СОДЕРЖАНИЕ

ЧАСТЬ I. КАК УСТРОЕН БЛОКЧЕЙН 5
Предисловие 7
Изобретения, изменившие мир 9
Введение в структуру блокчейн 14
Децентрализация управления 15
Хеширование информации 20
История криптографии 26
Асимметричная криптография 29
Цифровая электронная подпись 34
Квантовые вычисления 40
Теория игр и блокчейн 46
Блоки и их структура 50
Транзакции и балансы 56

ЧАСТЬ II. ПРАКТИЧЕСКИЕ РЕАЛИЗАЦИИ 61
Предыстория проекта Биткоин 63
Кто придумал Биткоин 67
Как устроен Биткоин 71
Майнинг в сети Биткоин 76
Биткоин как криптовалюта 83
Биткоин как ценность 88
Биткоин как инвестиция 93
Биткоин как средство платежа 98
Введение в Ethereum 103
Смарт-контракты 108
Токенизация 114
Доказательство владения 119
Альткоины 124
Форки 129
Анонимность в блокчейн 135

ЧАСТЬ III. БЛОКЧЕЙН-ИНДУСТРИЯ 141
Применение блокчейн 143
Блокчейн и государство 148
Блокчейн и общество 153
Инвестиции в ICO. 158
Криптовалютные биржи 163
Анализ криптовалютного рынка 169
Хранение криптоактивов. 175
Актуальные проблемы блокчейн 180
Новая картина мира (заключение) 184

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:

Decentralization	9ffefb933ed06a04b99dd172c8ee73f59ac7fc3d
Decentralisation	10406aa1f6c0c1610fa15455a6e43c73484dda32

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 2^{256} или примерно $1{,}2 \times 10^{77}$, 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 $5{,}7 \times 10^{38,}$ 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:

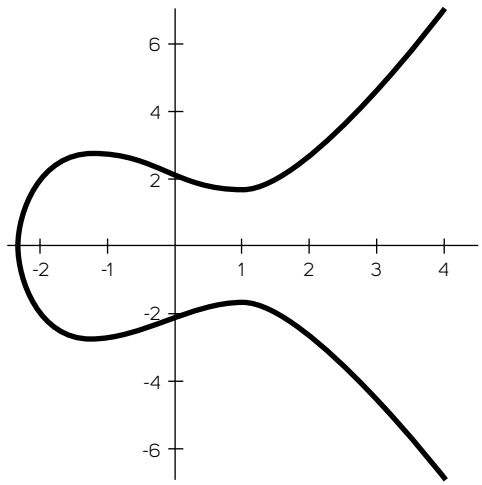
$$3^x \bmod 17 = 13$$

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 $3^4 = 81$, 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

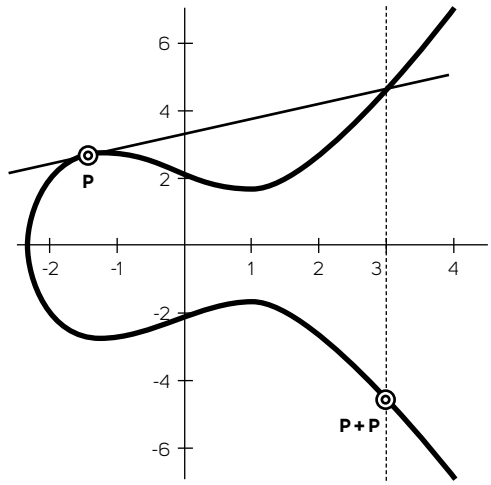
быстро и просто, а в обратную — исключительно сложно. И алгоритм DSA — не исключение. Если мы будем решать задачу для больших чисел путем простого перебора различных значений, то данный метод будет работать очень медленно. Поэтому вместо обычного перебора были разработаны алгоритмы, которые решают эту 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 $y^2 = x^3 + ax + b$. 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