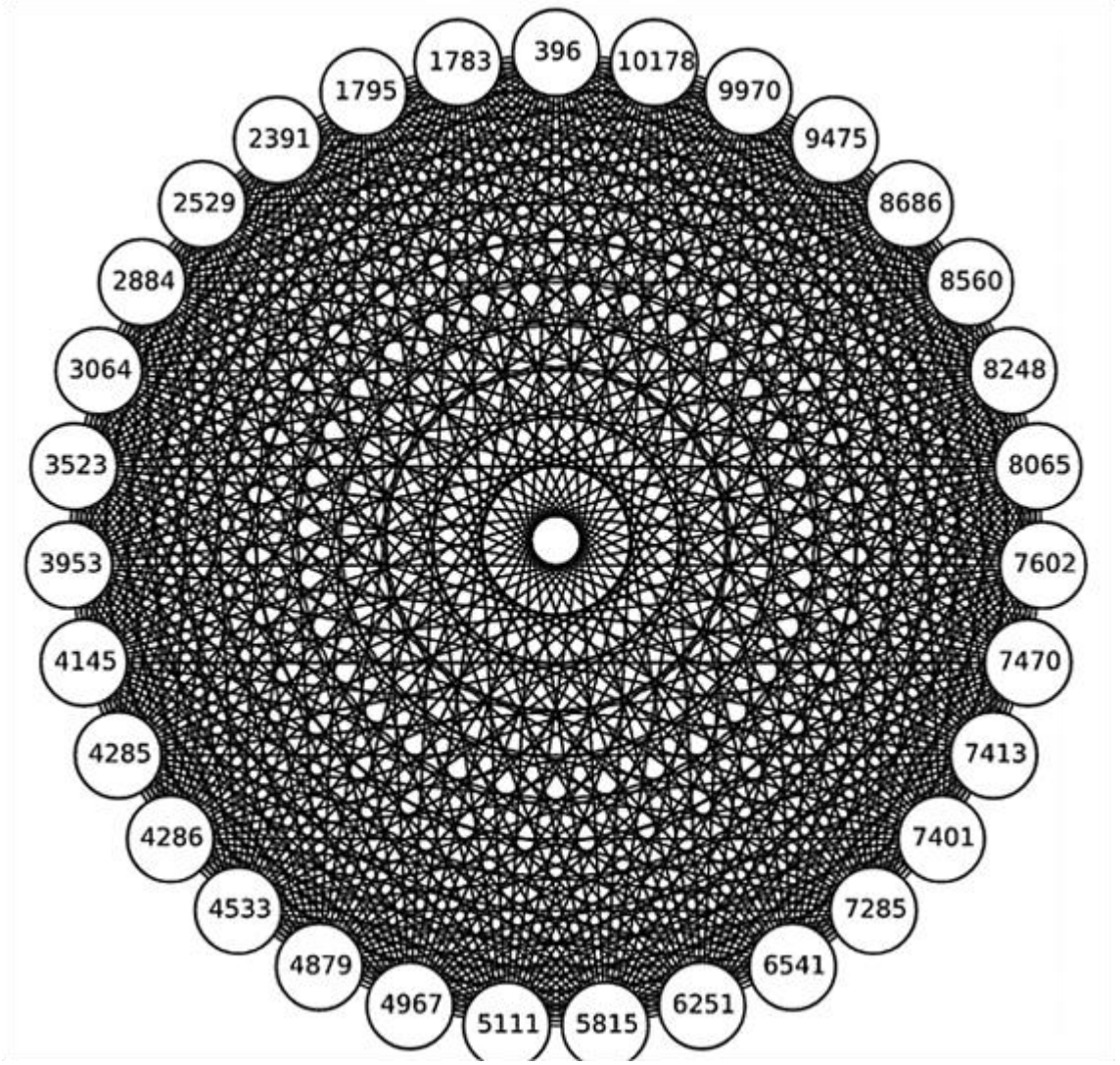
Криптостойкость данного алгоритма зависит от типа используемой хеш-функции. С учетом того, что процедура хеширования имеет сугубо односторонний характер, а также того факта, что хешируется значительное количество данных (256 пар), задачу обратного восстановления секретного ключа из открытого не способен решить даже квантовый компьютер. Но этот алгоритм тоже не совершенен. Во-первых, ключи имеют существенный размер (до 16 килобайт). Во-вторых, при формировании электронной подписи данным алгоритмом половина секретного ключа становится фактически публичным достоянием. Поэтому подпись на базе одного ключа целесообразно использовать лишь единожды, что также создает значительные неудобства для проектирования систем на базе этого алгоритма.

Следующий алгоритм, который также считается постквантовым, — это так называемая «криптография на решетках». Решеткой в математике называют периодическую сеть точек в n-мерной системе координат, где задано число n «базисных векторов», порождающих саму решетку. Вот простой пример решетки для прямоугольной системы координат с двумя заданными базисными векторами.



Сложная для вычисления задача в данном алгоритме — это нахождение так называемого SVP (Shortest Vector Problem) или «наиболее короткого вектора» для заданных базисных векторов при условии существенного увеличения размерности пространства n. Если рассматривать обыкновенную плоскую двумерную решетку, то найти глазами точку, наиболее близкую к заданному узлу решетки, для человека не составляет никакого труда. Однако если это будет делать компьютер, то в ход пойдут непростые математические вычисления. А если начать увеличивать количество пространственных измерений, то процесс превратится в весьма серьезную вычислительную задачу. Считается, что на данный момент сложность такой задачи превышает возможности квантового компьютера. Впрочем, из алгоритмов, базирующихся на криптографии на решетках, неуязвимым пока признается только непосредственно само шифрование. Цифровая электронная подпись уже подверглась взлому в 1999 году, а ее модифицированная версия — в 2006 году. В настоящее время математики работают над дальнейшим развитием алгоритма ЭЦП, чтобы разрешить эту проблему и предложить индустрии новый, более совершенный стандарт криптографической безопасности.

Наконец, рассмотрим, возможно, самый перспективный на текущий момент алгоритм — использование криптографии на базе изогений эллиптических кривых. Изогения — это метод, позволяющий отобразить точку, принадлежащую одной эллиптической кривой, в точку на другой кривой подобного же типа. Алгоритм преобразования точек представляет собой соотношение двух полиномов (многочленов) для каждой из координат точки по осям x и y. В случае если получить такое отображение считается математически возможным, то эти две кривые будут являться изогенными по отношению друг к другу. Для каждой из кривой можно рассчитать так называемый «j-инвариант», являющийся чем-то вроде «классификатора» эллиптической кривой и представленный в виде обычного числа. Для расчета j-инварианта используются коэффициенты из уравнения эллиптической кривой. Применяя различные значения коэффициентов, рассчитывают множество инвариантов, которые затем отображаются в виде графа. В полученном графе инварианты становятся его вершинами, а ребрами графа служат соединения тех инвариантов, эллиптические кривые которых изогенны друг другу. Собственно, нахождение путей в графе между вершинами или, другими словами, вычисление изогении между различными эллиптическими кривыми и есть та сложновычислимая задача, на базе которой строится данный криптографический алгоритм. Структуры, построенные на основе последовательно наложенных друг на друга графов эллиптических кривых, представляют собой очень красивые геометрические объекты, как, например, сложная «звезда изогений», показанная на рисунке:



Очевидно, что применение изогений существенно усложняет эллиптическую криптографию. Если в классическом варианте мы имеем дело только с одной эллиптической кривой, то в случае с изогениями — с целым их «семейством», что возводит решение задачи в дополнительную степень сложности. Даже квантовому компьютеру не под силу решить эту задачу за субэкспоненциальное время, что говорит об исключительной криптостойкости алгоритма, который с полной уверенностью можно считать «постквантовым». Скорее всего, данный алгоритм на текущий момент является наиболее пригодным для построения на его основе блокчейн-проектов, которые стремятся обеспечить максимальную безопасность данных для своих пользователей. А в свете активно развивающейся индустрии квантовых вычислений эта проблема становится действительно актуальной.

Теория игр и блокчейн

Когда мы рассматривали децентрализацию как способ управления, была обозначена проблематика сложности взаимодействия равных по правам субъектов в системах, где консолидирующий и управляющий центр отсутствует как класс. И ведь действительно, каким же наиболее эффективным образом равноправным участникам системы следует приходить к единым решениям, которые устроят если не абсолютно всех, то подавляющее большинство? Очевидно, должна существовать некая процедурно обусловленная форма общественного согласия, позволяющая принимать решения, обязательные к исполнению всем сообществом. При этом она не должна создавать неразрешимые конфликты, ведущие к разрушению системы в целом. Этот комплекс мер называется формированием правил для прихода к консенсусу, то есть единодушия во мнениях между заинтересованными лицами при принятии важных для системы решений без затратной, с точки зрения ресурсов, процедуры прямого голосования.

Совокупность стремлений участников системы извлечь собственную или общественную выгоду, преодолевая при этом явное или скрытое сопротивление других участников с противоположными интересами, можно описать словом «игра». Разумеется, для реализации своих целей каждый из участников оперирует той или иной специально разработанной стратегией, которая стремится к достижению максимального эффекта в решении поставленных задач. В математике существует специальный раздел, посвященный изучению оптимальных стратегий в играх. Он так и называется — «теория игр», и мы рассмотрим ее отдельные элементы, поскольку они являются

важным звеном при построении блокчейн-систем, которые почти всегда децентрализованы, а ее участники равноправны. Речь идет в первую очередь о методах формирования консенсуса между узлами сети при создании цепочки блоков, а также наборов транзакций в них. Но об этом чуть позднее. Сначала попробуем уяснить для себя, что же является эффективной или неэффективной стратегией при достижении общего согласия.

Эффективность стратегии неразрывно связана с понятием рационального поведения участников. Чтобы убедиться, что сотрудничество между участниками «игры» не всегда гарантировано, даже если это сообразуется с их общими интересами, рассмотрим известную «Дилемму заключенного». Она была представлена в 1950 году американскими математиками Мерилом Фладом и Мелвином Дрешером. В тюрьму почти одновременно и за одно и то же деяние попадают двое преступников. Небезосновательно предполагая возможный сговор между ними, полиция изолирует их друг от друга, а затем предлагает каждому одинаковые условия сотрудничества со следствием. Форма сотрудничества предполагает свидетельство одним заключенным против другого в обмен на немедленное освобождение. Также предполагается, что, если второй заключенный на сотрудничество с полицией не идет, он получает максимальный тюремный срок. В случае если оба отказываются сотрудничать, каждый получает минимальный срок. Если же имеет место взаимное обличение, то оба получают средний по длительности срок. Понятно, что, находясь в изоляции, заключенные не знают о решении друг друга. Какова же тогда в этом случае наиболее эффективная стратегия для каждого из заключенных?

Дилеммой эта ситуация называется потому, что для каждого отдельно взятого заключенного и при рассмотрении их как группы предпочтительные стратегии диаметрально противоположны по смыслу. Для конкретного заключенного выгоднее переложить всю вину на другого, и тогда у него есть шанс немедленно выйти из тюрьмы. Но двум заключенным как группе выгоднее молчать, поскольку суммарный срок заключения для обоих будет минимальным среди всех возможных исходов. То есть если по отдельности оба субъекта ведут себя рационально, то в совокупности результатом становится нерациональное решение. Подобная ситуация в какой-то степени отражает сложность проблематики, которую изучает теория игр, когда один участник пытается максимизировать собственный интерес в ущерб общей выгоде. В блокчейн-системах подобная практика реализуется на следующем наглядном примере.

Допустим, что в децентрализованной системе, хранящей цифровые активы, имеющие эквивалент денежной стоимости (например, криптовалюты), нашелся некий узел, который при помощи различных недобросовестных практик сумел навязать всей сети искусственную транзакцию, в результате которой стал обладателем огромного количества цифровых монет. Вопрос: кто выиграет от этой акции? Кто-то, возможно, подумает, что выигрывает злоумышленник, поскольку результатом его действий явилось прямое личное обогащение. Проиграли, безусловно, бывшие владельцы активов, которые потеряли их в результате атаки на сеть и на свои персональные счета. Остальные же участники системы не пострадали, оставшись при своих активах, до которых вредоносный узел не добрался. Однако это лишь поверхностные выводы. Своей атакой на сеть злоумышленник на самом деле совершил непоправимое — подорвал общее доверие к сети в целом. К ее концепции безопасности, криптографической неуязвимости, а также к протоколу формирования консенсуса. А это означает, что все ценностные активы, принадлежащие данной сети и имеющие монетарную или даже биржевую оценку, мгновенно утратят свою стоимость. Это касается в том числе и неправедно полученных активов самого злоумышленника. Что фактически превращает его действия из лично эффективных в общественно бесполезные. Сеть разрушается и прекращает свое существование. Победителей в данной ситуации нет, есть одни только проигравшие.

Этот пример очень хорошо показывает, насколько важен протокол общего согласия в децентрализованных системах. Он играет не менее существенную роль, чем криптостойкость используемых в системе алгоритмов шифрования данных. Какие же методы достижения консенсуса могут использоваться в блокчейн-проектах? Одним из наиболее популярных является консенсус на базе «Задачи о византийских генералах». Перенесемся в период позднего Средневековья, когда Византийская империя уже переживала упадок. Представим, что Византия находится в состоянии войны и император послал на захват одного из вражеских городов некоторое количество армий, во главе каждой из которых стоит генерал. Казалось бы, генералы — люди военные, не чуждые понятию верности и чести, однако в Византии того периода дела с этими личными качествами военачальников обстояли довольно скверно. В силу этого обстоятельства каждый из генералов с некоторой долей вероятности мог оказаться подкуплен противником, иначе говоря — стать предателем. В зависимости от степени своей лояльности каждый отдельный генерал мог напрямую последовать поступающему свыше приказу, а мог и осуществить прямо противоположные действия, тем самым способствуя поражению империи в войне. Возвращаясь к математике, рассмотрим варианты возможных исходов.

- Лояльные генералы, согласно приказу, вместе ведут свои армии в атаку на город — город взят, война выиграна. Очевидно, что это наилучший исход для Византии.
- Лояльные генералы, согласно приказу, одновременно отступают — город не взят, но все армии сохранены для будущих сражений. Данный исход можно считать промежуточным.

- Лояльные генералы атакуют, как и было приказано, однако генералы-предатели вместо атаки начинают отступать — в результате все армии уничтожены противником, а сама война Византией проиграна. Это наихудший из возможных вариантов.

Иногда задачу дополнительно усложняют присутствием главнокомандующего, который имеет право отдавать приказы нижестоящим генералам. Суть усложнения состоит в том, что сам главнокомандующий тоже может быть предателем. И тогда он будет отдавать разным генералам противоположные по смыслу приказы, чтобы гарантированно добиться наихудшего исхода для Византии. В этом случае наиболее эффективным поведением для всех генералов была бы стратегия полного игнорирования приказов главнокомандующего. Оставим в стороне вопросы военной дисциплины и сосредоточимся на том, каким образом можно было бы добиться наилучшего исхода в подобной ситуации. Очевидно, что если каждый генерал будет действовать по собственному разумению (скажем, равновероятно в отношении решения атаковать или отступать), вероятность благоприятного и даже промежуточного исхода для Византии крайне мала. Единственное оптимальное решение в данной ситуации — это прямой обмен информацией генералами между собой.

Информация, которой обмениваются генералы, может носить различный характер. Это могут быть сведения о численности каждой из армий либо просто обозначение своего намерения — атаки или отступления. Важно то, что каждый из генералов (допустим, что их число равно n) передает всем остальным генералам свою информацию и получает от них назад n-1 наборов подобных же сведений. Но это еще не все. Получается, что каждый генерал обладает неким объемом информации, полученным от всех остальных генералов при прямом общении. И он может как ретранслировать полученную информацию всем генералам, так и получить себе подобные же наборы данных от других. То есть каждый генерал располагает не только той информацией, которую он получил напрямую от каждого из прочих генералов, но и имеет в распоряжении всю коммуникационную картину в формате «какой генерал какому генералу что сообщил». Однако мы должны принимать во внимание тот факт, что один или даже несколько генералов могут быть предателями и, соответственно, намеренно искажать передаваемую информацию. Тем не менее всегда есть возможность проверить, что каждый конкретный генерал сообщал другим генералам, и найти либо совпадения, либо расхождения в информации. На базе полученных данных можно выявить часть нелояльных генералов и оценить их долю в общей массе. Математически доказано, что в случае более 2/3 лояльных узлов система считается устойчивой и консенсус может быть достигнут. В противном случае система утрачивает работоспособность и как следствие доверие участников.

Принцип устойчивости к «византийской проблеме» — это классическая задача из «теории игр», которая является важным элементом безопасности при формировании консенсуса в блокчейн-проектах. Каждый узел в системе должен строго следовать ее правилам, прописанным в виде алгоритмической логики программного обеспечения узла. Однако почти все программное обеспечение в блокчейн-проектах поставляется в виде открытого кода, который каждый узел может при желании модифицировать таким образом, чтобы попытаться получить преференции, которые ему в обычной ситуации не полагались. Но даже если какие-то несанкционированные сетью изменения будут все же внесены отдельным узлом (или даже группой узлов), для успешности атаки необходимо, чтобы таких узлов было достаточно много. Иначе остальная сеть будет отвергать информацию от нарушителей, поскольку она не будет соответствовать общим правилам, которыми руководствуется большинство. В этом и состоит суть консенсуса, который применяется для управления в децентрализованных системах. Целостность системы нарушается, если количество «инакомыслящих» узлов начинает превышать критическую массу, после чего происходит разделение сети, которое называется «форк». Узлы, исповедующие разные правила консенсуса, образуют разные сети, которые с момента разделения начинают жить отдельной жизнью, становясь, по сути, различными проектами, хотя и со схожей технологией — по крайней мере, на первых порах. К понятию «форк» как важному явлению в блокчейн-индустрии мы еще вернемся.

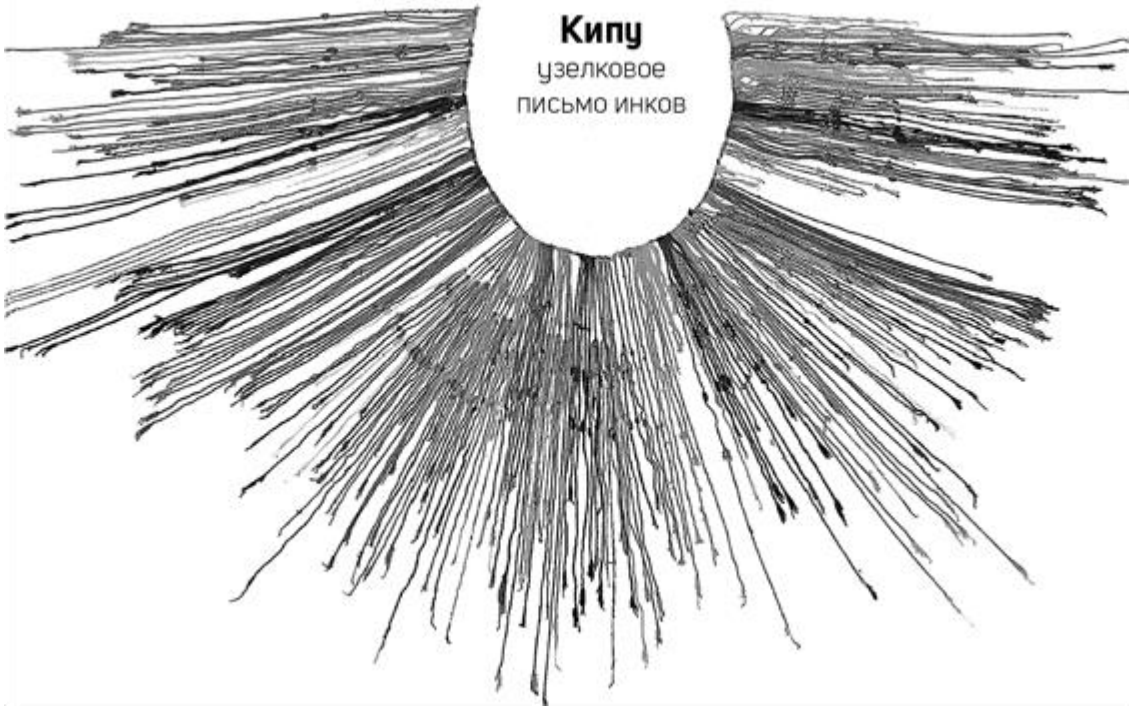
Для того чтобы пояснить работу консенсуса в блокчейн-средах на конкретных примерах, необходимо перейти к изучению структуры блоков и транзакций, а также рассмотрению принципов формирования блоков и их цепочек. В предыдущих главах мы поговорили обо всех важных составляющих элементах технологии блокчейн по отдельности и теперь можем начать собирать эти знания воедино, как гамбургер, ингредиенты которого были заранее приготовлены и разложены на столе, чтобы в определенный момент сложиться в совокупный кулинарный конструктив. Его мы и предложим к употреблению заждавшимся гостям, приглашенным на пиршество, прелюдия к которому несколько затянулась по причинам сугубо технологического свойства.

Блоки и их структура

В описании общих принципов построения структуры блокчейна архитектура децентрализованной базы данных была сравнена с бухгалтерской книгой, страницы которой являлись блоками, куда записывались финансовые транзакции. Было отдельно указано, что эти «страницы» упорядочены в строгой последовательности, которую нельзя поменять, так как они математически крепко сцеплены между собой специальными «криптографическими замками». Теперь, когда мы ознакомились с основными технологическими элементами блокчейн-сетей, включая криптографию, мы можем раскрыть более подробно, каким образом поддерживается целостность структуры

блоков и как это влияет на общую безопасность хранения информации в распределенных системах. Очевидно, что каждая блокчейн-система в отдельности имеет свои особенности структурного дизайна, и когда мы будем изучать самые популярные реализации различных проектов, мы эти особенности выявим и внимательно рассмотрим. Однако почти все системы, созданные на базе технологии блокчейн, имеют единые принципы формирования структуры и ее элементов. Поэтому целесообразно их рассматривать в рамках общего описания, так как в большинстве практических случаев они присутствуют в проектах в очень схожей технологической форме, без существенных различий.

Идея хранить информацию в виде связных списков возникла достаточно давно — гораздо раньше, чем появились сами компьютерные технологии. А именно — более 4000 лет назад у индейской цивилизации инков и их предшественников примерно в III тысячелетии до нашей эры. Речь идет о способе сохранения информации в виде так называемых «кипу» — хитросплетений нитей, нанизанных на единую веревочную основу и связанных между собой в зависимости от контекста записываемой информации. Каждая нить могла иметь свой цветовой код, а также специальные узлы, форма и количество которых являлись важными маркерами, определяющими значения и типы хранимой информации. Прослеживая начало и конец каждой из нитей, можно было определить весь путь формирования цепочки данных — от базовой веревки и до окончания ответвления. Общее число нитей в одном кипу могло достигать 2500. При помощи кипу инки как правящий класс всего союза индейских племён Центральных Анд могли учитывать все необходимые подконтрольные им ресурсы — войска, запасы продовольствия, численность населения и объем взимаемых налогов.



Появившиеся в тех местах в первой половине XVI века испанские конкистадоры далеко не сразу постигли утилитарный смысл этих странных веревочно-узловых конструкций, при помощи которых инки фактически управляли своей империей. Для того чтобы сломать установившийся порядок управления, испанцам пришлось навязать завоеванным территориям европейские принципы письменности и учета данных. Кипу были полностью вытеснены из обращения и забыты, и только в начале XIX века ученые начали их изучать на относительно системной основе. Им удалось расшифровать достаточно много информации, содержащейся в сохранившихся экземплярах. Поняв основные принципы логики построения подобной системы учета, ученые были весьма удивлены, что такая древняя цивилизация, будучи изолированной от более прогрессивного мира, сумела найти столь эффективный способ компактной записи и хранения данных, подчиняющийся логике связных информационных блоков.

Во второй половине XX века, когда информационные технологии начали медленно, но верно завоевывать мир, возникла необходимость в создании различных форм записи и хранения информации. Одной из таких форм стали связные списки — специальные структуры данных, каждая из которых содержала не только данные как таковые, но и специальные ссылки на подобные же структуры, как на предыдущие, так и на последующие. Это позволяло игнорировать естественный порядок хранения данных на различных носителях и руководствоваться при этом исключительно той информационной логистикой, принцип которой был заложен в наборе внутренних связей между блоками. В зависимости от логики решения поставленных задач формы списков данных в большинстве случаев могли

быть односвязными (однонаправленными) или двусвязными (двунаправленными). Также обе формы списков могли иметь кольцевую структуру, когда последний элемент ссылается на первый или наоборот. Пример простого односвязного списка показан на рисунке:

Собственно, в своем классическом виде блокчейн представляет собой односвязный список, когда каждый следующий блок в системе ссылается на предыдущий. Вопрос в том, что значит «ссылается»: каким образом это технологически реализовано, а главное, зачем он вообще это делает? Ответ прост — для поддержания целостности базы данных. Блок состоит из двух основных частей — заголовка, содержащего служебную информацию, и списка транзакций для передачи цифровых активов между участниками системы или просто записи фактов. Все это — набор данных, который можно отобразить в виде хеша стандартной длины. Вычислив хеш данных заголовка, мы фиксируем состояние всего блока, и любое вмешательство в его целостность немедленно приведет к тотальному изменению общего хеша. А что, если каждый новый блок будет содержать хеш от данных предыдущего блока как один из элементов своего заголовка? Тогда получится, что, хешируя данные одного заголовка, мы автоматически включаем туда хеш заголовка предыдущего блока, и таким образом получается форма сцепления блоков. Нам известно, что любое малейшее изменение в прообразе меняет его хеш до неузнаваемости. Это означает, что если мы вмешаемся в любой бит данных любого из блоков в середине цепочки, это приведет к пересчету всех хешей последующих блоков. Другими словами, изменятся данные всей цепочки.

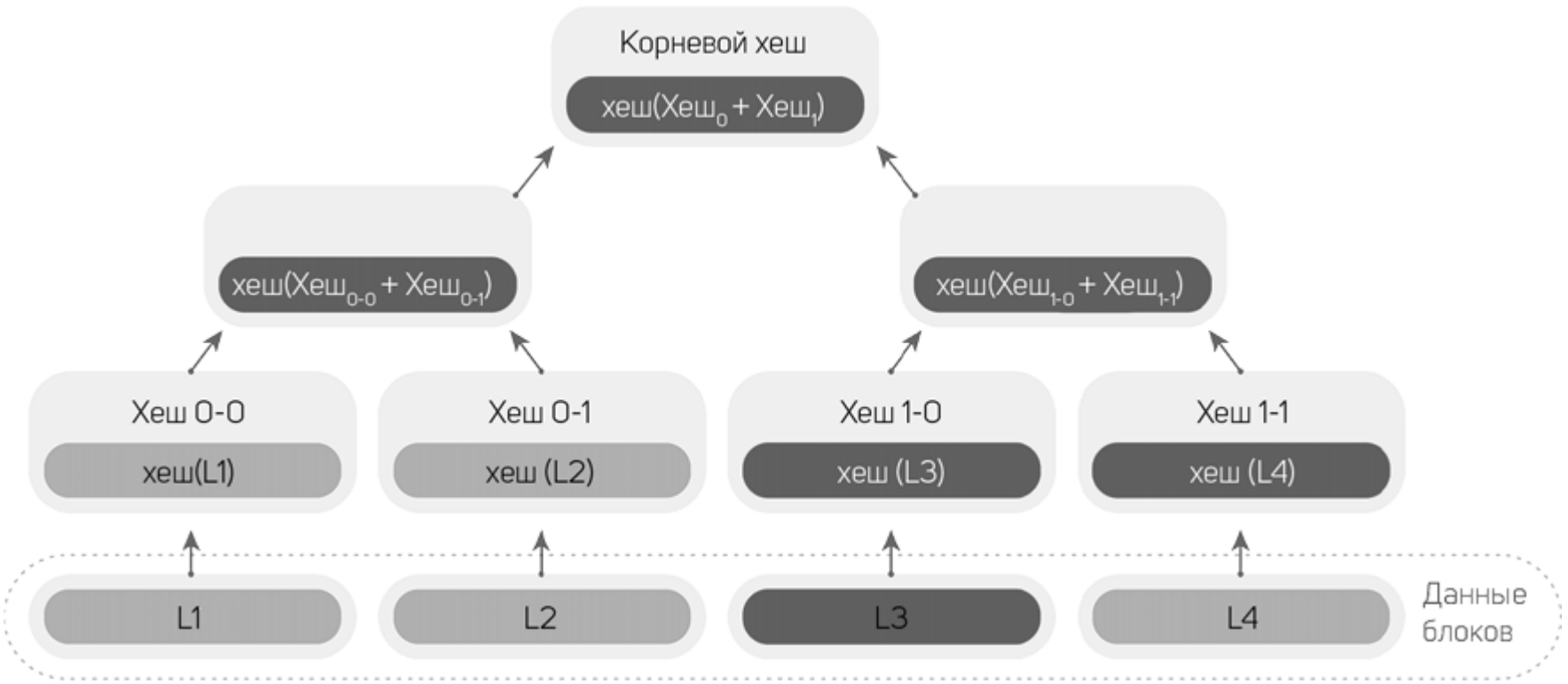
О чем в первую очередь нам говорит связная структура блоков? О том, что блокчейн — это система, куда можно только добавлять информацию, но нельзя менять или удалять. При этом добавить информацию возможно только в виде новых блоков и только в конец цепочки. Это, безусловно, порождает определенное неудобство при управлении информацией, помещаемой в блокчейн, но, с другой стороны, создает исключительную безопасность хранения данных в распределенном виде. Ведь вся база блоков копируется каждому участнику системы, и каждый из них имеет возможность записать туда что угодно. Другое дело, что эти изменения, будучи сделаны с нарушением правил системы, не будут приняты другими участниками сети. А соответствие правилам проверяется участниками системы чисто математически, поэтому подсунуть им искаженную информацию никак не удастся. Алгоритмы проверки информации, содержащейся в блоках, сразу же просигнализируют о нарушении целостности данных, и данный блок будет считаться неприемлемым для всей сети.

Есть и еще одно неудобство: поскольку данные можно только добавить, но нельзя удалить, даже если они в какой-то момент утратили свою актуальность, общая база с момента образования самого первого блока постоянно растет. Ее размер зависит от разных параметров — скорости создания новых блоков, количества транзакций, содержащихся в них, размеров самих транзакций. В зависимости от этих параметров, а также «возраста» базы данных ее размер уже через несколько лет активной работы может исчисляться сотнями гигабайт информации, которая постоянно копируется и синхронизируется между участниками системы. Решение задачи оптимизации размера базы данных в блокчейн должно стать приоритетом для разработчиков популярных систем, в противном случае это может создать дополнительные препятствия для развития перспективной технологии. Впрочем, предложения по решению этой проблемы уже существуют, и мы коснемся их в разделе, посвященном вопросам масштабирования технологии блокчейн.

Давайте рассмотрим структуру заголовка блока подробнее, чтобы понять, какого рода служебная информация в нем содержится. Понятно, что в разных практических реализациях структура блоков всегда отличается, но у них есть ряд общих элементов, которые встречаются в том или ином виде почти в каждом проекте. Как правило, первое, с чего начинается любой блок — это его порядковый номер. Самый первый блок называется «генезисным», он отличается от прочих тем, что не содержит ссылки на предыдущий блок по причине отсутствия такового. Обычно в блоке есть информация о номере его версии — это бывает необходимо, если впоследствии структура блока претерпит изменения, и в зависимости от номера версии алгоритмы программного обеспечения должны будут их по-разному обрабатывать. Затем, как отмечалось ранее, в заголовке содержится хеш заголовка предыдущего блока для поддержания целостности данных всей цепочки.

Важным элементом заголовка также является время создания блока. Оно записывается в виде числа, равного количеству секунд, прошедших с 1 января 1970 года — формат, принятый в многопользовательских и многозадачных операционных системах, таких, например, как Unix и совместимых с ней. Отдельно заметим, что число это достаточно велико, и через пару десятков лет должно произойти переполнение 32-битной ячейки памяти, обычно выделяемой для переменных, хранящих это значение в различном программном обеспечении. В случае если разработчики этих программ не внесут необходимые исправления, увеличив размер переменной, хранящей значения времени до 64 бит, то 19 января 2038 года по всему миру могут произойти массовые программные сбои. Произойдет это потому, что значения этого числа в силу специфики построения компьютерной архитектуры при выполнении программ будут интерпретироваться как имеющие отрицательные значения — со всеми вытекающими из этого алгоритмическими последствиями.

И, наконец, переходим к части заголовка, посвященной содержащимся в блоке транзакциям. Одним из значений в заголовке является число транзакций в блоке, а вот второе значение имеет загадочное название «корень Меркла». Это не что иное, как совокупный хеш всех транзакций, находящихся в данном блоке, вычисленный определенным образом. В 1979 году американский криптограф Ральф Меркл запатентовал алгоритм вычисления результирующего хеша для набора данных, построенных в виде двоичного дерева:



Согласно логике алгоритма Меркла, все транзакции в блоке делятся попарно, хешируются, и их хеши суммируются между собой. Если общее число транзакций изначально было нечетным и последней транзакции не хватает пары, то в этом случае ее собственный хеш просто удваивается. На следующем уровне «дерева» количество хешей уже вдвое меньше и их число уже гарантированно четное. Хеши опять разбиваются по парам, эти пары суммируются, и так далее, пока из них не останется только одно конечное число. В итоге на вершине дерева образуется результирующий, или корневой хеш, который и называется «корнем Меркла» и является фактически единым совокупным отпечатком всех транзакций блока. Понятно, что при изменении любой из транзакций в блоке все хеши дерева Меркла сразу же пересчитаются заново, и результирующий хеш также изменится, что будет являться маркером события, соответствующего вмешательству в данные блока. Таким образом, значение корня Меркла является «представителем» транзакционной части блока в его собственном заголовке. Будучи «подхешированным» к общим данным заголовка и, таким образом, опосредованно включенным в заголовок следующего блока, корень Меркла играет роль дополнительной гарантии неизменности транзакций, ранее записанных в блокчейн.

Помимо вышеописанных параметров структуры блока, в нем могут присутствовать элементы, связанные с непосредственным получением права на создание блока и его защиты от возможных будущих изменений. Речь идет о создании новых блоков в системах с доказательством работы. Но в данный момент говорить об этом несколько преждевременно, поэтому сначала ознакомимся со структурой транзакций и принципами ведения балансов в блокчейн-системах.

Транзакции и балансы

Все мы привыкли иметь дело с классическими банками: открывать счета, осуществлять платежи с одного расчетного счета на другой, получать на свой счет денежные средства. В последние пару десятилетий широкое распространение получили системы «банк — клиент», позволяющие управлять своими счетами через интернет. Несмотря на внешние различия, в первую очередь в части дизайна интерфейса подобных систем, их функционал является более-менее схожим для всех финансовых институтов, предлагающих такие услуги. Первым шагом к получению доступа к своим средствам через интернет в большинстве случаев является прохождение процедуры двухфакторной идентификации. Сначала пользователь вводит обычный пароль многократного использования, а затем система просит ввести специальный однократный код, который либо генерируется посредством специального устройства, либо может быть получен по SMS или электронной почте. Так исключается несанкционированный доступ к счету клиента, данные о котором хранятся на серверах банка, то есть централизованно. Если сервера банка по какой-то причине не работают, например, находятся на техническом обслуживании, то доступ к счету будет невозможен до момента, пока система не вернется к обычной работе.

Получив доступ к своему счету, клиент может проверить свой баланс, а затем осуществлять перевод средств с данного счета, также пользуясь системой генерации однократных кодов, поскольку этого требуют правила безопасности доступа к данным. У каждого счета есть свой номер, сгенерированный по определенным правилам и стандартам — либо самого банка, либо государства, в котором банк расположен. Отправляя платежи на другие счета, банк, как правило, взимает комиссию за свои услуги, размер которой устанавливает самостоятельно, в зависимости от своих бизнес-издержек, заложенной нормы прибыли и конкурентной ситуации на рынке банковских услуг. Очевидно, чтобы клиент мог совершать или получать платежи, банк сначала должен открыть ему расчетный счет и выдать реквизиты доступа в интернет-банк, иначе никакие входящие или исходящие переводы невозможны.

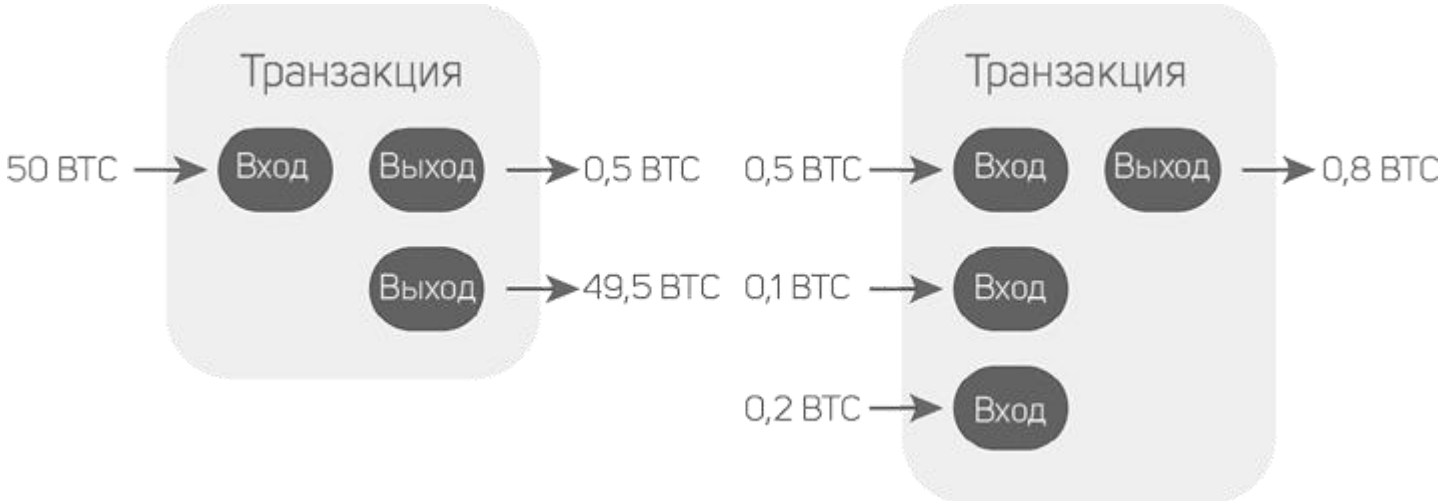
В блокчейн-системах все организовано совсем по-другому. Во-первых, там нет никаких банков или иных централизованных органов, контролирующих счета и платежи по ним. Во-вторых, никакие счета заранее не создаются, и балансов по ним никто специально не ведет. На первый взгляд это кажется немного странным, однако именно этим отличаются проекты платежных систем, реализованные на базе технологии блокчейн. Для того чтобы стать участником системы, пользователю необходимо сгенерировать себе пару ключей — закрытый и открытый, пользуясь алгоритмом асимметричной криптографии, который используется в конкретной блокчейн-среде. Ключи в паре всегда жестко связаны между собой — секретный может быть сгенерирован случайным образом, а открытый вычисляется из него математически. Впрочем, все это делается автоматически, при помощи программного обеспечения самой системы по запросу пользователя, то есть нажатием соответствующей кнопки в интерфейсе программы-клиента. Таким образом у пользователя появляется свой счет в системе, хотя правильнее было бы сказать — адрес. И этот адрес фактически является модификацией его открытого ключа, который при создании был обработан несколькими процедурами хеширования и специального символьного кодирования. Делается это не только для более удобного визуального восприятия адреса, но и для еще большего усложнения задачи восстановления связанного с ним закрытого ключа, поскольку односторонние хеш-функции, да еще использованные несколько раз подряд, исключительно усложняют любые попытки взлома адреса блокчейн-системы.

Напомним, что подобные сети являются децентрализованными, поэтому все действия пользователь совершает не на каком-то удаленном сервере, а непосредственно у себя на компьютере или мобильном устройстве. Там же хранятся и все необходимые ключи, в том числе и закрытые. В отличие от классического банка, вопросы хранения секретной персональной информации теперь возложены на самого

клиента. Если он потеряет секретный ключ, то автоматически утратит доступ к активам, которые связаны с адресом, сгенерированным на основе этого секретного ключа. В интернете можно найти огромное количество историй о несостоявшихся криптовалютных миллионерах, которые потеряли свои цифровые миллионы вместе с закрытыми ключами от своих адресов. Это достаточно серьезная проблема, поэтому вопросам безопасности хранения криптоактивов будет посвящена отдельная глава.

Теперь, когда у пользователя есть адрес в условной блокчейн-системе, разберемся, каким образом он сможет получать на него и затем переводить с него на другие адреса цифровые активы. Здесь нельзя еще раз не вспомнить аналогию с бухгалтерской книгой, которая состоит из страниц с финансовыми транзакциями: от кого переведено, кому, сколько и за что. Представим, что у нас есть несколько участников в какой-то бизнес-среде, которые постоянно обмениваются товарами, услугами и денежными средствами, а все факты совершения обмена при этом записываются в специальную книгу. Когда один из участников захочет перевести другому определенную сумму, ему для начала необходимо доказать, что он располагает этими средствами. Сделать это можно, только лишь указав на предыдущие входящие транзакции в пользу этого участника, то есть сослаться на них как на доказательство владения определенными активами. Причем сослаться можно не на какую-то одну конкретную транзакцию, а сразу на несколько, если одной будет недостаточно для того, чтобы набрать необходимую сумму для исходящего платежа.

Когда банк переводит деньги с одного счета на другой, он проводит следующие три операции: вычитает сумму перевода и сумму комиссии за перевод со счета отправителя и добавляет сумму перевода на счет получателя. Комиссию же банк оставляет себе как оплату за совершенную посредническую услугу. В блокчейн-системах никаких посредников нет, равно как и средства ниоткуда физически не вычитаются и никуда не прибавляются. Владелец активов просто указывает в транзакции адреса одного или нескольких получателей, то есть опять же формирует ссылки. В итоге транзакция представляет собой набор ссылок на входящие поступления на адрес плательщика, а также набор ссылок на исходящие адреса получателей его платежей. Для таких транзакций в блокчейн-среде оперируют понятиями «входы» и «выходы». Существует правило, что сумма всех средств на «выходах» должна быть равна сумме средств на «входах». Если у владельца адреса нет необходимости тратить все средства на задействованных в транзакции «входах» полностью, он формирует дополнительный «выход» в виде сдачи самому себе, чтобы поддержать равный баланс «входов» и «выходов». Очевидно, что «выход» для отправителя будет являться «входом» для получателя, и он сможет потом на него, в свою очередь, сослаться, когда будет совершать собственные исходящие платежи.



Какие выводы мы можем сделать из описания этой схемы? Во-первых, проанализировав с самого первого (генезисного) блока базы все «входы» на конкретный адрес и все «выходы» с него, можно легко выявить, сколько у владельца данного адреса осталось непотраченных «выходов». Это и есть баланс его счета. То есть баланс как таковой нигде не хранится, а просто вычисляется как сумма всех непотраченных «выходов». Во-вторых, указывая «выход» на конкретный адрес, отправитель предполагает, что в системе существует такой участник, у которого есть закрытый ключ к этому адресу. Иначе, если, например, ввести адрес получателя с ошибкой, то транзакция, на него ссылающаяся, все равно будет принята системой, но средства этой исходящей транзакции будут навсегда потеряны и исключены из обращения. Это связано с тем, что транзакции, помещенные в блок, прошедшие процедуру консенсуса и включенные в общую цепочку блоков, не смогут в будущем быть изменены. Некоторые проекты, например, Биткоин, формируют определенную защиту от ошибки, преобразуя адрес в формате шестнадцатеричного числа в алфавитно-цифровой формат, добавляя в конец полученного адреса его контрольную сумму. При вводе адреса получателя в соответствующее поле формы перевода средств в случае ошибки в расчете и сравнении контрольной суммы система выдаст предупреждение. Также довольно часто используется представление адреса в виде QR-кода, чтобы отправитель мог его отсканировать своим мобильным телефоном и автоматически преобразовать в правильный набор букв и цифр, составляющих адрес получателя.

Возникает вопрос: а может ли участник системы при переводе средств сослаться на «входы», которые ему самому не принадлежат, и каким образом это можно проверить? На самом деле для того, чтобы легитимно сослаться на «входы», необходимо в ссылке указать свой открытый ключ и свою цифровую электронную подпись, сформированную на базе закрытого ключа, связанного с адресом владельца. При помощи алгоритмов проверки цифровой подписи любой участник системы может удостовериться в том, что ссылка на «входы» действительно легитимна. А в случае ошибки проверки данная транзакция просто игнорируется и не включается в блок тем узлом, который его формирует для сети.

Подобная система формирования транзакций и ведения балансов называется UTXO (Unspent Transaction Output — «непотраченные транзакционные выходы»). Как было указано выше, для расчета баланса, связанного с конкретным адресом в системе, необходимо найти и проверить все связанные с ним «входы» и «выходы» с самого начала базы блоков. Плюс этого метода в том, что не нужно отдельно хранить состояние балансов и постоянно их актуализировать, тем самым получая экономию свободного места на носителях. Минус — это время, которое постоянно затрачивается на расчет баланса, особенно если база блоков достаточно выросла в своих размерах. Поэтому ряд проектов все же хранит специальные базы «актуального состояния», где, в частности, находятся и данные о балансах адресов, которые можно быстро оттуда получить.

Теперь рассмотрим, какая еще дополнительная служебная информация может помещаться в транзакции. Во-первых, это идентификатор транзакции с уникальным номером, который не может повторяться. Его получают из хеша самой транзакции, поскольку, как мы знаем, у криптостойких хеш-функций вероятность получения коллизии (то есть одинакового хеша для разных прообразов) очень и очень мала. Во-вторых, в тело транзакции обычно помещают хеш предыдущей транзакции в данном блоке — по аналогии с тем, как это делается в заголовках самих блоков. Наличие этой информации в каждой транзакции преследует ту же самую цель — поддержание целостности хранения данных и ее защиту от несанкционированного изменения. Также при описании ссылок на «входы» указывают открытый ключ адреса и электронную подпись, которая доказывает, что у автора транзакции имеется закрытый ключ от этой пары.

И последнее, что хотелось бы сказать о транзакциях в общем описании — это комиссия. Различные блокчейн-проекты взимают комиссию за транзакции, хотя бывают и такие, в которых все транзакции бесплатны. Комиссия существует для монетарной мотивации узлов, создающих блоки, — они забирают ее себе, наряду с основным вознаграждением за создание блока как такового. Об этом процессе мы подробно поговорим в главе о так называемом «майнинге», а здесь лишь упомянем, что комиссия в блокчейн-системах, как правило, не является фиксированной и каждый создатель транзакции сам решает, какую комиссию ему заплатить. Однако если эта комиссия окажется слишком низкой или вовсе нулевой, то транзакция может получить низкий приоритет при формировании новых блоков и будет включена в какой-то из них с большой временной задержкой. Что же касается непосредственной визуализации величины комиссии в теле транзакции, то здесь опять же применен подход максимальной практичности в организации хранения данных — никакой комиссии в транзакциях напрямую не указывается, а рассчитывается она как разница между суммой всех «входов» и «выходов», включая «сдачу», которая оказывается меньше как раз на величину комиссии.

Глава о транзакциях и балансах завершает первый раздел книги, содержащий описание общих принципов подавляющего большинства проектов на базе технологии блокчейн. Следующий раздел посвящен наиболее популярным сегодня практическим реализациям на базе технологии распределенного реестра.

Часть II
ПРАКТИЧЕСКИЕ РЕАЛИЗАЦИИ

Предыстория проекта Биткоин

Описание любого масштабного явления обычно начинается с истории его возникновения и переходит к последующему развитию. Но прежде чем приступать к рассказу об истории технологии блокчейн, нам нужно было ознакомиться с рядом научных и технологических

разделов. В противном случае у неискушенного читателя неизбежно возникли бы сложности с пониманием того, что же именно было изобретено и почему эта технологическая новинка имеет такое значение.

За последние несколько десятков лет было отмечено изрядное количество попыток придумать технологически защищенные цифровые деньги. Каждый возникший в этой сфере проект был основан на одной или нескольких технологиях, составивших впоследствии неотъемлемую часть концепции блокчейн. Однако ни один из них до момента появления сети Биткоин не смог объединить в себе все необходимые составляющие, чтобы получить законченное, защищенное, да и, в конце концов, просто элегантное решение задачи создания децентрализованного цифрового платежного средства. Теперь обратимся к непосредственной истории развития ранних решений для электронных денег.

В 1976 году, еще в доинтернетовскую эпоху, известный австрийский экономист Фридрих Август фон Хайек представил свою книгу под названием «Частные деньги». В ней содержались серьезные рассуждения относительно возможного устранения государственной монополии в управлении денежными эмиссиями, в том числе и предложения по созданию конкурентных финансовых систем. Фон Хайек писал также о возможных негативных последствиях злоупотребления общественным доверием со стороны национальных правительств. Эти предупреждения впоследствии во многом воплотились в реальности, когда финансовый мир начал содрогаться от системных кризисов, порождаемых безответственной политикой крупных банков и финансовых регуляторов ряда государств. Идеи фон Хайека нашли отклик у некоторых криптографов-энтузиастов, которые начали серьезно размышлять над проектированием независимых электронных денежных систем. Их интересовала в первую очередь возможность децентрализовать, а заодно и анонимизировать денежное обращение, избавив его от посредников, находящихся в большинстве случаев под жестким государственным контролем.

В 1982 году американский криптограф Дэвид Чаум опубликовал работу под названием «Слепые подписи и неотслеживаемые платежи», которая стала продолжением его исследований в области зашифрованных коммуникаций. Концепцию слепой подписи мы рассматривали ранее, поэтому читатель уже должен иметь представление о принципах ее работы. Именно на базе этой формы ЭЦП Чаум впоследствии создал первую систему обращения электронных денег, которую назвал eCash. Данный проект использовал технологию «слепой цифровой подписи» для авторизации и проверки цифровых банкнот, которыми обменивались контрагенты. При этом сам авторизатор играл роль банка — централизованного сервиса, основной функцией которого являлось обеспечение защиты системы от угрозы повторного расходования цифровых денег. Вместе с тем подобная централизация могла привести к возможной фальсификации клиентских балансов, если бы у владельцев системы возникло такое желание. Тем не менее это был первый проект, в котором были применены алгоритмы асимметричной криптографии для создания электронной платежной системы.

Для обеспечения функционирования проекта eCash в 1990 году в Нидерландах была зарегистрирована компания DigiCash, которая в период 1990–1995 годов сотрудничала с банками и крупными платежными системами, в том числе и такими, как VISA. Даже компания Microsoft не осталась в стороне и пыталась интегрировать данный проект в свою на тот момент новейшую и во многом революционную операционную систему Windows 95. Считалось, что наличие интереса со стороны столь серьезных партнеров гарантирует компании DigiCash отличные перспективы развития. Однако просчеты Чаума в стратегии ведения бизнеса привели в 1998 году компанию к банкротству, после чего ее активы были проданы, а сам проект закрыт.

Практически в то же время компьютерный инженер и выпускник Вашингтонского университета Вэй Дай представил документ с описанием проекта B-money, который автор определил как распределенную и анонимную электронную денежную систему. В этом проекте нашла свое отражение концепция транзакционной передачи цифровой наличности между владельцами ключей асимметричной криптографии — примерно по тому же принципу, как это было описано в главе, посвященной транзакциям и балансам в блокчейн. То есть транзакция в B-money формировалась через передачу цифровых активов на публичный ключ получателя, играющего роль адреса или счета, и закреплялась электронной подписью отправителя, сформированной при помощи его закрытого ключа. Как и в блокчейн, предполагалось, что и отправитель, и получатель всегда контролируют свои закрытые ключи и, таким образом, могут передавать цифровые деньги друг другу, одновременно математически доказывая свое право владения ими. К сожалению, концепция B-money так и не была реализована как проект, оставшись в истории лишь в виде описания, оказав, однако, довольно существенное влияние на дальнейшую эволюцию цифровых платежных систем.

В целом 1998 год был богат на важные события в мировой финансовой индустрии. Глобальный финансовый кризис, зародившись в Азии, прошелся, как ураган, по всему миру, нанеся существенный ущерб экономикам некоторых развивающихся стран. Это заставило многих задуматься о том, что существующая мировая финансовая система, имеющая в большой степени централизованную природу, достаточно уязвима перед лицом экономических кризисов. Причины же, их порождающие, обусловлены либо чрезмерной государственной «зарегулированностью» национальных экономик, либо же банальной некомпетентностью руководителей крупнейших финансовых институтов. Причем как коммерческих, так и имеющих статус государственных структур, включая в том числе центральные

банки. Возможно, именно тогда начали зарождаться идеи децентрализованного денежного обращения, позволяющего избежать исключительной зависимости от конъюнктурных решений конкретных персоналий, волею судеб держащих в руках политическую и экономическую власть в своих государствах. Как следствие, каждый новый появлявшийся проект, связанный с децентрализацией платежных процессов, впитывал в себя все эффективные методы, разработанные в этом секторе индустрии ранее, приближая, таким образом, создание решения, которое бы совершило настоящую революцию в системе денежных отношений.

Не исключением стал и проект Bit Gold, разработанный в том же году (хотя и публично представленный лишь в 2005) американским ученым венгерского происхождения Ником Сабо, специалистом в области криптографии, информатики и права. Созданная им система, помимо асимметричной криптографии, включала интересный элемент, который впоследствии сыграет важнейшую роль в технологии блокчейн, а именно — необходимость для пользователей системы решать сложные вычислительные задачи с целью формирования эмиссии электронных денег. Задача сводилась к поиску хешей специально заданного вида, где конечным результатом было нахождение строки данных, начинающейся с определенного количества бит с нулевым значением. Поскольку функция хеширования выдает алгоритмически зависимый, но заранее визуально непредсказуемый результат, необходимо перебрать достаточно большое количество различных исходных прообразов, чтобы в конечном итоге совершенно случайно получить такой хеш, вид которого будет удовлетворять условию задачи. В данном случае он должен содержать необходимое количество нулевых символов в начале строки данных.

Этот прием для формирования сложновычислимой задачи Ник Сабо позаимствовал у автора проекта Hashcash Адама Бэка, который еще в 1997 году задействовал похожий алгоритм в системе противодействия массовым рассылкам электронной почты. В проекте Бэка тоже было необходимо при отсылке каждого письма вычислять хеш, где первые 20 бит результата должны были являться нулями. Сама по себе задача, с вычислительной точки зрения, была несложной и подразумевала перебор максимум 220 вариантов (то есть примерно около 1 млн), на что обычному компьютеру требовалось всего несколько секунд. Однако подобную задачу необходимо было решать для каждого отсылаемого письма, и в случае, если количество адресатов в списке почтовой рассылки было значительным, то объем времени, затрачиваемый на расчеты, пропорционально увеличивался. Результат вычислений добавлялся к служебной информации, сопровождающей каждое электронное письмо, после он чего мог быть легко проверен компьютером получателя на «валидность» в части необходимого количества начальных нулей. Так спам-фильтрам было гораздо проще классифицировать полученное почтовое сообщение.

Следует отметить, что слово Gold в названии проекта Сабо было выбрано неслучайно — автор хотел сопоставить понятие сложновычислимых цифровых денег с золотом, которое трудно найти, добыть или подделать. Слиток золота или сделанное из него украшение можно получить только приложением серьезных усилий — сначала трудом геологов и шахтеров, затем литейщиков и, наконец, ювелиров. Ценность золота определяется комбинацией его редкоземельности, уникальных химических свойств и затраченного на его добычу и обработку труда. Далеко не последним фактором в составе ценности также является баланс спроса и предложения этого металла на мировом рынке. Но все же основную роль играет тот факт, что золото в руках владельца доказывает, что для его получения была проделана сложная работа.

В 1999 году в статье за авторством криптографов Маркуса Якобсона и Ари Джуелса впервые было введено понятие Proof-of-Work, или «доказательство работы». Данный термин относился к решению криптографической задачи нахождения секретного изначального прообраза, хеш которого удовлетворял бы по сложности определенным требованиям. При этом любой другой участник сети, получив данный рассчитанный прообраз, мог бы легко проверить его валидность, пропустив через процедуру хеширования. Это позволяло получить однозначное доказательство того, что сложная вычислительная работа действительно была проведена узлом, который претендует на признание за ним этого факта.

Ник Сабо в своем проекте Bit Gold, используя большинство ранее разработанных методик, действительно очень близко подошел к решению задачи создания защищенных цифровых денег. Однако в его системе существовала уязвимость, которую называют «Атакой Сибиллы» — когда в условиях нахождения в распределенной сети какой-то конкретный узел может попасть в окружение ряда других узлов, контролируемых злоумышленниками. Тогда атакуемый узел может стать жертвой, которая получает исключительно ложную информацию о сетевых транзакциях, а ее собственные транзакции, отправляемые в сеть, могут быть модифицированы атакующими узлами. Помимо этого, существовали и другие проблемы, которые в конечном итоге не позволили Сабо реализовать свой проект на практике. Например, ему так и не удалось решить проблему инфляции цифровых денег, которая неизбежно бы возникала при постепенном увеличении вычислительной мощности узлов, входящих в сеть.

Тем не менее труды создателей вышеописанных систем не пропали даром. Спустя непродолжительное время эти принципы найдут отражение в документе, который был представлен миру автором, имя которого тогда было неизвестно никому, а сейчас известно очень многим. Речь идет о человеке, тайна существования которого не разгадана и по сей день — о загадочном создателе технологии блокчейн

и, собственно, Биткоина как первого проекта, на ней построенного. Имя этого создателя — Сатоши Накамото, который 31 октября 2008 года представил криптографическому сообществу статью, описывающую принципы его революционного проекта, получившего спустя некоторое время мировую известность. Кто же такой этот Сатоши Накамото и в чем состояли главные отличия его проекта распределенных цифровых денег от подобных, ранее предложенных другими специалистами в области асимметричной криптографии?

Кто придумал Биткоин

По мере того как проект Биткоин начал получать широкую известность, многие задались вопросом: кто такой Сатоши Накамото? Существует ли в реальности человек с таким именем или же мы имеем дело лишь с экзотическим псевдонимом? Если попытаться написать имя «Сатоши Накамото» на японском языке, то придется задействовать три иероглифа. «Сатоши» означает «находчивый», «мудрый», «ясное мышление», часть фамилии «Нака» — это «взаимосвязи», а «Мото» — это «основа» или «происхождение». Поскольку реальный Накамото не оставил ни одного технического описания на японском языке, а все коммуникации вел на безупречном английском, был сделан однозначный вывод, что таинственный изобретатель является уроженцем англоязычной среды.

В какой-то момент дотошные журналисты сумели обнаружить проживающего в США человека с именем Сатоши Накамото, однако тот упорно отрицал свою причастность к созданию Биткоина. Впрочем, никто особо на этом и не настаивал. Дело в том, что найденный кандидат довольно неоднозначно соотносился с образом человека, который действительно мог бы создать подобный проект. К тому же он должен был быть обладателем значительного криптовалютного запаса, делающего его миллиардером и одним из самых богатых людей в мире. Носителем имени оказался пожилой американец японского происхождения, проживающий в городе Темпл-Сити, штат Калифорния.

Выпускник физического факультета Калифорнийского Политехнического Университета и увлекающийся железнодорожными моделями Дориан Сатоши Накамото однозначно обладает серьезными математическими способностями и даже владеет навыками программирования. Тем не менее сам он утверждает, что имеет достаточно слабое понятие о криптографии, а о самом проекте Биткоин узнал от журналистов лишь в тот самый день, когда они возникли на пороге его дома. Что, впрочем, не помешало ему тут же на всякий случай вызвать полицию. Кроме того, он заявил, что длительное время оставался безработным, перебиваясь случайными заработками, отчего его доходы сильно упали. Финансовые проблемы были столь серьезны, что, по его словам, он даже был вынужден отказаться от подключения к сети интернет у себя дома. В конечном итоге Накамото попросил «уважать право на личную жизнь и оставить его в покое», а на нескольких чрезмерно назойливых журналистов даже пытался подавать в суд. Но в то же время он выразил благодарность представителям криптосообщества — за моральную и даже материальную поддержку, которая ему была в определенной степени оказана. В итоге многие сделали вывод, что либо господин Накамото весьма искусно притворяется непричастным, либо он действительно говорит правду, и тогда придется затратить немалые усилия для поиска настоящего создателя Биткоина. Или «создателей» — если это не один человек, а целая группа людей, что также вполне вероятно.

Если предположить, что мы имеем дело с псевдонимом конкретного человека, то одним из лучших кандидатов на роль таинственного создателя технологии блокчейн был бы сам Ник Сабо, автор BitGold. Как известно, принципы построения обоих проектов были довольно схожи, причем Сабо остановился чуть ли не в одном шаге от успеха, который продемонстрировал Биткоин. Вместе с тем довольно подозрительным считался тот факт, что Сатоши Накамото в своем описании проекта Биткоин, цитируя многих предшественников по созданию цифровых денег, ни разу не упомянул Ника Сабо, хотя именно его проект был наиболее близок к творению Сатоши. Что же касается самого Ника Сабо, то он сразу решительно открестился от авторства и не предпринимал в дальнейшем никаких шагов для того, чтобы изменить существующее положение дел в этом вопросе. Вместе с тем Сабо выразил удовлетворение, что его исследования в области криптографии и цифровых денег получили столь успешное развитие в своем практическом применении. Правда, когда проект Биткоин только появился, Сабо его «как бы» не заметил и никоим образом не прокомментировал, хотя создание децентрализованных цифровых денег, было, без преувеличения, делом всей его жизни. Справедливости ради следует также отметить, что Ник Сабо действительно внес весомый вклад в создание технологии блокчейн, а также ввел в обиход понятие «умных контрактов», нашедших свое применение сперва в системе Ethereum (Эфириум), а затем и в других блокчейн-платформах.

Возвращаясь к вопросу поиска кандидатов на авторство Биткоина, надо сказать, что не все подозреваемые журналистами или представителями криптосообщества кандидаты отрицали эти предположения. В частности, в 2016 году австралийский ученый, программист и предприниматель Крейг Стивен Райт заявил, что именно он является автором проекта Биткоин. Однако он так и не смог предоставить убедительные доказательства своего авторства — когда его попросили сформировать цифровую электронную подпись на базе закрытого ключа, который использовался для подписи первых транзакций Биткоин (несомненно принадлежащих Сатоши Накамото), Райт это сделать отказался. За что ожидаемо был подвергнут общественному порицанию со стороны блокчейн-сообщества, которое обвинило его в банальном подлоге и обмане. Добавим также, что незадолго до декларации Райта об авторстве его дом в Сиднее

посетила полиция, поскольку в отношении него имелись подозрения в отмывании денег. После чего, по всей видимости, он решил привлечь к себе внимание подобным, хотя и весьма сомнительным образом. Еще одним фактором является мнение ряда специалистов о том, что знакомство Райта с технической стороной проекта Биткоин является довольно поверхностным, что также играет не в пользу признания его авторства.

Если начать изучать статьи, посвященные поиску создателя Биткоина, поневоле удивляешься — кого только не подозревали в авторстве этого проекта. Очень многие известные люди в IT-индустрии удостоились подобных предположений. Назывались имена и Билла Гейтса, основателя Microsoft, и Стивена Джобса, основателя Apple, и даже Илона Маска, одного из сооснователей компаний PayPal, Tesla и Space X. Все они, разумеется, довольно быстро отклонили любые формы своей причастности к созданию Биткоина. Среди авторитетных представителей криптосообщества предполагаемыми авторами Биткоина в разное время считали Гэвина Андерсена, основателя Bitcoin Foundation (некоммерческой организации, занимающейся стандартизацией, защитой и поощрением использования Биткоин во всем мире), а также Чарли Ли — автора проекта Litecoin, созданного как альтернатива Биткоину, с использованием его кода как базовой основы.

На самом деле список потенциальных кандидатов на роль создателя Биткоина настолько велик, что мы не будем его приводить целиком и рассматривать каждую персоналию в отдельности. Что же касается конкретно Гэвина Андерсена, то он состоял в переписке с настоящим Сатоши Накамото около двух лет, до момента неожиданного исчезновения последнего из всех видов коммуникаций весной 2011 года. Как заявил сам Накамото, «он удаляется, чтобы заняться более важными делами». В процессе их общения Андерсен полагал, что имеет дело с талантливым человеком японского происхождения, хорошо говорящим по-английски. Впрочем, получив от Накамото программное обеспечение клиента сети Биткоин, Андерсену с коллегами пришлось переписать около 70% кода, поскольку они посчитали его довольно «неряшливым». Кстати, именно этот фактор заставил их полагать, что Накамото создал Биткоин, скорее всего, в одиночку, в противном случае код не содержал бы столько ошибок и был бы более «читаемым». Впоследствии Андерсен какое-то время считал именно Крейга Райта тем человеком, с которым он общался как с автором Биткоина, но затем признал свою ошибку, и вопрос об авторстве вновь стал актуальным.

Наконец, поиском реального создателя занялась серьезная организация — Агентство Национальной Безопасности США. Специалисты этого ведомства провели лингвистический анализ всех текстов Накамото, которые тот помещал на различных форумах, посвященных тематике криптографии и создания цифровых платежных средств. В процессе анализа был использован метод так называемой «стилометрии», позволяющий исследовать стилистику написания текстов на основе статистического анализа повторений различных слов. Данный метод также называется «авторским инвариантом», отражающим некую количественную характеристику литературных текстов. Тексты Накамото сравнили с текстами других авторов, причем количество этих образцов исчислялось чуть ли не триллионами. В результате был получен уникальный «цифровой отпечаток» текстов Накамото, однозначно идентифицирующий его авторство. Обладая доступом к огромному хранилищу электронных сообщений, логов чатов и в целом архивов трафика центров обработки и хранения данных таких корпораций, как Google, Amazon и Facebook, специалисты АНБ получили возможность сравнить «отпечаток» Накамото с данными, принадлежащим не менее чем миллиарду человек. Известно, что на обработку данных ушло около месяца, и, по слухам, был получен положительный результат поисков, который АНБ тем не менее продолжает сохранять в секрете.

Почему же этот таинственный Сатоши Накамото решил сохранить инкогнито? На этот вопрос нет однозначного ответа, и мы можем лишь строить предположения о причинах, побудивших его к этому. Сделал он это лишь из природной скромности или руководствовался соображениями личной безопасности, понимая, что его изобретение может вызвать революцию в мире бизнеса и социальных взаимоотношений? Предполагал ли он, что правительства многих государств будут озабочены возникшей проблематикой децентрализации денежных эмиссий, анонимизации финансовых потоков и, как следствие, возможной утратой контроля над ними? В любом случае Сатоши Накамото исчез и никогда более не проявлял себя ни в интернете, ни в каких-либо СМИ. В последнем сообщении в ответ на предложение Андерсена принять приглашение от ЦРУ на встречу для разговора Накамото написал буквально следующее:

«Я надеюсь, что, поговорив с ними напрямую, мне удастся ответить на все их вопросы и развеять их сомнения. Я хочу попробовать убедить их в том, что Биткоин — это всего лишь более эффективное и не зависящее от действий политиков платежное средство. А не всемогущий, как они полагают, инструмент черного рынка, который будут использовать анархисты для борьбы с Системой».

Те, кому посчастливилось напрямую пообщаться с Накамото через интернет, отмечали его высокую образованность, а также серьезную квалификацию как специалиста в криптографии и программировании. Помимо этого, явно бросались в глаза либертарианские взгляды Накамото, а также его настороженность по отношению к правительствам государств, налогам, банкам и персонам, с ними связанным. Возможно, сохраняя свое настоящее имя в тайне, Накамото надеялся таким образом защитить Биткоин от вмешательства государства, результатом которого могло явиться то, что проект в конечном итоге так и не увидел бы свет. Сам Накамото упоминал, что работа по

созданию концепта Биткоин заняла у него не менее семи лет и он был убежден, что наконец решил задачу, которая оказалась не по силам его предшественникам. В любом случае настало время нам рассмотреть в деталях — что же из себя представляет проект Биткоин и каково его технологическое устройство?

Как устроен Биткоин

Следует признать, что при описании в предыдущих главах различных методик, подходов и технологий, применяемых для построения проектов на блокчейн, в качестве основы использовались принципы именно проекта Биткоин. Безусловно, спустя десять лет с момента своего появления Биткоин выглядит уже в какой-то степени архаичным по сравнению с более современными блокчейн-проектами. Однако именно Биткоин заложил основы для последующей эволюции технологии блокчейн. Мы не будем детально повторять технологические описания основных методов, использующихся в сети Биткоин, поскольку мы их уже рассмотрели ранее. Но вместе с тем Биткоин содержит и ряд дополнительных особенностей, которые не были предварительно описаны. И сейчас мы остановимся на них подробнее.

Для начала попробуем разобраться, каким образом в сети Биткоин формируется система адресации. Для того чтобы получить адрес в сети Биткоин, необходимо в первую очередь сгенерировать пару ключей, используя один из алгоритмов асимметричной криптографии. Биткоин, как и большинство других блокчейн-проектов, использует алгоритм дискретного логарифмирования в группе точек эллиптической кривой (ECDSA). Как известно, эллиптическая кривая описывается следующим уравнением:

$$y^2 = x^3 + ax + b$$

Биткоин использует форму данного уравнения в виде y2 = x3 + 7. Явное упрощение не должно вводить читателя в заблуждение — указанных коэффициентов вполне достаточно для того, чтобы создать значительную вычислительную сложность в части решения обратной задачи восстановления секретного ключа из публичного. Вообще данные для параметров эллиптических кривых взяты из рекомендаций консорциума SECG, который разработал «Стандарты для эффективной криптографии», использующиеся в том числе и в проекте Биткоин. Параметры рассчитаны таким образом, чтобы придать системе наименьшую уязвимость при попытке атаковать шифры, созданные на базе асимметричных криптографических методов. На текущий момент неизвестно ни об одной успешной попытке взлома алгоритма эллиптической криптографии, использующегося с параметрами, рекомендованными SECG. Возможно, эти задачи будут успешно решать квантовые компьютеры, но для этого им необходимо обзавестись достаточным количеством кубитов, а на это потребуется время, возможно, даже весьма значительное.

Вернемся к генерации ключей. Сначала случайным образом создается 256-битный закрытый ключ, а затем из него математически вычисляется публичный ключ точно такого же размера. Однако публичный ключ — это еще не совсем адрес Биткоин. Для того чтобы он стал адресом, с ним необходимо провести определенные процедуры. Сначала открытый ключ последовательно пропускают через два различных алгоритма хеширования (SHA-256 и MD5). В последнем случае его адрес укорачивается с 256 бит до 160. Затем к полученному результату в начало добавляют один байт идентификатора сети (основная сеть или тестовая), а в конец — четыре байта контрольной суммы адреса, которая также представляет собой часть хеша последнего результата. Контрольная сумма необходима для проверки, если ввод адреса осуществляется вручную: в случае ошибочного ввода система выдаст предупреждение. Транзакции в блокчейн являются безотзывными, поэтому отправитель криптосредств не имеет права на ошибку. Если адрес будет введен некорректно, средства отправителя уйдут «в никуда». А точнее — на адрес, от которого ни у кого из потенциальных пользователей сети не будет «отмычки» в виде секретного ключа. В результате никто не сможет предъявить права на эти средства, которые, таким образом, будут безвозвратно потеряны для системы.

Завершающий шаг в процедуре получения адреса Биткоин — его преобразование в более «читаемый» вид. Для этого блок данных в формате шестнадцатеричного кода (использующего цифры от 0 до 9 и буквы от A до F) преобразуется алгоритмом Base58 в строку, содержащую цифры, а также маленькие и большие латинские буквы. Данная процедура необходима, чтобы исключить из адреса символы, которые могут двояко трактоваться при ручном наборе: например, латинская маленькая l и большая латинская I или большая буква O и цифра 0. Все эти меры направлены на дополнительную защиту от ошибочного ввода адреса при совершении транзакций. По завершении всех необходимых процедур Биткоин-адрес может приобрести, например, следующий вид:

```
1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa
```

Теперь у пользователя есть свой адрес в сети Биткоин, хотя сама сеть об этом пока еще ничего не знает, поскольку пользователь осуществлял генерацию адреса на своем локальном устройстве. Но имея пару ключей и сформированный из них адрес, пользователь

может получать на него криптосредства, а затем отправлять их на любой другой адрес, который пожелает. И тогда с первой транзакцией, по мере ее распространения по сети, об этом адресе начнут узнавать как о новом участнике системы. Возникает вопрос: куда именно попадет транзакция? Логично было бы предположить, что она должна быть включена в блок, который в данный момент формируется сетью. Однако это не совсем так — сначала транзакция рассылается по всей сети через прямые соединения между различными узлами. При этом каждый из узлов, получив новую транзакцию, осуществляет ее проверку на «валидность». Узлы проверяют, располагает ли в действительности отправитель той суммой, которую он желает переслать. Осуществить такую проверку возможно, вычисляя все «непотраченные выходы» по предыдущим транзакциям в пользу данного отправителя. Также математически проверяется соответствие цифровой электронной подписи отправителя указанному им своему открытому ключу. Это нужно для того, чтобы удостовериться, что отправитель транзакции обладает закрытым ключом от адреса, с которого он собирается потратить деньги. Если транзакция успешно прошла все необходимые проверки, то она попадает во временное хранилище, которое называется «мемпул» (mempool).

Мемпул — это что-то вроде очереди транзакций, ожидающих, пока их включат в блок. Каждый узел самостоятельно определяет размер мемпула, который он будет у себя хранить. Разница между обычной очередью и мемпулом состоит в различной форме приоритизации поступающих на обработку транзакций. Если в обычной очереди данные обрабатываются в зависимости от времени их поступления, то в мемпуле их ранжируют по величине комиссии, которую отправители определили для своих транзакций. Как уже упоминалось, величина транзакционной комиссии устанавливается отправителем самостоятельно, исходя из его пожеланий в отношении скорости включения данной транзакции в ближайшие создаваемые блоки. Поскольку создатель блока забирает всю комиссию по всем включенным в него транзакциям в свою пользу, логично было бы предположить, что он будет в первую очередь включать в блок транзакции с наибольшей комиссией.

Если учесть тот факт, что размер блока в сети Биткоин ограничен одним мегабайтом, а средний размер транзакции составляет около 300 байт, то в один блок можно поместить около 4000 транзакций, что само по себе достаточно немного. Сеть Биткоин настроена таким образом, что каждый новый блок создается примерно один раз в десять минут, поэтому пропускная способность всей сети составляет около семи транзакций в секунду. В периоды повышенной нагрузки на сеть, когда количество транзакций может существенно возрасти, мемпул начинает сильно увеличиваться в своих размерах, в то время как скорость включения транзакций в блоки уменьшается. Поэтому, чтобы транзакция попала в новый блок как можно быстрее, отправители начинают увеличивать комиссию. В декабре 2017 года был отмечен рекордный размер мемпула — около 140 мегабайт, при этом количество транзакций, ожидающих обработки, превысило 200 000. Однако уже спустя полгода напряжение в сети Биткоин существенно снизилось, величина мемпула упала до единиц мегабайт, а комиссия за обработку транзакций вернулась к обычным значениям.

Как уже отмечалось, каждый участник сети, являясь равнозначным по правам с остальными участниками узлов, получает на свое локальное устройство (как правило, это обычный компьютер) всю информацию обо всех блоках и транзакциях сети Биткоин. Поскольку база блоков со временем растет, объем передаваемой для синхронизации информации постоянно увеличивается в размере. Очевидно, что, если узел получил информацию о созданных блоках ранее, ему уже не нужно ее обновлять, поскольку со временем она не меняется. Тем не менее он должен продолжать получать информацию о вновь создаваемых блоках, а также хранить у себя мемпул, куда постоянно поступают новые транзакции, еще не включенные в блоки.

Все эти данные имеют существенный размер: по состоянию на весну 2019 года объем базы данных Биткоин составлял около 570 000 блоков и занимал около 250 гигабайт на дисковом пространстве. Для тех, кто не желает выделять место для хранения столь приличного объема данных, имеет смысл воспользоваться возможностью получить статус «легкого клиента», когда вместо всего объема информации он скачивает себе только заголовки блоков без списка транзакций. В этом случае ему необходимо получить на свое устройство всего лишь несколько сотен мегабайт информации, что несопоставимо легче и быстрее, чем синхронизировать себе полную базу. Однако в этом случае данный «легкий» узел сети не сможет участвовать в создании новых блоков. Впрочем, этим занимаются далеко не все участники сети — весной 2019 года в сети Биткоин насчитывалось около 10 000 полных узлов, а число уникальных активно используемых адресов составляло около 640 000.

Исследуя принципы работы блокчейн в целом и сети Биткоин в частности, необходимо представлять себе механику создания новых блоков в распределенной сети. Понятно, что в конец цепочки всегда добавляется только один блок, который создается на тот момент только одним участником сети. При этом вся остальная сеть должна с этим согласиться посредством механизмов достижения консенсуса и синхронизировать у себя базу блоков вместе с новым, последним созданным блоком. Однако, как мы могли убедиться, количество полных узлов в сети исчисляется тысячами, и потенциально каждый из них может независимо от других узлов создать свой собственный блок и предложить его всей остальной сети для включения в общую цепочку блоков. Из этого факта неизбежно следует, что в течение небольшого временного интервала, исчисляемого минутами, в сети могут возникать конфликтующие между собой блоки, претендующие на включение в общую цепочку. Причем часть узлов может включить себе один блок, а часть — совершенно другой. С этого момента в

сети образуется разветвление, рассинхронизация базы блоков, иными словами — возникает проблема для всей сети в целом, которую необходимо решать.

Если мы хотим решить эту проблему, нам нужно рассмотреть процесс создания блока как такового. Чтобы создать блок, необходимо набрать из мемпула транзакций, пока хватает места в блоке, вычислить на их основе корневое значение дерева Меркла, на базе которого вместе с остальной служебной информацией будет сформирован заголовок блока. Далее следует поместить в заголовок создаваемого блока хеш заголовка предыдущего блока, чтобы продолжить непрерывность цепочки блоков, после чего новый блок готов и его можно отправить в сеть, чтобы остальные узлы включили его в свои цепочки. А теперь зададимся вопросом: а что, если достаточно большое количество узлов одновременно начнут предлагать свои блоки остальным участникам сети? Вне всякого сомнения, начнется полнейший хаос. Каналы связи будут перегружены пересылаемой для синхронизации информацией, неизбежно возникнет огромное количество различных вариантов разветвления цепочек — в общем, сеть фактически утратит целостность и, как следствие, работоспособность.

Чтобы избежать такого негативного сценария развития событий, необходимо сделать так, чтобы количество предлагаемых сети блоков для включения в цепочку было чрезвычайно малым. В идеале — чтобы в течение среднего временного интервала между созданием блоков (в сети Биткоин — около десяти минут) конкурирующие блоки в сети вообще отсутствовали. Но как этого достичь? Ответ прост: необходимо сделать процесс создания блоков настолько сложным, чтобы внутри кванта времени, выделяемого на создание нового блока, сети предлагалось минимальное количество новых блоков. В этом случае необходимым условием для их создания должно стать решение сложной вычислительной задачи — примерно такой, как описывалось в концепте «Доказательства работы», или Proof-of-Work. В сети Биткоин подобный процесс создания блока называется «майнингом», по аналогии с добычей полезных ископаемых, где необходимо затратить серьезные усилия, прежде чем можно будет извлечь драгоценный ресурс из шахты и реализовать его, получив материальную выгоду. Как же осуществляется цифровой майнинг в сети Биткоин?

Майнинг в сети Биткоин

Занимаясь интеграцией концепта Proof-of-Work в свой проект Bit Gold, который многие считают «предтечей» Биткоина, Ник Сабо столкнулся с проблемой, когда фиксированная сложность вычислительной задачи вела к потенциальной уязвимости, которая с большой вероятностью проявилась бы в будущем. Дело в том, что совокупная вычислительная мощность сети будет со временем естественным образом расти. Произойдет это по двум причинам: во-первых, вырастет общее количество узлов, а во-вторых, согласно закону Мура, усредненная вычислительная мощность отдельно взятого узла системы будет также постепенно увеличиваться. Таким образом, через какое-то время заложенная в логике проекта фиксированная сложность вычислительной задачи перестанет быть для сети проблемой. В конечном итоге сетевые узлы превратятся в «печатные станки» для электронных денег, что неизбежно спровоцирует в системе гиперинфляцию. Стоит ли сомневаться, что после этого все узлы системы будут материально демотивированы и едва ли захотят в дальнейшем участвовать в подобном проекте.

Напомним, что суть сложновычислимой задачи в проекте Bit Gold состояла в переборе хешей различных прообразов. А конечной целью было нахождение такого хеша, который бы считался для всей сети валидным — то есть в данном случае содержал определенное количество нулей в начале строки данных. Статическая сложность вычислительной задачи стала для Сабо одним из непреодолимых препятствий, которое так и не позволило BitGold увидеть свет. Однако Сатоши Накамото в своем проекте Биткоин эту задачу решил, и, как мы сейчас убедимся, достаточно элегантно.

На самом деле для данной проблемы напрашивается очевидное решение: если статическая сложность задачи является барьером для экономической стабильности системы, то необходимо сделать ее динамической. Как нам уже известно, для того, чтобы получить n нулевых бит в начале строки хеша, надо перебрать для хеширования максимум 2n прообразов. Очевидно, что чем больше число n, тем сложность задачи экспоненциально увеличивается. Накамото предложил хешировать заголовок создаваемого блока, начав с самой маленькой сложности. В этом случае нужно было получить всего восемь нулевых символов в начале строки хеша заголовка. Поскольку один символ занимает четыре бита, то необходимо было перебрать не более 232 вариантов, то есть около 4,3 млрд. А затем, по мере увеличения количества узлов в сети, которые пытаются искать валидные хеши, пропорционально поднимать сложность, увеличивая требования к количеству стартовых нулей.

Когда Накамото запустил свою сеть Биткоин в начале января 2009 года, в ней, помимо самого создателя системы, не было других участников. Поэтому первые блоки «намайнил» именно сам Накамото. Когда в сети Биткоин стали появляться другие узлы, сложность сети начала постепенно увеличиваться. Логика управления сложностью была заложена следующая: сложность сети должна быть такова, чтобы вне зависимости от количества узлов, которые ищут блоки, а также от их вычислительной мощности новый блок можно было бы найти в среднем не более и не менее чем за десять минут. Сложность пересчитывалась каждые 2016 блоков, то есть примерно один раз в две недели. Совокупное, реально затраченное время нахождения всех 2016 блоков разделялось на их количество, и полученный

результат сравнивался с десятиминутным эталоном. Если блоки находились в среднем быстрее, сложность увеличивалась — то есть поднимались требования к количеству нулей в хеше заголовка блока. Если медленнее — требования уменьшались.

Теперь следует сделать отступление, чтобы разобраться, каким образом перебираются хеши в процессе майнинга. Поскольку хешируется заголовок блока, это означает, что хешируемая информация довольно статична. А это, в свою очередь, говорит о том, что при неизменном прообразе мы будем все время получать один и тот же хеш. Что входит в противоречие с нашей целью — найти «золотой» хеш, чтобы он начинался с большого количества нулей. Давайте взглянем еще раз на структуру заголовка блока, чтобы понять: есть ли там какая-либо динамическая величина, которая будет меняться настолько быстро, чтобы у майнера была возможность хешировать миллионы, миллиарды или даже триллионы прообразов в секунду?

Порядковый номер блока — информация сугубо статичная, которая меняться не будет. Номер версии блока также представляет собой фиксированное значение. Теперь что касается времени создания блока, которое выражается в секундах, прошедших с 1 января 1970 года. Логично было бы предположить, что оно будет меняться не чаще раза в секунду, что для нашей задачи является крайне низкой динамикой. Число транзакций в блоке и вычисленное из них корневое значение дерева Меркла — информация также относительно постоянная. Однако бывают случаи, когда во время поиска валидного хеша майнеру поступают новые транзакции с более высокой комиссией, чем те, что он ранее включил в блок, — тогда блок будет иметь смысл пересобрать заново. Но данная процедура также имеет достаточно низкую динамику и проблем с необходимым разнообразием хешей не решает.

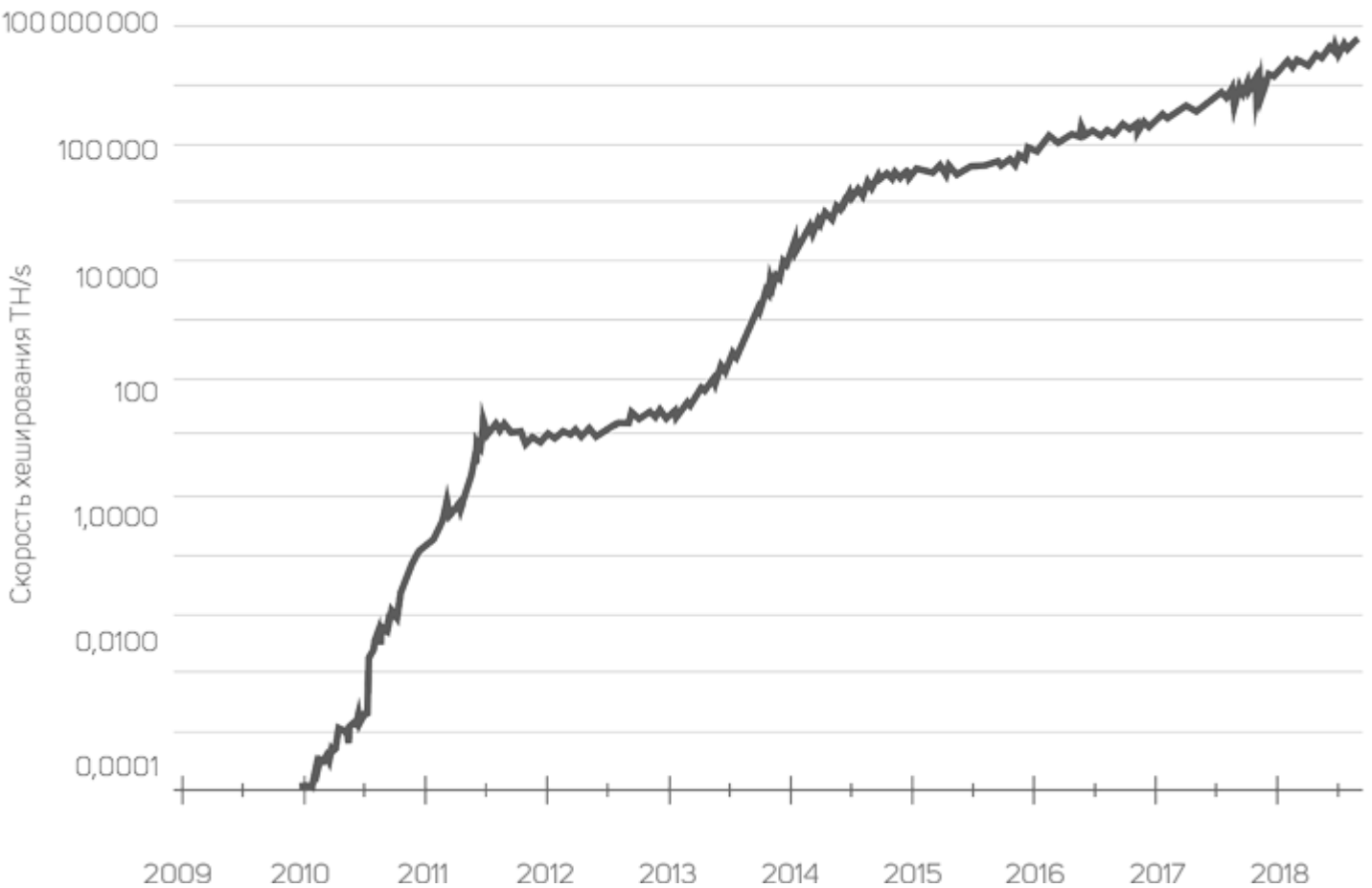
Получается, что коль скоро высокодинамичная информация в заголовке блока естественным образом отсутствует, для решения поставленной задачи необходимо вводить в процедуру майнинга некий искусственный элемент. Он не будет нести никакой полезной нагрузки, кроме как играть роль дополнительной составляющей заголовка блока, как прообраза для хеширования. И такой элемент действительно присутствует в заголовке каждого блока, и называется он «нонс» (nonce). Именно значение этого нонса майнер и будет исключительно быстро менять при переборе, открывая возможности для получения огромного количества разнообразных хешей, среди которых может оказаться и заветный «золотой» хеш с требуемым количеством нулей.

По сути, процедура майнинга и сводится к поиску подходящего значения этого самого нонса, который, будучи добавленным к заголовку блока, позволит майнеру вычислить валидный хеш, дающий ему право на создание нового блока, безусловно принимаемого всей сетью. Однако процедура поиска необходимого значения нонса достаточно сложна. В сети Биткоин используется алгоритм хеширования SHA-256, который предполагает два цикла по 64 итерации хеширования каждый. По состоянию на весну 2019 года сложность сети Биткоин требует наличия 18 первых нулевых символов для нахождения валидного хеша, соответствующим 72 нулевым битовым значениям. Что требует примерно 272 или около $5 \cdot 1021$ переборов хешей. Много это или мало? Давайте попробуем сравнить это число, скажем, с количеством песчинок на всех пляжах нашей планеты. Ученые сопоставляют количество песчинок с величиной, приближенной к 1018. Таким образом, сложность нахождения нужного нам валидного хеша с такими требованиями сопоставима с процедурой перебора всех песчинок примерно на 5000 планет, условно подобных Земле. Вот пример такого валидного хеша, с требованием по сложности в 18 начальных нулей:

```
000000000000000001621af297d27
d54b501f6a3d329399c29cf316932973ef
```

Как уже упоминалось, первые блоки сети Биткоин Сатоши Накамото находил самостоятельно и использовал для этого обычный компьютер. Как, собственно, и другие участники сети, которые стали постепенно в ней появляться. И на том самом начальном уровне сложности обычного процессора компьютера вполне хватало, чтобы находить блок за положенные в среднем десять минут. Однако по мере роста количества участников сети сложность стала автоматически пересчитываться в сторону увеличения, и в какой-то момент для обычного компьютерного процессора вычислительная задача стала «неподъемной». Тем не менее майнеры быстро нашли выход — они задействовали для поиска блоков не центральный процессор, а тот, который был установлен на их видеокартах. В силу специфики своей вычислительной архитектуры графический процессор гораздо быстрее рассчитывал хеши, чем центральный. Но через определенное время сложность возросла настолько, что и графический процессор перестал справляться с майнингом блоков. Правда, решение было найдено довольно скоро: в июне 2012 года компания Butterfly Labs начала поставлять специальное программно-аппаратное обеспечение под названием ASIC (Application-Specific Integrated Circuit, или «интегральная схема специального назначения»). Фактически это был небольшой специализированный компьютер, полностью оптимизированный только под одну задачу — перебирать хеши по алгоритму SHA-256 и делать это исключительно быстро. Началась эра сначала частного, а затем и промышленного майнинга Биткоина с использованием самых новейших аппаратных средств, производимых различными компаниями, активно конкурирующих между собой.

Для того чтобы понять, насколько увеличилась сложность сети за первые десять лет ее существования, рассмотрим понятие скорости перебора хешей, или «хешрейт» (hashrate). Различают хешрейт как отдельного устройства, так и совокупный хешрейт всей сети. Очевидно, что чем выше общий хешрейт сети Биткоин, тем выше сложность нахождения валидного хеша для создания блока. Иначе майнеры находили бы блоки слишком быстро, что противоречит логике, заложенной в блокчейн-систему. Вот как менялся хешрейт на протяжении десяти лет существования сети Биткоин (на примере логарифмического графика):



Первые устройства ASIC работали с хешрейтом 4,5 Гигахеш в секунду. То есть если бы они использовались в самом начале работы сети Биткоин на минимальной сложности, они находили бы валидный хеш примерно за одну секунду. Эта скорость была в 600 раз выше той, на которой вычислял первые блоки сам Сатоши Накамото, используя процессор своего компьютера. Устройства ASIC образца весны 2019 года, поставляемые компанией Bitmain, осуществляют перебор хешей со скоростью до 53 Терахеш в секунду. Это более чем в 10

000 раз быстрее по сравнению с первыми устройствами, представленными почти за семь лет до этого. Однако совокупный хешрейт сети Биткоин на своих пиковых показателях достигал совершенно космических значений — примерно 60 эксахешей в секунду, что составляет величину перебора всей сетью 6 · 1019 хешей за одну секунду. И тем не менее сложность задачи поиска валидного хеша такова, что даже настолько огромная совокупная вычислительная мощность всей сети позволяет майнить один блок за те же в среднем десять минут. О чем это говорит?

О том, что практически ни один конкретный индивидуум, даже обладая значительным количеством новейших высокоскоростных устройств ASIC, исчисляемых сотнями и даже тысячами, не сможет со своей майнинговой фермой самостоятельно осуществить майнинг хотя бы одного блока в сети Биткоин. Если, конечно, не допускать какую-то исключительную удачу, которая все равно не сможет проявляться на постоянной основе. Поэтому майнеры объединяются в огромные вычислительные пулы и таким образом распределяют как сложность задачи, так и вознаграждение за ее решение пропорционально между участниками пула, сообразно контрибуцированной вычислительной мощности от каждого из них. Первый такой пул открылся 18 сентября 2010 года, еще до появления устройств ASIC, когда майнинг в основном осуществлялся на процессорах и видеокартах. Впоследствии количество подобных пулов увеличилось, а затем они начали консолидироваться в более крупные объединения майнеров со всего мира.

Рассматривая майнинговые фермы, объединенные в вычислительные пулы, мы плавно подходим к основной проблеме майнинга на основе консенсуса Proof-of-Work — исключительно большому потреблению электричества при работе майнингового оборудования. Современный высокоскоростной ASIC типа Bitmain S17 Pro потребляет мощность 2250 Вт, что составляет значительную величину, особенно если учесть, что из таких устройств комплектуют целые майнинговые фермы. К тому же эти устройства в процессе работы довольно сильно нагреваются, и их необходимо постоянно охлаждать, на что также расходуется электроэнергия. Организуя свою майниговую ферму, предприниматель несет в первую очередь расходы на приобретение и доставку самого майнингового оборудования, а также на аренду и оснащение специального помещения, где будет функционировать ферма.

Но все же основной статьей расхода для «фермера» будет оплата потребленного на майнинг электричества. Именно его стоимость и является наиболее критичным параметром при расчете доходности от деятельности по майнингу различных криптовалют, в первую очередь Биткоина. Совокупное же годовое потребление электроэнергии всей сетью Биткоин сопоставимо с потреблением электроэнергии крупным государством, входящим в список первых 30 стран мира по данному параметру. Речь идет о величине в 30–35 тераватт-часов в год, что составляет примерно 0,5–0,6% всего суммарного потребления электроэнергии во всем мире. Аналитики прогнозируют, что если динамика увеличения потребления электричества сетью Биткоин сохранится на текущем уровне, то через три–четыре года Биткоин-майнеры начнут потреблять всю производимую в мире электроэнергию. Понятно, что подобный сценарий едва ли имеет шанс на реализацию — государственные регуляторы просто не позволят майнерам его осуществить.

Учитывая вышеизложенные факторы, следует признать, что будущее майнинга на базе консенсуса Proof-of-Work представляется достаточно туманным. Весьма вероятно, что правительства многих стран начнут ограничивать майнеров в потреблении ими электричества, например, через установку нормативных квот, которые им придется приобретать на специальных аукционах. Не исключено также, что в каких-то странах с особым дефицитом электроэнергии майнинг будет и вовсе законодательно запрещен. Особенно проблематичным представляется то, что все потребленное электричество уходит на решение математической задачи, ценность которой каждые десять минут полностью утрачивается. Иными словами, как только новый блок создан, решение задачи начинается сначала. Очевидно, что это исключительно неэффективное использование такого ценного ресурса, как электроэнергия — она расходуется фактически впустую, не принося человеческой цивилизации никакой существенной пользы (за исключением владельцев и сотрудников энергетических компаний).

Гораздо разумнее было бы поставить столь значительную вычислительную мощность на службу решению действительно насущных задач, например, на расчеты, связанные с поиском новых медицинских препаратов, или решения иных научных проблем, для которых требуются серьезные вычисления. Возможно, майнинг криптовалют в будущем эволюционирует в более эффективную для мирового сообщества форму, когда вычислительная работа при нахождении блоков будет направлена на решение полезных научных задач. Подобные проекты уже существуют, хотя и не завоевали пока популярности. В противном случае криптосообществу придется перейти на гораздо менее энергозатратные, чем Proof-of-Work, формы достижения консенсуса при создании блоков. И такие протоколы также активно разрабатываются и тестируются, чтобы впоследствии они могли занять доминирующую позицию в технологическом процессе создания новых блоков.

Возвращаясь к проблематике майнинга блоков в сети Биткоин, мы приходим к выводу, что это довольно дорогостоящая процедура для тех, кто инвестирует в нее свои материальные активы. Поэтому для них должна существовать прямая монетарная мотивация, чтобы они могли и дальше этим заниматься. Как упоминалось ранее, майнеры, создав блок, отчисляют в свою пользу всю комиссию от транзакций,

которые они поместили в тело созданного ими блока. Однако совокупная величина этих комиссий не так уж велика, чтобы оправдать понесенные затраты для тех, кто содержит дорогостоящие инфраструктуры для майнинга. Также до сих пор мы не заостряли внимание на достаточно важном аспекте: для того, чтобы начать осуществлять денежные транзакции в сети Биткоин, эти средства должны в сети изначально откуда-то появиться. Поэтому основным вознаграждением для тех, кому посчастливилось успешно осуществить создание блока, является так называемое «майнинговое вознаграждение». Речь идет о сумме, выраженной в цифровых монетах Биткоин, которую получает майнер в момент создания каждого нового блока. Теперь мы вплотную подошли к понятию «криптовалюта» на примере цифровых монет сети Биткоин. Что же это за монеты, как и в каком количестве они появляются в сети Биткоин и какова может быть их материальная ценность?

Биткоин как криптовалюта

Казалось бы, что может быть проще, чем процесс эмиссии электронных денег? Для этого не нужно расходовать ресурсы, подобные тем, что используются в процессе чеканки металлических монет или для печати бумажных банкнот. Если система обращения электронных денег уже создана и успешно функционирует, то задача непосредственного выпуска новых цифровых монет сводится к вводу желаемой суммы эмиссии в настройки системы субъектом, ее контролирующим. Однако при подобном централизованном управлении денежными эмиссиями нет никакой гарантии, что владельцы системы не увлекутся избыточным «печатанием» необеспеченных электронных денег, поскольку это неизбежно приведет к неконтролируемой гиперинфляции. А вместе с тем и неминуемой утрате ими какой-либо ценности как платежных средств одновременно с доверием со стороны пользователей системы.

Сатоши Накамото, создавая систему Биткоин, несомненно, был осведомлен о том, что может возникнуть проблема избыточности электронных денег, и заранее позаботился об устойчивости своей системы к подобного рода уязвимостям. В первую очередь он разработал механизм майнинга в виде сложновычислимой задачи, которая решается децентрализованно на конкурентной основе. Для того чтобы придать значимую монетарную мотивацию майнерам, было решено, что каждый вновь создаваемый блок будет привносить в систему небольшую порцию дополнительной денежной эмиссии. По мере роста стоимости цифровой монеты величина этой эмиссии должна со временем уменьшаться. Этот процесс будет происходить до тех пор, пока совокупное количество монет, выпущенных системой, не достигнет конечного, заранее заложенного при проектировании системы значения.

В качестве начального условия Накамото установил, что в момент запуска системы вознаграждение за создание блока будет составлять 50 биткоинов. А затем каждые четыре года оно будет сокращаться вдвое до тех пор, пока общее число биткоинов в системе не достигнет величины в 21 млн монет. Согласно расчетам, последний биткоин в системе будет создан около 2140 года, при этом уже к 2036 году будет получено более 99% всех монет. А после того как все монеты будут выпущены и вознаграждение за создание блока упадет до нуля, майнерам придется довольствоваться лишь транзакционной комиссией, которую они будут отчислять в свою пользу при создании новых блоков. Предполагается, что к тому моменту стоимость одного биткоина будет настолько велика, что даже отсутствие майнингового вознаграждения никак не скажется на мотивации майнеров, поскольку собираемая ими транзакционная комиссия с лихвой окупит все их издержки на майнинговые процедуры.

К середине 2018 года майнинговое вознаграждение уже дважды сокращалось от первоначально установленного Накамото значения — сначала в 2012 году до 25 биткоинов, а затем в 2016 до 12,5 монет. Следующее снижение вознаграждения ожидается в мае 2020 года, и его величина составит 6,25 биткоинов. При этом совокупная транзакционная комиссия может доходить до одного биткоина и даже более. Однако это происходит только во время повышенной нагрузки на сеть, когда транзакций становится слишком много и комиссия за их включение в блок растет. В обычное же время при отсутствии серьезной нагрузки совокупная комиссия всех транзакций в блоках составляет значительно меньшие суммы.

Ограничивая максимально возможный объем конечной эмиссии биткоинов величиной в 21 млн монет, Накамото преследовал в первую очередь цель защиты от инфляции. Создатель проекта надеялся, что стоимость биткоина в перспективе будет только расти и может в конечном итоге достичь весьма серьезных величин. Поэтому было определено, что каждый биткоин может дробиться на 100 млн частей, или, другими словами, иметь восемь знаков после запятой. Мельчайшую частичку в 0,00000001 биткоина впоследствии стали называть «сатоши» в честь создателя системы Биткоин. Очевидно, что если предел эмиссии жестко ограничен, то вместо инфляции система будет иметь дело с ее полной противоположностью — дефляцией, когда все товары и услуги, номинированные в биткоинах, будут со временем уменьшаться в абсолютных значениях своей стоимости. Но даже если когда-нибудь стоимость одного сатоши станет равна одному американскому центу, общая ценность всех монет биткоин составит около $21 трлн, что вполне позволит этой криптовалюте стать массовым платежным средством в мировом масштабе.

По сравнению с традиционными формами денег биткоин серьезно защищен от несанкционированного воспроизведения — на страже этого процесса стоят криптостойкие математические алгоритмы. Однако даже у системы Биткоин есть одна уязвимость, которую,

впрочем, чрезвычайно сложно реализовать даже в теории. Эта уязвимость называется «атакой 51%», и ее суть состоит в том, что в сети может появиться узел (или группа узлов) с исключительной вычислительной мощностью, составляющей более 50% всего совокупного хешрейта сети. Другими словами, эти узлы начинают майнить новые блоки быстрее, чем вся остальная сеть. В сети Биткоин есть правило, что в случае, если в системе образуются разветвления в цепочке блоков, сеть принимает более длинное ответвление за истинное. Таким образом, более короткое ответвление со всеми блоками, включенными в него, просто не принимается сетью и отбрасывается. Автоматически исключаются также все транзакции, которые были помещены в блоки не принятого сетью ответвления.

Подобный сценарий развития событий предполагает, что только лишь самого факта включения транзакции в один из блоков явно недостаточно. Согласно правилам, требуется определенное время, чтобы убедиться, что транзакция не попала в ветвление блоков, которое, возможно, будет отброшено в пользу какой-то более длинной альтернативной цепочки. Обычно считается, что любое из параллельных ответвлений не может быть длиннее шести блоков, то есть вероятность возникновения такой ситуации исключительно мала. Поэтому предполагается, что шести подтверждений для любой транзакции в сети Биткоина достаточно, чтобы она считалась окончательно состоявшейся. То есть если после блока, куда была помещена транзакция, в цепочку было включено еще пять блоков подряд, то это и есть те самые шесть подтверждений, необходимых для признания транзакции совершенной (один блок означает одно подтверждение). Другими словами, для полного подтверждения транзакции необходимо время, примерно равное шести десятиминутным отрезкам или одному часу. Возвращаясь к проблеме «атаки 51%», представим, что какой-то узел стал вычислительно превалировать в сети и именно его блоки стали складываться в ту цепочку, которую остальная сеть вынуждена признать истинной. Чем же это плохо для сети в целом?

Во-первых, доминирование одного узла или их группы, объединенных общей целью, может привести к тому, что этот консорциум злоумышленников может взять под контроль весь майнинг блоков и, как следствие, все новые транзакции сети. Помимо того, что они фактически монополизируют доход от вознаграждения за майнинг, они смогут включать в блоки только угодные им транзакции. И в первую очередь будут включаться транзакции, которые допускают повторное использование одних и тех же монет, то есть осуществляют «двойную трату». Единственное, что они не могут сделать — это вмешиваться в данные ранее созданных блоков, для этого даже 51% вычислительной мощности будет явно недостаточно. Дело в том, что в этом случае возникнет необходимость пересчитать все хеши блоков, начиная от изменяемого и заканчивая последним в цепочке с учетом внесенных модификаций. В результате нужно будет найти новые нонсы для всех пересобранных блоков и предложить сети новую цепочку довольно приличной глубины. В то же время вся остальная сеть продолжит обсчитывать и формировать блоки, начиная с последнего, принятого ранее всей сетью (то есть гораздо более позднего блока, нежели тот, который обсчитывают злоумышленники). Что же касается вопроса двойной траты, то это действительно может стать серьезной проблемой. Кстати, именно она в свое время не позволила создать децентрализованные цифровые деньги в «доблокчейновый» период. Для того чтобы понять, почему «атака 51%» позволит осуществлять двойную трату, рассмотрим следующий пример.

Предположим, в сети имеется узел, обладающий большей вычислительной мощностью, чем все остальные узлы вместе взятые. Данный узел выбирает какой-то из блоков в качестве «точки отсчета» и начинает осуществлять от нее майнинг новых блоков, не демонстрируя их некоторое время всей остальной сети. Одновременно с этим он будет расходовать имеющиеся у него криптосредства в основной цепочке, пока не дождется, что все они будут однозначно подтверждены сетью. То есть в основной цепочке появится еще минимум пять блоков после того, в который были помещены расходные транзакции вредоносного узла. Затем узел раскроет всей сети параллельно созданную им альтернативную цепочку — более длинную, поскольку вычислительная мощность этого узла была совокупно больше, чем у всех остальных, и сеть будет вынуждена признать данное ответвление как истинное. При этом старые блоки, ранее рассчитанные и подтвержденные всей сетью, придется отбросить, то есть придать им статус так называемых «осиротевших блоков» (orphanedblocks), утративших связь с главной цепочкой. Понятно, что вместе с ними будут автоматически отброшены и все расходные транзакции вредоносного узла, как будто их и не существовало вовсе.

Нетрудно догадаться, что альтернативные блоки, предложенные сети самим узлом-мошенником, никаких принадлежащих ему расходных транзакций содержать не будут. Таким образом, несмотря на то, что злоумышленник потратил свои средства ранее в «предыдущей реальности» и получил за них какие-то товары, услуги или даже иную криптовалюту, он через какое-то время возвращает все свои активы назад, и сеть будет вынуждена с этим соглашаться. Казалось бы, для любой блокчейн-системы, создающей блоки по принципу Proof-of-Work, это убийственная проблема. Однако на практике реализовать подобный сценарий исключительно сложно — и организационно, и монетарно, а в ряде случаев это может даже не иметь практического смысла. Попробуем объяснить, почему.

Начнем с того, что организовать подобную атаку легко лишь в теории. Представим себе, какой объем вычислительной мощности нужно задействовать, чтобы перехватить на себя более половины хешрейта какой-либо сети, особенно если это сеть Биткоин, совокупная скорость перебора хешей которой измеряется астрономическими величинами. Для оценки эффективности подобных атак для

злоумышленников необходимо оперировать понятием «стоимость атаки». Привлечение серьезных вычислительных мощностей — вообще операция крайне монетарно затратная. А если речь идет о порядках, требуемых для атаки на такую мощную сеть, как Биткоин, то здесь явным образом вырисовываются как минимум несколько практически не решаемых проблем.

Первая — это физическая невозможность задействовать для подобной операции требуемое количество компьютеров или устройств ASIC, поскольку их просто нереально консолидировать под единым управлением в таком объеме. Даже если правительство такой страны, как США, захочет провести подобную атаку с целью получения контроля над сетью Биткоин, исключительно маловероятно, что государственной институции даже такого уровня это будет под силу. Второй фактор, который необходимо принять во внимание, — это стоимость привлечения такого объема вычислительных ресурсов. С большой вероятностью она будет на порядки превышать тот экономический эффект, которого теоретически мог бы достичь злоумышленник в результате атакующих действий.

И, наконец, последний по порядку, но не по значению — это фактор утраты доверия к криптовалюте в целом после проведения успешной атаки на нее. Вне всякого сомнения, рыночная цена на нее обрушится почти до нуля, разорив при этом всех участников системы, включая самого атакующего. Очевидно, что наиболее уязвимы к подобным атакам «молодые» сети с относительно низким хешрейтом и, соответственно, с невысокой стоимостью атаки. Смысл атаки в таких случаях заключается даже не в реализации двойной траты, а скорее в нанесении ущерба сетям с целью их разрушения или как минимум блокирования их работоспособности на какое-то время. Ведь узел, получивший контроль над сетью, сам решает, какие транзакции включать в блоки, а какие нет. И он может создавать, например, одни лишь пустые блоки без транзакций, парализуя тем самым любые переводы криптовалют в пределах атакуемой сети.

В истории сети Биткоин был случай, когда 13 июня 2014 года майнинговый пул Ghash на несколько часов получил контроль над 51% вычислительной мощности всей сети. Произошло это естественным образом по причине значительного увеличения количества участников пула. Однако сразу же после того, как было зафиксировано превышение хешрейта, многие участники пула остановили свои процессы майнинга, а сам пул прекратил регистрацию и подключение новых пользователей. Это было сделано намеренно, с целью предотвращения возможных деструктивных последствий для сети в целом. Спустя некоторое время, когда суммарный хешрейт сети Биткоин существенно вырос, подобные ситуации ни для одного из подобных пулов уже возникнуть не могли.

В любом случае, как уже отмечалось, главным негативным результатом получения вычислительного контроля над сетью будет катастрофический подрыв доверия участников к системе в целом. В результате можно с большой вероятностью ожидать серьезное падение стоимости сетевой криптовалюты, выраженной в классическом денежном эквиваленте, который принято называть «фиатным». Название «фиатные деньги» относится к привычным для нас мировым валютам, эмитированным правительствами национальных государств или их консорциумами, такими, например, как Евросоюз. Фиатными деньгами мы все пользуемся ежедневно, а данный термин будем употреблять в дальнейшем как противопоставление понятию криптовалютных платежных средств.

Поскольку приобретение реальных товаров или услуг непосредственно за криптовалюты на текущий момент еще недостаточно развито, то для большинства майнеров процесс обмена заработанной криптовалюты на валюту фиатную является повседневной необходимостью. А это означает, что для всех участников сети (и в первую очередь самих активных майнеров) курс обмена криптовалюты на фиатные деньги является очень важным параметром. Понятно, что фиатный эквивалент криптовалюты отражает саму ее ценность, но каким же тогда образом можно эту ценность определить? От чего в первую очередь зависят курсы криптовалют в целом и биткоина в частности?

Биткоин как ценность

Через девять дней с момента запуска сети Биткоин, а именно 12 января 2009 года, Сатоши Накамото осуществил в ней исторически первую транзакцию. Он отправил в качестве теста десяток биткоинов другому участнику сети, который появился в ней почти сразу же после самого Накамото. Им оказался американский программист и криптоэнтузиаст Хэл Финни, который еще в 2004 году написал первый алгоритм Proof-of-Work для программного обеспечения протокола PGP, обеспечивающего функционал шифрования с открытым ключом. Транзакция была включена в блок под номером 170 и стала первой в истории физически осуществленной блокчейн-транзакцией между двумя участниками сети. Мог ли тогда предполагать Сатоши Накамото, что ради целей тестирования он расстался с цифровыми монетами, общая стоимость которых меньше чем через десять лет будет исчисляться десятками и даже сотнями тысяч долларов? На момент совершения первой транзакции биткоин никакой монетарной ценностью не обладал. Каким же образом так получилось, что вскоре за него стали выкладывать на криптовалютных биржах серьезные фиатные суммы?

Для того чтобы ответить на этот вопрос, необходимо понять, из чего складывается ценность биткоина. История обычных денег всем хорошо известна: сначала в ходу были только монеты из драгоценных металлов — золота и серебра. В этом случае они представляли ценность сами по себе. Затем человеческая цивилизация перешла на бумажные банкноты, которые сначала гарантировались золотыми запасами государственных банков, а после отмены золотого стандарта стали обеспечиваться внутренним валовым продуктом. По

крайней мере, этот факт всегда формально декларируется национальными правительствами. На самом деле реальная ситуация гораздо сложнее — экономика каждого государства постоянно сталкивается с такими явлениями, как инфляция, безработица, объем внешнего долга, а также прочими макроэкономическими факторами. Каждый из них оказывает свое влияние на ценность национальной валюты, и в том числе на колебание ее курса по отношению к валютам других стран мира.

Все национальные валюты, будучи формально обеспеченными достоянием своих государств, защищены от фальсификаций, насколько это технологически возможно. Для этого используются специальные способы изготовления бумаги для банкнот, применяется особая краска для печати, а на купюры наносят дополнительные элементы защиты — водяные знаки, порядковую нумерацию и голографические изображения. Все это, разумеется, не дает стопроцентной гарантии от возможного появления фальшивых денег, однако в подавляющем большинстве случаев проблем с доверием к бумажным банкнотам у людей не возникает. Основой доверия людей к фиатным деньгам являются следующие факторы:

- признание правительствами денежных банкнот законным платежным средством;
- обеспечение национальной валюты внутренним валовым продуктом, а также золотовалютными резервами государств;
- ограниченность денежных эмиссий с целью контроля за возможной инфляцией;
- физическая защита банкнот от подделок;
- доверие со стороны других людей, готовых принимать банкноты к оплате;
- относительно стабильный курс национальной валюты к валютам других государств.

Отсутствие хотя бы одного из вышеперечисленных факторов, как правило, существенно подрывает доверие к национальной валюте вплоть до полного отказа от ее использования в повседневных расчетах. Такую ситуацию можно было не так давно наблюдать в Зимбабве, когда исключительная гиперинфляция заставила граждан этой страны полностью перейти на расчеты в долларах США. Похожая картина сложилась также в настоящее время и в Венесуэле, где национальная валюта — боливар — подверглась масштабному обесцениванию. Это привело к тому, что для приобретения элементарных продуктов питания к оплате требовались буквально целые горы банкнот, уже давно не стоящих бумаги, на которой они были когда-то отпечатаны.

А теперь вернемся к биткоину и попытаемся примерить к нему те же самые факторы доверия, которые были перечислены в отношении фиатных денег. Коль скоро биткоины являются децентрализованными цифровыми деньгами, не имеющими единого эмиссионного центра, контролируемого каким-либо суверенным государством, о его признании официальным средством платежа пока речь не идет. Точнее, это может произойти в будущем, но каждое государство в отдельности должно будет выразить свое отношение к этому вопросу на добровольной основе. И вполне может сложиться так, что мнения разделятся: одни страны смогут признать биткоин и прочие криптовалюты средством платежа, а другие — нет.

Теперь что касается ограниченности эмиссий. Как мы знаем, эмиссия биткоина конечна в своем объеме и ограничена величиной в 21 млн монет. Таким образом, вопрос возможной инфляции отпадает, причем гарантией защиты будет не обещание какого-то правительства контролировать инфляционные процессы, а строгое соответствие заложенной математической логике проекта. То же самое касается и защиты от подделок — эмиссия биткоинов является чисто математическим процессом, базирующимся на децентрализованном решении сложновычислимых криптографических задач. Поэтому, в отличие от обычных банкнот, в данном случае имеется математически доказанная гарантия того, что «лишних» цифровых монет в системе не появится.

Одной из главных причин критики биткоина является отсутствие у него какого-либо ценностного обеспечения. Остановимся на этом чуть подробнее. Описывая концепт Proof-of-Work в одной из предыдущих глав, мы в качестве примера анализировали, на чем может базироваться ценность золота. Среди прочих аргументов отмечалось, что обладание золотом является результатом приложенного труда специалистов по его геологической разведке, шахтерской добыче, литейной обработке, грузовой транспортировке, промышленному производству из него изделий и, наконец, их продажи конечному потребителю. Очевидно, что в обычной рыночной ситуации стоимость изделия из золота — будь то слиток, монета или ювелирное украшение — не может быть меньше, чем совокупная стоимость затраченных трудовых и материальных ресурсов на его производство. Добавим также заложенную норму доходности для каждого из звеньев этой «цепочки ценности» и в итоге получим некую логически обоснованную стоимость конечного продукта, ниже уровня которой его производство не будет иметь никакого коммерческого смысла.

Теперь спроецируем эту ситуацию на процессы майнинга криптовалют, в частности — биткоина. И мы также увидим здесь цепочку формирования ценности, очень похожую на любую другую при производстве какого-либо продукта, включая в том числе и золото. Приобретение компьютеров или специализированного майнингового оборудования, аренда и оснащение помещений для криптоферм, оплата электроэнергии, необходимой для работы ASIC-майнеров, заработная плата IT-специалистов по обслуживанию фермы, налоговые платежи — вот далеко не полный перечень издержек предпринимателя-майнера. Что, в свою очередь, означает, что на каждый добытый при помощи майнинга биткоин приходится определенная сумма монетарных затрат, которая и будет нижней «граничной» планкой ценности конечного произведенного продукта — криптовалютной монеты. Когда Сатоши Накамото добывал свои первые биткоины, в силу минимальной сложности сети его издержки были близки к нулю, равно как и сама ценность биткоина на тот момент. Однако спустя годы процесс майнинга стал весьма затратным мероприятием.

Многие полагают, что биткоин (как и любая другая криптовалюта, полученная на базе механизма достижения консенсуса Proof-of-Work) обеспечен лишь электричеством, затраченным на его добычу. Можно, конечно, сказать и так, но, как мы могли убедиться, для майнинга биткоина одного только электричества недостаточно, хотя затраты на него явно превалируют над всеми остальными. Именно этот вид переменных затрат заставляет майнеров стараться, как они сами выражаются, «не падать ниже розетки», то есть фиатный эквивалент цены биткоина не должен быть меньше, чем стоимость электричества, израсходованного на его получение. А с учетом того, что рыночная стоимость электроэнергии со временем только увеличивается, равно как и растут необходимые объемы энергозатрат на добычу одной монеты, то в периоды особо значительных негативных колебаний курса биткоина на биржах майнинг может приносить и убытки.

Как ни странно, подобный сценарий развития событий был предусмотрен талантливым создателем проекта Биткоин — ведь сложностью добычи монет сеть управляет автоматически в обе стороны. И если майнерам становится невыгодно содержать свои фермы на каком-то уровне сложности, они могут отказаться от этой деятельности и отключить свое оборудование — навсегда или хотя бы на время. И тогда общий хешрейт сети начнет падать, а ее сложность — пропорционально уменьшаться, одновременно с этим понижая требования к объему потребляемого электричества на добычу одной криптомонеты. Однако на практике даже при существенной коррекции курса биткоина от ценовых максимумов в сторону значительного падения совокупная вычислительная мощность сети все равно активно увеличивается.

В течение только одного 2018 года хешрейт в сети Биткоин утроился, несмотря на то, что за этот же самый год биткоин подешевел почти вчетверо. Очевидно, что неиссякаемый оптимизм майнеров и их вера в восстановление и дальнейший рост стоимости биткоина превалируют над реалистичным анализом рыночной ситуации. Таким образом, есть все основания полагать, что подавляющее большинство майнеров склонны рассматривать периоды ценовой коррекции как события, носящие исключительно временный характер. В то время как восходящим ценовым трендам отводится роль относительно перманентного фактора.

И, наконец, один из важнейших факторов доверия к криптовалюте со стороны конкретного человека — это, собственно, его личное осознание того, насколько массовым является доверие к этому же активу со стороны других участников рынка. Именно это совокупное доверие общества также является существенным дополнением к ценности любого финансового актива, в том числе и криптовалютного. Когда в XVIII веке в Европе стали появляться бумажные деньги, доверие к ним было весьма слабым. В течение нескольких тысячелетий все торговые отношения строились на циркуляции монет, созданных из драгоценных металлов, в первую очередь — из золота. Разве что индейцы доколумбовой Америки оказались несколько в стороне от этих процессов. Они делали из золота все что угодно, кроме денег — по крайней мере, до тех пор, пока конкистадоры не «вовлекли» их в мировую финансовую систему. Что же касается бумажных ассигнаций, то эволюция доверия к ним заняла сотни лет. И это при том, что в течение длительного периода государственные банки продолжали гарантировать обмен банкнот на золото из своих резервов, практически до самой отмены золотого стандарта в 70-х годах прошлого века.

Напрашивается неизбежный вывод, что становление доверия к различным формам платежных средств — это лишь вопрос бытовой привычки, формировавшейся у людей сотнями, а то и тысячами лет. И в конечном итоге все дело оказывается только в сложившейся веками «репутации» материалов для изготовления денег, а также самих эмитентов, выпускающих их в обращение. Криптовалюты являются электронными, то есть физически неосязаемыми деньгами нового типа и поэтому для многих непривычными. Но у них, как мы убедились ранее, есть ряд серьезных преимуществ перед деньгами фиатными. А роль эмитента в данном случае принимают на себя математические алгоритмы, репутация которых строго научна и потому неоспорима.

Трудно говорить о формировании привычки и массового доверия в мировом масштабе к принципиально новой форме денег за те десять лет, которые существует технология блокчейн. Однако есть все основания полагать, что этот вид платежных средств завоюет мир гораздо быстрее, чем его исторические предшественники. Особенно если учесть, каким образом происходило становление рыночного

курса первой криптовалюты за начальные годы ее существования. В какой-то момент криптосообщество стало рассматривать биткоин не только как утилитарное средство быстрого, анонимного и недорогого платежа, но еще и как форму финансовой инвестиции. Многие инвесторы небезосновательно полагали, что подобные вложения могут принести их владельцу существенный доход за относительно короткий период времени. Насколько же сбылись их ожидания к текущему моменту?

Биткоин как инвестиция

На ранних этапах работы сети Биткоин многие майнеры, которые занимались добычей криптомонет на низких уровнях сложности, относились к этому не слишком серьезно. Скорее они видели в этом элементы игры, чем полагали себя частью финансовой системы нового типа. В результате с первыми полученными биткоинами майнеры поступали сообразно этому восприятию: делали друг другу тестовые переводы, дарили, выкидывали за ненадобностью или просто теряли вместе с секретными ключами от своих цифровых кошельков. Тем не менее уже 5 октября 2009 года биткоин получил свою первую в истории рыночную монетарную оценку, которая базировалась на реально проведенных сделках. За $1 давали 1309 биткоинов, то есть одна монета стоила около 0,08 американского цента.

Впрочем, курс довольно быстро стал расти. В связи с этим хотелось бы упомянуть об одной истории, которая произошла в конце 2009 года в Норвегии, где один местный студент по имени Кристофер Кох писал дипломную работу по криптографии. Один из разделов своей дипломной работы он решил посвятить такому относительно недавно появившемуся явлению из области криптографии, как проект Биткоин. В процессе исследования он в качестве теста приобрел 5000 монет биткоин, затратив на это сумму, примерно эквивалентную $27. Это соответствовало стоимости чуть больше половины цента за одну монету. После того, как диплом был написан и защищен, о приобретенных биткоинах Кох благополучно забыл. Однако ему пришлось вспомнить о них спустя четыре года, когда эта криптовалюта стала получать все большую известность и информация о ней стала активно распространяться по всему миру. Осознав, что является обладателем значительного количества цифровых монет, он бросился искать свои давно заброшенные виртуальные активы. Подобрать пароль от своего биткоин-кошелька бывшему студенту удалось с большим трудом, однако усилия того стоили. Выяснилось, что его полузабытая случайная инвестиция в $27 всего за несколько лет превратилась в драгоценный клад, стоивший около $1 млн. То есть за это время стоимость одного биткоина выросла в сотни раз. Благодаря своей дипломной работе Кох неожиданно стал состоятельным человеком. Потратив изрядную долю буквально упавшего на него с неба богатства на недвижимость, часть криптомонет Кох все же решил приберечь на кошельке в надежде на дальнейший рост биткоина, который и не замедлил произойти в последующие несколько лет.

Но далеко не все истории имели столь счастливый конец. Гораздо большую известность приобрел эпизод, связанный с первым в истории Биткоина приобретением физического товара за криптовалюту. Произошло это в конце мая 2010 года, когда американский программист Ласло Ханеч (Laszlo Hanyecz) бросил на биткоин-форуме клич, что готов заплатить 10 000 биткоинов, если ему доставят в город Джексонвилль, штат Флорида, две пиццы общей стоимостью примерно $25. Прошло целых четыре дня, пока контрагент по сделке не был найден, после чего пиццы были доставлены по означенному адресу, а соответствующая сумма в биткоинах была переведена в качестве оплаты. Произошло это 22 мая, и с тех пор этот весенний день стал первым и пока единственным отраслевым памятным днем для всей блокчейн-индустрии, который получил название Bitcoin Pizza Day. В этот день криптоэнтузиасты во всем мире едят пиццу и, используя отнюдь не лестные эпитеты, обсуждают провидческие таланты того незадачливого майнера, который заплатил за две пиццы эквивалент нескольких десятков миллионов долларов. Именно в сумму такого порядка те самые 10 000 биткоинов стали оцениваться через семь лет. Тем не менее нельзя сказать, что курс биткоина за первые десять лет своего существования только непрерывно увеличивался. Цена биткоина, как и любого другого финансового инструмента, была подвержена различным колебаниям и коррекциям в силу факторов самой различной природы — как технического, так и фундаментального характера.

Первая торговая площадка для обмена биткоинов на фиатную валюту появилась примерно через год после запуска проекта Биткоин — 6 февраля 2010 года начала свою работу биржа Bitcoin Market. Однако наибольшую известность в ранний период организованной торговли биткоинами завоевала другая биржевая площадка — Mt. Gox. Открылась она 17 июля 2010 года и довольно быстро снискала популярность среди биткоин-трейдеров, став, по сути, «биржей номер один» для реализации сделок с криптовалютой. Строго говоря, сайт проекта Mt. Gox был запущен еще в 2006 году для организации электронной биржевой торговли игровыми картами популярной настольной игры Magic The Gathering. Из сокращения названия игры, собственно, и взялось название биржи. Разработчик Джед Маккалеб, создавший биржу, весной 2011 года продал проект французскому программисту Марку Карпелесу, который в тот момент жил в Японии.

Как раз примерно на это время пришелся первый «бум» криптовалютной торговли, и цена биткоина начала расти. Однако уже в июне того же года биржа была атакована хакерами. В результате чего с биржевых счетов было украдено несколько десятков тысяч биткоинов, каждый из которых к тому моменту оценивался примерно в $32. Несмотря на то что «дыру» в безопасности системы удалось довольно

быстро ликвидировать, инвестиционное доверие к биткоину было серьезно подорвано. Владельцу биржи и его сотрудникам пришлось приложить немало усилий, чтобы остановить панику среди трейдеров. После чего курс биткоина медленно возобновил свой рост, постепенно «отыгрывая назад» произошедшее масштабное падение цены. Всесторонне учтя опыт прошедшей атаки, Карпелес приложил серьезные усилия для повышения безопасности работы биржи. Среди прочих мер была в том числе введена двухфакторная идентификация на базе генераторов одноразовых паролей, используемых трейдерами при входе на биржу.

Эпоха наивысшего расцвета и благоденствия Mt. Gox пришлась на последующие три года, хотя и в этот период у биржи иногда случались разного рода неприятности. В какой-то момент на деятельность торговой площадки обратили внимание финансовые регуляторы США. Результатом стало блокирование банковских счетов американского подразделения биржи, где размещалось около $4,5 млн. Средства в конечном итоге удалось вернуть, однако это не решило всех проблем с американской банковской системой в целом. Представители американской финансовой индустрии весьма скептически относились к деятельности биржи, подозревая ее в соучастии в массовом отмывании денег посредством торговли криптовалютами.

Тем не менее курс биткоина продолжал расти и к ноябрю 2013 года «пробил» отметку в $1200 за один биткоин. При этом через биржу Mt. Gox в тот период проходило около половины всех транзакций сети Биткоин. Однако в это же время работа биржи начала давать сбои, что особенно выражалось в задержках вывода средств клиентов со счетов Mt. Gox — как криптовалютных, так и фиатных. Трейдеры начали проявлять недовольство, а многие из них и вовсе ушли торговать на конкурентные биржевые площадки. В блокчейн-среде стали циркулировать упорные слухи о внутренних проблемах в Mt. Gox, пока, наконец, в феврале 2014 года не наступила трагическая развязка всей интриги. С начала февраля биржа прекратила осуществлять любые операции по выводу средств со счетов. А 23 февраля Карпелес опубликовал немногословное сообщение о полном крахе биржи, после чего сайт проекта пропал из интернета.

Среди клиентов биржи ожидаемо возникла паника. На некоторых блокчейн-форумах появилась информация в форме «утечки» внутреннего документа биржи, где говорилось о похищении хакерами 744 000 биткоинов с биржевых счетов. Еще через несколько дней, 28 февраля, руководство биржи подало официальное заявление о банкротстве. Это не замедлило максимально негативно отразиться на курсе биткоина — он рухнул до уровня в $550. Официально была признана потеря 650 000 биткоинов, хотя до конца так и не удалось выяснить, действительно ли имела место хакерская атака или же крах был инспирирован самим владельцем. Были подозрения, что Карпелес перевел огромное количество биткоинов, принадлежащих биржевым трейдерам, на некий тайный адрес в надежде впоследствии воспользоваться ими в личных целях. Несмотря на формально проявленную готовность Карпелеса всячески содействовать расследованию, весной 2019 года его приговорили к 2,5 года тюремного заключения. Пока шло следствие и судебное разбирательство, банкротные управляющие проектом сумели вернуть клиентам биржи некоторую часть средств, которые удалось обнаружить и консолидировать для последующих выплат. После краха Mt. Gox биткоину потребовалось около трех лет, чтобы восстановить ранее завоеванные ценовые позиции. При этом количество криптовалютных бирж за этот же период существенно выросло. В настоящий момент в интернете присутствуют сотни торговых площадок, активно предлагающих услуги обмена различных цифровых монет как друг на друга, так и на фиатные платежные средства.

К концу 2017 года вокруг блокчейн-индустрии сложилась ситуация, которую в криптосообществе стали называть «хайпом» — от английского слова hype, близкого по значению к понятиям «шумиха», «ажиотаж» или «навязчивая реклама». Этот период был отмечен особенно резким ростом почти всех криптовалют, и в первую очередь биткоина. Курс главной криптовалюты постоянно устанавливал ценовые рекорды, пока, наконец, перед самым Рождеством не достиг отметки, превышающей $20 000. К этому моменту про биткоин в мире не услышал только ленивый, включая и тех, кто никогда не имел отношения ни к информационным, ни к финансовым технологиям. Впрочем, начиная с января 2018 года биткоин подвергся серьезной ценовой коррекции, потеряв в течение года около 75% своей стоимости. Как результат многие инвесторы, которые имели неосторожность приобрести биткоин на ценовом пике, понесли серьезные финансовые убытки. Однако же те, кто делал инвестиции еще в первой половине 2017 года или ранее, до сих пор находятся в прибыльной зоне — настолько резко вырос курс биткоина во второй половине года. Даже в условиях сильного ценового падения вера в будущее биткоина все еще сохраняется у большинства как прямых инвесторов, так и у косвенных — майнеров. Данная категория предпринимателей продолжает наращивать уровень хешрейта в сети Биткоин исключительно высокими темпами. Это происходит несмотря на то, что майнинг в настоящий момент является практически неприбыльным, а местами даже убыточным мероприятием. И здесь необходимо понимать, от каких факторов зависит эффективность майнинга биткоина и схожих с ним криптовалют, добываемых на основе принципа доказательства работы (Proof-of-work).

Мы уже рассуждали о том, что предпринимателям, желающим заниматься этой деятельностью, приходится инвестировать значительные денежные средства в майнинговое оборудование и оснащение помещения, где оно будет установлено. Кроме того, майнеры несут расходы, связанные со значительным потреблением электроэнергии, оплатой рабочей силы системных инженеров, отчислением

налоговых платежей и так далее. Логично предположить, что далеко не любое место в мире подходит для эффективного майнинга криптовалют. Необходимо выбирать такие географические локации, где вышеперечисленные финансовые издержки можно минимизировать, насколько это удастся предпринимателю. Как оказалось, в мире не так уж много мест, где майнинг был бы настолько эффективен, чтобы издержки «майнингового фермера» не превышали доход от реализации добытых криптовалют, особенно в условиях существенной коррекции их рыночной стоимости.

На текущий момент в отрасли криптодобычи сложилась ситуация, когда около 80% майнинговых мощностей кристаллизовались в мировой промышленной «кузнице» — в Китае. Именно в этой стране естественным образом сложились условия, наиболее благоприятствующие этому виду деятельности. Если, конечно, не принимать во внимание несколько недружественную и откровенно настороженную позицию китайского правительства по отношению к криптовалютам в целом. Тем не менее основное оборудование для майнинга производится именно в Китае, поэтому местным майнерам нет необходимости заказывать дорогостоящую трансграничную доставку через полмира, а также нести дополнительные расходы на таможенные платежи. Электростанции в горных районах страны позволяют получить приемлемые расценки на электроэнергию, а относительно холодный климат в этих же регионах обеспечивает достаточно бюджетное решение проблемы перегрева оборудования. В случае, если выбрано технологическое решение в пользу водяного охлаждения, то, как правило, в этих же местах к услугам майнеров протекают холодные горные реки. Стоимость рабочей силы в периферийных районах Китая также относительно невелика, что является еще одним немаловажным фактором в пользу выбора именно этой страны для инвестиций в деятельность по майнингу криптовалют.

Считается, что подавляющая доля вычислительной мощности сети Биткоин контролируется всего четырьмя майнинговыми пулами, и все они находятся в Китае. Столь высокая концентрация совокупного хешрейта в пределах одной политической юрисдикции и под контролем всего лишь четырех управляющих субъектов, безусловно, не может являться позитивным фактором для технологии, призванной быть истинно децентрализованной. Однако криптосообщество считает эту ситуацию временной и верит в то, что майнинг в сети Биткоин со временем эволюционирует в более распределенную форму. В любом случае именно Биткоин пока остается наиболее популярным и востребованным криптоинструментом, совокупная ценность всей эмиссии которого составляет около половины капитализации всего криптовалютного рынка. Проект Биткоин был создан Сатоши Накамото как децентрализованная цифровая платежная система, а сами монеты биткоин должны были стать популярным средством платежа, которое постепенно стало бы вытеснять привычные фиатные деньги из повседневного оборота. Попробуем оценить, насколько за первое десятилетие своего существования проекту Биткоин удалось реализовать задуманное.

Биткоин как средство платежа

После того как цифровые монеты сети Биткоин получили серьезную монетарную оценку на финансовом рынке, владельцы значительного количества этих цифровых активов неожиданно для всех (а возможно, и для самих себя) стали состоятельными людьми. Криптовалютные капиталы многих из них оцениваются в сотни миллионов, а в некоторых случаях и миллиардов долларов. Разумеется, первым, на кого обратили внимание, стал сам создатель проекта Биткоин — Сатоши Накамото. Будучи первым майнером в собственноручно созданной им сети, он сумел добыть большое количество монет, поскольку начальный уровень сложности системы этому весьма благоприятствовал. Некоторое время считалось, что Накамото успел заработать около 1 млн монет, однако, по последним исследованиям, это число не превышает 700 000. Но даже в этом случае капитализация его состояния оценивается на данный момент примерно в $3,5 млрд. Так загадочный изобретатель попал в мировой рейтинг миллиардеров журнала Forbes, а в период ценовых рекордов биткоина Накамото даже занимал место в пятом десятке списка.

По этому поводу нельзя не припомнить небезызвестных братьев-близнецов Кэмерона и Тайлера Уинклвоссов. Бывшие студенты Гарварда и спортсмены-олимпийцы в свое время сумели отсудить у создателя Facebook Марка Цукерберга около $65 млн в качестве компенсации за якобы украденную у них идею социальной сети. Часть полученных средств братья удачно вложили в биткоин, когда он еще стоил чуть более $100 за монету. Предполагается, что они приобрели более 100 000 биткоинов, что делает их обладателями состояния, близкого к полумиллиарду (в зависимости, разумеется, от колебаний рыночного курса биткоина на биржах). Ходили слухи, что секретные ключи от своих биткоин-адресов предприимчивые братья распечатали на бумаге, которую затем разрезали на несколько частей и поместили каждую отдельно в банковские сейфы в разных городах США. Столь сложная операция была проведена, дабы защитить свои цифровые активы от возможного похищения сетевыми злоумышленниками.

Ну и, наконец, стоит еще раз упомянуть о бывшем владельце биржи Mt. Gox Марке Карпелесе, подозреваемом в хищении примерно 650 000 биткоинов, которые, как он сам утверждает, были украдены хакерами. Если он все же является тайным обладателем этого сокровища, то оно бы оценивалось в данный момент в сумму более $3 млрд, что сопоставимо с капиталом самого Накамото. Правда, в случае изобретателя технологии блокчейн легитимность приобретения им биткоинов не вызывает сомнений, поскольку они были получены абсолютно открыто при помощи майнинговых процессов.

Существует ряд платежных систем, построенных на базе технологии блокчейн, где присутствует значительное число активных участников, способных накапливать определенные объемы криптомонет. В связи с этим напрашивается законный вопрос: какие товары и услуги можно было бы оплачивать этими цифровыми деньгами? Ответ на самом деле очевиден: абсолютно те же, что и фиатными платежными средствами. Проблема состоит лишь в готовности продавцов принимать крипотовалюту к оплате. А для них, в свою очередь, встает вопрос легитимизации полученных доходов в криптовалюте, а также возможности конвертировать их в фиатные деньги с целью их законного бухгалтерского и налогового учета. Очевидно, что эти вопросы в каждом государстве решаются исходя из особенностей национальных финансовых законодательств, и далеко не везде для криптовалютных платежей, к великому сожалению, создан режим относительного благоприятствования. Поэтому покупка товаров и услуг за криптовалюты не получила еще по-настоящему массового распространения. Однако этот процесс медленно, но верно завоевывает различные деловые сферы, и есть надежда, что рано или поздно криптовалюты займут достойное место в мировом товарно-денежном обороте.

Время от времени в различных мировых СМИ публикуются рекламные сообщения о том, что тот или иной актив можно приобрести за биткоины или другую криптовалюту. Как правило, речь идет о предметах роскоши — дорогих виллах, яхтах, роскошных автомобилях или частных самолетах. Однако в последнее время все чаще появляется информация о том, что за цифровые деньги можно приобрести и самые обычные вещи из повседневного обихода. Но подобных точек продаж пока, увы, лишь единицы, и все они представлены интернет-магазинами с относительно небогатым товарным ассортиментом. Ведь для того чтобы этот вид оплаты стал массовым, необходимы разветвленные инфраструктуры платежных систем, которые будут обеспечивать денежные потоки с необходимыми конвертациями из одной денежной формы в другую. И такие системы уже начинают активно развивать свою деятельность в различных регионах мира, несмотря на то, что из всех стран пока только Япония признала криптовалюты официальным платежным средством.

Помимо платежных систем, существует еще один элемент, жизненно необходимый для успешного внедрения криптовалют в массовое обращение, — банкомат, выдающий наличные фиатные деньги за биткоины или иные популярные криптомонеты. Проекты по созданию и установке подобных денежных аппаратов уже существуют и активно наращивают объемы своего бизнеса по всему миру. Например, уже к началу 2019 года количество одних только биткоин-банкоматов превысило 4000, а ежедневно в мире устанавливается как минимум семь новых аппаратов. Причем не менее чем в трети из всех существующих банкоматов можно не только получить наличные деньги за биткоины, но и совершить обратную операцию по приобретению криптовалюты. Больше половины всех биткоин-банкоматов мира установлено на территории США, но и другие страны постепенно наращивают их количество, особенно отмечается позитивная динамика в Канаде и Австрии. Всего насчитывается более трех десятков производителей подобных банкоматов, а стоимость одного аппарата составляет около $10 000.

Одним из препятствий для массового распространения криптовалют является их виртуальность. Для многих людей, постоянно имеющих дело с монетами и банкнотами, неосязаемая форма денег непривычна, особенно если учесть относительную технологическую сложность их применения для оплаты товаров и услуг. Физические деньги часто становятся предметами коллекционирования, что для криптовалют едва ли могло стать возможным. Правда, в 2011 году некто Майк Кадвелл решил выпустить коллекционные биткоины в виде физических монет. Он создал дизайн металлической монеты, номинированной в биткоинах. Каждой монете соответствовал криптокошелек, содержащий количество биткоинов, равное номиналу монеты. При этом секретный ключ кошелька наносился на саму монету в виде кода и покрывался специальной голограммой, которую при необходимости можно было разрушить и получить доступ к ключу и к средствам на кошельке. Понятно, что после разрушения голограммы монета становилась фактически бесполезной, поскольку ключ переставал быть секретным для всех, кто мог видеть монету. Было выпущено несколько тысяч таких монет, почти все из которых были

раскуплены коллекционерами и криптоэнтузиастами. Впоследствии были попытки со стороны других производителей создать монеты, номинированные в биткоинах, в том числе и больших номиналов, однако широкого распространения они не получили.

Рассуждая о биткоине как о платежном средстве, объективности ради следует обратить внимание и на негативные стороны тех возможностей, которые дает криптовалюта, построенная на базе блокчейн-технологии. Речь идет об одном из самых важных ее свойств — анонимности. Именно неотслеживаемость криптовалютных платежей и технологическая невозможность связать транзакцию с непосредственным ее автором как физическим лицом привела к появлению целой криминальной индустрии, предлагающей различные незаконные товары и услуги с оплатой исключительно криптовалютами. Возникновение и существование подобного рода деятельности стало одним из главных факторов, препятствующих получению криптовалютами, и в частности биткоином, статуса официального платежного средства в большинстве государств. Но обратимся к непосредственной истории вопроса.

В 2011 году в сети интернет появился сайт под названием SilkRoad («Шелковый путь»). На этом торговом портале можно было приобрести широкий спектр нелегальных товаров и услуг — наркотики, украденные банковские карты, фальшивые деньги и даже услуги киллера. В качестве обеспечения анонимности продавцов и покупателей сайт использовал прием платежей исключительно в биткоинах. Владельцем сайта был некто Росс Ульбрихт, житель США, исповедующий экстремальные политические взгляды, отрицающие любую форму государственного вмешательства в жизнь людей. Годовой объем продаж сайта в 2012–2013 годах оценивался примерно в $12–15 млн, а суммарный объем сделок в криптовалютном эквиваленте приближался к 10 млн биткоинов. Всего услугами сайта успели воспользоваться около 100 000 покупателей и продавцов. В конечном итоге Ульбрихт был арестован и в 2015 году приговорен к пожизненному заключению, а сайт SilkRoad был закрыт. Тем не менее сам факт появления и существования подобного сервиса остался темным пятном на репутации биткоина как средства совершения анонимных платежей в интернете. Впоследствии официальные лица ряда государств и регуляторов приводили эту историю в качестве примера и объяснения, почему признание криптовалют официальным средством платежа является преждевременным, а то и вовсе недопустимым.

В защиту цифровых денег можно привести аргумент, что многие полезные предметы из привычного обихода могут использоваться не только по своему прямому назначению, но и в откровенно криминальных целях. Например, банальные кухонные ножи бесчисленное множество раз становились орудием преступлений. Однако они никогда не были законодательно запрещены к продаже и использованию для резки продуктов на кухнях всего мира. Да и самые обычные денежные купюры постоянно используются для совершения преступлений — в первую очередь имеющих коррупционный характер. Тем не менее это не стало причиной их полного изъятия из обращения в пользу иных платежных форм. Напрашивается логичный вывод, что возможное криминальное применение ряда бытовых предметов — это естественное следствие самого факта их существования. Но их запрет принес бы человеческой цивилизации больше вреда, чем имеется пользы от их наличия. Поэтому было бы справедливым и к криптовалютам применить подобный взвешенный подход. Вместо массовых запретов следовало бы бороться с возможным незаконным использованием криптовалют, привлекая для этого профессиональные государственные службы.

Завершая раздел, посвященный Биткоину, хотелось бы еще раз отметить, что этот проект стал пионером-первопроходцем в новейшей высокотехнологичной отрасли, которую представляет собой блокчейн. С момента его появления прошло почти десять лет, и вполне логично, что многие в криптовалютной индустрии считают Биткоин несколько устаревшим и не отвечающим современным требованиям проектом. Но благодаря именно таким критикам у Биткоина начали появляться конкуренты. К началу 2019 года в блокчейн-индустрии насчитывалось уже более 2000 различных криптовалют, имеющих хотя бы одну биржевую оценку. Конечно, в рамках данной книги мы не сможем рассмотреть большую часть этих проектов. Однако мы остановимся на самых значимых из числа так называемых «альткоинов», или альтернативных Биткоину криптовалютах. Каждый из этих проектов пытался создать какие-то уникальные ценностные предложения, выгодно отличающие его от своего «прародителя». И первым следует рассмотреть проект Ethereum, который иногда называют Биткоин 2.0 в силу того, что он поднял блокчейн-технологию на следующую ступень своего развития.

Введение в Ethereum

Спустя примерно пять лет с момента появления сети Биткоин — первой системы, созданной на базе технологии блокчейн, в молодой криптоиндустрии обращалось уже довольно приличное количество проектов. Большинство из них были в значительной степени «биткоиноподобными» и отличались от своего генезисного прообраза лишь в мелких «косметических» деталях. Однако и сам проект Биткоин, равно как и большинство его последующих клонов, представляли собой те же самые, обычные децентрализованные платежные системы, достаточно примитивные по своим возможностям. Тем не менее, оценив все преимущества технологии блокчейн, зарождающаяся на ее основе индустрия начала формировать запросы на более сложный функционал блокчейн-сетей. Криптосообщество осознало необходимость в получении более прогрессивных технологических средств, позволяющих начать построение децентрализованных проектов на новом качественном уровне.

И такой инструментарий действительно был предложен в конце 2013 года одним из криптоэнтузиастов, известным сообществу на тот момент как редактор журнала Bitcoin Magazine. Им был Виталик Бутерин, 19-летний канадский программист с русскими корнями, представивший описание проекта Ethereum, возможности которого привлекли к себе повышенное внимание. В Ethereum были представлены совершенно новые концепции, далеко выходящие за рамки потенциала привычных блокчейн-проектов. Более того, данный проект совершенно не позиционировался как платежная система, а фактически являлся блокчейн-платформой нового поколения. Самым главным нововведением стала система так называемых «умных контрактов», или, как их принято называть в криптоиндустрии, смарт-контрактов. Структуру и принципы работы смарт-контрактов мы рассмотрим позднее, а сейчас отметим основные свойства, отличающие проект Ethereum от Биткоина и ему подобных систем.

Начнем с формирования адресов. Как и проект Биткоин, Ethereum использует схожий алгоритм их создания, но не преобразует их в более «читаемый» вид, оставляя хеш публичного ключа практически без изменений. Это было сделано отчасти еще и потому, что Ethereum, как упоминалось выше, не задумывался изначально как платежная система. Поэтому формирование адресов с более удобной визуализацией, помогающей ручному набору, в этой системе делать не стали. Помимо различий в формировании адресации, создателями проекта было принято решение, что блоки в системе будут создаваться значительно быстрее, чем в сети Биткоин. При этом их размер будет ограничен не количеством байт, а требуемой вычислительной мощностью на обработку данных блока. Подобные меры действительно были оправданными, поскольку наличие смарт-контрактов, как мы убедимся при их более подробном изучении, фактически обязывает разработчиков вводить такого рода лимиты.

Майнинг в сети Ethereum существенно отличается от принципов, на основе которых работает Биткоин, хотя тоже использует для нахождения блоков принцип доказательства работы (Proof-of-Work). Управление сложностью вычислительной задачи, как и в Биткоин, зависит от совокупного хешрейта сети. Однако сама степень сложности значительно снижена, поэтому на создание блока Ethereum требуется гораздо меньше времени. В настоящий момент среднее время создание блока в сети Ethereum составляет около тринадцати секунд — по сравнению с десятью минутами в сети Биткоин. То есть пока в сети Биткоин создается один блок, в Ethereum их будет около пятидесяти. Это привело к тому, что база блоков и транзакций сети Ethereum уже сопоставима по размеру с базой Биткоина, и это несмотря на то, что сеть Ethereum возникла на шесть с половиной лет позже, чем проект, положивший начало блокчейн-индустрии. Для расчетов внутри сети, в том числе для оплаты транзакционных комиссий и формирования вознаграждения за майнинг, используется криптовалюта под названием «эфир» (Ether). В случае, когда сложность поиска валидного хеша при майнинге относительно невысока, блоки в сети создаются довольно быстро. А значит, и величина вознаграждения за майнинг пропорционально невелика и совершенно несопоставима по ценности с премией для создателей блоков в сети Биткоин.

Описывая принципы децентрализованного майнинга в сети Биткоин, мы рассматривали ситуацию коллизии в случае, если разные узлы находят блоки в пределах десятиминутного временного интервала. Образующиеся при этом ответвления в цепочке блоков в конечном итоге должны быть отброшены сетью в пользу более длинной цепочки. Похожий принцип используется и в сети Ethereum. Однако из-за того, что блоки в ней создаются почти в пятьдесят раз быстрее, ситуация с возникновением конкурирующих найденных блоков встречается примерно во столько же раз чаще. Поэтому сеть Ethereum почти всегда находится в состоянии, при котором у нее имеются альтернативные цепочки, угрожающие целостности сети, так что постоянно надо делать выбор в пользу более ценного для системы ответвления. В Ethereum для этого используется протокол GHOST (Greedy Heaviest Observed Sub Tree — «жадное и наиболее весомое из известных ответвлений»). Он отдает предпочтение тем ответвлениям с блоками, на добычу которых было затрачено больше вычислений.

Исходя из того, что конкурирующие блоки довольно часто создаются почти одновременно, возникает вопрос, как вознаграждать майнеров. Если поощрять только одного майнера-победителя, тогда для остальных, также нашедших блок, это станет существенной демотивацией. Поскольку майнеры-конкуренты проводят столь же сложную вычислительную работу, создатели системы решили, что будут выделять часть вознаграждения еще максимум двум параллельно найденным, но не принятым сетью блокам. Такие блоки назвали

uncles (от английского uncle — «дядя»), поскольку они являются родственными в силу общего «блока-предка». Майнеры, их создавшие, также получают определенную премию, хотя и меньшую, чем те, которые создают блок, принятый сетью как истинный, — для этого существует специальная формула распределения вознаграждения.

Сама непосредственная процедура майнинга эфиров также отличается от проекта Биткоин. В сети Ethereum используется совершенно иной алгоритм поиска валидных хешей, который разработчики назвали Ethash. Проблема исключительного расхода электроэнергии на добычу биткоинов всегда вызывала озабоченность у создателя проекта Ethereum Виталика Бутерина. Поэтому он решил бороться с чрезмерным увеличением совокупного хешрейта в своем проекте, и в первую очередь — с использованием для майнинга устройств ASIC. В связи с этим было принято решение об усложнении алгоритма перебора хешей до уровня, при котором потребовалось бы существенно больше оперативной памяти, чем алгоритму SHA-256, используемому в сети Биткоин.

Как известно, крупные майнеры получают серьезные вычислительные мощности, конструируя фермы, составленные из устройств ASIC. Наличие ферм считается негативным фактором для любой блокчейн-сети, поскольку они усиливают степень централизации майнинга. А это, в свою очередь, противоречит первоначально задуманному плану — максимально устранить любые возможные точки избыточной консолидации вычислительной мощности при управлении сетью. В одном из своих многочисленных интервью Виталик Бутерин рассказал историю о том, что он, будучи в весьма юном возрасте, проводил много времени за популярной компьютерной игрой World of Warcraft. Время от времени его виртуальный персонаж терял свои способности из-за коррекции игрового баланса, который периодически проводили разработчики компании Blizzard, не считаясь с мнением игрового сообщества. После каждого подобного изменения в правилах игры молодой человек испытывал сильное эмоциональное потрясение из-за того, что его личные усилия для развития своего персонажа практически сводились к нулю. Это происходило из-за неких централизованных решений, на которые лично он не мог никоим образом повлиять. По всей видимости, психологические травмы юности оказали значительное влияние на мировоззренческие позиции Бутерина, который пришел к выводу, что централизация управления есть абсолютное зло.

Несмотря на принятые Бутериным меры по усилению требований к объему памяти для майнинга, полностью защититься от появления ASIC-устройств для сети Ethereum, к сожалению, не получилось. Однако удалось существенно снизить хешрейт для добычи криптомонет этим видом устройств и, как следствие, повысить степень децентрализации майнинга, сделав его таким образом более конкурентным. Если сравнить два майнинговых устройства для сети Биткоин и Ethereum, то мы увидим, что майнер для добычи эфиров перебирает хеши в десятки тысяч раз медленнее, чем его биткоиновый аналог. Это происходит потому, что при майнинге эфиров алгоритм Ethash предусматривает постоянное обращение в оперативную память, где размещены дополнительные данные, необходимые для корректной работы майнинговой процедуры. Эти частые обращения замедляют работу алгоритма настолько, что разница в скорости перебора хешей составляет не менее четырех порядков.

Этот подход позволил также сохранить возможность майнинга монет эфира обычными графическими процессорами видеокарт, что серьезно повышает степень децентрализации процесса нахождения новых блоков Ethereum. В целом же вся сеть Ethereum потребляет чуть ли не втрое меньше электроэнергии, чем сеть Биткоин, хотя и эта величина продолжает оставаться весьма значительной. Поэтому разработчики проекта Ethereum по-прежнему серьезно озабочены проблемой энергоемкости своего проекта и планируют в ближайшее время коренным образом пересмотреть принципы создания блоков в сети. В настоящее время сеть Ethereum находится в процессе постепенного отказа от майнинга на основе протокола консенсуса Proof-of-Work в пользу принципа «доказательства владения» (Proof-of-Stake), которому будет посвящен отдельный рассказ.

Что же касается основной расчетной криптовалюты сети Ethereum — эфира, то в отличие от биткоинов, которые подлежат разделению на 100 млн частей, или могут принимать минимальное значение в восьмом знаке после запятой, эфир разделяется на квинтиллион частей, или на целых 18 десятичных знаков. Мельчайшая частица эфира называется Wei в честь Вэй Дая, создателя проекта B-money, одна миллионная часть эфира названа Szabo в честь Ника Сабо, изобретателя смарт-контрактов и автора проекта Bit Gold, считающегося наиболее близким к самому проекту Биткоин. И, наконец, одна тысячная часть эфира получила название Finney в честь Хэла Финни, одного из разработчиков криптографического PGP-протокола и контрагента Сатоши Накамото по самой первой сделке в сети Биткоин в январе 2009 года.

Еще одним важным отличием от биткоинов является то, что эмиссия эфиров на текущий момент никак специально не ограничена и, таким образом, может быть подвержена инфляции в будущем. Когда Виталик Бутерин представлял свой проект, он одномоментно создал и продал инвесторам около 60 млн монет эфира, выручив за них биткоины на сумму примерно $18,5 млн. Еще около 12 млн монет эфира Бутерин поместил в резервы для будущего финансирования развития проекта. Подобный единовременный выпуск монет обычно называют премайнингом.

Сама платформа была запущена 30 июля 2015 года. С тех пор за прошедшие без малого четыре года при помощи уже обычных процедур майнинга было проведено эмиссий на чуть более чем 30 млн монет. Таким образом, их общее количество превысило 100 млн с совокупной текущей капитализацией чуть менее $20 млрд. По своей популярности эфиры прочно удерживают второе место в криптовалютной индустрии после биткоинов и обращаются почти на всех биржах, предлагающих услуги по торговле криптовалютами. Если биткоин обычно называют «криптовалютным золотом», то эфиру достался титул «серебро».

Каждый день в мире совершается свыше полумиллиона транзакций в сети Ethereum. Если обратиться к принципу учета балансов монет на адресах системы, то здесь возникает еще одно важное отличие от сети Биткоин. Как известно, транзакции в блокчейн представляют собой цепочки электронных подписей, которые можно проследить по всей базе блоков. Таким образом, всегда есть возможность автоматически рассчитать баланс любого из адресов, сопоставив его входы как доход и выходы как трату. Непотраченные выходы и будут являться актуальным балансом адреса. Этот принцип называется UTXO, или «учет непотраченных транзакционных выходов», и мы уже уделяли некоторое время его рассмотрению. В сети Ethereum решили, что будет целесообразно вести базу актуальных состояний для каждого из адресов сети. Этот способ учета хотя и требует дополнительного хранения определенного объема данных, но все же несравнимо удобнее принципа UTXO, при котором нужно постоянно получать актуальные состояния адресов через расчеты.

Одновременно с этим принцип хранения актуальных состояний позволил разработчикам ввести в платформу Ethereum уникальный на момент ее появления функционал смарт-контрактов, который, собственно, и стал главным ценностным предложением проекта. Что же такое смарт-контракты и каким образом их реализация в сети Ethereum повлияла на развитие технологии блокчейн в целом?

Смарт-контракты

В процессе внедрения новых технологий разработчики систем, использующих биткоины в качестве платежного средства, постоянно сталкивались с проблемой создания более сложных моделей проведения транзакций. Особенно в тех, где могли бы присутствовать какие-то условия, отличные от стандартных. Сатоши Накамото пытался предусмотреть подобную ситуацию и, начиная с первой же версии программной реализации клиента сети Биткоин, поместил в него так называемую систему скриптов для обработки транзакций. Фактически это была упрощенная форма языка программирования стекового типа, когда все его команды обрабатываются в порядке очереди «слева направо от того, как они были указаны в самом скрипте».

Скрипт-язык Биткоина содержит около восьми десятков различных команд, каждая из которых выполняет определенную алгоритмическую операцию. От элементарной, вроде сравнения двух числовых значений, до более сложных — хеширования данных или алгоритма проверки цифровой электронной подписи. В подавляющем большинстве случаев в параметрах выхода каждой транзакции помещается стандартный скрипт под названием P2PKH, или Pay to Public Key Hash. Этот скрипт реализует процедуру оплаты на хеш публичного ключа, которым, собственно, и является биткоин-адрес получателя транзакции.

Для обработки нестандартных платежных ситуаций отправитель может составить собственный скрипт, содержащий дополнительные условия для обработки транзакции. Хотя, надо сказать, выбор у него небогатый. Например, имеется возможность реализовать функционал мультиподписи или сделать так, чтобы отправляемые средства нельзя было потратить ранее указанного в скрипте времени. Однако по-настоящему замысловатых алгоритмических конструкций для обработки транзакций с дополнительным набором условий подобными средствами создать практически невозможно. И дело не только в ограниченном наборе команд биткоин-скрипта, а в первую очередь в том, что данный язык является «неполным по Тьюрингу». Что это означает?

В 1936 году Алан Тьюринг, будущий герой криптографической войны с германским шифровальным устройством «Энигма», предложил модель вычислительной машины в форме математической абстракции. Полученную модель впоследствии стали называть «Машиной Тьюринга». Эта логическая вычислительная конструкция послужила инструментом для доказательства наличия или отсутствия алгоритмического решения для различных задач. Что же касается «полноты по Тьюрингу», то одним из ее критериев является наличие в языке программирования команд, на базе которых можно построить алгоритмические циклы. Скрипт-язык сети Биткоин не предоставляет операторов обработки циклов, а значит, и возможности реализации на нем сложных вычислительных алгоритмов весьма ограничены. В отличие от Биткоина, в проекте Ethereum подобная возможность предусмотрена, а реализована она как раз с использованием функционала смарт-контрактов. Попробуем разобраться, что же они собой представляют.

Как уже неоднократно упоминалось, автором концепции является Ник Сабо, который еще в 1994 году впервые представил форму исполняемых электронных контрактов в децентрализованной среде. Сабо определил этот вид виртуального соглашения как «протокол передачи информации, обеспечивающий автоматическое исполнение сторонами условий сделок». Преимуществами такой формы заключения контрактов автор считал конфиденциальность, низкие затраты на проведение операций и отсутствие необходимости привлечения посредников для обеспечения доверия для сторон по сделкам. Если сравнивать электронные контракты с обычными, то

очевидным отличием будет возможность смарт-контракта контролировать лишь математически доказуемые условия сделки, в то время как в обычном контракте изложенные в нем условия могут носить и нечеткий, то есть описательный характер. В конечном итоге Ник Сабо ограничился лишь теоретическим представлением своей модели, а непосредственная реализация данного концепта увидела свет только спустя два десятка лет в проекте Ethereum.

В целом процесс формирования смарт-контракта похож на обычную транзакцию, которая содержит ряд дополнительных элементов, придающих ей уникальные свойства. В первую очередь речь идет о программном коде, который подлежит децентрализованному исполнению при помощи так называемой виртуальной машины Ethereum (EVM) непосредственно на узлах сети, создающих блоки. В коде смарт-контракта описана алгоритмическая логика обработки сделок между пользователями сети и владельцем смарт-контракта, поместившим его в блокчейн, введя его, таким образом, в действие. С этого момента смарт-контракт присутствует в одном из блоков цепочки, и любой желающий участник сети может активировать его работу путем отправки транзакции на адрес контракта в системе. То есть смарт-контракт является полноправным субъектом сети, который может принимать и формировать транзакции. Но делает он это не самостоятельно, а только когда код контракта запускается на исполнение виртуальной машиной Ethereum на узле майнера при создании нового блока. Как происходит этот процесс?

Для простоты смарт-контракт можно сравнить с торговым автоматом, который продает, например, напитки. Покупатель помещает в автомат определенную денежную сумму наличными или при помощи банковской карты, а аппарат выдает выбранный товар сообразно внесенным средствам. Если данную ситуацию спроецировать на блокчейн-сеть, то активация смарт-контракта происходит в момент, когда в блок помещается транзакция, отправляющая в адрес контракта какие-то криптовалютные активы. Обрабатывая подобную транзакцию, майнер находит блок, где содержится смарт-контракт, и при помощи виртуальной машины запускает его код на обработку, подавая ему «на вход» данные транзакции. Результат действия смарт-контракта может быть разным, что обусловлено логикой алгоритма, заложенной в сам код контракта. Это может быть просто внесение изменений в состояние системы либо формирование контрактом ответных транзакций — одной или даже нескольких. Не следует также забывать, что смарт-контракты запускаются не только майнерами, но и обычными узлами. Это происходит в моменты, когда они обрабатывают транзакции, связанные со смарт-контрактами, в том числе и при проверке получаемых от майнеров блоков на валидность. Подобный протокол предполагает, с одной стороны, некоторую вычислительную избыточность, а с другой — обеспечивает дополнительную гарантию стабильности работы системы в целом.

В отличие от скрипт-языка Биткоин, код смарт-контрактов пишется на языках программирования, удовлетворяющих критериям полноты по Тьюрингу. Наиболее распространенным языком смарт-контрактов Ethereum является объектно-ориентированный язык Solidity, семантически схожий с популярным языком программирования JavaScript. Однако непосредственно в тело смарт-контракта помещают не исходный текст, написанный, например, на том же Solidity, а прошедший через процедуру компиляции — так называемый «байт-код». Данный код представляет собой компактный набор команд низкого уровня, предназначенный для исполнения виртуальной машиной Ethereum.

В силу того, что любая блокчейн-система является децентрализованной средой, где каждый блок и каждая транзакция доступны для изучения любым участником сети, то и смарт-контракты Ethereum не являются исключением. Но поскольку контракт хранится в блокчейн-базе в формате байт-кода, для того, чтобы разобраться с принципом его действия, используются специальные декомпиляторы. Это программы, приводящие код в относительно «читаемый» вид, хотя и далекий от исходного — того, в котором он был изначально создан программистом смарт-контракта. Декомпилятор не может восстановить исходные названия переменных, а также все комментарии, сделанные программистом к своему коду. Таким образом, воспроизведение изначальной логики алгоритма после процесса декомпиляции кода смарт-контракта становится непростым делом. Бывают, правда, и обратные ситуации, когда создатели смарт-контрактов публикуют исходный текст своего кода для обеспечения большей прозрачности и доверия к своим алгоритмам. Для публикации используются внешние интернет-ресурсы, где можно ознакомиться с текстами кодов в легко читаемой форме, содержащей необходимые комментарии.

Как и любая обычная компьютерная программа, смарт-контракт обладает различными функциональными возможностями. То есть для одних смарт-контрактов достаточно нескольких строк кода, а другие могут представлять собой сложные алгоритмы, состоящие из сотен и даже тысяч строк. Это говорит в первую очередь о том, что с точки зрения приложения вычислительных усилий смарт-контракты отнюдь не равноправны — для обработки каждого из них требуется различное процессорное время. Из этого обстоятельства вытекает логичный вопрос: каким же образом формировать мотивацию майнера при обработке подобных контрактов? А что, если код смарт-контракта будет содержать, например, бесконечный цикл, который введет компьютер обработчика в состояние «зависания», когда он будет бесконечно пытаться выполнять один и тот же набор операций по кругу? Чтобы защитить систему от подобных ситуаций, в Ethereum предусмотрена модель оплаты вычислительной мощности при помощи специального «топлива» для обработки

смарт-контрактов. Такой вид «топлива» в Ethereum обычно называют «газ», поскольку этот термин созвучен его английскому написанию (gas), хотя есть и другие варианты перевода этого слова.

Как ни странно, главная расчетная криптовалюта сети Ethereum — эфир — была создана в первую очередь для важнейшей утилитарной цели — оплачивать газ для обработки смарт-контрактов. Сам газ является счетной, но немонетарной величиной и напрямую отражает объем затрачиваемого вычислительного ресурса на запуск кода смарт-контракта майнером. Для каждого оператора байт-кода сети Ethereum существует его фиксированная «стоимость», номинированная в единицах газа. Простые операторы вроде арифметических действий «стоят» дешевле. Тогда как сложные, например, процедуры хеширования — дороже. То есть в систему изначально было заложено подобие «прайс-листа», на основе которого всегда можно рассчитать, сколько газа уйдет на обработку конкретного смарт-контракта. Поскольку обычные транзакции на перевод криптовалюты от одного адресата к другому тоже требуют вычислительной обработки, то и у них имеется свой эквивалент «газовой стоимости». Обычно стандартная транзакция обходится в 21 000 газа, вопрос только в том, сколько стоит сам газ.

Ценообразование на газ всегда зависит от текущей нагрузки на сеть Ethereum. Если в очереди на обработку и включение в блок стоит много транзакций, майнеры начинают отдавать приоритет тем, чьи отправители указали более высокую стоимость газа. Перед стартом первой версии клиента сети Ethereum было установлено, что единица газа будет стоить 10 000 Gwei, или одну стотысячную долю эфира. Сейчас эта цена считалась бы исключительно высокой, поскольку цена монет эфира с момента запуска проекта очень сильно выросла, хотя и далека от своего исторического максимума. Тем не менее если покупать газ по такой цене, то стоимость отправки обычной транзакции сегодня обошлась бы в сумму около $30.

Понятно, что с ростом стоимости монеты эфира цена газа пропорционально падала, за исключением коротких периодов, когда нагрузка на сеть существенно возрастала. В этом случае отправители транзакций боролись за их приоритетное включение в ближайшие создаваемые блоки путем увеличения цены на газ. На весну 2019 года средняя стоимость газа колебалась в пределах 2–4 Gwei, что приравнивает комиссию за обычную транзакцию примерно к одному-двум американским центам. При отправлении транзакции можно указать и меньшую цену газа, чем текущая рыночная. В этом случае транзакция будет обрабатываться дольше, чем обычно, а если цена выставлена сильно ниже рынка, то транзакция может и вовсе не попасть в обработку.

Посылая в сеть транзакцию для взаимодействия со смарт-контрактом, отправитель может лишь примерно предполагать, какой объем газа потребуется для ее обработки. Поэтому он указывает не точное значение газа, а величину с запасом, то есть максимум газа, который он готов позволить «сжечь» для своей транзакции. Точное значение будет установлено майнером при непосредственной обработке транзакции и смарт-контракта, причем с отправителя будет взыскан именно реально затраченный объем, а неиспользованный остаток будет ему возвращен. В случае же, если лимита газа для обработки смарт-контракта не хватит, его выполнение будет досрочно прекращено и «сделка» не состоится. При этом уже использованный газ возвращен не будет, а его стоимость поступит в доход майнера.

Если проанализировать все транзакции блока, в том числе связанные со смарт-контрактами, можно рассчитать совокупный объем газа, требуемый на обработку всего блока. Поэтому в сети Ethereum размер блока ограничен не объемом в байтах, как в Биткоине, а в максимально допустимом количестве газа на один блок. Получается, что в блоке может быть и небольшое число транзакций, но многие из них могут оказаться весьма «газозатратными», поэтому лимит может быть достигнут довольно быстро. На текущий момент лимит на один блок составляет величину около 8 млн единиц газа, что позволяет поместить в один блок Ethereum максимально чуть меньше четырех сотен стандартных транзакций. Предполагается, что лимит газа на блок будет расти по мере естественного увеличения вычислительных возможностей узлов сети.

Теперь становится понятно, почему концепт смарт-контрактов имеет ряд очевидных преимуществ по сравнению с контрактами обычными. Однако нельзя не обратить внимание на то, что и здесь есть свои уязвимости. Поскольку смарт-контракты создаются самими участниками сети, в этом процессе присутствует так называемый «человеческий фактор». Такой, например, как профессиональная квалификация программистов, создающих алгоритмы и программные коды. За несколько лет существования проекта Ethereum было отмечено много случаев, когда ошибки, допущенные программистами при написании кодов смарт-контрактов, приводили к серьезным финансовым потерям.

Этот факт часто используется в критических оценках подобных систем, поскольку его сложно избежать в силу полной открытости и децентрализации сети. В феврале 2018 года сводная группа экспертов объявила, что около 34 000 смарт-контрактов в сети Ethereum имеют потенциальные проблемы и уязвимости, о которых пока не подозревают их владельцы. Были случаи, когда из-за ошибок в кодах смарт-контрактов злоумышленники похищали десятки миллионов долларов. Для того чтобы минимизировать риски, авторам

смарт-контрактов рекомендуется уделять больше времени их тестированию, а также заказывать аудит кода у признанных профессионалов отрасли.

Наконец настало время рассмотреть, какие функции в основном выполняют смарт-контракты в сети Ethereum на текущий момент. Согласно статистике, всего в сеть было помещено чуть менее 2 млн смарт-контрактов, из которых около полумиллиона находятся в «активном» состоянии. Общее же количество транзакций, связанных со смарт-контрактами, оценивается более чем в 100 млн. Определенная часть смарт-контрактов обеспечивала деятельность децентрализованных криптовалютных бирж, поддержку внебиржевых сделок между контрагентами, а также организацию криптоигр, некоторые из которых завоевали широкую популярность. Но все же подавляющее большинство смарт-контрактов были задействованы для обеспечения выпуска и обращения цифровых криптожетонов, или так называемых токенов. Именно проект Ethereum дал старт интереснейшему и весьма масштабному явлению в цифровом децентрализованном мире под названием «токенизация», описание которого потребует отдельного подробного рассказа.

Токенизация

Каждая блокчейн-платформа имеет свою основную криптовалюту в виде цифровых монет, или, как их еще называют, коинов — от английского слова coin («монета»). Эмиссия собственной криптовалюты обычно продиктована необходимостью создавать монетарную мотивацию для узлов, поддерживающих стабильную работу сети. В частности, в проектах Биткоин или Ethereum существуют собственные базовые криптовалюты, которые используются как для выплат майнингового вознаграждения, так и оплаты транзакционных комиссий. В дополнение к этому эти криптовалюты применяются еще и как платежные средства и даже как инструменты для инвестиций. Хотя, например, первоначальная идея проекта Ethereum подобного использования своих монет не предполагала, но это стало одним из естественных последствий эксплуатации возможностей проекта. Для поддержки децентрализованных проектов, которые хотели бы иметь собственные цифровые активы, платформа Ethereum предложила возможности для их создания. Данный тип активов начали называть цифровыми криптожетонами или просто токенами (от английского token — «жетон»). Главное отличие токенов от коинов — отсутствие собственной блокчейн-инфраструктуры; они стали технологической надстройкой над уже существующей сетью, которая обеспечивала их эмиссию и децентрализованное обращение.

Для чего же разработчикам проектов на базе сети Ethereum могли понадобиться собственные токены и почему они не захотели использовать для своих нужд уже имеющуюся криптовалюту сети — эфир? Во-первых, они не хотели попадать в зависимость от ценовой рыночной конъюнктуры монет эфира. Колебания цены базовой криптовалюты проекта могли быть весьма значительными, и, как показали дальнейшие события, эти предположения оказались верными. Но главной причиной был тот факт, что эфир подходил далеко не для всех проектов, поскольку их потребности выходили за рамки обычных свойств криптомонет. У ряда проектов возникла необходимость создать новый тип цифровых активов, коренным образом отличающийся от привычных базовых криптовалют, использующихся как средство платежа. И об этих отличиях мы сейчас поговорим подробнее.

В общем случае любой токен следует рассматривать как счетную единицу, которая совершенно не обязательно должна представлять собой цифровые деньги, хотя именно в этом качестве криптотокены приобрели наибольшую известность. Достаточно большое количество проектов интегрировали в свои системы специальные платежные токены, обладающие своей собственной внутренней ценностью, никак не связанной с колебаниями стоимости монет эфира. Подобные токены получили название «утилитарных» (utility) или «полезных» токенов и олицетворяли собой либо внутренние деньги для своих проектов, либо иные формы учетных единиц. Например, баллы программы лояльности какой-то компании или нечто подобное. Утилитарные токены предназначены для одной основной цели — служить расчетным эквивалентом для предлагаемых проектами товаров или услуг. Они не являются активами, имеющими какое-то ценностное обеспечение, а формирование их рыночной стоимости с теоретической точки зрения не должно зависеть от успехов или неудач проекта. Тем не менее реалии таковы, что объем спроса на утилитарные токены влияет на их рыночную цену, а сам спрос формируется в зависимости от степени популярности того или иного криптопроекта, предлагающего свои токены к реализации.

Создавая свои проекты, разработчики, как правило, отчаянно нуждаются в инвестициях. Редко когда они имеют возможность покрыть все расходы на создание проекта самостоятельно — это больше свойственно крупным корпорациям, имеющим собственные финансовые резервы. А группа программистов-энтузиастов, разработавших интересную идею для своего проекта, скорее всего, предпримет попытку профинансировать ранние этапы создания проекта через привлечение внешних средств. Для проектов, создающихся в криптосреде на базе технологии блокчейн, выпуск собственных токенов стал отличной возможностью собирать значительные средства для разработки. Такие процессы получили название «первичное размещение монет» или ICO (Initial Coin Offering) — по аналогии с известным термином IPO (Initial Public Offering), когда компания выпускает свои акции для выхода на фондовую биржу и привлекает таким образом денежные средства для дальнейшего развития.

Если какой-либо проект позиционирует выпускаемые токены не как утилитарное средство для расчетов внутри создаваемой системы, а как виртуальные акции собственной компании, то речь идет о совсем другом типе токена как цифрового актива. Необходимо принять во внимание тот факт, что когда инвестор приобретает такие токены, он, по идее, должен стать совладельцем компании-эмитента. То есть получить все сопутствующие привилегии, включая дивиденды от ее деятельности и право голоса при принятии важных решений. Мы не будем сейчас касаться юридических аспектов в отношении приобретения подобных токенов. Заметим лишь, что в данном случае мы имеем дело с так называемыми «инвестиционными» (security) токенами, которые призваны отражать юридическое право владения приобретателем пропорциональной частью проекта.

Проводя процедуры первичного размещения токенов в сети Ethereum, владельцы проектов используют для этого смарт-контракты. Они составляют код контракта таким образом, что при поступлении от какого-либо инвестора любой суммы, номинированной в монетах эфира, ему выдается взамен соответствующее количество токенов проекта, в зависимости от условий размещения. Смарт-контракт в данном случае осуществляет контроль над эмиссией и распространением токенов. Если владельцы проекта захотят, например, поощрить раннее приобретение своих токенов, они могут предложить более низкие цены на них по дате инвестиции. В этом случае смарт-контракт должен обработать текущую дату и сравнить ее с заложенной в условия таблицей дисконтов, определяя таким образом актуальную стоимость токена для текущего временного периода. Таким же способом смарт-контракт может проводить и выкуп токенов у инвесторов по задекларированной владельцами контракта цене, принимая токены и выдавая взамен монеты эфира в соответствующем эквиваленте. Бывают и случаи, когда нужно избавиться от лишних токенов путем их «сжигания» — например, пересылая их на несуществующий адрес в сети, к которому ни у кого из участников нет секретного ключа.

Следует с сожалением констатировать, что владельцы многих криптопроектов довольно часто не делают акцентов на принципиальных различиях между видами токенов, которые они предлагают инвесторам к продаже. В криптовалютной индустрии стали нередки случаи, когда под эгидой ICO распространялись не инвестиционные, а чисто утилитарные токены, которые никакого права владения не давали. Подобные прецеденты быстро привлекли внимание финансовых регуляторов различных стран, которые начали активную деятельность по законодательному разделению типов токенов, одновременно разъясняя инвесторам разницу между ними. Понятно, что каждое государство по-разному формировало свое отношение к новой форме привлечения капитала. Какие-то страны поспешили создать для проектов, проводящих ICO, режим наибольшего благоприятствования и довольно быстро внесли в законодательства своих стран соответствующие изменения и дополнения. Другие заняли выжидательную позицию, не решаясь идти на радикальные меры ни в одну, ни в другую сторону. А отдельные юрисдикции сразу высказали свое негативное отношение к подобным процессам и даже применили ряд репрессивных воздействий на локальную криптоиндустрию, обязав владельцев проектов вернуть инвесторам ранее привлеченные через ICO средства.

Несмотря на то что утилитарные и инвестиционные токены доминируют в криптоиндустрии в целом, список видов цифровых токенов не ограничивается только лишь двумя их ипостасями. Имеются все основания предполагать, что наиболее перспективной формой токенизации будет «дигитализация», или превращение обычных финансовых активов в цифровую форму. Речь идет о фиатных валютах, акциях корпораций, сырьевых товарах или производных инструментах, таких как фьючерсы, опционы или контракты на разницу цены. Для каждого из этих финансовых активов имеется возможность выпустить токены, которые будут обращаться в децентрализованных блокчейн-средах со всеми вытекающими из этого преимуществами. Однако такие токены будут иметь и ряд особенностей. В первую очередь их цена будет целиком и полностью зависеть от колебаний рыночной стоимости «подлежащего актива» на классических финансовых рынках. Другими словами, их цена должна быть всегда стабильной по отношению к своим базовым активам. Именно поэтому данный тип токенов назвали «стейблкоинами», то есть «стабильными монетами», если дословно переводить с английского.

Вторым важным отличием от утилитарных токенов является необходимость организации механизмов полного обеспечения стейблкоинов соответствующими базовыми активами. Очевидно, что подобные модели можно реализовать лишь централизованным способом, то есть средствами специальных депозитариев, которые будут хранить у себя необходимые объемы базового обеспечения. Депозитарии подобного типа должны принимать к себе на хранение базовый актив, а взамен выдавать пользователю надлежащие стейблкоины. То же самое касается и обратной операции — когда депозитарий, принимая обратно стейблкоины, обязуется обменять их на равный объем хранимого в обеспечении базового актива. В качестве примера можно рассмотреть проект Tether, который обеспечивает эмиссию стейблкоинов американского доллара в сетях Ethereum и Биткоин (через надсетевую инфраструктуру Omni Layer).

Стейблкоин Tether в 2015 году был выпущен гонконгской компанией Tether Limited, которая обязалась его эмитировать и обеспечивать. Необходимость токенизации доллара была продиктована значительным спросом со стороны трейдеров криптовалютных бирж, которые хотели совершать обмен криптовалют не только друг на друга, но и на аналоги фиатных валют, представленных в цифровой форме. Таким образом они желали защититься от колебаний цены на криптовалюты, временно выведя свой капитал в эквивалент фиатной

валюты. А многие из них просто хотели реализовать для себя конвертацию криптовалют в токены доллара, чтобы потом обменять их напрямую у эмитента на доллары обычные, получив их из хранилища посредством банковского платежа.

Логично было бы предположить, что если какая-то компания выпускает, скажем, 1 млн стейблкоинов доллара США, то на ее банковском счету должно быть не менее 1 млн физических долларов, которыми эти токены обеспечены. Однако механизмы обеспечения стейблкоинов базовыми активами лежат за пределами контроля блокчейн-сетью как таковой и представляют собой централизованный сервис, основанный на доверии. Таким образом, обеспечение «прозрачности» деятельности лежит на самом эмитенте. В случае с Tether прозрачность деятельности депозитария была обеспечена в явно недостаточной степени. От внешних финансовых аудитов компания всегда отказывалась, а между тем общая эмиссия токенов USDT (Tether) превысила к весне 2019 года $2,5 млрд. Неудивительно, что компания постоянно становится объектом пристального внимания финансовых регуляторов как в самом Гонконге, так и в стране эмитента долларов — США, где регуляторы с 2018 года запретили компании операции с резидентами страны. Тем не менее стейблкоины Tether продолжают пользоваться исключительной популярностью у криптотрейдеров, и проблем с доверием у них, по крайней мере, на текущий момент, не возникает.

Несмотря на организационные и регулятивные сложности токенизации классических финансовых активов, этот процесс постепенно набирает популярность. Появляются проекты, которые предлагают токенизацию драгоценных металлов или акций биржевых компаний. Помимо сети Ethereum, на рынке стали появляться и другие токенизирующие платформы, однако им пока непросто бороться с лидером отрасли, который консолидирует подавляющее большинство выпускаемых токенов. Для того чтобы придать отраслевой токенизации системную форму, проект Ethereum разработал специальные стандарты для различных типов токенов. Наиболее популярным стандартом на текущий момент является ERC-20 — именно в этом формате выпущено большинство токенов различных проектов. Этот стандарт описывает набор технических спецификаций для выпускаемых токенов, чтобы они принимались всей сетью и могли взаимодействовать с другими токенами системы, будучи совместимы между собой по формату.

Довольно часто у владельцев токенов возникает необходимость совершать обмен одних токенов на другие. Базовый функционал сети Ethereum не позволяет совершать прямой обмен разными токенами в пределах одной транзакции. Для того чтобы участники сети могли обмениваться между собой разными активами, требуется не менее двух транзакций, имеющих форму встречной сделки. Поскольку все транзакции в блокчейн-сетях являются «безотзывными», то в таких случаях вопрос обеспечения доверия между сторонами становится достаточно актуальным. Наиболее популярным методом реализации обмена являются криптовалютные биржи, посредством которых и совершается подавляющее большинство сделок с токенами, в том числе стандарта ERC-20. Существует также ряд децентрализованных бирж, которые специализируются исключительно на обмене токенов сети Ethereum между собой.

За неполные четыре года существования сети Ethereum в ней было эмитировано чуть менее 200 000 токенов различных типов — утилитарных, инвестиционных и ряда других. Подобные масштабы токенизации говорят о том, что отрасль криптотокенов активно развивается, и в ближайшее время мы сможем увидеть все больше проектов, базирующихся на этом типе цифровых активов. По некоторым оценкам, в индустрии создания децентрализованных приложений на базе платформы Ethereum задействованы сотни тысяч IT-специалистов во всем мире, и их число продолжает расти. Развиваются и возможности самой сети Ethereum: ее разработчики, и в первую очередь сам Виталик Бутерин, постоянно ищут возможности для улучшения работы сети и решения тех проблем, которые неизбежно возникают в процессе эксплуатации проекта. Это и чрезмерный рост размера базы блоков, и, конечно же, объемы затрачиваемого на майнинг электричества. В настоящее время сеть Ethereum находится в состоянии переходного периода от энергоемкого типа консенсуса Proof-of-Work к более прогрессивному алгоритму, который позволит избежать исключительных энергозатрат, поскольку базируется совершенно на ином принципе. Он называется «доказательством владения», или Proof-of-Stake, и уже активно используется в ряде проектов криптоиндустрии. Являясь, по сути, основной альтернативой алгоритму доказательства работы, этот принцип постепенно начинает вытеснять своего энергетически неэффективного конкурента.

Доказательство владения

При анализе принципов защиты блокчейн-сетей при помощи алгоритма доказательства работы явным образом очерчиваются как ее преимущества, так и недостатки. Очевидным достоинством концепта является математическая строгость постановки вычислительной задачи, решение которой дает неоспоримое право на вознаграждение за создание блока. Одновременно с этим имеют место и негативные аспекты, а именно — высокие энергозатраты, которые используются достаточно нерационально, поскольку польза от полученных результатов вычислений заканчивается непосредственно в момент создания каждого нового блока. Понятно, что подобный метод достижения консенсуса в децентрализованных средах получает массу критических отзывов, связанных с неэффективным использованием энергоресурсов. Этой проблемой многие криптоэнтузиасты были озабочены еще со времен раннего периода работы сети Биткоин, заранее просчитывая ситуацию, при которой совокупные энергозатраты всей сети будут расти вместе с популярностью криптопроекта. Эта проблематика серьезно обсуждалась криптосообществом, когда в июле 2011 года на одном из самых популярных

биткоин-форумов прозвучала революционная идея о том, что от энергозависимого майнинга можно все-таки отказаться. В качестве замены концепту доказательства работы была предложена модель «доказательства доли владения», которую в криптосообществе принято с тех пор называть Proof-of-Stake (PoS).

Автор идеи, укрывшийся за форумным псевдонимом Quantum Mechanic, сообщил о возможности использовать потенциал владения криптовалютой вместо контрибуции вычислительной мощности узлами сети, как это делается при обычном майнинге. Другими словами, было предложено выдать право создавать блоки тем узлам, на балансе которых располагалось значительное количество криптомонет в течение относительно продолжительного времени. Идея была полностью поддержана и развита криптосообществом. Примерно через год, в августе 2012 года, разработчиками Скоттом Нэдалом и Санни Кингом была представлена платежная система Peercoin. Это была первая блокчейн-сеть, добавившая элементы доказательства владения к привычному принципу доказательства работы, создав, таким образом, гибридный механизм консенсуса. Протокол Proof-of-Work (PoW) в сети Peercoin использовался для формирования новых денежных эмиссий в виде вознаграждения для майнеров, создающих блоки, наряду с транзакционными комиссиями — по аналогии с сетью Биткоин. Однако вместе с PoW блоками в сети могли появляться и блоки, которые создавались на основе принципа доказательства владения.

Для того чтобы создать блок, необходимо было провести действия, отдаленно напоминающие майнинг. Только вот создателей блоков на основе доказательства владения решили называть не майнерами, а валидаторами, то есть узлами, подтверждающими блоки. Сам же процесс создания блока стали называть форжингом или минтингом, от английских слов forging и minting, означающих «выковывать» и «чеканить». Прежде чем приступить к созданию блока, валидатору необходимо было показать, каким объемом криптомонет он владеет. Так же как и при майнинге, нужно было хешировать определенные параметры, такие как данные предыдущего блока, текущее время и адрес, на котором располагались принадлежащие валидатору средства. Полученный хеш сравнивался с произведением двух значений, которые представляли собой количество монет у валидатора и продолжительность владения ими. Как только удавалось получить хеш, меньший по значению, чем это произведение, блок считался созданным. Очевидно, что чем больше у валидатора монет и чем дольше он ими владел, тем выше шансы, что произведение этих чисел будет весьма велико и превысит случайно полученный хеш, который всегда можно рассматривать и как обычное число. Поскольку в процессе хеширования есть только один постоянно меняющийся параметр — время в полных секундах, то и сам хеш может меняться лишь один раз в секунду. Валидатор, создавший блок, непосредственное вознаграждение за это не получал, зарабатывая лишь совокупную комиссию от транзакций, помещенных им в блок.

Как следует из алгоритма создания блоков Proof-of-Stake, значительных энергозатрат для этого не требуется. Однако это не означает, что у данного типа консенсуса нет недостатков или неудобств. Валидатор, создающий блоки по принципу Proof-of-Stake, фактически замораживает средства на своем счету и вынужден не использовать их достаточно длительное время, чтобы не потерять накопленный потенциал для возможного создания блоков. Для самой сети это не очень хорошо, поскольку скорость обращения денег внутри нее может существенно замедлиться, что негативно скажется на возможностях ее использования и развития. Подобный метод создания блоков мотивирует узлы в первую очередь к накоплению, а не расходованию средств. Таким образом, их чрезмерная консолидация под контролем одного или нескольких узлов может привести к повышению степени централизации процессов управления сетью вопреки изначальному замыслу. Также на процесс создания блоков практически не оказывают никакого влияния узлы с относительно небольшой долей владения криптомонетами, поскольку у них практически отсутствуют шансы стать валидаторами в силу своего незначительного финансового потенциала.

Для устранения этих недостатков была разработана модификация протокола Proof-of-Stake, где были представлены механизмы делегирования полномочий валидаторов от рядовых участников сети к избранным ими узлам. Каждый узел посредством специальной транзакции может отдать свой голос одному или нескольким потенциальным кандидатам в валидаторы. Получившие большинство голосов узлы-делегаты могут и не обладать значительным количеством монет, но зато они готовы контрибуцировать свои вычислительные возможности для поддержания стабильной работы сети, получая за это относительно скромную транзакционную комиссию. Подобный принцип назвали «делегированным доказательством владения» (DPoS), и именно эта форма протокола Proof-of-Stake впоследствии получила наиболее широкое распространение в проектах, которые решили отказаться от энергозатратного алгоритма доказательства работы.

Отличие DPoS от классической формы доказательства владения состоит в том, что валидаторы, получившие право делегирования, уже не перебирают хеши, чтобы найти подходящее его значение. Вместо этого они формируют очередь из подобных им делегатов, чтобы договориться о строгом порядке формирования блоков. Каждому из валидаторов выделяется определенный временной период, в течение которого он имеет право создать блок, принимаемый всей сетью. Сам период может быть довольно коротким и исчисляться единицами секунд — это зависит от протокола сети и того, насколько большую пропускную способность участники сети хотят получить для своих транзакций. В случае если по какой-то причине валидатор пропустил свою очередь, право создания блока переходит к следующему по

порядку валидатору. Сам порядок имеет единые для всех правила формирования, при этом каждый валидатор вычисляет его самостоятельно. Понятно, что у всех валидаторов этот рассчитанный порядок должен в точности совпадать, иначе работа сети может быть нарушена.

Преимущества формы Proof-of-Stake с делегированием полномочий очевидны. Во-первых, узлы с незначительными балансами имеют хотя и косвенное, но пропорциональное своему финансовому балансу влияние на выбор узлов-валидаторов. В своей совокупной массе эти узлы с большой вероятностью не позволят крупным игрокам захватить и централизовать процессы управления сетью. Непосредственным созданием блоков будут заниматься узлы, наилучшим образом для этого предназначенные и облеченные доверием большинства узлов сети. И, наконец, что также немаловажно, отсутствует необходимость блокирования на счетах больших объемов криптосредств, чтобы валидатор имел возможность постоянно доказывать свою финансовую состоятельность и получать таким образом права на создание блоков в сети.

Это не означает, что концепт доказательства владения не имеет потенциальных проблем. Этот протокол также может быть подвержен различным атакам, одной из которых теоретически может стать знакомая нам «Атака 51%». Правда, в отличие от систем с доказательством работы, где требуется захватить не менее половины всей вычислительной мощности сети, в случае с Proof-of-Stake необходимо получить контроль над половиной и более всех криптомонет проекта. Однако последствия такой атаки имеют схожую негативную природу в обоих концептах, поскольку автоматически приводят к подрыву доверия к сети в целом и обесцениванию локальной криптовалюты, разоряя и самого атакующего.

Одной из возможных сложностей на пути данной формы консенсуса может быть атака Nothing at stake, или «ничего на кону». Подобная ситуация происходит, когда недобросовестный валидатор пытается создать и подписать блоки в различных ответвлениях цепочки, которые образовались случайным или намеренным образом. В случае с доказательством работы такое поведение майнера нерационально, поскольку он таким образом распределяет свою вычислительную мощность между ветвлениями и уменьшает собственные шансы на создание блока в любом из них. В модели доказательства владения он, напротив, ничем не рискует, поскольку не затрачивает ни средств, ни вычислительных ресурсов на создание блоков в конкурирующих ответвлениях. А между тем подобная деятельность гарантированно приведет к нарушению консенсуса, к которому сеть в итоге не сможет прийти. Каждый проект, использующий модель Proof-of-Stake, пытается противостоять этой проблеме с различной степенью эффективности.

Еще одним важным свойством Proof-of-Stake в его классической форме является отсутствие аналога вознаграждения за майнинг. Поскольку майнинга как такового нет, то отсутствуют и серьезные инфраструктурные затраты на его поддержание. Поэтому считается, что поощрением валидатора может быть только собираемая транзакционная комиссия. Однако в этом случае возникает известная дилемма «курицы и яйца»: если нет майнинговых эмиссий, то откуда вообще возьмутся деньги в системе? Этот вопрос различные проекты, желающие использовать принцип доказательства владения, решают по-разному. Некоторые идут по пути, который проложил пионерский Proof-of-Stake проект — Peercoin. В нем, как уже упоминалось, была реализована гибридная модель консенсуса, когда ранние блоки создавались при помощи майнинга с доказательством работы. Затем к ним стали «подмешивать» блоки, созданные валидаторами посредством протокола доказательства владения. После чего PoS блоки начали доминировать в цепочке, а PoW применялся только для того, чтобы совершить дополнительную эмиссию, объем которой постоянно сокращался по мере роста общего количества монет в системе. Известны также проекты, которые решили не интегрировать у себя протокол доказательства работы вообще, а всю эмиссию создали в первом, генезисном блоке, разместив ее на адресах, контролируемых разработчиками. Впоследствии эти монеты постепенно были проданы новым участникам сети, сформировав таким образом внутрисетевое денежное обращение. В этом случае проекты, как правило, использовали модель DPoS, которая позволяла быстро и эффективно формировать блоки с транзакциями.

Возвращаясь к проекту Ethereum, важно иметь в виду, что он находится в процессе перехода от одного типа консенсуса к другому. Еще в 2017 году разработчики проекта анонсировали грядущие изменения, связанные с переходом от майнинга к Proof-of-Stake. В первой половине 2018 года появились обновления, обусловленные переходным периодом. Было анонсировано постепенное снижение награды за майнинг — этот процесс назвали «ледниковым периодом» для сети Ethereum. Ходят слухи, что планируется ввести довольно жесткие правила для валидаторов по «имущественному цензу». Предполагают, что минимальный порог для блокирования валидаторами средств составит не менее 1500 монет эфира, что даже по текущему, претерпевшему значительную от своего максимума коррекцию курсу соответствует фиатной сумме более $200 000. И эти средства валидатор теоретически рискует утратить, поскольку они могут быть уничтожены, если узел будет уличен в атаке Nothing at stake, то есть в одновременном подписании конкурентных блоков в разных ветвлениях цепочки. Окончательные правила будут объявлены разработчиками при выпуске обновления, которое заменит протокол консенсуса в сети Ethereum на доказательство владения.

Все эти меры находят как положительный, так и отрицательный отклик в криптоиндустрии. Вне всякого сомнения, недовольными остаются те, кто ранее инвестировал значительные средства в майнинг монет эфира. Переход на Proof-of-Stake оставит их не у дел, если, конечно, они не использовали для майнинга видеокарты. Дело в том, что графические процессоры являются универсальным инструментом для этой деятельности и могут быть при необходимости переориентированы на майнинг других криптовалют. Раздаются также тревожные голоса, предупреждающие о возможных проблемах с безопасностью при переходе на PoS протокол. Положительно же оценивают предпринятые разработчиками шаги те представители криптосообщества, кто считает, что энергетически неэффективный майнинг является серьезным препятствием для активного развития технологии блокчейн. Объясняют они свою позицию тем, что майнинг представляет собой исключительно ресурснозатратный процесс, который оказывает негативное влияние на экологическую обстановку в мире и подвергается критике в том числе и на государственных уровнях.

Альткоины

Способность человека к критическому анализу является одним из основных драйверов развития цивилизации. Философия скептицизма базируется на понятии сомнения в истинности установленных в обществе догматов как принципа мышления. Именно скептицизм, заставляющий подвергать сомнению идеализм окружающих нас сущностей, мотивирует к изменениям и улучшениям приобретенных человечеством научных, культурных и социальных достижений. Несомненно, не в последнюю очередь из-за этого отдельные представители криптоиндустрии посчитали ранние блокчейн-сети недостаточно совершенными и принялись создавать новые, более прогрессивные по своим возможностям проекты. В какой-то момент этот процесс принял лавинообразный характер, когда общее число криптопроектов начало исчисляться тысячами, и стало решительно невозможно охватить и проанализировать весь объем связанной с ними информации.

Капитализация Биткоин, то есть совокупная ценность всей его эмиссии, сопоставима со всеми остальными существующими криптомонетами вместе взятыми. Его авторитет в блокчейн-индустрии настолько велик и непререкаем, что все криптовалюты, появившиеся позднее, называют «альткоинами», то есть полагают альтернативными именно Биткоину. Первые альткоины появились спустя всего лишь несколько лет после запуска сети Биткоин, а именно — в 2011 году. Эти проекты пытались преодолеть те, по их мнению, неудобства, которые естественным образом сложились в самом Биткоине. При этом один из новоявленных альткоинов практически полностью скопировал логику функционирования своего предшественника, просто изменив параметры процессов, в нем происходящих. Этот проект получил название Litecoin, что само по себе говорит о том, что он является облегченной версией Биткоина.

Проект Litecoin был разработан американским программистом Чарли Ли, которого некоторое время даже подозревали в авторстве Биткоина. Хотя трудно уловить логическую связь между фактом сохранения инкогнито в одном проекте и раскрытия себя в более позднем и менее популярном. Тем не менее подобные идеи обсуждались в криптосообществе — по крайней мере, до тех пор, пока внимание не переключилось на иные, более одиозные кандидатуры. Как бы там ни было, Litecoin сумел отвоевать у рынка свою собственную нишу и до сих пор входит в десятку самых больших по капитализации альткоинов. Что же отличает этот проект от своего более «массивного» прообраза?

Основные отличия можно описать цифрой «4». Именно этот множитель был выбран автором проекта для масштабирования параметров сети Биткоин. Блоки в Litecoin создаются в четыре раза быстрее, то есть в среднем за 150 секунд, а предел конечной эмиссии установлен на уровне вчетверо большего значения — 84 млн монет. Для формирования адресов так же, как и в Биткоин, используется алгоритм хеширования SHA-256, зато механизм майнинга был существенно изменен. Для нахождения новых блоков в сети Litecoin применяется специальный алгоритм Scrypt, задействующий большие объемы оперативной памяти. Это позволяет оказывать противодействие майнингу с использованием ASIC, хотя в конечном итоге эти устройства все равно были представлены на рынке.

Что касается рыночного спроса на монеты Litecoin, то он находится на среднем уровне. Довольно долго цена держалась в диапазоне $2–4 за монету, но во время большого «хайпа» цена достигла своего исторического максимума в $358. Затем она снизилась до уровня примерно $80, где и пребывает в настоящее время, а общая капитализация Litecoin составляет немногим менее $5 млрд (около 5% от капитализации Биткоина). Монеты Litecoin являются довольно популярным финансовым инструментом для спекулятивной торговли, и их часто можно встретить в листингах многих криптовалютных бирж и брокерских компаний.

Еще одним популярным альткоином, постоянно оспаривающим вторую позицию по капитализации у Ethereum, является Ripple, разработанный одноименной компанией для организации процессов обмена валют между финансовыми институтами, и в первую очередь банками. Ripple был изначально задуман и создан для B2B-индустрии, то есть для деловой среды, где все взаимодействие осуществляется исключительно между юридическими лицами. Это, впрочем, не помешало многим частным криптотрейдерам рассматривать криптовалюту Ripple как инструмент для инвестирования и помещать туда достаточно существенные капиталы с целью

извлечения дохода от курсовой разницы. Проект Ripple имеет достаточно много отличий от привычных блокчейн-сетей, некоторые из которых нам целесообразно будет рассмотреть.

Интересно, что одной из ключевых персон, имевших отношение к появлению Ripple, стал бывший создатель файлообменной сети eDonkey и биржи Mr. Gox Джед Маккалеб. Именно он в 2012 году в сотрудничестве с инвестором Крисом Ларсеном предложил разработчику платежного протокола Ripplepay Райану Фуггеру создать специальную криптовалюту, которую можно было бы использовать в межбанковских валютно-обменных операциях. Правда, уже через год Маккалеб покинул компанию Ripple и основал ее прямого конкурента — проект Stellar, который также входит в первую десятку криптовалют по капитализации. В чем же был основной смысл создания этих проектов?

При совершении трансграничных банковских платежей, подразумевающих конвертацию из одной национальной валюты в другую, традиционно использовалась дорогостоящая межбанковская посредническая инфраструктура. Именно ее эксплуатация и стала причиной высоких комиссий, которые клиенты банков вынуждены были оплачивать при совершении переводов. Иногда, если при переводе требовалась конвертация валют стран третьего мира друг на друга, комиссии могли составлять курсовой эквивалент десятков долларов, что делало переводы небольших сумм не имеющими никакого экономического смысла. Кроме того, эти переводы могли занимать значительное время, что также было крайне неудобно для многих клиентов традиционных финансовых институтов.

Проект Ripple был призван эту ситуацию коренным образом исправить и освободить клиентов банков от непомерных комиссионных платежей в пользу мировых финансовых сетей, играющих роль посредников в процессах денежных переводов и валютных конвертаций. Одновременно с этим планировалось существенно сократить время среднего платежа, предложив наилучшие курсы конвертации из одной национальной валюты в другую. Для этого необходимо было вовлечь в проект большое количество банков со всего мира, создав им необходимую мотивацию в виде сокращения издержек на трансграничные платежи. Считается, что Ripple решает эту задачу достаточно успешно, сводя посредством своей распределенной сети контрагентов напрямую и подтверждая транзакции в среднем всего за четыре секунды. Все больше банков становятся новыми участниками сети Ripple, что говорит об активном развитии проекта.

Что касается технологических аспектов, то у Ripple имеется одно важное отличие от традиционных блокчейн-сетей, а именно — отсутствие майнинга. Весь объем эмиссии криптовалюты Ripple был сгенерирован сразу при старте проекта, а общее количество монет составило целых 100 млрд единиц. Кстати, именно столь высокий объем эмиссии позволил этой криптовалюте попасть в топ-лист по капитализации. При этом 60 млрд монет хранятся в специальном резерве и полностью изъяты из оборота. Криптовалюта проекта используется для прямых межбанковских транзакций, которые отображаются в общем распределенном реестре. Комиссия в сети присутствует как защита от транзакционного спама, но поскольку майнинга в сети нет, она просто сжигается, уменьшая таким образом совокупную циркуляцию монет. Общая пропускная способность сети Ripple составляет около 1500 транзакций в секунду, что является весьма серьезным показателем для подобной децентрализованной сети.

Возвращаясь к обзору популярных альткоинов, нельзя не упомянуть об одном из конкурентов платформы смарт-контрактов Ethereum — проекте EOS. Он был запущен в январе 2018 года компанией block.one и также позволяет создавать смарт-контракты в распределенной блокчейн-сети. При этом для их написания используется популярный язык программирования C++. В отличие от Ethereum, где для создания смарт-контрактов существует специально разработанный для этого язык Solidity, в платформе EOS разработчикам можно применить привычные инструменты для написания программного кода. Сеть использует в качестве протокола консенсуса «делегированное доказательство доли» (DPoS), благодаря чему транзакции в ней подтверждаются всего за четверть секунды. Узлы, создающие блоки, избираются непрерывной процедурой голосования из числа владельцев наибольших балансов локальной криптовалюты EOS. При этом узел-делегат, не создавший за сутки ни одного блока, автоматически освобождается в дальнейшем от этой почетной обязанности.

Интересной особенностью формата транзакции в сети EOS является хранение в ней хеша предыдущего блока. Это дает возможность избежать дублирования транзакций в ответвлениях (форках) и однозначно идентифицирует, в каком из ответвлений в данный момент находится конкретный пользователь сети. Комиссия за транзакции в сети EOS отсутствует, а криптовалюта служит для использования в смарт-контрактах и поддержки обращения токенов, созданных в системе. Всего в обороте находится около 900 млн монет EOS. Текущая капитализация эмиссии составляет чуть менее $5 млрд, что позволяет проекту находиться в первой пятерке по данному параметру. Как и в проекте Ripple, майнинг в сети EOS отсутствует, а монеты можно получить только через их приобретение у разработчиков напрямую либо посредством криптовалютных бирж. При первичном размещении криптомонет EOS совокупно за все раунды ICO разработчикам удалось собрать около $185 млн на дальнейшее развитие платформы.

И наконец, последний проект из числа наиболее популярных альткоинов, который хотелось бы рассмотреть, называется IOTA. Изначально он был задуман для передачи данных и платежей без комиссии между устройствами в так называемом «интернете вещей». Концепт «интернет вещей» (Internet of Things) был разработан для сетевого взаимодействия между собой различных устройств, таких, например, как бытовые приборы. Технологи-визионеры предрекают, что недалек тот день, когда человек сможет делегировать права на финансовые операции обычным домашним устройствам, которые смогут автоматически закупать необходимые ресурсы для своего бесперебойного функционирования. И сеть IOTA как раз может стать удобной средой для совершения подобных транзакций.

Примечательно, что проект IOTA не использует блокчейн-структуру в ее классическом понимании. То есть в сети отсутствуют блоки как таковые, а есть лишь набор транзакций, которые связаны между собой, образуя так называемые направленные ациклические графы. В этом виде графов отсутствуют циклы, а их ребра всегда однонаправлены. Базируясь на этом принципе, в сети IOTA каждая новая транзакция подтверждает две старые, а из подобных подтверждений формируется целая «паутина» верификаций, защищая сеть от проблемы двойной траты. Криптовалюта сети называется «йота», а ее эмиссия конечна и составляет астрономическую величину в 2 779 530 283 277 761 монет. В силу отсутствия блоков майнинг в сети также не предусмотрен, а все транзакции освобождены от комиссий. Для удобства использования монет йота их считают в миллионах, или в MIOTA. Капитализация проекта на текущий момент составляет около $900 млн.

Рассматривая проекты различных альткоинов, периодически можно столкнуться с реализациями, названия которых являются производными от имен популярных блокчейн-проектов. При этом сами они позиционируются как модифицированные копии своих базовых прообразов, начавшие с какого-то момента жить самостоятельной жизнью. Такие альткоины называются форками проектов. Каким образом они появляются и становятся частью блокчейн-индустрии?

Форки

Случается так, что группа единомышленников, ранее объединенная под эгидой некоего сообщества — творческого, политического, коммерческого или какого-либо иного, в определенный момент утрачивает внутреннее взаимопонимание. Обычно это выражается в констатации серьезного расхождения во взглядах на то, что они сообща пытаются создавать или развивать. И тогда консорциум распадается, реорганизуясь в новые группы, каждая из которых по-своему понимает эффективные пути дальнейшего развития. Так создается разветвление с общей историей, но различным будущим. Процесс этот естественен, бесконечен и даже привычен, поскольку постоянно проявляется в совершенно различных сферах человеческой жизнедеятельности. Блокчейн-индустрия не стала исключением и в этом случае, так как открытая форма представления в ней различных проектов немало способствовала возникновению подобных процессов самым естественным образом.

Действительно, подавляющее большинство проектов на базе технологии блокчейн публикуют исходные тексты своих программ в открытом виде, чтобы с ними могли ознакомиться любые желающие. Причин тому несколько. Обычно открытый код логичен, если речь идет об организации децентрализованной сети с равными правами для участников, где сам разработчик не имеет никаких особенных преференций. Кроме того, наличие открытого кода гарантирует участникам сети полную прозрачность всех происходящих в ней процессов, равно как и их полное соответствие принятым протоколам консенсуса. Наконец, это позволяет любому желающему осуществить проверку кода на наличие вредоносных элементов, которые теоретически могли быть заложены в программу на этапе ее разработки. Другими словами, предоставление разработчиками открытого кода является необходимой мерой, обеспечивающей доверие к проекту со стороны всех его участников.

Однако у этой традиции обеспечения прозрачности есть и оборотная сторона. Она создает максимально благоприятные условия для заимствований исходного кода третьими лицами — частично или полностью. Неважно, были ли эти лица ранее частью команды разработчиков или же речь идет о совершенно сторонних субъектах, которые таким образом решили улучшить проект, введя в него изменения и дополнения сообразно собственному видению эффективности и полезности. Так возникает ответвление от базового проекта, которое в блокчейн-индустрии принято называть «форком», что в переводе с английского означает «вилка». С понятием форка мы уже знакомились при рассмотрении возникающих ответвлений в цепочке блоков в моменты, когда различные узлы в один момент времени могли создавать конкурирующие блоки. Но данный тип форков не приводил к появлению новых проектов, поскольку протоколы консенсуса в любом из концептов блокчейн-сетей в обязательном порядке подразумевали выбор истинной цепочки с одновременным отбрасыванием ложных ответвлений.

Но есть и другой вид форков, и с ними все несколько сложнее, поскольку речь идет о непосредственных изменениях в коде клиентской части блокчейн-проекта. Выделяют два варианта таких форков — мягкий (софтфорк) и жесткий (хардфорк). В большинстве случаев форки инициируются самими разработчиками проекта, когда необходимо внести какие-то изменения в его логику. Если изменения не привели к обязательному требованию замены программного обеспечения узла, то речь идет о софтфорке. При активации софтфорка в

сети отсутствует необходимость согласования новых правил со старыми узлами. Софтфорков может быть достаточно много — по сути, они происходят с выходом новых версий программного обеспечения клиентского узла, который не привносит никаких необратимых изменений ни в правила сети, ни в формат хранения данных.

С хардфорками же дело обстоит иначе. В случае если часть узлов не примет новые изменения и не обновит свое программное обеспечение, они более не смогут никаким образом взаимодействовать с узлами, которые согласились на эти фундаментальные модификации. Если число упорствующих достаточно велико, они могут самоорганизоваться в отдельную сеть, которая продолжит исповедовать старые принципы, принятые до масштабных переработок кода проекта. Либо же, наоборот, группа активных узлов сети, желающая внедрить прогрессивные, по их мнению, изменения, наталкивается на консерватизм разработчиков, которые отказываются их интегрировать в код и настаивают на нецелесообразности изменений. В обоих случаях наступают одни и те же последствия — образуется хардфорк, который порождает две базы блоков вместо одной, и каждая из них с этого момента начинает свою собственную жизнь в блокчейн-индустрии.

Образовавшийся в результате хардфорка новый проект получает свою команду разработчиков, сформированную или на базе ранее созданной инициативной группы, или же по воле какого-то предпринимателя, в ряде случаев намеренно инициировавшего разделение. Проект получает новое имя — как правило, производное от базового названия. Локальная криптовалюта также переименовывается и получает отдельный рыночный тикер, то есть сокращенное наименование из нескольких символов. А затем код проекта модифицируется с учетом особенностей, которые и стали основными причинами разделения проектов на два ответвления. В целом подобный процесс аналогичен тем, которые происходят и в обычной бизнес-среде, когда из какой-то компании выделяется команда, создающая собственный бизнес на базе приобретенного опыта и иногда даже части активов, заимствованных на предыдущем месте работы.

Во избежание путаницы, используя в дальнейшем понятие «форк», мы будем иметь в виду именно «хардфорк». Попробуем теперь ответить на вопрос: негативным или позитивным событием является возникновение форков для базовых проектов? Как часто бывает, ситуацию здесь можно рассмотреть с двух сторон. Безусловно, появление конкурирующего проекта, очень схожего по функционалу с базовым, приводит к размытию аудитории пользователей между двумя сетями. В базовом проекте, хотя, как правило, и не сильно, но падает спрос на локальную криптовалюту, а на биржах происходит снижение объемов торговли по ней. Но есть в этом процессе и один положительный момент для держателей, которые владели значительными объемами базовой криптовалюты до разделения проектов. Дело в том, что в момент создания форка база данных блоков копируется в новое ответвление один к одному. И только затем между этими базами появляется рассинхронизация по спискам транзакций, которые начинают создаваться в каждом из ответвлений независимо друг от друга. Что это означает?

А означает это, что владельцы криптовалюты в базовом проекте автоматически получают ровно такой же баланс в новой сети, номинированный в криптовалюте форка. Это происходит потому, что все старые транзакции в обоих проектах до совершения разделения остаются совершенно идентичными. Поэтому, если новая криптовалюта получает какую-то рыночную оценку, то для ее держателей это может расцениваться как дополнительная монетарная прибыль, поскольку их балансы в основной сети остаются без изменений. Полученную в результате форка криптовалюту они могут продать на биржах и получить дополнительный доход, который отчасти компенсирует им неудобства, связанные с разделением проектов. Понятно, что с большой вероятностью рыночная стоимость криптовалюты форка будет существенно ниже базовой, но любая цена выше нуля уже будет представлять собой чистый доход, который, по сути, упал на них с неба.

Логика создания форков основана на преодолении фундаментальных ограничений их базовых прообразов. Уже через несколько лет после запуска сети Биткоин начали очерчиваться его возможные пределы масштабирования. Рассматривались факторы, связанные в первую очередь со скоростью обработки транзакций и размером блока, который был ограничен величиной в один мегабайт. Исторически первым форком Биткоина стала реализация BitcoinXT, возникшая 15 августа 2015 года. Отличием от классического Биткоина в этом форке было увеличение размера блока до восьми мегабайт, после чего планировалось ежегодное удвоение размера блока. Поначалу форк был благосклонно воспринят биткоин-сообществом, а количество узлов BitcoinXT выросло примерно до 4000. Однако уже в 2016 году его популярность пошла на спад, а число узлов снизилось до пары десятков, что означало фактическую «смерть» самого форка.

Незавидная судьба BitcoinXT не остановила попытки создать форк Биткоина, призванный отобрать пальму первенства у проекта-прародителя. 1 августа 2017 года был запущен, наверное, самый «громкий» из форков сети Биткоин — проект Bitcoin Cash. Поддержанный известным активистом блокчейн-сообщества и криптовалютным инвестором Роджером Вером, данный форк начал завоевывать популярность в криптоиндустрии. Его суть во многом напоминала BitcoinXT, поскольку он также предусматривал увеличение размера блока до 8 Мб. Кроме того, в Bitcoin Cash было реализовано еще несколько технологических новшеств, таких как

ускоренное изменение сложности сети и введение нового типа транзакций с усиленной криптозащитой. Спустя год после запуска Bitcoin Cash размер блока в его сети был увеличен еще вчетверо — до 32 мегабайт.

Одним из главных факторов внимания к форку была поддержка производителя устройств AISC из Китая и нескольких крупных майнинговых пулов. Очевидно, что интерес был продиктован желанием этих субъектов увеличить рынки сбыта оборудования и привлечь к процессу майнинга еще большее количество узлов. Хотя следует отметить, что далеко не все майнеры высказывались в пользу увеличения размера блока, поскольку это потенциально приводило к снижению собираемой ими транзакционной комиссии. Преследуя краткосрочные монетарные цели, майнеры не особенно заботились о будущем развитии проекта Биткоин, поскольку их вполне устраивал имеющийся дефицит места в блоках с ограниченным размером. Дело в том, что рост нагрузки на сеть автоматически приводил к росту комиссий, указываемых отправителями, желающими как можно быстрее поместить свои транзакции в ближайший создаваемый блок.

Специалисты криптоиндустрии подсчитали, что только один Биткоин претерпел около семи десятков относительно известных форков, при этом подавляющее большинство из них так и не смогли завоевать сколько-нибудь значимую популярность. Поначалу известие о каждом новом приближающемся форке негативно влияло на рыночную стоимость биткоин-монет. Но когда форки стали появляться, что называется, «пачками», этот процесс утратил влияние на цену базового криптоактива, а стоимость монет форка редко когда превышала даже $1. Причиной большинства создаваемых форков Биткоина в тот период было исключительно желание создателей монетизировать повышение общественного интереса к криптосфере. При этом они не особенно заботились о тех ценностных предложениях, которые эти форки могли предоставить индустрии.

После резкого всплеска интереса мирового сообщества к криптовалютам в конце 2017 года и последующей за ним значительной ценовой коррекции количество форков пошло на спад, и на них практически перестали обращать внимание. Криптосообщество вернуло фокус своего интереса на развитие базового проекта Биткоин, который продолжал доминировать в криптоиндустрии в столь же значительных масштабах, как и до периода активного появления множества своих модификаций.

Разумеется, форки могут возникать не только у Биткоина. Если посмотреть на альткоины в целом, то, наверное, самый известный форк произошел в сети Ethereum вскоре после того, как эта сеть была запущена для массового использования. Весной 2016 года было проведено успешное ICO проекта по децентрализованному управлению инвестициями The DAO, построенного на базе платформы Ethereum. Название проекта расшифровывается как «Децентрализованная автономная организация». Он стал хорошим примером нового подхода к организационному управлению через его децентрализацию в блокчейн-среде. Проект был всецело поддержан самим автором Ethereum Виталиком Бутериным, и отчасти благодаря этому при размещении токенов The DAO была собрана огромная сумма в 12 млн монет эфира. На тот момент привлеченные инвестиции оценивались в сумму около $165 млн, а по нынешним временам она была бы близка к $3 млрд.

Но уже 17 июня руководители The DAO объявили о хищении примерно 30% всех привлеченных монет эфира на сумму около $50 млн. Это известие спровоцировало панику на рынке, и эфир сильно потерял в цене. Через некоторое время выяснилось, что произошло. В коде смарт-контракта The DAO обнаружилась уязвимость, связанная с так называемыми «рекурсивными вызовами», когда программная процедура давала возможность циклически запускать саму себя. Это позволило выводить деньги с кошелька The DAO на ее специально созданные дочерние структуры бесконечное количество раз посредством многократного разделения материнской компании. Перед сообществом пользователей сети Ethereum встала серьезная дилемма: проводить ли хардфорк всей сети, отменяя транзакции злоумышленника, или признать такие ситуации как естественно возникающие в децентрализованной открытой среде и постараться в дальнейшем не допускать подобных уязвимостей.

Большинство пользователей системы, включая самого Бутерина, высказались за хардфорк. Однако у этого решения нашлись и противники, которые посчитали любые формы «транзакционных откатов» нечестной практикой. Они утверждали, что данный прецедент оставляет широкие возможности для будущих вмешательств, что является серьезной угрозой независимому существованию самой системы. Поэтому когда хардфорк, вопреки протестам, все-таки произошел и инвесторам The DAO вернули украденные средства, несогласные с этим решением пользователи образовали ответвление, в котором подобные возвраты средств не были проведены. Этот форк получил название Ethereum Classic, что подчеркивает его ортодоксальность в отношении возможного вмешательства в свободную работу сети. Несмотря на отсутствие поддержки со стороны создателя Ethereum и неприятие сообществом в целом, сеть Ethereum Classic сумела выжить. Существует она и сейчас, хотя стоимость монеты форка с тех пор практически не выросла и составляет около 4% от цены монеты основной сети.

Резюмируя вышесказанное, хочется отметить, что, несмотря на возлагаемые авторами форков радужные надежды, подобные клоны проектов так и не смогли занять значимое место в блокчейн-индустрии. Можно с уверенностью констатировать, что подавляющее большинство форков буквально растворились среди тысяч других проектов, построенных на базе технологии распределенного реестра. Новые проекты в блокчейн-индустрии появляются достаточно быстро и в огромном количестве. Этому, безусловно, способствует открытость исходного кода более ранних проектов, откуда разработчики новых блокчейн-стартапов заимствуют целые сегменты, чтобы сэкономить время и ресурсы на воспроизведение уже существующих модулей и процедур.

В конечном счете это позволяет технологии блокчейн развиваться гораздо быстрее, чем в условиях, когда исходные тексты проектов не публиковались их разработчиками. Возможно, в том числе и благодаря этой технологической открытости в самой криптоиндустрии появилось гораздо более значимое, чем обычные форки, явление, сформировавшее даже определенный ее сектор. Речь идет о проектах, обеспечивающих повышенную анонимность для своих пользователей. Теперь разберемся с закономерно возникающим вопросом: почему подобные проекты оказались настолько востребованными в среде, где анонимность и без того является неотъемлемой частью технологии?

Анонимность в блокчейн

Когда-то очень давно желание вкладчика любого из банков держать свое имя в тайне считалось почтенным и респектабельным. Особенно если речь шла о весьма крупных суммах. Причин, побуждающих клиентов банков сохранять инкогнито, было великое множество, не будем даже брать на себя труд их перечислять. Впрочем, самих банкиров эти причины не особо интересовали, поскольку они считали себя обязанными свято хранить банковскую тайну и сберегать средства клиентов в своих хранилищах сколь угодно долго. Продолжительное время в банковской индустрии были популярны номерные счета на предъявителя, когда любой заявившийся в банк субъект, сообщивший кассиру пароль от счета, мог получить доступ к средствам. А при желании — изъять их даже в полном объеме. Но те «благословенные» времена безвозвратно канули в Лету, поскольку в какой-то момент правительства большинства государств озаботились проблемой ухода своих граждан от законного налогообложения.

С тех пор уже несколько десятков лет все банки и прочие финансовые организации проводят обязательные процедуры идентификации своих клиентов. Понятие же банковской тайны более не является сакральным и имеет скорее негативную коннотацию в глазах национальных финансовых регуляторов. Эти правительственные организации осуществляют строгий надзор над финансовой индустрией своих стран и при наличии подозрений вправе обвинить подконтрольные им кредитные институты в одном из смертных грехов современного делового мира — пособничестве в отмывании денег. Однако вместо фокусной борьбы с реальными преступниками на мировую финансовую отрасль набрасывают «сеть с мелкой ячейкой», куда зачастую попадают небольшие организации и частные лица среднего достатка, чьи финансовые операции могут показаться банкам и их регуляторам не вполне прозрачными, а значит — подозрительными.

Особенно непросто приходится тем, кто проводит финансовые сделки за пределами страны своей налоговой резиденции. Существует немалая вероятность, что банки могут закрыть им счета или как минимум заблокировать средства на них. Причем сделать это подчас без особых оснований, поскольку у банка нет никакого желания рисковать своей лицензией, которую регулятор в случае серьезных процедурных нарушений может и отозвать. Не справляясь с огромными объемами поступающей от банков информации, регуляторы начинают постепенно перекладывать свои функции по борьбе с отмыванием денег на плечи самих финансовых институтов. Те же, в свою очередь, вынуждены реинвестировать свой доход не в развитие основной деятельности, а на усиление инфраструктур по контролю над клиентами и их финансовыми потоками. Действия со стороны банков по отношению к своим клиентам становятся все более строгими, что, безусловно, не идет на пользу мировой экономике в целом. Поэтому нет ничего удивительного, что в ответ на эти действия со стороны человеческой цивилизации возникла естественная реакция в виде блокчейн-проектов, где анонимность стала одной из главных ценностей самой технологии. И эта ценность оказалась востребованной у потребителей финансовых услуг во всем мире.

Сама модель хранения данных и управления ими в блокчейн подразумевает, что пользователи сети осуществляют свои операции от имени обезличенных адресов, в общем случае представляющих из себя хешированные криптографические ключи. Таким образом, невозможно сопоставить какое-либо физическое лицо с его блокчейн-адресом, за исключением некоторых особых ситуаций. Одним из вариантов может стать добровольная декларация владельцем своего адреса и признание факта обладания размещенными на нем средствами. Либо к подобному выводу можно прийти логическим путем, как, например, в случае с Сатоши Накамото. Ни у кого не вызывает сомнений, что он был первым майнером в сети Биткоин, а значит, все майнинговые вознаграждения за создание самых ранних блоков сети оседали на принадлежащих именно ему адресах.

Несмотря на то что определить физического владельца конкретного адреса в блокчейн-сети не представляется возможным, тем не менее в большинстве случаев любой желающий может отследить баланс этого счета и все криптовалютные переводы, с ним связанные. В

какой-то момент выяснилось, что такая ситуация устраивает далеко не всех пользователей сетей, построенных на технологии блокчейн. Эти пользователи пожелали получить повышенную степень анонимности — такую, чтобы невозможно было определить ни количество средств, лежащее на счетах конкретного участника сети, ни какие их объемы он переводит между счетами. Востребованность дополнительной секретности привела к появлению ряда проектов, которые были готовы своим пользователям ее обеспечить, применяя для этого различные криптографические алгоритмы, связанные с сокрытием исходных цифровых подписей к транзакциям.

Еще в июле 2012 года в криптомире появился проект Bytecoin, обеспечивающий полную анонимность транзакций в блокчейн. Создателями системы стали семеро разработчиков, которые применили в своем проекте протокол CryptoNote, обеспечивающий повышенную секретность. Однако к моменту запуска сети для широкого использования выяснилось, что 80% монет Bytecoin уже выпущены и заранее распределены между самими разработчиками и аффилированными с ними лицами. Это вызвало недоверие к проекту со стороны новых, независимых пользователей системы. Учитывая это обстоятельство, двое разработчиков Bytecoin — Рикардо Спаньи и Франсиско Кабаньяс — решили создать форк данной системы с целью устранить ее недостатки и по возможности улучшить функциональность. Несмотря на то что они использовали значительную часть уже созданного ранее кода Bytecoin, на доведение системы до работоспособного состояния все же потребовалось некоторое время. Новая система была запущена в апреле 2014 года, получив название Monero, что в переводе с языка эсперанто означает «монета».

Проект Monero использует протокол защиты Proof-of-Work, хотя поначалу сеть была запущена без майнинга, который стал доступен только через несколько недель. В сети применяется протокол CryptoNote, который обеспечивает процесс так называемой «обфускации», то есть «запутывание» или «перемешивание» информации, которую содержат транзакции сети. Для реализации данной цели применяется метод кольцевых подписей, благодаря которому сторонний наблюдатель никак не может определить, кто является истинным отправителем или получателем транзакции. Спустя несколько лет, к концу 2017 года, в программный код сети был дополнительно интегрирован алгоритм RingCT, который обеспечивает сокрытие пересылаемых сумм. Обычно в криптосистемах, подобных Биткоину, у пользователя имеется только один секретный и один публичный ключ. В сети Monero для каждого из адресов есть «ключ для трат», аналогичный секретному, а также дополнительный «ключ для просмотра», который он может раскрыть третьим лицам для проверки своих транзакций.

Применение механизма кольцевой электронной подписи не позволяет другим участникам сети правильно определить непотраченные выходы для конкретного адреса и вычислить его баланс. А все исходящие отправления всегда производятся на однократно используемые адреса, что окончательно делает невозможным отслеживание перемещений средств от одного физического участника сети к другому. Однако процедура формирования кольцевой подписи предполагает заимствование из блокчейн-базы определенного количества публичных ключей, принадлежащих сторонним участникам сети. Размещение этой маскирующей информации в теле транзакции приводит к ее существенному увеличению, превышая средний размер транзакции в сети Биткоин примерно в восемь раз. Безусловно, подобная информационная избыточность делает систему громоздкой для использования, что является очевидным недостатком.

Тем не менее криптовалюта Monero сумела завоевать популярность — ее часто применяют для оплаты покупок в онлайн-играх и в интернет-казино. Monero входит в число самых популярных криптовалют с капитализацией чуть более $1 млрд. Эмиссия Monero не имеет конечного предела, однако в системе заложено снижение вознаграждения за майнинг после превышения величины в 18,4 млн выпущенных монет. Блоки в сети Monero создаются каждые две минуты, что позволяет довольно быстро подтверждать транзакции пользователей.

Немногим раньше проекта Monero появилась система DASH — DigitalCash, или «цифровая наличность». Система была придумана и разработана Эваном Даффилдом и запущена 18 января 2014 года. Как и в прочих проектах, восходящих к заимствованному из Биткоина коду, для майнинга здесь используется протокол доказательства работы. Отличие DASH состоит в том, что майнерам достается только 90% от вознаграждения за майнинг, тогда как оставшиеся 10% идут на финансирование одобренных участниками сети проектов, связанных с самой системой. При этом сама процедура майнинга в DASH гораздо менее энергозатратная, чем, например, в сети Биткоин.

Управление сетью DASH полностью децентрализовано. Для обработки транзакций используется инфраструктура мастер-нод («мастер-узлов»). Этим узлом может стать любой желающий из числа участников проекта, готовый внести 1000 монет DASH в виде залога, обеспечивающего его добропорядочное сетевое поведение. Одной из основных функций мастер-нод является обфускация транзакций посредством алгоритма PrivateSend. Речь в данном случае идет о перемешивании платежей, проходящих в несколько раундов, количество которых определяет сам отправитель денежных средств. Каждый раз для перемешивания избирается новая мастер-нода, общее число которых на текущий момент уже превысило 5000. Сумма платежа разбивается на части, каждая из которых

анонимизируется, а затем совпадающие по объему части перемешиваются. В качестве мотивации своей деятельности мастер-ноды получают 50% от майнерского вознаграждения за найденные сетью блоки.

Интересно также отметить, что для майнинга в сети DASH используется принцип хеширования, состоящий из целых одиннадцати функций, имеющих различную алгоритмическую природу. Это опять же сделано в целях противодействия ASIC-майнингу, хотя производители оборудования все же сумели эти трудности преодолеть, представив соответствующие устройства на рынке. Всего в сети выпущено чуть более 8 млн монет с общей капитализацией около $1 млрд. Проект достаточно популярен и сопоставим по объемам использования со своим прямым конкурентом — системой Monero.

И, наконец, хотелось бы рассказать о проекте, который специалистами криптоиндустрии по праву считается одним из наиболее перспективных в части полной анонимизации финансовых транзакций, использующихся в децентрализованных платежных системах. Проект ZCash, появившийся в конце октября 2016 года, довольно быстро получил известность и признание как действительно анонимная платежная сеть. Популярность проекта-анонимизатора достигла такого уровня, что даже полицейская служба Евросоюза (Европол) выразила обеспокоенность использованием возможностей данной сети для различных действий криминального характера. Какие же отличия ZCash от других его собратьев по повышенной анонимизации платежей вызвали такую тревогу у европейских правоохранительных органов?

Для создания анонимности в ZCash используется протокол доказательства с нулевым разглашением zk-SNARK, являющийся, по сути, функционально расширенной версией слепой электронной подписи. Сама сеть использует два типа адресов: приватный «z-адрес» и открытый «t-адрес», а транзакции возможны между этими типами адресов в любой из четырех комбинаций. В зависимости от того, является ли адрес отправителя или получателя в транзакции z-адресом, шифруется информация о входах или о выходах либо скрывается вообще вся информация, включая сумму перевода. При использовании «t-адресов» информация остается открытой. Для обеспечения формирования транзакций создается так называемый «кортеж» ключей, состоящий из ключа траты, ключа просмотра и расходного адреса. Причем ключ просмотра и платежный адрес математически вычисляются из ключа траты, который аналогичен по своему смыслу обычному приватному ключу.

Таким образом, пользователи сети сами решают, спрятать или открыть информацию о своих транзакциях в блокчейн. В случае ее сокрытия отследить происхождение каждой отдельной монеты ZCash не представляется технологически возможным. Фактически о совершенных транзакциях знают только сами отправители и получатели, оставляя незашифрованной лишь метку времени создания платежа. Помимо собственно перевода средств, участники сети могут пересылать друг другу зашифрованные сообщения. Проект ZCash допускает также использование мультиподписей в случаях, если возникает необходимость совместного управления счетом несколькими пользователями одновременно. Для реализации этого функционала необходимо задать «весовые» правила для каждой из подписей и величину минимального совокупного их «веса» для того, чтобы транзакция стала валидной для сети.

Протокол консенсуса в сети базируется на доказательстве работы, блок создается за 150 секунд, а эмиссия ZCash, как и в Биткоине, ограничена величиной в 21 млн монет. В качестве поощрения разработчики выделяют до 10% всей эмиссии на дополнительное вознаграждение майнеров в течение первых четырех лет с момента запуска сети для широкого использования. В случае если какая-либо из транзакций не была включена в первые 20 блоков с момента ее помещения в мемпул, она считается просроченной и более не учитывается сетью. Комиссия за транзакции фиксирована и составляет незначительную величину в 0,0001 монеты. Система ZCash замыкает второй десяток рейтинга криптопроектов по капитализации, выпустив около 6 млн монет общей стоимостью порядка $450 млн.

На этом описание наиболее популярных универсальных криптопроектов можно завершить и перейти к третьей части книги, где будут затронуты не менее интересные темы. Во-первых, мы поговорим о практическом применении технологии блокчейн в различных сферах человеческой жизнедеятельности. Коснемся такой важной темы, как отношения криптоотрасли и государства. Значительная часть завершающего раздела будет посвящена инвестициям в криптопроекты, включая торговлю криптоактивами на финансовых рынках. И, наконец, завершим мы книгу некоторыми философскими рассуждениями о перспективах технологии блокчейн и о том, как она могла бы изменить привычную нам картину мира уже в недалеком будущем.

Часть III
БЛОКЧЕЙН-ИНДУСТРИЯ

Применение блокчейн

В предыдущем разделе книги мы уделили достаточно внимания наиболее популярным децентрализованным платформам, построенным на базе технологии блокчейн. Эти проекты универсальны по своей сути и не могут быть отнесены к какому-то конкретному сектору делового или социального мира. Лучше всего они подошли бы под определение финансовых платформ, поскольку их функционал заточен именно под эту деятельность. Речь идет в первую очередь о цифровых платежных системах, позволяющих осуществлять быстрые и анонимные денежные переводы на базе распределенной сети. Но это только одна из множества форм применения блокчейн-технологии, возможности которой выходят далеко за пределы одних лишь финансовых операций.

В главе, где мы рассматривали концепт цифровой электронной подписи, в качестве примера мы привели процедуру интернет-голосования на выборах в государственные органы власти в Эстонии. Система I–Voting, впервые примененная на местных парламентских выборах в 2007 году, стала первой в своем роде, использующейся на столь высоком государственном уровне. По статистике, около трети всего электората Эстонской Республики использовали интернет и технологии асимметричной криптографии для изъявления своей избирательной воли. Однако проведение выборов в Эстонии с использованием технологии блокчейн пока еще только планируется к реализации. Как ни странно, первой страной, которая на практике задействовала блокчейн для проведения выборов, стала далеко не самая высокотехнологичная страна в мире — африканское государство Сьерра-Леоне. В марте 2018 года там были проведены президентские выборы, где технология блокчейн использовалась для проверки поданных избирателями голосов. Хочется верить, что раз уж в такой небогатой и политически нестабильной стране используют столь прогрессивные технологии, то высокоразвитые государства тем более не должны отставать. Использование блокчейн в процедурах голосования обеспечивает им максимальную прозрачность и доверие, поскольку математические алгоритмы предполагают технологическое устранение человеческого фактора, оказывающее потенциальное косвенное влияние на результаты выборов.

Блокчейн открывает широкие возможности и для организации торговли на рынках сырья и драгоценных металлов. При помощи этой технологии процессам торговли сырьевыми контрактами можно придать более стабильную и прозрачную форму. Речь идет о том, чтобы ускорить рыночные взаиморасчеты, упростить привлечение финансирования под совершаемые сделки, а также упорядочить вопросы прав владения подлежащими активами. Что же касается драгоценных камней (например, алмазов), то и здесь технология блокчейн может оказать серьезное влияние на рынок, где они обращаются. Промышленные компании, занимающиеся добычей и обработкой алмазов, в частности, южноафриканская компания De Beers, планируют выпускать специальные паспорта для каждого драгоценного камня и помещать информацию о них в блокчейн. Таким образом, мировой рынок бриллиантов может практически полностью оказаться под децентрализованным контролем, который позволит значительно ограничить возможный криминальный оборот драгоценных камней. Существует также ряд проектов, занимающихся токенизацией прав владения на золотые слитки различного веса. Непосредственно само золото никуда физически не перемещается и находится в охраняемых централизованных депозитариях, в то время как специально эмитированные стейблкоины, жестко привязанные к хранимому золоту, торгуются на различных криптовалютных биржах и используются в прямых, внебиржевых сделках.

Кроме того, блокчейн почти идеально подходит для построения локальных рыночных площадок с участием множества небольших частных игроков. Отличное применение таких маркетплейсов — продажа излишков электроэнергии, получаемой из возобновляемых источников. Существует много небольших частных мини-электростанций, работающих, как правило, на основе солнечной или ветряной энергии. В случае если при выработке электричества образуются некоторые излишки, они могут быть реализованы в энергосетях общего пользования. Однако из-за отсутствия рыночной инфраструктуры часто непросто найти контрагентов по таким сделкам. Более того, случается, что единственным покупателем электричества является сам владелец сети — локальный энергетический монополист. Очевидно, что предлагаемая в этом случае закупочная цена далеко не всегда отвечает рыночным условиям, а в ряде случаев энергетическая компания и вовсе может отказаться от подобных соглашений. Построение блокчейн-проектов по заключению прямых сделок между производителями и потребителями электричества является достаточно полезной и перспективной задачей. Поэтому первые реализации подобных прогрессивных концептов уже начали свою работу в энергоотраслях некоторых стран.

Весьма полезным блокчейн может оказаться и в области медицины. С его помощью можно организовать децентрализованное хранение медицинских данных пациентов. Например, выписок из их медицинских карт, историй болезней, назначенных лекарств и прочей информации, которая обычно распределена между множеством медицинских учреждений. Консолидировать эти данные, как правило, очень тяжело, а зачастую и невозможно. Понятно, что информация в самой блокчейн-базе должна храниться в зашифрованном виде. При этом доступ к ней, полностью или частично, вправе выдать только лишь сам пациент по запросу больницы или клиники, в которую он обращается за врачебной помощью. Помимо этого, блокчейн может быть использован для отслеживания цепочек поставок лекарств в целях борьбы с их фальсификацией. То же касается и учета производства и поставок лекарств, содержащих наркотические вещества, — подобные препараты должны подлежать строгому контролю. Наконец, при помощи блокчейна можно существенно облегчить работу

отрасли страховой медицины, помещая в распределенную базу смарт-контракты, проводящие автоматические выплаты за оказанные врачебные услуги. Разумеется, такие смарт-контракты, прежде чем производить выплаты, должны будут проверять выполнение всех необходимых условий конкретного договора страхования.

Борьба с контрафактом не ограничивается лишь сферой производства медицинских препаратов. Все отрасли, связанные с производством товаров и их логистикой, пытаются решить подобные проблемы. В блокчейн-индустрии уже появляются проекты, предоставляющие сервисы специальной маркировки товаров с последующим помещением информации о месте производства и всей цепочке поставок товарных партий в распределенный реестр данных. Эта информация впоследствии может быть востребована и проверена любым участником сети, чтобы убедиться в легальном происхождении приобретаемых им товаров. Следует добавить, что подобная форма товарной маркировки хорошо защищена от несанкционированного воспроизведения, поэтому ожидается, что степень доверия потребительского рынка к таким моделям борьбы с фальсификациями будет достаточно высока.

Интересными могут стать блокчейн-решения для туристической индустрии. Как и в большинстве отраслей, на ценообразование туристического продукта существенное влияние оказывает посредническая наценка, которая может доходить до трети конечной стоимости и даже более. В этом случае применение блокчейн-технологии, позволяющее осуществлять прямые сделки между производителями и потребителями туристических услуг, полностью устраняет дорогостоящую посредническую маржу из конечного ценообразования. Речь идет об услугах по приобретению билетов на различные виды транспорта, бронированию отелей, а также продаже побочных продуктов, связанных с туризмом, например, экскурсий. Конечно, при децентрализации процессов распространения услуг, связанных с исполнением обязательств вне блокчейн-систем, неизбежно возникнут конфликтные ситуации, требующие разрешения. И это является одной из основных проблем дезинтермедиации бизнеса, когда посредническая роль полностью устраняется из процедуры приобретения товара или услуги. Однако варианты решений уже существуют, и мы позднее их рассмотрим.

Относительно недавно мир социальных сетей начали сотрясать скандалы, связанные с утечкой персональных данных пользователей. Речь шла в том числе и о нескольких миллионах участников социальной сети Facebook, чьи данные оказались в распоряжении третьих фирм, использующих их как в коммерческих, так и в политических целях. Подобные проблемы случались и с другими социальными сетями. Конечно же, виной всему было недостаточно внимательное отношение компаний, управляющих проектами, к хранению персональных данных своих пользователей. А в ряде случаев речь могла идти даже о целенаправленной продаже данных заинтересованным лицам. Но если проанализировать эту ситуацию более глубоко, становится понятно, что корень проблемы находится именно в области организации централизованной формы хранения данных. При этом вышеописанные инциденты следует рассматривать как естественные последствия использования подобной модели.

Напрашивается вывод, что этих проблем можно избежать, лишь децентрализовав хранение данных пользователями социальных сетей и мессенджеров. И в данном случае технология блокчейн вновь может прийти на помощь. Применение технологии распределенного реестра позволит пользователям самим контролировать свою личную информацию — ее публикацию, хранение и использование. Децентрализованно хранимую и зашифрованную криптостойкими алгоритмами информацию просто невозможно использовать сторонним лицам в незаконных целях. Разумеется, в работе с подобными системами будут возникать и свои неудобства — в первую очередь из-за невозможности удалять ранее помещенную туда информацию. Но преимущества будут существенно превалировать над всеми прочими факторами, связанными с использованием децентрализованных систем. Конечно, проектам на базе технологии блокчейн будет весьма непросто отвоевать свою долю рынка у популярных централизованных социальных сетей. Однако хочется надеяться, что со временем им это удастся, поскольку спрос на безопасность хранения персональных данных имеет явную тенденцию к росту.

Наконец, блокчейн начинает активно применяться в индустрии развлечений, и в частности — в организации азартных игр и букмекерских ставок. Как известно, казино и букмекерские компании извлекают свои доходы от заложенных в условия игр и событийных пари так называемого «отрицательного математического ожидания» для своих клиентов. Что это такое? Любая игра или спор подразумевают, как правило, три варианта конечного исхода: выигрыш, проигрыш или ничью. Обычно организатор игры несколько дисбалансирует условия выплат клиентских выигрышей в свою пользу. Другими словами, клиент получает чуть меньше денег, чем ему бы полагалось с точки зрения справедливого распределения вознаграждения, которое напрямую зависит от вероятности возникновения самого выигрышного события. Именно этот дисбаланс и формирует относительно гарантированную прибыль организатору в случае значительных совокупных объемов игровых сделок за длительный временной период.

Организатор приема игровых ставок — классический элемент централизации, отчисляющий в свою пользу комиссионное вознаграждение. Оно может принимать различные формы, в том числе и скрытые — в виде вышеописанного дисбаланса в условиях выплат. Технология блокчейн позволяет данный централизующий элемент устранить, тем самым обратно сбалансировав условия игровых сделок для обеих сторон. Сегодня уже можно наблюдать проекты по организации азартных игр, где единый организатор

отсутствует. В результате отпадает необходимость создания условий, ставящих одну из сторон в неравноправное положение. К тому же само по себе применение технологии блокчейн обеспечивает полную прозрачность и честность при непосредственном проведении игр, поскольку код подобных платформ открыт для проведения аудита любым субъектом, принимающим участие в проекте.

Можно долго перечислять отрасли, где технология блокчейн могла бы применяться с различной степенью эффективности. Еще раз отметим, что основной целью внедрения этой технологии является снижение или полное устранение посреднической роли и связанных с ней издержек. Немаловажным фактором также является обеспечение прозрачности всех правил и процедур с целью существенного повышения доверия потребителей к подобным системам в целом. Одновременно с этим для поддержания работоспособности таких проектов возникает необходимость в обеспечении трансграничного движения капитала между криптовалютным и фиатным мирами. А это, в свою очередь, не может не вынуждать правительства различных государств обратить свое пристальное внимание на происходящие в криптосфере процессы, чтобы не утратить контроль над налоговыми поступлениями от подконтрольной им деловой среды.

Как уже отмечалось ранее, наибольшее беспокойство у правительственных регуляторов вызывают процессы, связанные с возможной легализацией финансовых средств, полученных незаконным путем. Это нередко подвигает правительственных чиновников на действия, однозначно препятствующие развитию прогрессивных технологий в современном финансовом мире, в число которых входит и блокчейн. Действительно, факт весьма непростых взаимоотношений между блокчейн-индустрией и государством очевиден, но некоторые их аспекты требуют детального рассмотрения.

Блокчейн и государство

Научные дисциплины, изучающие деловой мир, однозначно полагают государственное управление наименее эффективной формой менеджмента как такового. Оснований тому предостаточно: низкие управленческие компетенции политических назначенцев и явный недостаток (или, напротив, избыточность) подконтрольных руководящему субъекту ресурсов. Как правило, негативное влияние на управленческие процессы оказывают нечетко поставленные стратегические цели, слабые системы контроля исполнительской дисциплины, размытые формы личной ответственности и, что тоже немаловажно, — низкая монетарная мотивация управленцев. Наконец, использование политического популизма как инструмента получения и удержания государственной власти в большинстве случаев подрывает любую экономическую модель, даже если ранее она относительно успешно эксплуатировалась. Характер государственного управления базируется на политических идеологиях — правого, центристского или откровенно левого толка. Политическая стратегия государства осуществляется демократическими или авторитарными методами, во втором случае нередко сосуществуя с развитой коррупционной системой.

Доходы любого государства формируются, как правило, из двух основных источников — налоговых поступлений от предпринимателей и трудоспособного населения, а также от добычи и реализации природных ресурсов. Государство в данном контексте мы будем определять как совокупность бюрократических институтов, необходимых для обеспечения его функционирования. Очевидно, что контроль над уплатой налогов является важнейшим фактором, обеспечивающим само существование государственной управленческой инфраструктуры. Поэтому именно этому вопросу большинство чиновников уделяют повышенное внимание. Какие же методы контроля использует государство? Начнем с того, что важнейшая системная составляющая деловой среды большинства стран мира — это национальный финансовый рынок. Именно система денежных отношений определяет состояние экономики государства: будет ли она активно и поступательно развиваться, либо же ее ожидают стагнация и неизбежно последующая за ней экономическая депрессия.

Понимая исключительную важность состояния финансовой индустрии, государство всегда пытается оказывать на нее управленческое влияние, иначе говоря — регулировать. Для этого у государства имеются необходимые инструменты — свод отраслевых законов, а также инфраструктура бюрократических и силовых ведомств. Разумеется, высокая регулятивная строгость сформировалась в финансовой отрасли не сразу, а в результате определенной эволюции. В течение довольно продолжительного периода истории цивилизации финансовые рынки различных государств функционировали на основе обычной саморегуляции. Однако глобальные финансовые кризисы заставили органы государственной власти пересмотреть свои подходы к регулированию в сторону ужесточения. От типично либертарианских моделей ряд государств (в том числе демократических) начали переходить к откровенно протекционистским и даже репрессивным формам воздействия на подконтрольные им финансовые индустрии.

За последнее десятилетие широкое распространение получила регулятивная стратегия, где доминантной идеей является борьба с отмыванием денег субъектами деловой среды, уклоняющимися от законодательно установленных налоговых платежей. Появление же технологии блокчейн с ее собственной децентрализованной и никому не подвластной инфраструктурой, а также с заложенной неотъемлемой анонимностью максимально усложнило процессы необходимого контроля над движением финансовых потоков. Правда, до тех пор, пока первые проекты, построенные на базе блокчейн-технологии, не получили относительно широкого распространения, власти не обращали на них серьезного внимания. Особенно с учетом того, что технологическая сложность самого концепта построения

платежных систем на основе блокчейна являлась существенным барьером для понимания сути происходящих процессов и того, как это может повлиять на финансовую индустрию в целом.

Однако довольно скоро капитализация криптовалютного рынка стала исчисляться десятками и даже сотнями миллиардов долларов. Это заставило правительства ряда стран осознать, что стратегия дальнейшего игнорирования явления под названием «блокчейн» может привести к непоправимым последствиям для их государственных бюджетов. Перед чиновниками встала нелегкая задача: как выразить свое отношение к новому финансово-технологическому феномену и как затем управлять связанными с ним рисками для национальных экономик? Здесь следует сделать уточнение, что градус радикализма тех шагов, которые национальные правительства предпринимают в отношении криптоиндустрии, напрямую зависит от степени свободы политической конкуренции в конкретной юрисдикции.

В странах с истинной парламентской демократией государственные чиновники вынуждены соизмерять свои публичные высказывания с производимым политическим эффектом, который может оказать влияние на результаты следующих выборов. Очевидно, что никто из политиков не имеет желания прослыть среди своего электората закоренелым ретроградом, стоящим на пути научно-технологического прогресса. Более того, многие из них пытаются разыграть перед своими избирателями «технологическую карту», чтобы поднять имидж своей партии и представить себя в роли сторонников технологического развития страны. Однако, будучи ответственными за исполнение государственного бюджета, чиновники сохраняют постоянную озабоченность возможной утратой контроля над финансовыми потоками и налоговыми поступлениями. Поэтому в ряде случаев представители правящих партий или коалиций сохраняют публичный нейтралитет и достаточно редко на практике поддерживают какие-либо проекты, связанные с криптовалютами.

В государствах, где безраздельно властвует авторитаризм, у представителей правящих партий отсутствует необходимость конкурировать с другими политическими силами. Поэтому их позиции однозначны и в большинстве случаев характеризуются набором запретительных мер, существенно ограничивающих применение криптовалютных систем в пределах данной юрисдикции. Например, ряд стран пытается запретить майнинг, приобретение, продажу и даже в некоторых случаях хранение криптовалют. Кроме того, ограничивается или полностью запрещается деятельность криптовалютных бирж наряду с работой соответствующих платежных систем. Но эти репрессивные меры наталкиваются на естественную технологическую сложность или даже полную невозможность их осуществления, поскольку блокчейн-системам присущи такие свойства, как децентрализация и анонимность использования.

Выходит, что ни одному государству не под силу вмешаться в деятельность любой из существующих децентрализованных блокчейн-сетей, отслеживать внутри нее платежи, а также блокировать и конфисковать средства, связанные с сетевыми адресами. В классическом мире фиатных денег государство всегда может осуществить данный комплекс мер при помощи банков как централизованных и лицензированных финансовых институтов, всегда готовых к сотрудничеству с властями. Но вот в блокчейн-сетях реализовать эти меры не представляется возможным. Единственный шанс у регуляторов оказывать хоть какое-то влияние на криптосреду — разместить между криптовалютным и фиатным мирами пункты своеобразного «пограничного контроля». Для этого регуляторы мобилизуют банки и фиатные платежные системы, которые получают распоряжения отслеживать движения капиталов их клиентов между этими финансовыми средами, имеющими столь различную природу.

Не остаются в стороне и государственные органы исполнительной власти, вкупе с национальными парламентами проявляющие активность в создании и продвижении новых законотворческих инициатив в отношении криптоиндустрии. Начиная с осени 2017 года на криптовалютном рынке начался настоящий бум, после чего многие страны стали принимать законы, ограничивающие обращение криптовалют в пределах национальных юрисдикций, внедряя их с различной степенью строгости. Наиболее радикально поступили такие государства, как Боливия и Непал — они полностью запретили какую-либо деятельность, связанную с криптовалютами. Недалеко от них отстоят Кыргызстан, Индонезия, Ливия и Алжир — там была запрещена покупка и продажа криптовалют, однако четкого отношения к процедурам майнинга обозначено не было. Но более остальных на мировой криптовалютный рынок повлияли такие страны, как КНР, США и Южная Корея.

Считается, что в Китае сосредоточено около 70–80% всего мирового майнинга криптовалют Очевидно, что действия правительства КНР по отношению к крипторынку оказывают наиболее существенное влияние на его капитализацию. То есть речь идет о фиатных эквивалентах стоимости наиболее популярных криптовалют — биткоина, эфира и им подобных. В сентябре 2017 года Китай запретил торговлю криптовалютами и проведение ICO, а фиатные и криптовалютные средства, уже собранные разработчиками проектов, было предписано вернуть инвесторам обратно. Помимо этого, власти начали ограничивать майнеров в приобретении электроэнергии и вообще стали откровенно препятствовать их деятельности. Это сподвигло многих криптофермеров начать перемещение своих дата-центров за пределы Китая в другие, более подходящие для этого страны. Правительство Южной Кореи также распорядилось прекратить привлечение инвестиций через ICO, а в дополнение был издан закон о запрете криптовалютных транзакций с анонимных сетевых адресов.

Соединенные Штаты приравняли токены, распространяемые посредством ICO, к ценным бумагам со всеми вытекающими регулятивными последствиями, делающими проведение данного мероприятия весьма сложным и затратным процессом. В отношении же биткоина как криптовалюты возникла некоторая регулятивная коллизия — ряд судебных прецедентов определяли его как обычную валюту, в то время как комиссия по биржевым фьючерсам CFTC приравняла биткоин к биржевым товарам. Некоторые штаты, например, Нью-Йорк и Вашингтон, ввели обязательное лицензирование для компаний, ведущих деятельность, связанную с криптовалютами. Кроме того, на операции с этой категорией активов было введено специальное налогообложение, конечные ставки которого зависят от штата.

Если говорить о позитивных шагах в сторону легализации криптовалютного рынка, то здесь, безусловно, лидером является Япония, которая стала первой и пока единственной страной, признавшей криптовалюту официальным средством платежа. Также здесь существует официальное лицензирование и регуляция для криптовалютных бирж. Среди стран Европы наиболее благоприятной юрисдикцией для проведения ICO можно назвать швейцарский кантон Цуг, где еще в 2017 году было принято дружественное криптосреде законодательство. Лидером в процессе создания регулятивной базы для блокчейн в Евросоюзе является небольшое островное государство Мальта, где в середине 2018 года был принят закон о виртуальных финансовых активах. Законодательная база Мальты определила понятия, связанные с различными типами криптотокенов, которые возможно использовать в проектах, построенных на базе технологии блокчейн. Результатом стали огромные потоки инвестиций в мальтийские компании, занимающиеся разработкой блокчейн-проектов. Не осталась в стороне и Эстония, которая ввела для криптовалютных бирж упрощенное лицензирование, характер которого сначала был даже более «заявительным», чем «разрешительным». К концу 2018 года в Эстонии было выдано более 500 подобных лицензий, после чего регуляторы задумались о некотором усложнении процесса лицензирования во избежание появления злоупотреблений со стороны некоторых участников рынка.

Несмотря на положительные сдвиги во взаимоотношениях государства и блокчейна, в этой сфере остается еще много неразрешенных проблем, не позволяющих перейти к формированию сбалансированной регуляционной политики в отношении к криптосреде. Одной из основных сложностей, как уже упоминалось, является анонимность финансовых транзакций в блокчейн. И до тех пор, пока разработчики проектов не предложат приемлемые для регуляторов формы деанонимизации финансовых потоков, а также не создадут необходимые инфраструктуры для идентификации участников подобных сетей, говорить о взаимопонимании с государством не приходится. Вне зависимости от того, насколько технология блокчейн будет считаться прогрессивной и прорывной, национальные правительства не будут торопиться поддерживать ее массовое внедрение и использование. По крайней мере до того момента, пока проекты, на ней построенные, не начнут удовлетворять стандартным законодательным требованиям, обычно предъявляемым к участникам финансовой индустрии.

Чтобы ускорить приближение эпохи, когда правительства стран начнут благосклонно смотреть на блокчейн-индустрию, необходимо провести огромную работу по сближению мировоззренческих позиций разработчиков криптопроектов и государственных чиновников. Для реализации этой задачи целесообразно было бы в каждой стране создать профильные ассоциации, а в их рамках — рабочие группы для взаимодействия с правительством. Только ведение конструктивного диалога позволит решить важнейшую задачу интеграции новой технологии в инфраструктуры деловой и социальной среды различных государств. В некоторых странах эта работа уже активно проводится криптосообществом, а где-то предпринимаются лишь первые попытки.

Помимо непосредственных функций контроля за уплатой налогов и противодействия отмыванию денежных средств, у государственных финансовых регуляторов есть еще одна не менее важная задача. Речь идет о защите потребительского финансового рынка от возможных злоупотреблений и откровенного мошенничества со стороны компаний и лиц с сомнительной репутацией. Финансовые регуляторы стараются предостеречь сообщество, состоящее в основном из непрофессиональных инвесторов, от необдуманных шагов, связанных с вложениями в криптопроекты. Но что по этому поводу думают сами представители сообщества? Как они воспринимают относительно новую технологию, на базе которой выросла целая отрасль?

Блокчейн и общество

Долгое время изучение криптографических протоколов для создания децентрализованных платежных систем было уделом узкой прослойки энтузиастов, называющих себя «шифропанками». И даже когда появилась первая блокчейн-сеть, созданная Сатоши Накамото, интерес к ней со стороны людей, не имеющих отношения к криптотехнологиям, некоторое время оставался близким к нулевым значениям. Популярные СМИ практически не освещали новости из криптомира, а какую-то относительно актуальную информацию о криптовалютах можно было почерпнуть лишь на узкопрофессиональных интернет-форумах. К концу второго года существования сети Биткоин в ней едва набиралось около тысячи активных адресов, но спустя еще полгода их число резко увеличилось более чем в двадцать раз. К моменту банкротства биржи Mt. Gox — значимого события в зарождающейся криптоиндустрии — количество активных пользователей насчитывало уже около 150 000. Затем их число только увеличивалось, хотя иногда и претерпевало некоторые коррекции в сторону уменьшения — как правило, после окончания периодов активного роста цен на криптоактивы.

Логично предположить, что первым поколением криптоэнтузиастов были представители индустрии информационных технологий, в первую очередь — программисты. В силу своих профессиональных компетенций они раньше и быстрее остальных сумели разобраться в принципах работы новой технологии. Именно они получили возможность извлечь определенный доход от инвестиций в криптовалюты еще на самом раннем этапе их существования. И действительно, некоторые весьма прозорливые IT-специалисты не упустили открывшегося им шанса и извлекли весьма ощутимую инвестиционную прибыль. Те же, кто пошли дальше в своих устремлениях, приняв участие в создании криптопроектов, завоевавших популярность на рынке, стали мультимиллионерами. В итоге информация об успехах первых криптоинвесторов, распространившаяся среди их друзей и знакомых, наилучшим образом способствовала росту интереса к криптовалютам у людей, не имеющих отношения к информационным технологиям.

Узнав о том, что на финансовом рынке появился некий актив нового типа, на котором делаются миллионные состояния, многие бросились на криптовалютные биржи. Однако большинство даже не взяли на себя труд хотя бы немного изучить природу явления, в которое они собрались вкладывать свои деньги. В результате многие незадачливые инвесторы понесли убытки, после чего поспешили навесить на криптовалюты ярлыки инвестиционного пузыря и даже финансовой пирамиды. Надо сказать, что это мнение было с энтузиазмом подхвачено многими представителями сообщества, которые имели еще меньшее представление о криптовалютах, нежели те, кто уже успел вкусить горечь финансовых потерь от неудачного размещения своих капиталов. Давайте попробуем разобраться, насколько критические оценки криптовалют как объекта инвестирования были близки к истине.

Немецкий философ, социолог и экономист Карл Маркс в своем труде «Капитал» описал общественно-экономическую формацию под названием «капитализм», утверждая, что его значимой фазой является периодически возникающий кризис перепроизводства. Подобная цикличность предполагает сменяемость периодов активного экономического роста и последующей за ним неизбежной депрессии. И действительно, на протяжении ста с лишним лет со времени публикации Марксом своих работ мир несколько раз сотрясался от финансовых кризисов различной степени тяжести, которые затем сменялись длительными экономическими стагнациями. Государствам требовались многие годы, чтобы ликвидировать последствия коллапсов, после чего, дождавшись некоторого оживления рынков, снова начать движение к экономическому подъему.

Почти всегда финансовому кризису предшествовало состояние «перегретости» национальных экономик, которое выражалось в том, что избыток свободных инвестиционных средств в руках участников рынка приводил к «перекупленности» торгующихся на нем инструментов. На фондовых биржах отмечалась исключительная активность, когда деньги массово вкладывались в акции компаний, истинное финансовое положение которых было подчас весьма плачевным, однако мало кто из инвесторов обращал на это должное внимание. В итоге на рынке надувался так называемый «биржевой пузырь» с характерной высокой долей спекулятивной составляющей в стоимости ценной бумаги. Проще говоря, под спекулятивной частью имеется в виду наценка над реальной стоимостью активов компании, чьи акции публично торгуются на бирже. И когда происходит финансовый кризис, переоцененные акции падают до уровня стоимости активов компании-эмитента, а иногда и ниже, поскольку рынок имеет дело с так называемыми «паническими продажами». Один из первых известных миру инвестиционных пузырей возник во время биржевой торговли луковицами тюльпанов в Нидерландах в 1636–1637 гг. Непомерно раздутый «тюльпаноманией» рынок в конечном итоге обрушился и привел к массовым банкротствам среди участников инвестиций на поздних циклах.

На рынке торговли криптовалютами происходят все те же самые процессы, что и на обычных биржевых площадках, на которые оказывают влияние факторы, связанные с человеческой психологией. А это, в свою очередь, означает, что в периоды высокого массового спроса на инвестиционные инструменты спекулятивная составляющая в их цене начинает серьезно доминировать над реальной. Таким образом, понятие инвестиционного пузыря может быть связано с любым из биржевых инструментов, безотносительно к его природе, включая и криптовалюты. Для инвестора, торгующего на финансовых рынках любого типа, важно определить степень его «перегретости» и решить, какие риски он готов принять. Многие аналитики в отношении криптовалют полагают, что спекулятивная составляющая в их стоимости занимает буквально все 100%, поскольку о реальной ценности речь в данном случае идти не может. Однако чуть ранее на примере биткоина мы выяснили, что некоторые криптовалюты все же обладают своей внутренней ценностью, базирующейся на издержках при ее добыче.

Еще одно излюбленное критическое направление, связанное с криптоактивами, — это отождествление их с финансовой пирамидой. Что ж, попробуем проанализировать и эту позицию. Финансовые пирамиды, увы, — довольно частое явление в современном мире. Оно берет свое начало от знаменитой схемы, придуманной неким Чарльзом Понци, выдававшим в 1919 году в США векселя, по которым он обязывался на каждую взятую $1000 выплачивать $1500 в течение трех месяцев. Столь высокий процент Понци объяснял инвестициями в систему обмена международными почтовыми купонами, имевшими положительную для него курсовую разницу. Однако он не упоминал о том, что приобретенные купоны нельзя обналичить, а можно лишь обменять на почтовые марки. Разумеется, никаких купонов Понци не приобретал, сосредоточившись исключительно на привлечении под свою схему денежных средств от кредиторов. Ему

удалось собрать около $4 млн и создать при этом около 7 млн обязательств по обратным выплатам. Пирамида рухнула в августе 1920 года, а сам Понци получил пятилетний срок в американской тюрьме за мошенничество.

Впоследствии финансовые пирамиды нередко возникали в разных странах мира, используя самые разные модели привлечения средств. Однако у всех этих схем можно выявить ряд общих признаков, которые однозначно указывают, что инвесторы имеют дело с мошенничеством. Среди основных атрибутов пирамиды стоит отметить обещание ее участникам выплат, не связанных с непосредственной коммерческой деятельностью компании, официально стоящей за схемой. Одновременно с этим любая пирамида характеризуется обязательным наличием агрессивной рекламной кампании, сопровождающей процесс привлечения средств. Но самое главное — это однозначная централизация и строгая иерархичность создаваемой пирамиды. На ее вершине всегда находится организатор как главный конечный бенефициар схемы в целом. Уровнями ниже могут располагаться наемные или добровольные сборщики средств, получающие комиссию от их привлечения. Первое время организаторы пирамиды действительно осуществляют выплаты более ранним вкладчикам — за счет средств, привлеченных от более поздних. Однако в конечном итоге всегда настает такой момент, когда любые выплаты прекращаются, после чего пирамида обрушивается, а ее вкладчики остаются ни с чем.

А теперь сопоставим ситуацию с финансовыми пирамидами с криптовалютами на примере биткоина. К сожалению для критиков, сам по себе децентрализованный характер построения сети Биткоин делает невозможным существование какого-либо единого выгодоприобретателя, обогащающегося за счет других вкладчиков. Сеть Биткоин не имеет владельца, не ведет никакой коммерческой рекламы продаж криптомонет и не обещает выплат, за исключением вознаграждения, изначально заложенного для участников сети протоколом конкурентного майнинга. Справедливости ради следует отметить, что пример Биткоина в данном случае слишком идеалистичен. В криптоиндустрии существует немало других проектов, полная децентрализация которых хотя и декларируется разработчиками, но по факту отнюдь не является таковой. Выпускаемая при этом криптовалюта формируется в виде стартовой эмиссии на основе премайнинга и помещается в резервы, контролируемые владельцами проектов с целью последующей реализации. И вот только в этом случае существует вероятность злоупотреблений со стороны разработчиков проекта, когда инвесторы, поместившие свои средства в данные криптотокены, могут впоследствии понести убытки. Причин тому достаточно много, и о проблематике инвестиций в ICO мы еще поговорим в отдельной главе.

Случается, что некоторые люди, так и не сумев составить собственное мнение относительно какого-либо явления, формируют свое видение на основе высказываний известных персон. За десять лет существования криптоиндустрии на ее счет был выражен целый спектр мнений разной степени авторитетности. Примечательно, что редкие высказывания носили умеренный характер — большинство из них склонялись к оценочным экстремумам либо в виде искреннего восторга и поддержки, либо же, напротив, агрессивного неприятия, сопровождающегося апокалиптическими предсказаниями. Представители бизнеса, в первую очередь высокотехнологичного, отзывались в целом положительно. Известные экономисты и инвесторы-миллиардеры были склонны к негативным сценариям относительно того, куда криптовалюты могут привести их излишне оптимистично настроенных приобретателей. Однозначно поддержали идею криптовалют бизнесмены Илон Маск и Ричард Брэнсон, а также бывший глава Федеральной резервной системы США Бен Бернанке. Против выступили такие знаменитые инвесторы, как Уоррен Баффет и Джордж Сорос. Глава компании Microsoft Билл Гейтс поначалу высказался в поддержку криптовалют, но затем изменил свое мнение на более сдержанное.

Нельзя не отметить еще один немаловажный фактор, формирующий мнения общества о криптосреде. Дело в том, что многие аналитики совершенно справедливо разделяют понятия «блокчейн» и «криптовалюта». При этом первое, как правило, получает позитивную оценку и предсказание блестящего будущего, в то время как второму достается лишь негатив и критика с искренними пожеланиями скорейшего отмирания за полной, по их мнению, ненадобностью. Интересным индикатором в данном случае выступают крупные коммерческие организации и банки, которые, декларируя полное неприятие криптовалют, одновременно с этим разрабатывают масштабные проекты по созданию внутрикорпоративных и даже отраслевых блокчейн-сред. Целью этих проектов является организация обмена и децентрализованного хранения информации. Для их реализации корпорации даже объединяются в крупные консорциумы, получающие значительное финансирование со стороны их участников.

Представители криптосообщества довольно болезненно реагируют на негативные высказывания специалистов разных уровней, чей авторитет зачастую самими криптоэнтузиастами ставится под сомнение. Как правило, это выражается в виде язвительных оценок способностей критиков как экспертов, взявшихся предсказывать будущее технологического развития человеческой цивилизации. Сейчас трудно загадывать, какая из сторон окажется в итоге правой в своих суждениях. Однако нельзя отрицать высокий уровень интереса со стороны общества к технологии блокчейн в целом и криптовалютам в частности. Появление криптосреды породило такие новые секторы финансовой индустрии, как биржевая торговля криптовалютами и привлечение инвестиций через ICO. Как прямое следствие этого процесса возникли совершенно незнакомые потребителям финансовых услуг риски, которые в ряде случаев привели к существенным

финансовым потерям среди непрофессиональных инвесторов. Поэтому в следующем разделе мы поговорим о криптоторговле и инвестициях, а также о том, как управлять различными рисками, неизбежно при этом возникающими.

Инвестиции в ICO

В 2016 году — $100 млн, уже через год — $6 млрд, а за 2018 год — более $22 млрд. Это не что иное, как инвестиции в первичные размещения криптотокенов или, иными словами, в ICO проектов, созданных на базе технологии блокчейн за последние несколько лет. В главе, посвященной токенизации, мы немного коснулись вопроса проведения массовых привлечений средств в криптопроекты, которые на сленге еще иногда называют «краудсейлом токенов» — от английского tokens crowdsale (дословно — «массовая продажа токенов»). Теперь самое время рассмотреть этот процесс в деталях. Наша цель — понять, что именно подвигло массу инвесторов вложить без преувеличения огромные средства в приобретение виртуальных криптоактивов. Более того, еще и эмитированных никому доселе неизвестными проектами, появившимися буквально из ниоткуда, что не мешает им претендовать на революционные изменения в различных деловых сферах, и в первую очередь в финансовой индустрии.

В основном проекты задумывались и предлагались к реализации группами молодых специалистов из IT-сферы с привлечением представителей научного мира — как правило, из числа обладателей магистерских и докторских степеней по математике и экономике. Именно последние и придавали проектам необходимый академический лоск, создавая для них сложные математические и эконометрические аппараты, производящие должное впечатление на инвесторов. И действительно, создавать впечатление было необходимо — в противном случае реализовать основную цель стартовой части проекта, то есть сбор существенных инвестиций, было бы весьма проблематично.

До недавнего времени, чтобы привлечь инвестиции в разработку своих блокчейн-проектов, их владельцам нужны были всего три вещи — описание своей идеи, криптовалютный хайп в обществе и отсутствие регуляции криптоотрасли. Описание концепта проекта подавалось в виде документа под названием «Белая книга», по-английски White paper. В нем, как правило, вначале обозначалась некая проблема, а затем предлагался метод ее решения путем использования технологии блокчейн. В большинстве случаев подобные документы содержали разделы, посвященные выпуску собственной криптовалюты проекта, где указывалась ее начальная стоимость при первичном размещении. Наконец, описания концептов завершались дорожной картой с определением этапов развития проекта, привязанных к конкретным временным периодам их реализации.

В назначенный срок криптомонеты проекта поступали в продажу, а инвесторы могли их приобрести за фиатные деньги или за другую криптовалюту, имеющую широкое хождение — как правило, биткоины или эфиры. Бывали моменты, когда объем выставленных на продажу токенов не позволял удовлетворить имеющийся на них спрос — слишком много инвесторов желали вложить свои средства в проект в надежде на скорое увеличение его капитализации. В таких случаях могло быть два варианта развития событий: либо токены доставались тем, кто успел приобрести их раньше, либо владельцы проекта собирали заявки со всех желающих, а затем распределяли их между инвесторами пропорционально запрошенным объемам. Понятно, что каждому покупателю в итоге доставалось токенов меньше, чем им бы хотелось, но все-таки они имели возможность приобрести хотя бы какую-то их часть и не остаться полностью за бортом процесса первичного размещения криптоактивов.

Несмотря на привлекательность процедуры ICO для разработчиков проекта, далеко не все из них шли на такие мероприятия. Некоторые девелоперы посчитали невозможным для себя осуществлять первичное размещение монет, организовав при этом их распределение либо на основе майнинга, либо в виде обычной розничной продажи участникам сети. В последнем случае приобретение монет носило сугубо утилитарный характер, поскольку локальные токены требовались для уплаты транзакционных комиссий внутри системы. Конечно, их могли покупать и со спекулятивными целями, однако разработчики официально не позиционировали криптовалюту проекта как инвестиционный финансовый инструмент.

Сатоши Накамото создал сеть Биткоин, где никакого ICO не подразумевалось вовсе — криптомонеты в этой среде добываются посредством конкурентного майнинга. Преимущество в данном случае имели те узлы, которые начали добычу монет раньше других участников сети, воспользовавшись благоприятным моментом, когда сложность вычислительной задачи для майнинга находилась еще на относительно низких значениях. Таким образом, первые майнеры биткоина, включая самого Накамото, сумели сколотить изрядный капитал, когда цена на этот криптоактив взлетела до небес. А вот разработчик Ethereum Виталик Бутерин свое ICO все же провел, собрав средства для фонда, гарантирующего долгосрочное финансирование развития своего проекта. Но при этом он был отнюдь не первым, кто осуществил подобную процедуру.

Пионером в области проведения первичного размещения криптомонет считается проект Mastercoin (впоследствии переименованный в Omni), который в 2013 году собрал около $500 000 для разработки проекта. К концу того же года его капитализация превысила $100 млн,

и уже в 2014 году Mastercoin вошел в семерку самых крупных криптовалют в индустрии. Проект был создан как надстройка над инфраструктурой сети Биткоин, чтобы придать ей большую безопасность и стабильность. Также проект предусматривал возможность создания криптовалютных инструментов с более сложными правилами обращения, чем сами монеты биткоина, не изменяя при этом протокол базовой сети. Несмотря на первичный инвестиционный интерес к криптовалюте проекта сразу же после его запуска, котировки впоследствии начали неумолимо снижаться, и даже всплеск «хайпа» в конце 2017 года не смог вернуть их в область исторических максимумов. В дальнейшем капитализация продолжила свое стремительное падение, сократившись почти в сто раз до около $1,5 млн.

История проекта Mastercoin во многом показательна, потому что обещания разработчиков вошли в противоречие с функционалом, внедренным в реальности, и ценностями, которые в конечном итоге проект смог предложить своим пользователям. Не последнюю роль в утрате инвестиционного интереса к проекту сыграли, конечно же, следующие за ним конкуренты. И здесь в первую очередь следует еще раз вспомнить проект Ethereum, ICO которого было проведено вслед за Mastercoin уже летом 2014 года. Как упоминалось ранее, всего за 42 дня проект собрал внушительную сумму в $18 млн, при этом средняя стоимость одной монеты эфира составила около 30 американских центов. На пике же своей стоимости в январе 2018 года монета котировалась по цене чуть менее $1400. Однако, как и подавляющее большинство своих криптовалютных «собратьев», эфир утратил более 90% своей стоимости от ранее достигнутых ценовых пиков уже к концу того же 2018 года.

После ICO проекта Ethereum размещения перестали быть редкостью, а «золотой век» публичных размещений криптомонет пришелся на 2017 год, когда процесс их проведения принял лавинообразный характер. Именно в течение этого года получило наибольшее распространение явление, которое впоследствии назвали «криптовалютным хайпом». Толпы непрофессиональных инвесторов, в большинстве своем имевших весьма туманное представление о технологии блокчейн, уверенно вкладывали свои деньги в различные криптопроекты. При этом многие проекты существовали лишь в виде общего описания идей, изложенных в сопутствующих «белых книгах».

В ряде случаев разработчики проектов обещали реализовать функционал, заведомо не имеющий на тот момент (да и позднее тоже) технологического решения. Однако бравых криптоинвесторов это никоим образом не смущало — они активно скупали все токены подряд, надеясь на по меньшей мере десятикратный рост их стоимости в ближайшем будущем. Подобные инвестиционные ожидания получили в криптосообществе сленговое название totheMoon, то есть «взлет до самой Луны». Еще одним мотивирующим фактором для криптоинвесторов был так называемый «синдром FOMO» — «страх не успеть» (Fear Of Missing Out). Речь шла о боязни упустить время для инвестирования своих средств в активно растущую криптоотрасль и в итоге остаться за бортом шанса на быстрое извлечение сверхприбыли.

И действительно, стоимость очень многих криптоактивов росла как на дрожжах. Драйверами роста стали главные криптовалюты — биткоин и эфир, а остальные токены котировались уже к одной из этих двух монет. Таким образом, рост стоимости флагманских криптовалют по отношению к фиатным деньгам увлекал за собой и остальные криптоактивы. Впрочем, мало кто из них дорожал непосредственно по отношению к биткоину или эфиру, хотя имели место и такие случаи. «Белые книги» проектов обещали выпуск первых версий продуктов не ранее чем через год или более, поэтому инвесторы вынуждены были принимать планы разработчиков исключительно на веру. Бизнес-аналитики многократно пытались обратить внимание инвесторов на явный дисбаланс в оценке капитализации криптопроектов по сравнению с классическими стартапами. Однако эти предупреждения не нашли у целевой аудитории должного понимания. Отрезвление к инвесторам пришло чуть позднее.

Во-первых, на массовые ICO обратили внимание правительства и финансовые регуляторы различных государств. Декларируя одной из своих функций защиту интересов инвесторов, эти институты начали в спешном порядке вводить меры по ограничению и контролю за сбором инвестиционных средств крипторазработчиками, проводимым практически в условиях финансового «дикого Запада». Сначала инвестиции в ICO запретили в США — одной из самых строгих юрисдикций в мире по части финансового регулирования и контроля. Затем подобные меры были введены в Китае, причем в гораздо более жесткой форме — власти не только запретили проведение любых ICO, но еще и предписали разработчикам вернуть ранее привлеченные средства инвесторам в полном объеме. Несмотря на то что еще ряд государств последовали примеру США и Китая, запреты, введенные именно в этих двух странах, оказали максимально негативное влияние на финансовые потоки в криптоиндустрии.

Разумеется, некорректно было бы считать, что последующий за безудержным ростом обвал котировок криптовалют был вызван исключительно факторами внешней среды, в частности, регулятивными мерами. Так уж устроены законы финансового мира, что никакое высокодинамичное однонаправленное изменение стоимости каких-либо активов, не имеющее явных фундаментальных причин, помимо эмоциональных, не может длиться слишком долго. Рано или поздно к любым торгуемым инструментам, пусть даже и продуктам новейших технологий, будут применены классические принципы монетарной оценки. И в случае, если стоящие за этими активами

проекты-эмитенты не смогут продемонстрировать своим инвесторам разумную бизнес-стратегию, правильное рыночное фокусирование и реальный охват потребительского рынка, то падение их капитализации — всего лишь вопрос времени.

Что касается будущего ICO, то явление это, несомненно, получит дальнейшее развитие с учетом накопленного ранее опыта в индустрии. Изменения коснутся и регулятивных аспектов — в первую очередь чтобы придать инвесторам юридические права на владение приобретаемыми криптоактивами. В настоящий момент в мире очень мало стран, законодательства которых признают инвестиции в ICO наравне с классической куплей-продажей долей или акций в обычных компаниях. В большинстве случаев приобретаемые на ICO или биржах токены, даже если они имеют инвестиционный статус, не дают никакого юридического права инвесторам на пропорциональную долю владения компанией-эмитентом. То есть владелец таких токенов не будет иметь в юридическом лице, которое управляет проектом, никаких прав — ни при голосовании по стратегически важным вопросам, ни при распределении дивидендов, ни при продаже компании новым инвесторам. Более того, многие разработчики проектов предпочитают распространять утилитарные токены вместо инвестиционных, что является очевидным введением потенциальных приобретателей в заблуждение относительно их прав на владение долей проекта, в который они собрались вкладывать свои средства.

Не менее очевидным является факт, что попытки сбора средств посредством ICO при наличии лишь одной «белой книги» в виде файла в формате PDF, который разработчик выкладывает на сайт проекта, безвозвратно уйдут в прошлое. Прежде чем начать привлекать инвестиции, владельцам проектов придется озаботиться необходимыми юридическими процедурами: регистрацией компании, при необходимости — получением лицензий, а также подготовкой проспекта эмиссии, утвержденного местным финансовым регулятором. Но что еще более важно, к моменту проведения ICO у проекта уже должен будет существовать так называемый MVP (Minimum Viable Product), или «минимально жизнеспособный продукт», содержащий в себе первичный этап реализации проекта. Это необходимо для того, чтобы показать инвесторам не только серьезность намерений разработчика, но и работоспособность предлагаемого проектом технологического концепта.

Многочисленные ICO ожидаемо привели к появлению огромного количества криптотокенов — как утилитарных, так и инвестиционных. Логично предположить, что и разработчикам проектов, и новоявленным инвесторам было необходимо обменивать криптоактивы как друг на друга, так и на фиатные деньги. Для этого потребовались электронные торговые площадки, которые позволили заключать такие сделки достаточно быстро и на основе цен, максимально приближенных к среднерыночным. Так появилась инфраструктура криптовалютных бирж, построенных с использованием различных технологических решений и отмеченных разнообразием предлагаемых к торгам инструментов. Следующая глава как раз и будет посвящена обсуждению этого важного элемента криптоиндустрии.

Криптовалютные биржи

Впервые в своей истории с понятием «биржа» человечество столкнулось в 1406 году, когда в городе Брюгге, ныне принадлежащем Бельгии, а в те времена находившемся в составе герцогства Бургундия, была организована первая площадка для вексельных торгов. Основали ее выходцы из семьи финансистов Ван дер Бурсе, фамилия которой в переводе с латинского означает «кошелек». Она и дала название подобным торговым площадкам, которые впоследствии стали называть «биржами». Поначалу биржи были преимущественно товарными, но позднее на них стали торговаться и разного рода ценные бумаги. В 1730 году появилась первая биржа в Японии — по торговле рисом, а вот в США первая организованная торговая площадка была создана только в 1792 году в Нью-Йорке.

К началу XX века биржи получили повсеместное распространение — они действовали почти во всех развитых странах мира. С момента своего появления и практически до конца прошлого века торговля на биржах осуществлялась при помощи биржевых маклеров, которые заключали сделки с контрагентами, используя собственный голос. Именно выкрики маклеров, в которых содержались название торгуемого инструмента, его цена и направление сделки (покупка или продажа), и являлись так называемыми «биржевыми ордерами», то есть поручениями на совершение сделок от уполномочивших их на это клиентов. Время начала и окончания торгов отмечалось ударами специальных биржевых колоколов, которые продолжают использовать некоторые биржи и поныне как дань старинной традиции.

Развитие интернета и информационных технологий активно способствовало постепенному вытеснению шумной толпы биржевых маклеров из торговых залов. Сделки на современных биржевых площадках заключаются посредством специально разработанных компьютерных систем. Они позволяют гораздо быстрее и эффективнее сводить между собой контрагентов по сделкам, а также вести учет по всему объему проводимых участниками биржи торгов. Подключение биржевых площадок к сети интернет позволило существенно расширить число трейдеров, участвующих в торгах, — теперь там присутствуют не только крупные участники рынка, но и трейдеры, оперирующие относительно небольшими объемами финансовых инструментов. Тем не менее вывод акций на биржевые торги остается сложным и дорогостоящим процессом, особенно для малых и средних компаний, не достигших серьезного уровня доходности.

Как же устроена работа бирж? В упрощенной форме это можно объяснить следующим образом. Участники торгов посылают в биржевую систему свои предложения по сделкам: какой инструмент и по какой цене они желали бы купить или продать. Затем весь объем этих предложений, или «ордеров», анализируется программным обеспечением биржи, задача которого — найти прямое сопоставление встречных заявок, чтобы сформировать из них сделку. Допустим, кто-то из биржевых трейдеров желает продать сто унций золота по цене $1300 за унцию, а кто-то за эту же цену хочет определенный объем золота приобрести. В случае существования подобных ордеров в один момент времени биржа осуществляет их «матчинг», то есть регистрирует совпадение трейдерских торговых пожеланий. После чего сделка считается заключенной — один трейдер отдает золото и забирает деньги, а другой, получая это золото, расстается с оговоренной в ордере суммой.

Понятно, что ордеров, не нашедших свою встречную «пару», в системе всегда гораздо больше, чем тех, которые были исполнены при формировании сделки, поэтому биржевая платформа постоянно отображает наборы ордеров по спросу и предложению на каждый отдельно взятый торгуемый инструмент. Ордера сортируются от наилучшей цены к наихудшей, и те два, которые представляют собой наиболее близкие значения между спросом и предложением, находятся на самой вершине списка. Ценовая разница между ними составляет понятие «биржевого спреда», то есть минимального котировочного разрыва, препятствующего матчингу, то есть совершению сделки. Небезосновательно считается, что ценообразование на биржевые активы, стихийно формирующееся в процессе торгов, является наиболее справедливым и максимально приближенным к текущим рыночным значениям. Разумеется, это утверждение будет верным лишь при условии, что на бирже имеется достаточно большое количество участников, торгующих данным инструментом значительными объемами — другими словами, только когда инструмент имеет высокую ликвидность.

Очевидно, что когда в мире появилось такое явление, как криптовалюта, у ее владельцев автоматически возникла необходимость в электронных торговых площадках для обмена этих инструментов нового типа сначала на фиатную валюту, а затем и на другие криптоактивы. В разделе, посвященном биткоину как инвестиции, были описаны первые криптобиржи, которые на данный момент уже прекратили свое существование. Значительные потери криптомонет по причине либо хакерской атаки, либо внутренних злоупотреблений привели к банкротству первой наиболее популярной биржи Mt. Gox. Тем не менее впоследствии начали появляться новые торговые криптоплощадки, более устойчивые к факторам внешней и внутренней среды. Многие из них сумели развить свою деятельность до поистине мировых масштабов, оперируя суточными объемами торгов, которые исчисляются миллиардными суммами в долларовом эквиваленте.

Конечно же, совокупный объем торгов по всем биржам криптоиндустрии еще весьма далек от классических бирж. Даже на пике своей популярности в декабре 2017 года общий объем торгов на криптобиржах составлял около $50 млрд в сутки, в то время как среднесуточный объем на Нью-Йоркской фондовой бирже (NYSE) насчитывает около $1,5 трлн. Не так далеко от нее отстоит и биржа NASDAQ со средними объемами $1,3 трлн в сутки. К весне 2019 года объемы криптовалютных торгов и вовсе снизились до $30 млрд в сутки. Однако не будем забывать о том, что криптовалютная индустрия еще очень молода, подвержена существенным ценовым колебаниям и находится под значительным регулятивным давлением, в отличие от своих классических собратьев.

Появление тысяч новых криптопроектов потянуло за собой массовые эмиссии различных криптотокенов, владельцам которых очень хотелось получить для них монетарную биржевую оценку. Для этого разработчикам проектов было необходимо договориться хотя бы с одной относительно популярной биржей, чтобы их токены стали доступными для торгов. В период криптовалютного хайпа это была задача не из простых, а точнее сказать, не из дешевых. Интеграция каждой новой криптовалюты влекла за собой целый комплекс необходимых процедур, связанных с изменением программного обеспечения биржевых торговых платформ.

Не последнюю роль играли также вопросы безопасности — ведь если в программном коде проекта, выпускающего новые токены, существовали уязвимости, они автоматически «унаследовались» и самой биржей, которая должна была хранить значительное количество торгуемых криптоактивов в своих депозитариях. В случае успешных хакерских атак биржи рисковали утратить значительную часть этих токенов и были бы вынуждены возмещать ущерб трейдерам из собственных капитальных резервов. Только за первую половину 2018 года с криптобирж было украдено средств на $761 млн, а совокупные биржевые кражи за все время существования криптоиндустрии уже исчисляются миллиардами. Не в последнюю очередь из-за этого «входной билет» для желающих поместить свои токены на особенно популярные криптобиржи исчислялся миллионами долларов. В дополнение к этому существовала вероятность, что через какое-то время эти токены ожидает процедура делистинга (исключения из биржевого списка торгов). Это могло произойти в первую очередь из-за низких объемов торгов данными инструментами, что сделало бы процесс их поддержания в биржевых системах низкоэффективным или даже убыточным.

Большинство моделей построения криптовалютных бирж созданы на основе принципов централизации в виде классической архитектуры «клиент — сервер». Другими словами, трейдер должен подключаться к биржевому серверу, а также пересылать в депозитарий биржи

свои активы (как фиатные, так и криптовалютные) для того, чтобы получить возможность ими торговать. С этого момента он утрачивает контроль над собственными торговыми средствами и делегирует бирже все вопросы, связанные с безопасностью их хранения. Ему необходимо доверять биржам, по крайней мере до тех пор, пока он не решает отозвать свои средства обратно на свои криптокошельки или банковские счета.

История знает немало случаев, когда трейдеры не по своей воле навсегда расставались со своими активами полностью или частично. Происходило это из-за разного рода проблем, связанных как с хакерскими атаками, так и с вредоносными действиями самих сотрудников или владельцев биржевых площадок. Также централизованные криптобиржи всегда были и будут уязвимы для действий репрессивного характера со стороны силовых или регулирующих органов тех юрисдикций, где они зарегистрированы. Все эти факторы в своей совокупности привели к тому, что в индустрии стали появляться биржи, технологически построенные совершенно по иному принципу.

Давайте вспомним, что сама природа криптоактивов базируется на децентрализованных началах. А если это так, то было бы совершенно логичным строить биржевые системы также на основе распределенной архитектуры — когда у трейдера не было бы необходимости отдавать под контроль организаторам биржевых торгов, то есть третьим лицам, свои активы. Другой вопрос, какие преимущества и недостатки несет в себе децентрализованный принцип построения биржевой площадки. Безусловно, централизованная биржа будет работать гораздо быстрее и надежнее в части нахождения и подтверждения матчинга ордеров, поскольку все торговые заявки находятся в одном месте и доступны для анализа алгоритмам биржевой платформы.

У децентрализованных бирж сервера, разумеется, отсутствуют. Каждый трейдер оперирует персональной клиентской платформой, которая обменивается информацией с другими такими же терминалами через прямые соединения по принципу peer-to-peer («равный к равному»). Где же тогда хранится база ордеров, каким образом осуществляется их матчинг, а также как исполняются сделки, включая физическое перемещение торгуемых активов между контрагентами?

Если детально не рассматривать механизмы работы децентрализованных бирж, то в общем случае все отправленные в систему ордера реплицируются между всеми ее участниками. При этом узлы биржевой сети самостоятельно осуществляют матчинг ордеров, предлагая остальным участникам варианты по сопоставлению сделок, чтобы сеть выбрала лучшие из них по согласованным параметрам оценки, приходя таким образом к общему консенсусу. Иногда сеть может делиться на так называемые «федерации», когда во главе каждой из них стоит или выборный, или специально назначенный узел. Данные субъекты системы отвечают как за распространение информации в своем сегменте, так и за матчинг ордеров внутри него, взимая за это комиссию. Правда, в этом случае информация не покидает пределы своих федераций, ограничивая ликвидность торгуемых инструментов, но зато существенно ускоряя общий процесс работы биржи.

Очевидным преимуществом децентрализованных бирж является отсутствие централизованного руководящего субъекта, способного контролировать процесс торгов, вмешиваться в него или пытаться проводить ценовые манипуляции. Для хакеров децентрализация создает непреодолимые препятствия по несанкционированному доступу в общее хранилище активов, поскольку таковое просто отсутствует. Все активы хранятся на компьютерах участников сети под их собственным контролем, а сами участники при этом анонимны, так как в подобной среде не проводится их идентификация в силу того, что проводить ее некому и негде.

Наконец, такие биржи практически неуязвимы для регулятивных воздействий — их работу просто невозможно остановить каким-либо административным предписанием, а счета трейдеров не могут быть заморожены или конфискованы. Теоретически возможно вывести из строя один или несколько узлов биржевой сети, но сделать это со всей сетью исключительно сложно. Тем не менее даже децентрализованные биржи нуждаются в минимальном управлении — хотя бы для того, чтобы разрабатывать и актуализировать общие правила проведения торгов, а также вести листинг торгуемых инструментов. Как правило, эти задачи реализуются через выборные комитеты, однако процесс их формирования подчас непрозрачен, и в ряде случаев результатом является появление управляющего органа, практически целиком аффилированного со структурой разработчиков биржевой системы. Как нетрудно догадаться, такой подход фактически централизует работу биржи, нанося ущерб самой идее создания торговой системы на основе распределенной архитектуры.

Таким образом, децентрализованные биржи пока не получили должного распространения из-за ряда сложностей, связанных с их проектированием, и в первую очередь — из-за технологического несовершенства при обмене активов из разных блокчейн-сетей, несовместимых между собой. Дело в том, что в блокчейн-средах все транзакции являются безотзывными, и очень важно синхронизировать действия обеих сторон таким образом, чтобы ни у одного из контрагентов не возникло желание после получения активов отказаться от исполнения своей части обязательств. Поскольку постоянно надеяться на добрую волю контрагентов в распределенных системах не приходится, необходимо либо вводить посреднические элементы вроде эскроу-сервисов, либо изобретать иные способы гарантировать исполнение обязательств по сделкам.

Для решения этой задачи была разработана концепция так называемых «атомарных свопов». Слово «атом» в переводе с греческого языка означает «неделимый», хотя ученые давно сам этот факт опровергли. Тем не менее термин, что называется, прижился и даже используется в технологии блокчейн, чтобы показать, что обязательства по децентрализованной сделке должны быть гарантированно исполнены обеими сторонами без необходимости наличия доверия между ними. Принцип работы атомарного свопа подразумевает, что сделка либо будет выполнена в полном объеме обоими контрагентами, либо же будет отменена без финансового ущерба для всех участников процесса обмена активами. Непосредственная технологическая реализация атомарных свопов зависит от особенностей конкретных блокчейн-сред, внутри или между которыми проводятся сделки.

Первый атомарный своп был реализован 20 сентября 2017 года между блокчейнами Decred и Litecoin. Не вдаваясь глубоко в детали, отметим лишь, что подобные сделки потребовали дополнительных инфраструктурных надстроек над основными сетями, что, безусловно, осложнило процессы обмена. С тех пор многие команды блокчейн-технологов работают над совершенствованием концепции атомарных свопов, чтобы в обозримом будущем биржи с распределенной архитектурой смогли все же получить значимые преимущества над своими централизованными конкурентами.

Возвращаясь к тому, для чего, собственно, были созданы криптовалютные биржи, следует обратить внимание на две основные категории пользователей этого сервиса. Первая — это позиционные инвесторы, которые приобретают криптовалюты для долговременного хранения, чтобы извлечь из их роста значительный доход. Вторая — трейдеры-спекулянты, которые осуществляют инвестиции на краткосрочной или среднесрочной основе, чтобы попытаться получить доход как от роста, так и от падения стоимости определенных криптоактивов. Для понимания принципов и подходов спекулятивной торговли следует рассмотреть финансовый анализ ценовых движений криптовалютных инструментов.

Анализ криптовалютного рынка

На протяжении всей финансовой истории — от создания первых торговых площадок и до наших дней — биржевые трейдеры всегда стремились каким-то образом предсказывать ценовые движения на торгуемые активы. Со времен Средних веков и до начала XX века для этих целей использовался широкий спектр приемов — от астрологических и религиозных практик до применения подходов, которые можно даже считать близкими к научным. Разумеется, главенствующую роль в принятии инвестиционных решений играла добываемая всеми правдами и неправдами различного рода инсайдерская информация. Скорость получения открытой информации также играла важную роль — например, после сражения при Ватерлоо в июне 1815 года финансовый дом Ротшильдов первым получил известие о победе британской армии над войсками императора Наполеона. Это позволило банку Ротшильдов сначала основательно сбить цены на облигации правительства Великобритании, а затем в течение того же торгового дня скупить их уже по существенно более низкой цене.

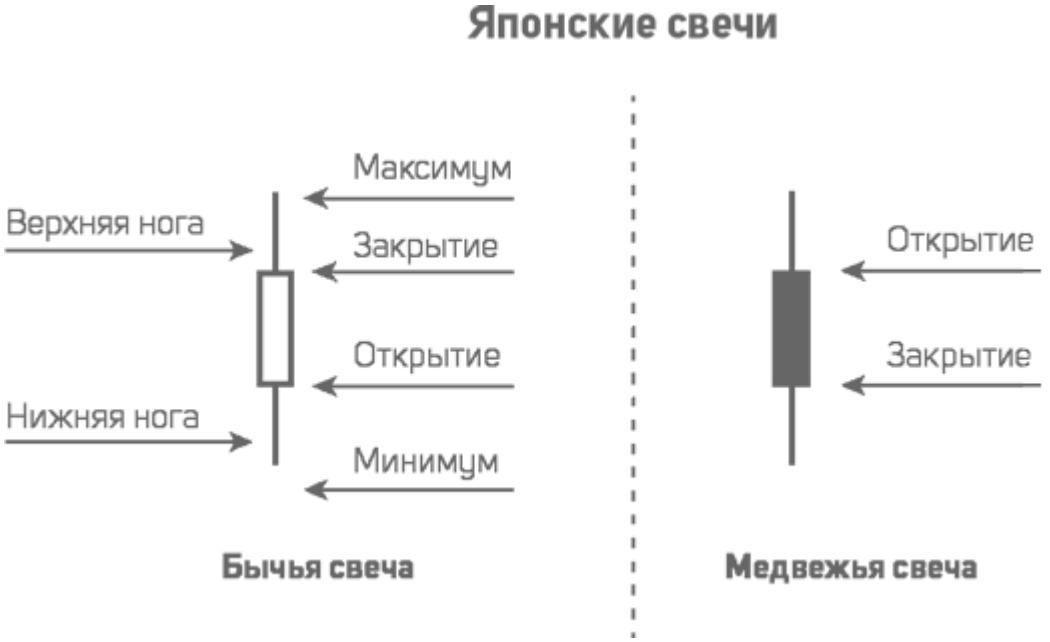
Однако подобные случаи были скорее исключением, чем правилом, поэтому в обычной торговой практике стали появляться попытки собирать и обрабатывать информацию, связанную с эмитентами тех или иных ценных бумаг, чтобы принимать взвешенные решения об их приобретении или продаже. В конечном итоге эти процессы эволюционировали в различные модели ценового прогнозирования, которые в своей совокупности и сформировали понятие анализа финансовых рынков. В современном финансовом мире широко применяются два основных вида рыночного анализа — фундаментальный и технический. Первый относится к методам прогнозирования на основе финансового анализа производственных и торговых показателей компаний — эмитентов ценных бумаг. Если же речь идет, например, о национальных валютах, то в ход идет рассмотрение макроэкономических показателей стран, выпускающих данную валюту. Также к важным показателям фундаментального анализа относятся значимые новости, связанные с эмитентом финансового инструмента — будь то компания или государство. Второй метод анализа — технический — имеет под собой чисто психологическую основу и базируется на анализе ценовых графиков торгуемых инструментов, а также применении к ним различных математических алгоритмов для выявления закономерностей движения цены. Рассмотрим оба вида анализа.

Считается, что появление фундаментального анализа связано с событием, произошедшем чуть менее ста лет назад, в 1934 году, когда была опубликована книга «Анализ ценных бумаг» за авторством двух американских экономистов Бенджамина Грэма и Дэвида Додда. В своей книге авторы постарались предложить системный подход к анализу ценных бумаг с целью определения их реальной стоимости относительно текущей рыночной. В результате такого анализа становилось возможным выявить либо недооцененность, либо явную переоцененность рассматриваемых биржевых бумаг, чтобы затем принять в их отношении соответствующее торговое решение. Впоследствии принципы фундаментального анализа получили активное развитие, существенно расширив спектр анализируемых факторов, которые в той или иной степени влияют на ценовые рыночные движения. В какой-то момент этих факторов стало так много, что критики подобных аналитических методов начали говорить о невозможности учесть абсолютно все события, влияющие на цену, поскольку большинство из них имеют труднопредсказуемый, а то и вовсе случайный характер.

Типичным примером применения фундаментального анализа для прогнозирования движения национальных валют является рассмотрение таких макроэкономических параметров, как инфляция, безработица или учетные ставки центральных банков. Как правило, изменение одного из этих показателей влечет за собой существенные ценовые изменения национальной валюты либо в сторону укрепления, если параметры экономически благоприятны, либо в направлении ослабления — в обратных случаях. Нередко рынки, питаемые слухами и предположениями, к моменту выхода фундаментальной новости уже могут исчерпать соответствующее ей движение и даже испытать обратную коррекцию в случае, если эффект от ожидания события оказался несколько завышен.

В отличие от своего фундаментального «коллеги», технический анализ опирается на уже произошедшие события, то есть на исторические котировки, из которых составляются графики ценовых движений на разных временных периодах. Затем, исследуя подобные графики, технические финансовые аналитики пытаются выявить ценовые паттерны, то есть относительно устойчивые закономерности движения цены на торгуемый актив. Основанием для подобного прогнозирования является предположение, что трейдерская психология срабатывает у всех участников рынка примерно одинаково, поскольку большинство из них руководствуется одними и теми же методами технического анализа.

Несмотря на то что главным инструментом технического аналитика является график ценовых котировок, построение которого, если не использовать компьютеры, требует серьезной ручной работы рутинного характера, этот вид анализа на пару сотен лет старше анализа фундаментального. Зародился он в Японии в XVIII веке после создания в Токио товарной биржи по торговле рисом. Около 1750 года трейдеры начали отмечать ценовые движения специальными рисунками, которые впоследствии назвали «японскими свечами». Такая свеча представляет собой графический конструктив, отображающий наиболее важные ценовые уровни за определенный временной интервал. Речь идет о цене на начало и конец периода, а также локальный максимум и минимум цены в пределах данного временного отрезка. При этом если свеча отражает восходящий рынок, то тело свечи «полое», а если нисходящий — окрашенное.

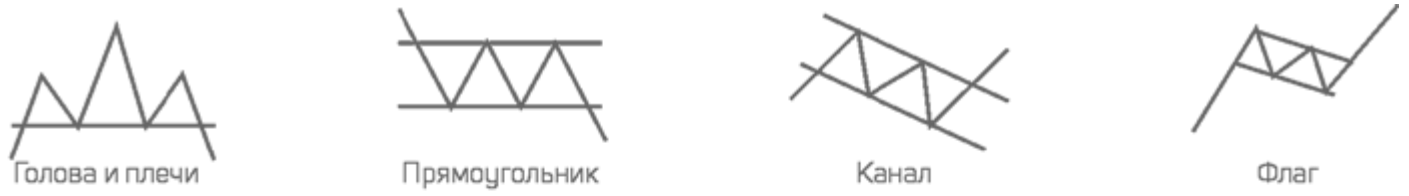


Японские рисовые трейдеры начали создавать подобные свечи в конце каждого торгового дня, а затем, накопив достаточную статистику, стали искать закономерности движения цены в зависимости от сочетания получившихся свечных фигур. Комбинации начали получать свои уникальные названия, а затем их стали определенным образом трактовать, предсказывая рыночные движения. Впоследствии из этих толкований были составлены объемные манускрипты, описывающие всевозможные комбинации свечных фигур и связанные с ними прогнозы ценовой динамики.

С появлением и развитием компьютерной техники технический анализ пережил свое второе рождение — теперь составление графиков можно было поручить вычислительным машинам, существенно расширив как временной охват, так и количество возможных графических элементов для анализа. Используя сначала алфавитно-цифровые, а затем и графические дисплеи, аналитики начали применять к массивам исторических котировок математические алгоритмы с различными техническими индикаторами.

Благодаря анализу ценовых графиков в относительно широких временных диапазонах появилась возможность выявлять так называемые «тренды», то есть однозначно направленные тенденции движения цены. Комбинаторика графически отображаемых ценовых изменений позволила старинному японскому графическому анализу фигур пережить второе рождение, только уже в современной интерпретации. В

технической аналитике стали мелькать такие термины, как «голова и плечи», «двойные и тройные вершины», «треугольники» и «ромбы» — как графические фигуры продолжения или изменения трендовых движений.



Разумеется, и у технического анализа нашлись свои критики, которые небезосновательно считали, что исследование ценовой истории имеет мало общего с ценовым будущим. Говорилось также, что любая относительно значимая фундаментальная новость неизбежно разрушает все ранее сделанные технические прогнозы в силу историчности, а значит, реактивности отображаемых процессов на ценовых графиках. Тем не менее и у фундаментального, и у технического анализов существует огромное количество последователей, в большинстве случаев использующих сразу оба аналитических направления, полагая, что одно всегда дополняет другое. Каждый день в финансовом мире появляется множество аналитических статей и прогнозов в отношении всех финансовых инструментов, котирующихся на рынках.

Криптовалюты также не стали исключением. Но давайте порассуждаем, какие виды анализа могут быть применимы к данному типу финансовых активов и почему. Начнем с того, что подавляющая часть фундаментального анализа для криптовалют подходит достаточно слабо в силу отсутствия централизованного эмитента и, как следствие, невозможности его экономического анализа. В первую очередь это относится к криптовалютам на основе децентрализованного конкурентного майнинга, таким, как биткоин, эфир и им подобные. А это означает, что никакие суверенные макроэкономические показатели различных государств или их объединений (например, ЕС) не могут оказать прямого влияния на стоимость децентрализованных криптоактивов. Справедливости ради следует признать, что косвенное влияние на стоимость криптовалют все же будет, но только в части влияния макроэкономического индикатора на ту фиатную валюту, к которой непосредственно торгуется сам криптоактив. Однако в настоящее время это влияние ничтожно, и в анализе ценового движения криптовалют им можно смело пренебречь.

Тем не менее фундаментальные новости для криптовалют существуют и могут значительно влиять на их стоимость. Другое дело, что подобные новости в большинстве случаев производят однократный эффект, поскольку часто связаны с решениями национальных правительств об ограничении или запрете хождения криптовалют. Более того, существует довольно ограниченный набор стран, новости из которых могут оказать серьезное влияние на криптовалютные котировки. Это в первую очередь Китай, США, Южная Корея и Япония, то есть страны, где сосредоточены наибольшие объемы торговли криптовалютами на соответствующих биржах.

В случае если криптоактив выпускается централизованно и, что очень важно, является не утилитарным, а инвестиционным токеном, то фундаментальный анализ отчасти применим и к оценке показателей управляющей компании-эмитента. Классическая оценка здесь едва ли может быть использована в силу того, что управляющая компания в большинстве случаев представляет собой недавно созданный

стартап, который, как правило, еще даже не начал извлекать из проекта монетарную прибыль. Поэтому в анализе следует уделять внимание таким типичным для стартапов параметрам, как опыт членов команды разработчиков проекта, предлагаемая к реализации стратегия, актуальность продукта и его рыночное позиционирование, объем привлеченных инвестиционных средств, наличие MVP и так далее.

Гораздо более эффективным в отношении криптовалют выглядит анализ технический, поскольку он, как уже упоминалось, завязан на психологию участников рынка. А это означает, что поведенческие паттерны криптотрейдеров немногим отличаются от тех, что мы привыкли видеть на рынках классических. Многие технические аналитики признают работоспособность различных индикаторов, и в первую очередь графических — речь идет как о трендовых линиях, так и о специальных фигурах, подающих трендовые сигналы. Немаловажную роль играют также сильные ценовые психологические уровни, характеризующиеся «красивыми» значениями — 1, 10, 100, 1000 и так далее.

Как уже отмечалось, технический анализ исторически предшествовал фундаментальному, поскольку его принципы опираются на легко собираемые данные о торгах на конкретных площадках и обращены «назад» во времени. По мере упорядочивания сбора и циркуляции информации об эмитентах или макроэкономических показателях государств в помощь техническому анализу приходит фундаментальный. В этих аспектах криптофинансы во многом повторяют путь фиатных торгуемых инструментов.

В заключение хотелось бы сказать несколько слов о торговых стратегиях, применяемых трейдерами на криптовалютных рынках. Как и на классических финансовых рынках, глобально можно выделить два стратегических подхода — спекулятивный и позиционный. Первый — это краткосрочный, при внутридневной торговли, когда позиции открываются и закрываются трейдером в течение одного дня, до поддержания позиций в течение нескольких дней, максимум недели. Подобная стратегия подразумевает, что торгуемая криптовалюта имеет достаточно хорошую волатильность, то есть высокие амплитуды возможных котировочных колебаний, и можно получить прибыль, правильно «поймав» нужный ценовой выброс.

Второй — инвестиционный — описывается принципом buy and hold, то есть «купить и держать». Такие торговые позиции инвесторы могут держать месяцами и даже годами — в надежде на существенный рост цены. Однако, бывает и так, что за время содержания позиции торгуемый криптоактив может достигать как исторических пиков, так и беспрецедентных провалов своей стоимости. Долгосрочных держателей криптовалютных портфелей на сленге называют «ходлерами» — от искаженного английского слова hodl (hold — «держать»). Это популярное в криптосреде слово было запущено в оборот в декабре 2013 года одним из пользователей популярного форума BitcoinTalk. Будучи в состоянии алкогольного опьянения (как потом признался сам автор мема), он допустил ошибку и написал I am hodling, и эта фраза была подхвачена другими участниками форума. Впоследствии она получила широкое распространение в качестве описания консервативного инвестиционного поведения с расчетом на долгосрочный восходящий ценовой тренд.

Заканчивая раздел, посвященный инвестициям в криптовалюты, хотелось бы обратить внимание на одну немаловажную проблему, с которой сталкивается множество инвесторов, особенно тех, которых можно описать тем самым словом «ходлеры». Речь идет о долговременном хранении приобретенных криптовалют в условиях относительно нестабильной среды, в которой обращаются критоактивы. Здесь можно упомянуть целый ряд факторов: и технологические уязвимости в коде криптокошельков, и хакерские атаки, и банкротства криптобирж. Недостаточное внимание к вопросам безопасности и управления рисками приводит к печальным для инвестора последствиям. Теме управления этими рисками и будет посвящена следующая глава.

Хранение криптоактивов

В разделе, посвященном биткоину как инвестиции, был описан случай с норвежским студентом, который, работая над дипломом по теме криптографии, закупил для тестовых целей несколько тысяч биткоинов за символическую сумму. Позабыв о своем приобретении на годы, он впоследствии обнаружил, что цена на имеющиеся у него криптоактивы взлетела до небес. Ему пришлось потратить изрядное количество сил и времени на то, чтобы восстановить доступ к своему биткоин-кошельку. История имела счастливое завершение, поскольку бывшему студенту все же удалось восстановить пароль от своего кошелька, и он смог в полной мере распорядиться неожиданно обретенным богатством.

Однако не все истории заканчивались столь же благополучно — владельцы криптомонет нередко утрачивали свои секретные ключи от кошельков самыми разными способами. Самый популярный из вариантов потерь — это банальный выход из строя компьютерного оборудования, в первую очередь жестких дисков, где хранились драгоценные данные. Решение проблемы безопасного хранения цифровых монет стало одним из наиболее востребованных у молодого криптосообщества, поэтому индустрия не замедлила отреагировать на возникший общественный запрос. Это выразилось в планомерном выпуске в свет различных проектов, позволяющих с разной степенью успешности решать задачу относительно надежного сбережения криптоактивов, ценность которых возрастала с

каждым днем. Попробуем теперь разобраться в том многообразии методов хранения криптовалют, которые доступны пользователям на сегодняшний день.

Как и обычные фиатные деньги, криптовалюты хранятся в специальных кошельках. Глобально существует разделение на два типа криптокошельков — на так называемые «горячие» и «холодные». Горячие кошельки — это те, которые расположены на устройствах пользователей, подключенных к интернету, либо же представляют собой централизованные интернет-сервисы, которыми в том числе могут быть и криптобиржи. Криптовалютные средства, хранящиеся на горячих кошельках, в любой момент доступны для осуществления с ними транзакций, другими словами — для траты. Холодными же называют кошельки, которые не имеют постоянной связи с телекоммуникационным миром и чем-то напоминают сейф — прежде чем потратить содержащиеся на них криптоактивы, необходимо провести ряд процедур, чтобы извлечь их из хранилища.

Горячие кошельки делятся на те, которые их пользователи контролируют самостоятельно, и на такие, где функции управления и контроля делегированы третьим сторонам, то есть централизованным сервисам. Как известно, права на обладание криптосредствами обеспечиваются контролем над соответствующими приватными ключами от счетов, к которым они привязаны. Поэтому каждый пользователь решает сам: возьмет ли он на себя труд и риск содержать самостоятельно свои приватные ключи и обеспечивать безопасность их хранения, либо же эти функции он доверит одному из популярных интернет-сервисов, предоставляющих функционал кошельков для различных криптовалют. Первый способ подразумевает, что пользователь должен стать узлом соответствующей блокчейн-системы. Это означает, что ему придется полностью или хотя бы частично загрузить на свое устройство базу данных блоков, к которой привязаны его криптосредства. Обычно для этого требуется выделить значительное место на локальных устройствах хранения данных и постоянно актуализировать базу блоков, что может занимать определенное время.

Уязвимости этого способа хранения криптосредств заключаются в том, что устройство пользователя, будучи подключенным к интернету, может быть подвержено хакерским атакам с целью похитить приватные ключи. Кроме того, существует множество различных компьютерных вирусов — так называемых «троянских коней», которые могут внедрить на компьютере пользователя специальный код для поиска приватных ключей от различных блокчейн-сред и пересылки их разработчику вируса. Обладание же приватным ключом от блокчейн-адреса равносильно получению полного контроля над находящимися на нем криптомонетами. Наличие целого букета угроз безопасности при самостоятельном поддержании инфраструктуры приватных ключей заставляет многих технически неискушенных пользователей доверять свои криптосбережения профессионалам. Речь идет о сервисах, предлагающих централизованные решения для хранения различных криптовалют.

Несомненно, отсутствие полного контроля над собственными криптосредствами может вызывать у владельцев беспокойство за их сохранность. Само собой разумеется, что все популярные проекты централизованного хранения криптовалют уделяют повышенное внимание вопросам защиты от взлома, имея в штате квалифицированных специалистов по компьютерной безопасности. Тем не менее подобные сервисы подвергаются рискам хакерских атак в гораздо большей степени, чем частные владельцы криптовалют. А к технологическим угрозам добавляются также риски иного свойства — связанные с возможными злоупотреблениями со стороны владельцев или сотрудников управляющих проектами компаний. История с пропавшими биткоинами биржи Mt. Gox еще у многих свежа в памяти, а это далеко не единственный случай, когда пользователи централизованных сервисов по тем или иным причинам теряли свои криптоактивы.

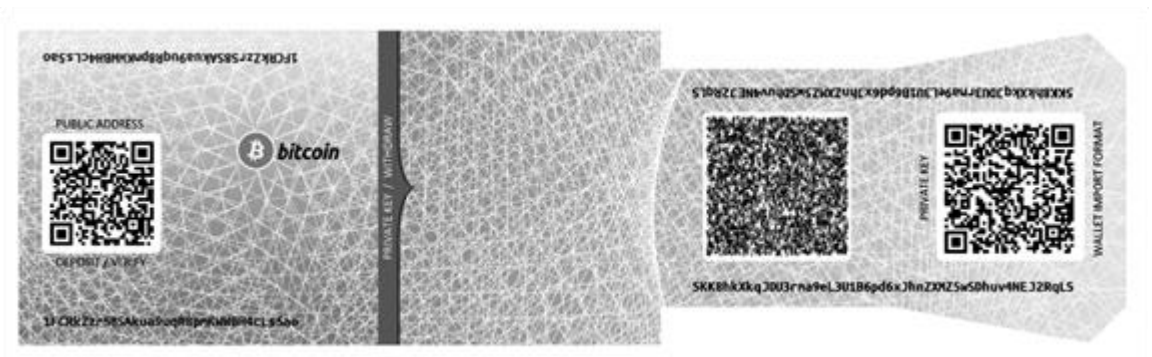
Управление рисками для пользователей централизованных сервисов хранения криптовалют должно выражаться в первую очередь во взвешенном подходе к выбору самой площадки. Необходимо учесть такие факторы, как продолжительность существования компании, ее история и репутация, а также отсутствие прецедентов по взлому системы безопасности и хищения криптоактивов. Юрисдикция регистрации и наличие лицензии также имеют большое значение — по крайней мере, это означает, что деятельность компании находится под регулятивным надзором, подразумевающим постоянное прохождение разного рода аудитов — финансовых и технологических. Учитывая всевозможные риски, вполне реально выбрать подходящую форму хранения своих криптосбережений на горячих кошельках, однако если пользователь стремится в вопросах безопасности к абсолюту, ему имеет смысл сосредоточиться исключительно на кошельках «холодного» типа. Какие же преимущества и недостатки имеет этот вид хранения криптовалют?

В роли холодного хранилища может выступать любое компьютерное устройство, не имеющее подключения к интернету. Большую популярность приобрели аппаратные решения, с виду напоминающие обычные устройства флеш-памяти. Собственно говоря, подобные аппаратные кошельки в большой степени ими и являются, с той лишь разницей, что на них содержится специальное программное обеспечение для хранения криптовалют. Часто эти устройства оснащены небольшим жидкокристаллическим экраном, на котором при подключении устройства к компьютеру отображается различная полезная информация, например, состояние криптовалютного баланса кошелька.

Устройства подключаются к компьютерам только в момент совершения транзакции, поэтому украсть с них приватный ключ — дело исключительной сложности. Кроме того, некоторые устройства содержат еще и специальную кнопку формирования электронной подписи транзакций, которую необходимо физически нажимать при осуществлении перевода, что делает похищение секретной информации делом практически неосуществимым. Наиболее популярными моделями аппаратных криптокошельков на текущий момент являются Trezor, Ledger Nano S и KeepKey. Все они — из числа недешевых, но при этом обеспечивают достаточно высокий уровень безопасности хранения криптовалют. Что само по себе исключительно важно, особенно если речь идет о хранении сумм, имеющих значительный фиатный эквивалент.

Для самых крупных частных или институциональных владельцев криптовалютных запасов существуют даже специальные подземные бункеры, которые по степени защищенности мало чем отличаются от самых серьезных банковских хранилищ. В мире существуют компании, которые предоставляют достаточно дорогой, но исключительно надежный сервис по хранению значительных объемов цифровых ценностей. Массивные стальные двери, пуленепробиваемые стекла, барьеры от электромагнитного воздействия, строжайшая форма идентификации посетителей — вот неполный перечень атрибутов мест, где хранятся криптоактивы на миллиарды долларов в виде приватных ключей их владельцев. Несмотря на то что подобные структуры находятся под постоянными атаками киберпреступников, еще никому не удавалось преодолеть все каскады защиты, чтобы завладеть хотя бы одним из хранимых там секретных ключей.

В завершение описания видов холодного хранения криптовалют нельзя не отметить еще один весьма простой, но вместе с тем достаточно защищенный способ. Речь идет, как ни странно, о кошельках, представленных в обыкновенной бумажной форме. В конце концов, если владение криптовалютным счетом базируется исключительно на контроле связанного с ним приватного ключа, то почему нельзя его просто распечатать на бумаге и хранить в сейфе или даже банковской ячейке? В интернете существует немало сервисов, позволяющих превратить любой блокчейн-счет в распечатку с парой QR-кодов, отображающих публичный и приватный ключи. Существует дополнительная возможность повышения безопасности путем шифрования ключей специальным паролем — это необходимо для случаев, если бумажный кошелек будет украден или даже просто сфотографирован злоумышленником.



Такие бумажные кошельки часто используются для передачи криптовалют в подарок третьим лицам, у которых пока нет соответствующего программного обеспечения и ранее созданных счетов в блокчейн-системах. Имея на руках «бумажный сертификат» с парой ключей и кодами к ним, новые владельцы могут в любой момент перенести лежащие на них криптосредства в любой из выбранных горячих кошельков и затем, при необходимости, совершать с ними транзакции.

Описанными в данной главе методами хранения криптовалют список отнюдь не исчерпывается. Существуют еще несколько менее распространенных методов, например, кошельки с мультиподписью или фрагментированные ключи. В первом случае для отправки транзакции необходимо иметь несколько приватных ключей, то есть речь идет о совместном подтверждении переводов средств с кошелька. Второй метод подразумевает, что приватный ключ разбивается на несколько частей, которые хранятся в разных местах.

Возможно, в ближайшем будущем появятся и совершенно новые методы хранения «цифрового золота». Однако почти у всех владельцев криптовалют возникает один и тот же вопрос: какая стратегия ее хранения является оптимальной?

Совокупный опыт представителей криптосообщества свидетельствует о том, что наиболее приемлемой и удобной формой хранения криптоактивов является комбинация горячего и холодного кошельков. То есть основные крипторезервы следует хранить на оффлайновых аппаратных кошельках, а подчас даже и на бумажных, в то время как на горячих кошельках целесообразно держать лишь небольшие суммы для того, чтобы в любой момент иметь возможность совершать с ними транзакции. Или же если владелец криптовалют является активным биржевым трейдером и ему необходимо постоянно проводить торговые операции, то большая часть его активов будет лежать на биржевых кошельках, хотя это и сопряжено с дополнительным риском. Так называемые «ходлеры», которые серьезно вложились в криптовалюты на долгосрочной основе, безусловно, большую их часть будут хранить на холодных кошельках как на наиболее безопасных.

Если построить график, отображающий интерес мирового сообщества к криптовалютам, мы увидим кривую, имеющую в разное время свои взлеты и падения. На направление движения этого графика оказывает влияние множество различных факторов — социальных, деловых, регулятивных, а также чисто технологических. Во многом от последнего из перечисленных факторов будет зависеть, смогут ли криптовалюты в обозримом будущем хотя бы в какой-то значимой степени потеснить в мировой экономике валюты фиатные. На пути активного развития блокчейна стоит еще множество сложных проблем, не имеющих на данный момент оптимального решения и не позволяющих криптовалютам конкурировать с их фиатными «коллегами» на равных. Какие же актуальные задачи стоят перед технологией блокчейн и в каком направлении следует искать пути их решения?

Актуальные проблемы блокчейн

Большинство людей в развитых странах привыкли использовать для оплаты товаров и услуг удобные банковские карты вместо наличных денег. Платежные карты давно и прочно вошли в повседневный обиход, несмотря на некоторые неудобства, связанные с их использованием. Ведь карты легко могут быть утеряны или украдены вместе с бумажником. Их могут скопировать в момент передачи недобросовестным продавцам для оплаты, при этом подпись можно подделать, а пин-код — подсмотреть. Еще более благоприятной средой для мошенничества является интернет, где орудует множество банд киберпреступников. Только в 2014 году совокупные потери от хищений средств с банковских карт во всем мире составили более $16 млрд, и эти цифры с каждым годом только растут. Почему же мировая финансовая индустрия не спешит переводить карточные платежи в форму, казалось бы, несоизмеримо более безопасных криптовалютных операций?

Для того чтобы ответить на этот вопрос, необходимо понять масштабы объемов транзакций, проходящих внутри хотя бы одной из самых популярных карточных систем — Visa или Mastercard. В обычные дни финансовые потоки в этих системах измеряются тысячами транзакций в секунду. В периоды же повышенной активности, например, в дни предновогодних распродаж, пиковые нагрузки могут составлять 20 000–40 000 транзакций в секунду. А теперь подсчитаем, что в этом плане могла бы предложить самая популярная платежная блокчейн-система — сеть Биткоин.

Как мы помним, размер блока в этой системе составляет 1 мегабайт, а средняя транзакция занимает объем около 250–300 байт при том, что каждый новый блок в сети формируется в среднем за 10 минут. Нехитрые расчеты показывают, что пропускная способность сети Биткоин составляет примерно семь транзакций в секунду, после чего ее следует сравнить с показателями скорости обработки операций в крупных карточных сетях. И это только один параметр, по которому мы пытаемся сравнивать две принципиально разные финансовые технологии. Более того, этот показатель — всего лишь одна из составных частей большой проблемы, которая стоит на пути возведения криптовалют в относительно равный конкурентный статус с фиатными средствами платежей. Имя этой проблемы — масштабируемость.

Технология блокчейн сама по себе обладает массой достоинств, которые мы самым детальным образом рассмотрели в этой книге. Теперь же пришло время поговорить и о некоторых ее недостатках, а точнее — о тех аспектах, которые препятствуют быстрому распространению продуктов, базирующихся на технологии распределенного реестра. Блокчейн-продукты имеют слабо выраженную способность к масштабированию, в первую очередь из-за скорости подтверждения транзакций, а также из-за постоянно нарастающего объема базы данных блоков в силу невозможности удаления ранее помещенной в них информации. Другими словами, если условием задачи является быстрая обработка огромного количества микротранзакций, блокчейн с этим будет справляться далеко не лучшим образом.

Представим ситуацию, когда платежная система, построенная на базе блокчейн-технологии, учитывает, скажем, приобретение чашки кофе в одной из крупных сетевых кофеен типа Starbucks. Речь идет о транзакции с передачей ценности в эквиваленте нескольких долларов. Сначала транзакция должна быть подтверждена, то есть помещена в блок, который будет принят всей децентрализованной

сетью. А затем, для верности, помимо этого блока, в нисходящую за ним цепочку должны поместиться еще как минимум несколько последующих блоков. Этот процесс, безусловно, займет определенное время. Вопрос, будут ли ждать покупатель и продавец минуты, а то и десятки минут, чтобы платежная транзакция получила все необходимые подтверждения? С большой долей вероятности они выберут более быстрый способ подтверждения оплаты.

Теперь обратимся еще к одной важной детали — чашек кофе может быть очень много. Считается, что в мире ежедневно выпивается минимум 1,5 млрд чашек кофе, немалая часть из которых приобретается в ресторанах и кафе. Если связанные с ними платежные операции начать помещать в блокчейн, то база данных блоков будет расти в своем размере космическими темпами. А ведь речь идет о децентрализованной форме хранения данных, что подразумевает постоянную репликацию и синхронизацию данных между всеми полными узлами сети. Современные блокчейн-среды физически неспособны обрабатывать такое количество мелких транзакций, при том, что мы рассмотрели всего лишь одно наименование товара — чашку кофе. Из чего напрашивается вывод, что классическая модель записи и хранения транзакционной информации в блокчейн никоим образом не годится для учета массовых микротранзакций — ни по скорости обработки, ни по требуемым объемам хранения данных. Каким образом можно было бы решить эту проблему?

Одним из вариантов решения может стать так называемый «шардинг» (от английского слова shard — «осколок»). В отличие от избыточного копирования полной базы данных блоков между участниками сети, концепция шардинга в технологии блокчейн подразумевает разделение базы данных на определенное количество частей, каждая из которых копируется только определенной группе сетевых узлов. Для поддержания целостности распределенной инфраструктуры данных необходим точный математический расчет количества частей полной базы, объема каждой из них и количества узлов в каждой из групп, хранящих свои сегменты базы данных. Понятие «целостность» в данном случае подразумевает близкую к 100% гарантию того, что в любой момент времени каждому из узлов сети будет доступна для синхронизации любая из частей полной базы данных блоков.

В настоящее время многие разработчики блокчейн-проектов занимаются исследованием возможностей внедрения концепции шардинга. Одной из первых о подобных разработках объявила команда девелоперов проекта Ethereum во главе с Виталиком Бутериным. Но какая-либо работоспособная модель шардинга на суд общественности до сих пор не представлена. Тем более что шардинг отнюдь не является панацеей от «раздуваний» баз данных блоков, а лишь позволяет получить временную отсрочку от негативного влияния данной проблемы. Шардинг однозначно улучшит ситуацию в блокчейн-средах, где микротранзакции либо отсутствуют полностью, либо не являются доминирующим транзакционным типом. Что же касается платежных блокчейн-систем, претендующих на массовое использование в повседневной жизни, гораздо более перспективным решением проблемы масштабирования выглядит концепция протокола «молниеносной сети» — Lightning Network.

При попытке адаптации сети Биткоин к микроплатежам мы сталкиваемся еще с одной проблемой — комиссионной. Как известно, в данной сети присутствуют транзакционные комиссии, которые собираются майнерами при формировании блоков. Помимо монетарной мотивации майнеров, комиссии выполняют еще одну важную функцию — защиту от транзакционного спама, который теоретически может серьезно замедлить скорость работы сети. В фиатном эквиваленте комиссии могут составлять приличные суммы, что делает формирование микротранзакций делом совершенно бессмысленным. Если чашка кофе, к примеру, стоит $2, а комиссия за транзакцию по ее оплате составит близкую сумму, кто же будет готов отдать двойную цену ради удовольствия оплатить покупку криптовалютой? Вот как раз для таких ситуаций и была разработана модель Lightning Network.

Фактически Lightning Network является инфраструктурной надстройкой над блокчейн-системой. При этом речь идет не только о сети Биткоин — подобные концепты разрабатываются и для других популярных блокчейн-сред. Сеть «молниеносных переводов» состоит из узлов, которые, образуя пары между собой, формируют так называемые двунаправленные «платежные каналы». Каждый из двух узлов блокирует определенную величину средств для созданного канала, сумма которых и составляет его платежную пропускную способность. При этом узлы могут образовывать каналы с несколькими узлами одновременно, создавая целую сеть, внутри которой могут формироваться пути для быстрых транзитных операций с невысокой комиссией.

Передача средств осуществляется путем изменения взаимных балансов на узлах канала до тех пор, пока на одном из узлов не закончатся средства, то есть канал не будет считаться «истощенным». В любой момент узлы могут закрыть канал и зачислить в свою пользу средства, равные актуальному взаиморасчетному балансу. Таким образом, быстро и исключительно дешево решается проблема микротранзакций для платежей популярными криптовалютами. Но эта модель также не лишена недостатков, главным из которых является отсутствие долгосрочной мотивации узлов сети поддерживать платежные каналы в силу скромного дохода. По текущим оценкам, содержание узла Lightning Network приносит его владельцу доход всего около 1% годовых. При этом каждый узел платежных каналов должен блокировать собственные средства для функционирования сети, оставаясь постоянно в режиме онлайн и подвергаясь, таким образом, риску хакерской атаки.

Еще одна проблема функционирования подобной сети — возможная избыточная централизация, когда на самых активных узлах может накапливаться значительная криптовалютная ликвидность. В случае отключения узла от сети средства других пользователей, направивших свои платежи через данную инфраструктуру, могут оказаться в долгосрочной блокировке. Существуют в этой сети и возможности для мошенничества, особенно если один из узлов канала надолго пропадает из сети. Тем не менее концепция модели Lightning Network продолжает свое активное развитие — только в сети Биткоин по состоянию на весну 2019 года имеется более 40 000 платежных каналов, и их число продолжает увеличиваться.

Следует добавить, что модель «молниеносной сети» не является единственным средством масштабирования блокчейн. Мы не будем подробно останавливаться на технологическом описании прочих концептов, таких как, например, направленные ациклические графы или методики уменьшения размера транзакции за счет изъятия из нее цифровых электронных подписей. Отметим лишь, что пока ни один из существующих методов не смог в полной мере решить проблему пропускной способности или избыточных объемов хранения данных.

Помимо чисто технологических, блокчейн имеет проблемы и социального характера. Как отмечалось в главе, посвященной майнингу биткоина и описанию протокола Proof-of-work, данный метод эмиссии криптовалют характеризуется исключительной энергоемкостью и косвенно наносит дополнительный ущерб окружающей среде. В силу своей концептуальной сложности очень многие пользователи плохо понимают все преимущества и недостатки технологии распределенного реестра. Влияние «криптовалютного хайпа» нередко приводит к тому, что отдельные представители делового сообщества пытаются перестраивать свои существующие проекты на блокчейн. Следует постоянно иметь в виду, что такая недостаточно продуманная стратегия вместо создания дополнительной ценности может разрушить даже вполне успешный до этого бизнес.

Регулятивная среда также редко бывает дружественной как к самим блокчейн-проектам, так и к методам их финансирования, в частности, посредством ICO. Имеются все основания предполагать, что в будущем строгость процедур регулирования блокчейн-индустрии будет лишь только усиливаться. К тому же не будем забывать, что владельцы криптовалют по определению анонимны, поэтому продавцам, принимающим к оплате криптосредства, придется выполнять регулятивные требования по идентификации своих клиентов. Что же касается крупных финансовых институтов, в первую очередь банков, то они в ряде случаев небезосновательно видят в технологии блокчейн угрозу самому своему существованию, поскольку она предполагает децентрализацию и устранение финансового посредничества. Хотя справедливости ради следует отметить, что многие банки начали применять блокчейн-технологии для оптимизации собственных издержек и повышения конкурентоспособности своих финансовых продуктов.

На текущий момент с уверенностью можно констатировать лишь несколько основных выводов: что блокчейн является весьма перспективной технологией, что у нее есть ряд достаточно серьезных проблем и что над их решением работают лучшие умы как мировой математической науки, так и IT-индустрии. Конечно, на это потребуется некоторое время, и быстрых прорывов ждать не приходится — криптосообщество будет решать задачи шаг за шагом. И затем, когда произойдет накопление определенной критической массы полезных идей, инструментов, моделей и концептов, они в своей совокупности смогут приблизиться к решению актуальных проблем, стоящих перед блокчейн-технологией.

Новая картина мира (заключение)

Прошло уже более десяти лет с момента, когда в первой блокчейн-сети проекта Биткоин появился генезисный блок. Это событие ознаменовало появление целой хайтек-индустрии и впоследствии повлияло на жизнь многих людей. Были те, кто сумел обогатиться на ранних инвестициях в криптовалюту, а также те, кто смог вовремя продвинуть заинтересовавшие инвесторов идеи, успев собрать значительные суммы на ICO. А были и иные, кто, поверив обещаниям разработчиков, вложил свои средства в новые криптомонеты, которые обесценились уже через несколько месяцев. Блокчейн-индустрия может вызывать восторги и разочарования, порождать надежды и их крушение, подвигать к тотальным изменениям в философии построения бизнес-моделей, равно как и приводить исследователей в технологические тупики, из которых, на первый взгляд, не существует выхода. Одним словом, идет нормальный эволюционный процесс, неизбежно сопровождающий любое жизнеспособное инновационное явление.

Есть мнение, что у технологии блокчейн больше вопросов, чем ответов, но давайте признаем, что десять лет — слишком малый срок, чтобы делать поспешные выводы. Американский физик, бывший министр энергетики США и лауреат Нобелевской премии Стивен Чу как-то сказал: «Каменный век закончился не потому, что закончились камни». Безусловно, технология блокчейн в данный момент все еще находится в своем собственном «каменном веке». Однако те принципы открытости обмена информацией, которые приняты в блокчейн-индустрии, дают все основания предполагать, что ее развитие будет происходить весьма быстрыми темпами. В первую очередь этому будет способствовать синергия всех вовлеченных в процесс специалистов — предпринимателей, инженеров и ученых. Ожидает ли блокчейн дальнейший эволюционный прогресс в виде «бронзового» и «железного» веков — покажет время. Несомненно

одно — мы имеем дело не только с новой концепцией учета, хранения и передачи ценности, но и с новой технологической философией, которая может вызвать тектонический сдвиг в устоявшейся тысячелетиями модели социальных и деловых взаимоотношений.

Речь идет в первую очередь о трансформации понятия посредничества. Блокчейн если и не устраняет эту роль полностью, то, по крайней мере, может существенно снизить ее доминирование путем предложения концепции децентрализованных взаимоотношений между контрагентами. Какие же последствия может повлечь за собой этот факт? Высвобождение посреднической маржи — мощнейший фактор, позволяющий перераспределить драгоценные человеческие и финансовые ресурсы от непроизводительного функционала в пользу созидательного. Конечно, далеко не все формы посредничества по определению являются балластом для мировой экономики, но существует целый ряд типовых посреднических операций, от которых человечеству можно безболезненно избавиться. И основным инструментом для этого может служить технология блокчейн, использование которой в построении принципиально новых проектов в части их архитектурной идеологии позволит произвести масштабную дезинтермедиацию в сфере коммерческих и прочих услуг.

Что касается роли государства и финансового регулирования, здесь необходимо принять во внимание, что природный консерватизм бюрократических институтов будет скорее препятствовать развитию технологии блокчейн, нежели ему способствовать. Остается лишь надеяться, что найдутся правительства, которые примут стратегию допущения разумных рисков в отношении регулирования криптосреды. Что, в свою очередь, будет способствовать дальнейшему прогрессу в развитии как финансового сектора, так и сервисной инфраструктуры в целом. Это даст неоспоримое преимущество перед странами, исповедующими охранительные принципы в отношении классических финансовых моделей, гарантирующих им кажущуюся стабильность, но вместе с тем и неизбежный застой в технологическом развитии. В любом случае было бы неразумно игнорировать стратегические тренды в мировой индустрии информационных технологий, поскольку это неизбежно приведет к технологическому отставанию и инфраструктурной деградации.

Обратимся к статистике, которая обычно говорит сама за себя. Только лишь за один 2018 год количество разработчиков блокчейн в мире увеличилось в 33 раза, а спрос у коммерческих компаний на специалистов по блокчейн-решениям за тот же год вырос на 517%. Деловая социальная сеть LinkedIn опубликовала данные своих исследований, где блокчейн-разработчики названы самыми востребованными специалистами на американском рынке труда. Многие университеты по всему миру открывают у себя кафедры по подготовке специалистов для блокчейн-индустрии, но этот процесс развивается, к сожалению, не так быстро, как бы того хотелось мировому бизнесу, связанному с информационными технологиями. Все это говорит о масштабном интересе к технологии блокчейн как таковой, а также о том, что с ней все больше связывают перспективы дальнейшего развития деловой и социальной среды.

Возвращаясь к цитате американского адвоката Николаса Кляйна, с которой началась эта книга, попробуем предположить, поставят ли когда-нибудь памятник блокчейну. За первые десять лет существования технологии она испытала на себе весь спектр эмоций со стороны сообщества: от равнодушия или сдержанного оптимизма до агрессии и поистине библейского фанатизма. Ее подвергали анафеме правительства и государственные регуляторы, но прославляли носители либертарианских или анархических идей. Иные аналитики вешали на криптопроекты ярлыки финансовых пузырей и пирамид, но были и те, кто возвещал о новой картине мира, который уже никогда не станет прежним. Одни авторитетные визионеры прогнозировали, что биткоин будет стоить миллионы уже в ближайшие годы, прочие же, напротив, предрекали ему бесславный конец. А кто-то даже подсчитал, что проект Биткоин «хоронили» уже ни много ни мало 334 раза, и это, скорее всего, не предел.

Одно пока можно сказать с уверенностью: технология блокчейн находится в начале пути своего развития. Суждено ли ей изменить привычные централизованные методы управления бизнесом, государствами и социумом в целом? Получат ли криптовалюты шанс хотя бы в некоторой степени потеснить в обращении классические платежные средства? Поможет ли это сделать процессы передачи ценности более прозрачными и более справедливыми для общества? Если большинство из этих вопросов в будущем будут решены положительно, то можно будет надеяться, что благодарные потомки действительно воздвигнут блокчейну памятник.

Таллин, Эстония
2018–2019