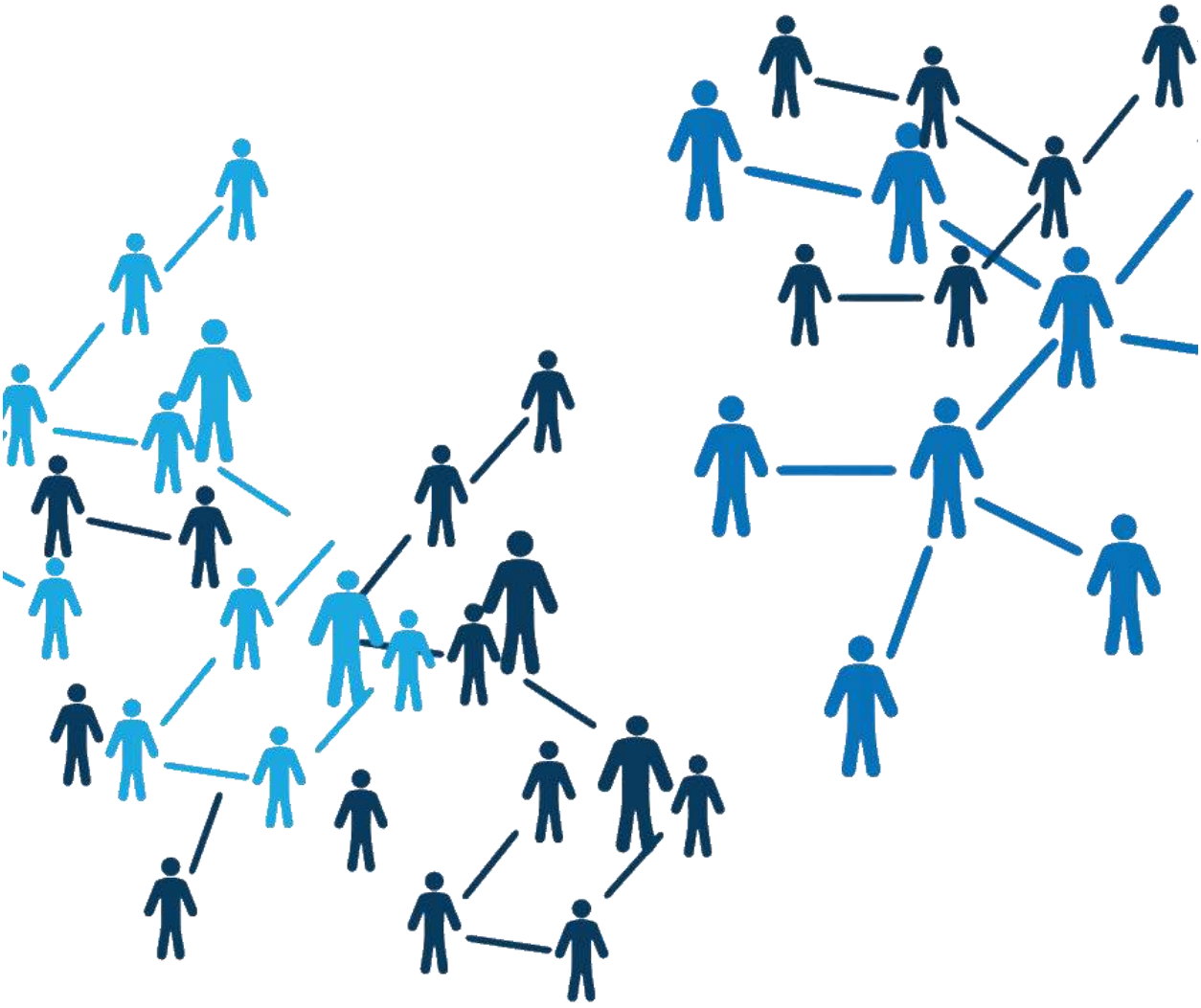
Адам Теппер

БИТКОЙН – ДЕНЬГИ ДЛЯ ВСЕХ



Оглавление

Предисловие переводчика

Кажется, предисловий для такой маленькой книжечки получается многовато, но так или иначе мне придется написать несколько слов. Я взялся за перевод этого текста, во-первых, в качестве некоей дани уважения погибшему коллеге (и другу), с которым я работал на протяжении нескольких последних лет; во-вторых, потому что эта книга – действительно отличное введение в биткойн для людей, не разбирающихся в информационных технологиях. Мне кажется, появление этого текста – достаточно обстоятельного, и в то же время не слишком длинного – на русском языке будет полезно. Чем больше людей познакомится с биткойном, тем меньше будут его бояться – ведь незнакомые вещи отпугивают, а в таинственном биткойне нет абсолютно ничего страшного.

Несколько замечаний по поводу собственно перевода. Ряд англицизмов – «майнинг», «блокчейн», «хеширование» и т. п. – широко употребляется в русскоязычных статьях, касающихся биткойна, и попытка избавиться от них, как мне кажется, не сулит ничего хорошего по отношению к смыслу текста; в самом деле, можно, конечно, переводить «майнинг» как «добычу» или «выработку», «блокчейн» как «цепочку блоков» (что звучит несколько неуклюже), но как тогда называть «майнера» – «старатель»? «добытчик»? – это уже чересчур.

Само слово «биткойн» также, очевидно, остается без перевода. В тексте оно употребляется как в единственном числе («биткойн» в субстанциальном смысле, как «деньги»), и во множественном («биткойны» в конкретном виде, как «монеты»).

Если в тексте употребляется слово «доллар» без дальнейших указаний, то имеется в виду доллар США.

Английский текст книги доступен для скачивания на сайте www.independentreserve.com (требуется регистрация), там же можно заказать бумажную версию.

Не будучи профессиональным переводчиком, я с радостью приму поправки и уточнения, если таковые возникнут.

Хочу поблагодарить Ольгу Юрьеву за первоначальную вычитку текста и Вацлава Егурнова за титаническую работу по редактуре.

Алексей Жихаревич

Предисловие Адриана Пржеложны

Адам Теппер трагически погиб в автомобильной катастрофе в феврале 2015 года, до того, как закончил эту книгу. Как близкий друг Адама и его бизнес-партнер в бесчисленном множестве проектов я обязан был закончить то, что он начал, завершив его рукопись и выпустив эту книгу в печать.

Я хотел бы подчеркнуть, что, хотя я и внес некоторые изменения и правки в эту книгу, я твердо уверен, что они соответствуют тому, что сделал бы сам Адам, имей он такую возможность. Эта книга, таким образом, остается работой Адама Теппера, и соответствует его авторскому замыслу.

Особая благодарность тем, кто пожертвовал деньги семье Адама, а также сделал пожертвование через страницу Биткойн Ассоциации Австралии, чтобы помочь оплатить публикацию этой книги. Также спасибо Биткойн-посольству в Австралии и тем, кто потратил время на вычитку книги и отзывы о ней на разных стадиях.

Адам был добрым, умным и страстным молодым человеком с четким видением будущего, в котором биткойн может изменить жизнь людей к лучшему. Любимым писателем Адама был Ричард Фейнман за его способность объяснять сложные и кажущиеся недоступными идеи ясными и простыми словами. Такой талант был присущ и самому Адаму, и эта книга является великолепным тому подтверждением. Я надеюсь, что вам доставит удовольствие изучение биткойна посредством слов и мыслей Адама Теппера.

Адриан Пржеложны

Адам Теппер

13 февраля 1981 – 26 февраля 2015 гг.

Предисловие

Поскольку я – один из основателей Independent Reserve, онлайн-сервиса для обмена валют, специализирующегося на обмене биткойна на другие валюты, меня часто просят разъяснить, что такое биткойн, и почему он важен. В самом начале я, вероятно, не слишком хорошо объяснял это людям, ведь биткойн соединяет множество разных идей, в большинстве своем непривычных. Альберт Эйнштейн однажды сказал: «Если вы не можете объяснить нечто просто – значит вы сами не понимаете этого достаточно хорошо», – и я думаю, что до некоторой степени это и было причиной того, что изначально я испытывал трудности, объясняя другим, что такое биткойн.

Сегодня я все еще встречаю людей, которые никогда не слышали о биткойне, и они спрашивают меня, что это такое. Обычно я отвечаю наиболее коротким образом, объясняя практические выгоды биткойна и опуская более интересные подробности о том, как он работает. Если человек заинтересовался, я готов отвечать на его вопросы до тех пор, пока он не достигнет понимания на устраивающем его уровне. В этом же состоит цель моей книги, и я расположил главы книги схожим образом. Предполагаемая аудитория этой книги – люди, которые абсолютно незнакомы с биткойном и совершенно незнакомы с компьютерными науками в целом. Она предназначена для читателя, который хочет понять основы того, как работает биткойн, и заодно разобраться в технологиях. Книга начинается с обзора биткойна в практическом смысле, затем я разбираю идеи, лежащие в основе биткойна, и наконец отвечаю на некоторые более общие вопросы, которые задают мне о биткойне сегодня.

Адам Теппер

деньги – металлические и бумажные знаки, являющиеся мерой стоимости при купле-продаже, средством платежей и предметом накопления

валюта – денежная система страны, а также денежные единицы этой системы

Часть I

Что такое биткойн

Глава первая
Введение в биткойн

Биткойн – это валюта, и таким образом это деньги. Деньги не всегда были тем, чем они являются в нашем понимании сегодня, и по существу биткойн – это очередное развитие идеи денег. Одним из ключевых факторов, выделяющим биткойн в сравнении с другими, хорошо известными, валютами, такими как американский доллар ($), британский фунт (£) или евро (€), является то, что биткойн – это электронная валюта, что в общем означает, что биткойн хранится в электронном виде, на компьютерах[1], и передается электронным способом через Интернет. Перспектива электронных денег может сбить с толку или обескуражить многих людей, точно так же, как электронная почта могла бы смутить кого-нибудь в 1980-е, когда ее описывали как письма, хранящиеся и отправляющиеся электронно, через интернет. Сегодня электронная почта настолько распространена, что бумажные письма, особенно личные письма, считаются старомодными, громоздкими и, помимо всего прочего, медленными.

Первые пользователи электронной почты в конце 1980-х или начале 1990-х, могут помнить, что в самом начале она была не слишком полезна, потому что у большинства ваших друзей, членов семьи и коллег не было ни электронного адреса, ни даже, возможно, интернет-соединения. Друзья задавали вопросы вроде: «Что такое e-mail и как этим пользоваться?». Это было время, когда еще не было Gmail, не было Google, не было даже Hotmail. Электронные почтовые ящики преимущественно предоставляли интернет-провайдеры. Но вскоре у большинства людей появились электронные адреса, и сегодня уже кажется крайне необычным, если у кого-нибудь вообще нет электронного адреса, точно так же, как если у человека нет мобильного телефона.

Я говорю об электронной почте, потому что это великолепная аналогия биткойну. Электронная почта взяла процесс отсылки писем, использовавшийся много тысяч лет, и приспособила его для передачи и хранения писем в электронном виде. За относительно короткое время процесс обмена рукописными письмами стал архаичным и непривычным методом общения. Было бы трудно представить, что мы должны снова отправлять письма по почте для ежедневного общения и ждать ответа несколько дней или неделю. Стоит также упомянуть, что за последние двадцать или тридцать лет способы, которыми мы используем электронную почту, тоже несколько изменились. Мы имеем доступ к электронному ящику со всех наших устройств; мы можем отправлять большие вложения и разнообразное содержимое; мы можем использовать электронную почту, чтобы назначать встречи, которые появляются в наших календарях. Все эти идеи не были изначально заложены при создании электронной почты, но стали ее развитием, основанным на том, как мы используем почту. Конечно, есть много других форм электронного общения, которые развились позже. Это развитие относится к постоянному усовершенствованию электронной коммуникации вообще. А ведь изначально очень немногие люди видели преимущества использования электронной почты.

[1] Биткойны можно хранить в неэлектронном виде, например, на бумаге, но это, скорее, исключение, чем правило. Транзакции, однако, всегда электронные.

Это возвращает нас к биткойну. Как электронная почта стала тем, что вывело общение в электронную эпоху, так и биткойн является тем, что выводит в электронную эру нашу денежную систему. Перед тем, как мы рассмотрим, каким образом биткойн сможет это сделать, стоит бросить взгляд на историю денег, чтобы выстроить перспективу.

Глава вторая

История денег

Деньги сегодня – это очень сложная система. Большую часть времени она работает, но время от времени катастрофически ломается. Хоть система и сложна, большая часть сложных вещей незаметна для нас при ежедневном ее применении. На протяжении большей части нашей жизни денежная система почти не изменилась – это нечто, с чем мы все выросли, и большинство из нас, вероятно, не тратило много времени на обдумывание того, как она работает. Деньги не всегда были одинаковы. Одним из самых больших изменений за последние сто лет стало размещение большинства основных валют на свободном рынке в противовес определению цены относительно золота или серебра текущим правительством. Это был весьма значительный прогресс денежной системы, однако давайте оглянемся назад еще дальше, чтобы посмотреть, как изменились деньги за тысячи лет использования в различных обществах.

Я помню, когда я был ребенком, я спросил отца: «Что люди делали до денег?». Мой отец объяснил, что «в старые дни» люди применяли систему бартера, используя овец и других животных в качестве валюты. Ребенком мне было трудно представить, как бы это могло работать, но в сущности именно так работали деньги несколько тысяч лет назад. У овец и вообще скота были в этом смысле определенные недостатки. Их было сложно хранить, трудно перемещать и нелегко делить. На протяжении человеческой истории разные культуры использовали для этих целей различные товары. В качестве денег использовались морские ракушки и рис, а затем драгоценные металлы, золото или серебро, которые позже стали привычными, поскольку они имели множество качеств, удобных для валюты: они были долговечными, портативными, делимыми и редкими.

Чтобы осуществить транзакцию с использованием драгоценного металла, например, золота, можно определить ценность предмета как стоимость некоторого количества золота. Это решение было несовершенным, поскольку процесс оценки чистоты металла и его веса не способствовал быстроте транзакций. Государства позднее улучшили этот процесс, чеканя стандартизированные монеты, содержавшие определенное количество драгоценного металла, вес и подлинность которых были подтверждены государством. Это интересный момент в истории денег. Он интересен потому, что, хотя монеты содержали предписанное количество золота или серебра, ценность им придавал знак государства, и торговцам не нужно было анализировать чистоту и подлинность монет как таковых. Следовательно, доверие теперь переключилось на государство. Правительствам не потребовалось много времени, чтобы понять, что поскольку ценность монет заключается в знаке монетного двора, будет дешевле выпускать монеты, содержащие меньшее количество драгоценного металла, чем обозначенный вес монеты. Этот шаг в истории денег был изменением, превратившим монету из единицы веса в единицу стоимости.

По мере расцвета европейской торговли в Средние века, распространилась идея векселя, посредством которого торговец мог предложить кредитную линию доверенному покупателю. Товары поставлялись покупателю в обмен на вексель, по которому он обязывался совершить платеж в определенный день в будущем. При условии, что покупатель был уважаемым человеком, или вексель был одобрен заслуживающим доверия поручителем, продавец мог затем представить его банку для выкупа по сниженной цене до ожидаемой даты. Эти векселя также использовались продавцом как форма оплаты, чтобы делать дополнительные закупки у своих

поставщиков. Таким образом векселя – ранняя форма кредита – стали одновременно и средством обмена, и средством сбережения.

В двенадцатом столетии английская монархия ввела систему, основанную на схожих предпосылках – закладные, посредством которых монархия могла делать платежи, основанные на ожидаемых налогах, которые еще не были получены. Они также были известны как тэлли (деревянные палочки с насечками). Казначейство обнаружило, что они также могут быть использованы в качестве денег. Когда корона исчерпывала свои ресурсы, она могла использовать тэлли, представляющие будущие налоговые выплаты короне, как форму платежа ее собственным кредиторам, которые в свою очередь могли либо сами собирать налоги непосредственно с плательщиков, либо использовать эти тэлли для уплаты собственных налогов правительству. Таким образом, тэлли были приняты как средство обмена для некоторых типов транзакций и как средство сбережения. Казначейство вскоре осознало, что оно может выпускать тэлли, не обеспеченные никакими конкретными налоговыми выплатами. Делая это, казначейство создало новые деньги, обеспеченные общественным доверием и верой в государство, а не конкретными доходами.

Примерно в то же время банки начали выпускать бумажные купюры, весьма правильно названные «банкнотами», которые обращались тем же способом, каким выпущенная государством валюта обращается в наши дни. Только купюры, выпущенные самыми большими, наиболее кредитоспособными банками были широко приняты. Бумаги меньших, менее известных заведений имели хождение только локально. Вдалеке от дома они принимались по сниженной цене, если принимались вообще. Распространение типов денег шло рука об руку с умножением числа финансовых институтов.

Банкноты были формой обеспеченных денег, которые могли быть обращены в золото или серебро по предъявлению в банк. Поскольку банки выпускали значительно больше бумаг, чем хранили золота и серебра на депозитах, внезапная утеря доверия к банку могла вызвать массовый выкуп банкнот, что приводило к банкротству.

Использование банкнот, выпущенных частными коммерческими банками как законного платежного средства было постепенно вытеснено выпуском банкнот, разрешенных и контролируемых национальными правительствами. Банку Англии было дано исключительное право выпускать банкноты в Англии в 1694 году, что таким образом положило конец использованию частной валюты в королевстве. Австралия приняла подобный закон более чем два столетия спустя, в 1910, а за ней последовали Соединенные Штаты в 1913.

Разрешенные правительством валюты были формой обеспеченных денег, поскольку они были частично обеспечены золотом или серебром и теоретически могли быть превращены в золото или серебро. Во времена президента Никсона доллар США был выведен из «обеспеченного золотом» стандарта в 1971, что вызвало коллапс международной Бреттон-Вудской валютной системы. Большинство основных мировых валют были затем размещены на открытом рынке, полностью потеряв связь с драгоценными металлами, теперь ценность валюты базировалась исключительно на экономике и надежности выпускающего ее правительства.

Разобравшись в истории денег, мы также можем увидеть их слабость. Теперь рассмотрим более детально работу биткойна и его преимущества перед существующими формами денег.

Глава третья

Работающий пример

Технология, обеспечивающая работу биткойна, очаровывает. В первый раз я услышал о биткойне несколько лет назад, почти сразу, как он появился в 2009 году. Мой друг Джо, человек, которому нравится рекламировать новейшие технологические тренды, сказал мне, что «один парень придумал, как создать интернет-деньги». Я не понимал, в чем смысл этой фразы, и полагаю, что в то время мой друг тоже этого не понимал.

Я больше не вспоминал о биткойне до того, как некоторое время назад, в ноябре 2012 года, заметил онлайн-рекламу, в которой было что-то про биткойн, и подумал, что надо бы взглянуть. Первая вещь, которую я отметил – это то, что биткойн, чем бы он ни был, продавался за 10 долларов США, и так было уже некоторое время. Я ожидал, что он будет стоить не больше нескольких центов, или даже долей цента. Конечно, ничего не зная о биткойне в то время, я не мог понимать, сколько должен стоить биткойн, но предполагая, что в обращении имеются миллионы биткойнов, 10 долларов казались существенной цифрой, и мне стало любопытно разузнать все поподробнее. После прочтения множества найденных мной в интернете материалов я был все также далек от понимания того, чем был биткойн или как он работал. Только после тщательного перечитывания и исследования перекрестных ссылок на различные ресурсы я начал складывать картинку в своей голове. Определенно, я не назвал бы это глубоким или доскональным пониманием, у меня еще оставалось множество вопросов.

Однако биткойн захватил мой интерес, и, будучи программистом, я решил написать свою примитивную программу, которая позволила бы мне отправлять и получать биткойны (она никогда не публиковалась, это был просто эксперимент, чтобы посмотреть, как это работает и удовлетворить мое любопытство). Я никогда не закончил эту программу, но провел две или три недели за ее разработкой, и занимаясь этим, в конечном счете, я пришел к пониманию того, как работает биткойн, и был глубоко впечатлен и поражен лежащей в его основе технологией. Она поражала, поскольку элегантно сводила вместе множество несхожих принципов программирования в систему, о которой раньше никто не мог и подумать, и которая могла теперь эффективно использоваться в качестве денег.

Не желая попусту рекламировать идею, относительно которой у меня были сомнения, не окажется ли она очередным «вечным двигателем», я дождался момента, когда я достаточно глубоко понял биткойн, прежде чем передать эти знания моему бизнес-партнеру Адриану Пржеложны. Я был встречен со скепсисом именно того уровня, что и ожидал. Через месяц он заметил мне: «Биткойн действительно поразительная вещь – я вот купил немного».

Так что же такого было в биткойне, что мы оба сочли поразительным, и что позже привело нас на путь создания компании, так сильно завязанной на биткойн? Во второй части книги мы займемся технологиями, лежащими в основе биткойна, но для начала я должен объяснить, как он работает на высоком уровне. Биткойн – это нечто среднее между физической валютой и чековой книжкой. Пока что мы можем провести только эту аналогию, но начнем хотя бы с этого.

Используя этот пример, скажем, пусть я хочу послать моему другу Джо 50 долларов (USD). Я могу выписать чек с его именем на нем, написать сумму и поставить свою подпись внизу чека. В идеальном мире это прекрасная система. Джо получает чек, и он не может изменить сумму. Если

чек будет украден, то это не поможет вору, потому что на чеке стоит имя Джо. И если украдут мою чековую книжку, то она не будет иметь никакой ценности для кого-либо, потому что на чеках еще нет моей подписи. Это хорошая система в теории, однако на практике она имеет ряд недостатков. Во-первых, сам по себе чек – это не деньги. Чек – это по существу письмо в банк, разрешающее банку выдать Джо 50 долларов из моих денег, которые там хранятся. Покуда Джо не принесет чек в банк, он не знает наверняка, есть ли у меня эти 50 долларов. Банку может потребоваться несколько дней или неделя для того, чтобы выдать Джо эти средства. Подписи очень легко подделать, так что, если кто-то заполучил мою чековую книжку, ему будет не особенно сложно выписать мошеннический чек. В Австралии чековые книжки не используются уже примерно поколение, само понятие для нас настолько же архаично, как и торговля золотыми слитками, но удивительным образом эта система преобладает во многих странах, включая Соединенные Штаты.

Давайте сравним эту транзакцию с транзакцией, которую использует биткойн – скажем, я хочу послать моему другу Джо 50 биткойнов (XBT[2]). Первое ключевое различие между примером с чековой книжкой и биткойном состоит в том, что в случае с чековой книжкой 50 долларов хранит для меня банк. Биткойн, однако, больше похож на наличные, и 50 биткойнов могут храниться физически на вашем компьютере[3]. Скажем, у меня есть 50 биткойнов в цифровом кошельке на моем мобильном телефоне, которые я хочу послать Джо на его мобильный телефон. Сперва я спрашиваю у Джо его биткойн-адрес. Когда я отправлю деньги на адрес Джо, их можно будет потратить только при помощи секретного ключа, который хранится на телефоне Джо. Никто другой не сможет воспользоваться этими деньгами без доступа к его телефону.

Итак, при помощи программы на моем телефоне я начинаю транзакцию, которая посылает 50 биткойнов с моего личного биткойн-адреса на биткойн-адрес Джо. Затем я ставлю на эту транзакцию цифровую подпись, используя секретный ключ на моем телефоне, и отправляю эту информацию в Интернет, так что она видима всему миру. Это правда, я ничего не посылаю непосредственно Джо, я отправляю информацию для всей биткойн-сети.

Далее происходит вот что: когда остальные компьютеры в биткойн-сети получают информацию о моей транзакции, они проверяют, что у меня действительно есть 50 биткойнов в кошельке, и что моя подпись правильна. Если все в порядке, они помечают транзакцию как достоверную, и вскоре она становится частью официального глобального биткойн-гроссбуха, известного как «цепочка блоков» или «блокчейн», и хранится в нем (подробнее об этом мы расскажем ниже).

Тем временем, программа на телефоне Джо, вместе со всем остальным миром, подтверждает начатую мной транзакцию. Практически мгновенно эта транзакция отображается на его телефоне как приход в 50 биткойнов.

---

[2] XBT принят как стандартное обозначение валюты для биткойна. В других обозначениях валют первый символ обычно означает страну, выпустившую валюту. В некоторых местах до сих пор используется альтернативное обозначение BTC.

[3] Когда я говорю «компьютер», на самом деле я имею в виду любое электронное устройство, где установлена соответствующая программа. Это может быть мобильный телефон, ноутбук или подобное устройство.

Если я отправил деньги Джо, я больше не могу снова потратить эти 50 биткойнов, поскольку биткойн-сеть больше не признает эти 50 биткойнов принадлежащими мне, и их можно потратить, только если использовать секретный ключ Джо. Взглянем на эту ситуацию с другого ракурса: транзакция, которую я начал, была в сущности «письмом» в биткойн-сеть, передающим Джо мое право потратить 50 биткойнов. Это же просто!

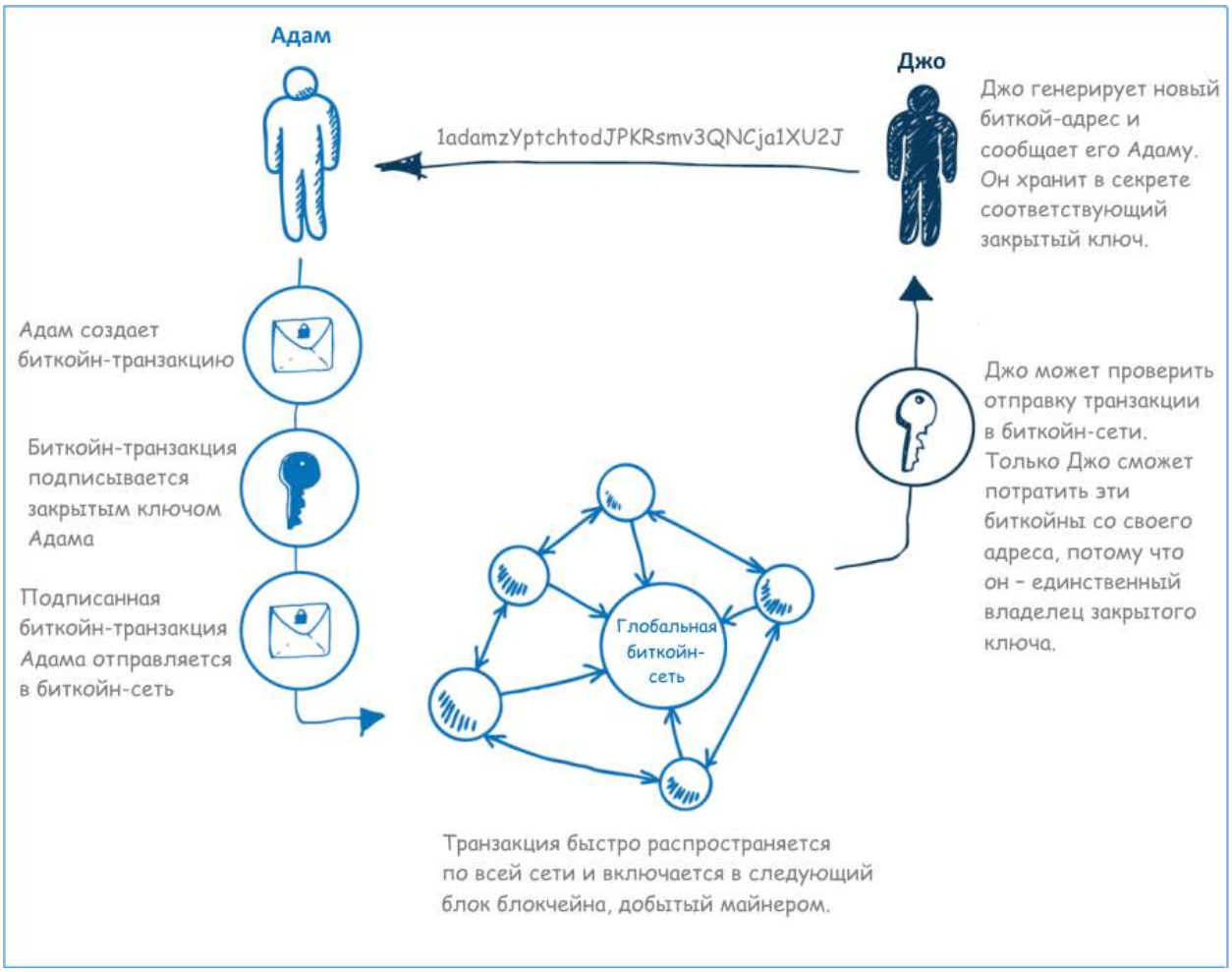


Рис. 1. Адам посылает Джо биткойны через биткойн-сеть

Давайте рассмотрим эту модель более внимательно и проанализируем некоторые различия между биткойном и чековой книжкой. В случае чековой книжки есть центральный банк, который обрабатывает транзакции. В случае биткойна центрального обработчика транзакций или начальства нет –используется децентрализованная модель, в которой каждый участник сети, включая получателя, может удостоверить подлинность транзакции. Это быстрый процесс. Для менее рискованных транзакций с небольшими суммами этот процесс занимает не больше нескольких секунд. Для более рискованных транзакций с большими суммами транзакция может быть безопасно признана завершенной примерно через полчаса. Сравните это с банковским чеком или SWIFT-переводом, для которых обычно требуется от 1 до 5 дней.

Другая схожая деталь, которую вы должны были заметить, – то, что биткойн-транзакции подписывают, точно так же, как и старомодные чеки. Однако, разница в том, что с подделкой

подписи на бумаге может управиться и шестилетний ребенок, тогда как подделка цифровой подписи, используемой в биткойн-транзакции, практически невозможна[4].

Еще один интересный момент – то, что стоимость обработки транзакции и время выполнения согласованы, и они не зависят от суммы транзакции[5]. Используя вышеприведенный пример, я мог бы послать Джо долю цента в биткойнах, чтобы оплатить роялти, которые он получает за свой платиновый альбом, или я мог бы послать ему два миллиона долларов, чтобы приобрести его успешную компанию. В любом из этих случаев комиссия за транзакцию будет одинаковой, практически нулевой, а время выполнения почти моментальным. Так достигается эффективное бесплатное и безопасное движение денег в международном масштабе со скоростью электронной почты.

Наконец, стоит заметить, что поскольку биткойн-сеть охватывает весь интернет, неважно, где физически находимся мы с Джо. Мы можем сидеть в одной комнате или в разных частях света – это не имеет значения. Это не влияет ни на скорость, ни на стоимость транзакции.

[4] Технически «невозможность» взлома не доказана ни для одной формы программного шифрования или цифровой подписи, но можно обоснованно заявить, что подделать цифровую подпись настолько сложно, что это почти невозможно во всех практических случаях применения.

[5] Ниже мы увидим, что в качестве предосторожности от мошенничества разумно подождать полчаса, чтобы подтвердить транзакцию со значительной суммой, но обычно все транзакции можно увидеть уже через несколько секунд.

Глава четвертая

Как добывают биткойн

В предыдущей главе мы рассмотрели повседневный пример того, как можно использовать биткойн, чтобы переслать деньги между участниками сети. Однако, вот вопросы, которые мне обычно задают: как генерируют биткойны, как их вводят в экономику, и откуда биткойн получает свою ценность. Перед тем как дать ответ на эти вопросы, давайте вспомним об истории денег, которую мы обсуждали во второй главе.

До двадцатого столетия деньги были хотя бы частично обеспечены драгоценными металлами, такими как золото или серебро. Наряду с другими важными качествами, которые делали золото и серебро пригодными в качестве валюты, был тот факт, что эти металлы были относительно редки. Существовал стабильный, но медленно увеличивающийся приток золота и серебра, пока их добывали из земли. Добыча требовала множества времени, усилий и издержек. Если бы золото и серебро были в изобилии, и их было бы легко получить, тогда каждый бы занимался добычей, и они перестали бы быть ценными, соответственно, они перестали бы быть пригодными в качестве денег.

Хотя добыча биткойна и добыча золота сильно различаются на практике, принцип, лежащий в их основе, одинаков, и поэтому генерация биткойнов стали схожим образом называть «добычей биткойна». Подобно золоту, любой человек может добывать биткойн, имея соответствующие ресурсы. Если бы вы захотели добывать золото в наши дни, вы могли бы заняться этим, но помните, что значительная часть золота у поверхности Земли уже давно добыта. Таким образом вам потребовалась бы толика удачи плюс большой геологический и логистический опыт – в результате большинство людей являются потребителями золота, а не добытчиками!

Способ, которым осуществляется добыча биткойна, состоит в том, что биткойн-сеть вводит относительно небольшие объемы биткойнов в экономику через регулярные интервалы. Биткойн-протокол задает математическую задачу, которая построена таким образом, чтобы ее можно было решить примерно за десять минут. Когда задача решена, человеку, владеющему компьютером, решившим задачу, выдается заданное количество биткойнов. В самом начале, возможно, эти задачи решал всего один личный ноутбук. Следовательно, задача была относительно легкой, чтобы имеющийся в наличии ноутбук мог решить ее в пределах десяти минут перед повторением процесса снова. В этот момент, когда биткойн был в младенчестве и никто другой не использовал его, один биткойн не стоил чего бы то ни было. Поэтому такое упражнение в добыче, которое требовало небольших объемов электричества, извлекало некоторый объем биткойнов, которые ничего не стоили.

Однако, с течением времени два, потом три, потом тысячи ноутбуков и домашних компьютеров пытались решить задачу, которая обновлялась каждые десять минут. С тысячей компьютеров, которые пытались решить задачу, сеть скорректировала уровень сложности, чтобы он стал в тысячу раз выше, чем вначале. Поэтому у каждого участника был примерно один шанс из тысячи, чтобы решить задачу и добиться какого-либо вознаграждения.

Я не знаю в точности, сколько стоил биткойн в этот момент истории, но он стал кое-чего стоить, даже если это была совсем небольшая сумма. Использование компьютера двадцать четыре часа в сутки недорого стоит в нормальных условиях, когда вы просто бродите по

интернету, но, если вы будете использовать компьютер двадцать четыре часа в сутки для решения математической задачи, вы увидите, что процессор используется почти на 100%. Этот процесс увеличивает потребление энергии и повышает расходы на электричество. Люди начали подсчитывать стоимость использования машин для добычи биткойна и соотносить ее со статистической вероятностью решения задачи за выделенный период времени. И с этого времени биткойн стал обладать некоторой ценностью, пусть даже только в силу его редкости, а не в силу полезности для столь небольшого круга людей.

Затем люди поняли, что чем использовать старый ноутбук или ПК для вычислений, будет более эффективно сконструировать компьютеры, предназначенные специально для добычи биткойна, и ни для чего более. Люди начали запускать не один, не два, а целые фермы компьютеров в своих квартирах и жилых помещениях. Эти компьютеры добывали биткойн и потребляли электричество. Некоторые умные люди позже поняли, что ГП (графические процессоры) на видеокартах были гораздо более производительны для решения специфического типа задач, предлагаемого в добыче биткойна, и написали программы, чтобы использовать преимущества видеокарт и добывать биткойны быстрее.

Как вы можете видеть, увеличилось не только количество людей, добывающих биткойн, но и количество машин, которые использовались этими людьми, и мощность этих машин. Задача для решения каждые десять минут была теперь в сотни тысяч или может быть в миллионы раз более трудной, и майнер с простым ноутбуком имел бы очень маленькие шансы добыть хоть что-нибудь.

После фазы ГП-майнинга, как ее называли, производители оборудования стали разрабатывать сверхбыстрые платы, специально предназначенные для добычи биткойна, делающие ГП-майнинг медленным и устаревшим. Биткойн-майнинг в наши дни – это полноценная индустрия с компаниями, инвестирующими миллионы долларов в оборудование для добычи биткойна. Сегодня, подобно использованию маленькой лопатки для добычи золота, вы не можете рассчитывать начать добычу биткойна на домашнем компьютере и ожидать получить деньги, ведь для этого потребуются обширные ресурсы. Несколько ферм для добычи биткойна были запущены в Исландии, где геотермальное электричество обеспечивает дешевый источник энергии, что совмещается с минимальными требованиями к охлаждению серверов из-за низких температур.

Пусть так, если вы не можете позволить себе золотую шахту, вы, вероятно, можете купить какую-то долю в ней. Схожим образом сейчас работают компании, обеспечивающие то, что называется «майнинг-пул». Он работает таким образом, что вы присоединяетесь к объединению тысяч пользователей, которые используют домашние компьютеры для добычи биткойна, и гарантированно получаете небольшой процент, соответствующий вкладу вашего личного компьютера в общий объем добычи – однако, не рассчитывайте разбогатеть!

Я много говорил о том, как работает биткойн-майнинг, и об истории биткойн-майнинга, но у процесса добычи биткойна есть еще две важные роли в биткойн-сети помимо генерации новых биткойнов для майнеров. Во-первых, в дополнение к решению математических задач, биткойн-майнеры также обрабатывают транзакции. В третьей главе я дал пример отправки 50 XBT моему другу Джо, и эта транзакция была отправлена в биткойн-сеть. Данные этой транзакции дошли до множества майнеров, активно добывающих биткойн, и когда один из них успешно решил

математическую задачу, он также обработал эту транзакцию, вместе со всеми остальными биткойн-транзакциями за последние десять минут, и включил их в блокчейн (гроссбух биткойна). Другими словами, эти майнеры выполняют необходимую функцию в биткойн-сети: помимо введения денег в экономику, они обеспечивают функции обработки платежей, которые позволяют биткойн-транзакциям работать.

Есть и третья ключевая роль, которую играет процесс добычи. Чем больше майнеров в биткойн-сети, тем более трудной становится математическая задача. Чем сложнее задача, тем более безопасной и устойчивой к мошенническим транзакциям становится сеть. Мы пока не будем обсуждать этот момент, но вернемся к нему позже в этой книге.

Глава пятая

Зачем использовать биткойн

Теперь, когда у вас есть элементарное понимание некоторых принципов, лежащих в основе биткойна, пришло время рассмотреть преимущества биткойна перед другими видами денег и понять, как вы могли бы его использовать. Биткойн выгоднее обычной валюты практически во всех обстоятельствах, когда возможна электронная транзакция. Однако, перед тем как рассмотреть его преимущества, стоит отметить имеющиеся альтернативы. Когда мы говорим об альтернативах, мы не только сравниваем биткойн с другими валютами, такими как доллар, фунт или евро, но мы также должны рассмотреть разные виды транзакций. Способ, которым мы используем деньги, сильно зависит от используемых сумм, вида покупаемых нами товаров и услуг, а также взаимного расположения участников.

В простейшем случае мы используем физическую передачу наличных, когда банкноты или монеты переходят из рук в руки. Передача наличных лучше всего работает для сумм примерно от пяти центов до тысячи долларов. Очевидно, возможно передавать и большие суммы, но в большинстве случаев люди считают более удобным использовать другие методы оплаты, если сумма превышает тысячу долларов. Что касается меньших (чем нижний предел) сумм, тут мы ограничены наименьшим номиналом валюты. Передача наличных имеет ограниченное применение, поскольку оба участника должны находиться в одном месте.

Для передачи больших сумм между физическими лицами часто используются банковские чеки. Банковский чек обычно стоит около пяти долларов, так что не слишком экономно использовать их для сумм, меньших пятисот долларов. На практике, в большинстве случаев сумма банковского чека не ограничена, но это довольно неудобный процесс, требующий от обоих участников появления в филиале банка, таким образом обычно использование банковских чеков для транзакций ограничивается пределами одной страны. Участники также должны встретиться лично, чтобы передать чек, или ждать несколько дней, пока чек доставят почтой.

Для торговцев удобными средствами являются электронные платежи или кредитные карты. Это относительно дорогой вариант для торговцев, поскольку они должны платить, чтобы создать торговый канал с банком, а также платить банку несколько процентов от суммы каждой транзакции в качестве комиссии за обработку транзакций. Более того, в случае возврата платежа, когда транзакция оказывается мошеннической, торговец рискует и он должен вернуть деньги. Это в особенности касается торговцев, занимающихся онлайн-бизнесом, поскольку они получают только данные кредитных карт, но не видят сами карты. Возможности электронных платежей и кредитных карт, как правило, ограничены суммами от десяти до десяти тысяч долларов.

Международные SWIFT-переводы являются основным методом передачи денег между странами. SWIFT-переводы обычно неэкономичны для сумм, меньших тысячи долларов, из-за высоких комиссий, взимаемых банками. SWIFT-переводы – это очень медленная форма транзакций: получатель получает платеж через несколько дней. В процессе перевода также возникают ошибки, приводящие к еще большим задержкам.

Я описал некоторые наиболее распространенные методы передачи денег между людьми, но, разумеется, это не исчерпывающий список. Существуют также большие фирмы, занимающиеся переводами, как Western Union, а также большое число специализированных

фирм, занимающихся международными переводами, которые могут пересылать небольшие суммы денег быстрее и экономичнее, нежели SWIFT или Western Union. Другая группа компаний включает PayPal и подобные ему компании, действующие в качестве обработчика и страхователя платежей между торговцами и банками. И, опять же, это не все. Вы, наверное, начали уже понимать, что наше представление о транзакции сильно зависит от того, что мы пытаемся сделать, и что у нас имеется большое разнообразие слабо связанных систем, имеющих преимущества и недостатки в зависимости от обстоятельств.

Вернемся к биткойну. Биткойн позволяет мне отправить любую сумму денег *в любое место* мира *мгновенно* и *бесплатно*. Какой другой метод проведения транзакций имеет столь широкий охват?

Давайте продолжим. Биткойн позволяет торговцам получать платежи без риска возврата. Формулируя это по-другому, если торговец получил платеж в биткойнах, нет риска, что банк или третья сторона может позже объявить этот платеж мошенническим; платежи в биткойнах окончательные. Конечно, продавцы и покупатели могут платить третьей стороне за услуги условного депонирования, если это им нужно. Это также и благо для покупателей, в частности тех, кто делает покупки онлайн. Если вы когда-нибудь совершали онлайн-покупку с помощью кредитной карты, вы должны представлять расстройство, когда вашу карту не принимают, потому что вы в этот момент путешествуете, или делаете покупку, которую продавец считает рискованной. Например, если вы покупаете оборудование на несколько тысяч долларов, продавец может попросить вас подтвердить вашу личность и адрес. Это неудобно и разочаровывающе и для продавца, и для покупателя, приводит к нежелательным задержкам и усилиям по обработке транзакции с обеих сторон. С биткойном транзакции мгновенны, бесплатны и не представляют никакого риска для продавца.

Преимуществ еще больше, если вы торговец, который часто имеет дело с международными покупателями, например, в туристической индустрии. Представьте, что вы сдаете яхту внаем. Покупатель заказывает яхту за неделю перед праздниками. Вместо того, чтобы беспокоиться по поводу комиссий за перевод, знакомиться с иностранной валютой и ждать несколько дней, чтобы деньги дошли, можно отправить депозит в биткойнах – откуда угодно, бесплатно и мгновенно, в валюте, с которой знакомы и покупатель, и продавец. Если наем яхты окажется тайным подарком невесте на помолвку, он также не будет виден в отчетах по кредитной карточке.

Другое большое преимущество биткойна в том, что биткойн-транзакция не требует ни от одной из сторон предоставления важной информации другой стороне. Это совершенно противоположно тому, как работают кредитные карты или электронные платежи. Каждый раз, когда вы делаете покупку в магазине при помощи кредитной карты или электронного платежа, вы должны передать данные вашей карты и пин-код или подпись. Интересно задуматься над тем, каким важным кажется нам спрятать пин-код от других людей, и в то же время как просто мы готовы ввести его в машинку, принадлежащую абсолютно незнакомому человеку. Устройства для кражи пин-кодов известны в Австралии, но они гораздо больше распространены в других частях света, это особенно касается международных путешественников. Использование биткойна полностью снимает этот риск. Вы можете делать покупки в любом месте мира, платить любому

незнакомцу, не беспокоясь о том, что ваши данные потом могут использовать в мошеннических целях.

Другой пример обстоятельств, при которых биткойн имеет значительные преимущества над другими методами проведения транзакций – это оплата маленьких сумм. Ребенок может захотеть пойти в магазин и купить там за десять центов шоколадку или леденец, или продавец может захотеть продать мелодию звонка для мобильного телефона за пятьдесят центов онлайн. Без биткойна такого рода маленькие покупки могут осуществляться только за наличные, так как для большинства других средств требуется, чтобы сумма платежа покрывала комиссии за транзакцию. Биткойн предоставляет то, что сейчас называют «микроплатежи», в случае со столь маленькими суммами, или даже еще меньшими суммами, меньше одного цента. Более того, биткойн – это не кредитная линия, это цифровой эквивалент наличных, так что вам не нужно быть взрослым, чтобы его использовать.

Что насчет случая с путешественником, которому срочно нужно послать сто долларов маме в свою страну? SWIFT-перевод будет дорог для обеих сторон и займет несколько дней. Сервис наподобие Western Union будет быстрее, но еще дороже. Биткойн работает мгновенно и бесплатно.

Биткойн можно пересылать между участниками анонимно. У этой анонимности нет никаких ограничений, мы более подробно рассмотрим это в следующих главах, а сейчас достаточно сказать, что, когда я осуществляю биткойн-транзакцию, мне не нужно беспокоиться о том, кто проведет платеж: банк или компания-оператор кредитных карт, которые хранят всю историю моих покупок. Мне не нужно открывать свою личность продавцу, и существует множество обоснованных и разумных причин, по которым я мог бы предпочесть остаться анонимным.

Другое большое преимущество биткойна в том, что его выпуск контролируем. Как мы кратко рассмотрели в предыдущей главе, биткойн генерируется посредством процесса добычи, и скорость генерации биткойна контролируется самим протоколом. Мы рассмотрим это подробнее в дальнейшем, но можно сказать, что выпуск биткойна предсказуем, контролируем, и недоступен для манипуляций со стороны отдельной личности, организации или правительства. Мы много раз наблюдали на протяжении истории, включая недавнюю историю, примеры того, как правительства негативно влияют на выпуск денег, генерируя больше денег в угоду собственным сиюминутным экономическим интересам. Эти интересы часто представляют полный контраст с интересами людей, являющихся держателями валюты. Мы видели, как это может привести к инфляционной спирали, которая может разрушить всю экономику. Биткойн не может быть предметом такого рода манипуляций, поскольку выпуск контролируется самим протоколом, и его объем заранее известен всем, кто использует биткойн.

Ранее мы сказали, что у биткойна есть общие черты с наличными, однако возможности наличных ограничены, когда речь идет о защите от случайной потери или кражи. Биткойн также не обладает иммунитетом к потерям такого рода, однако ему присуще множество свойств, которые позволяют людям защитить свои деньги от потери или кражи. Это делает его гораздо более безопасным вариантом для ношения в заднем кармане, чем кошелек, полный наличных.

Обычная валюта не предназначена для электронной эры. Это система денег, которая использовалась сотни, если не тысячи, лет, задолго до изобретения электричества, не говоря уже о развитии компьютеров и интернета. Она использовалась с тех времен, когда торговля осуществлялась лицом к лицу, когда не было даже мысли о том, что можно переслать песню с одного конца света на другой за небольшую плату между сторонами, которые никогда даже не говорили друг с другом. На протяжении двадцатого столетия финансовые учреждения приспособили свои древние системы к электронной эре и разработали новые системы, которые соответствовали требованиям современности. За время службы этих систем, по мере расширения требований электронной коммерции, на их базе строились новые системы, выполняя задачи, для которых они не были изначально предназначены. В результате мы имеем со скрипом работающую банковскую систему, которая не рассчитана на огромное разнообразие электронных транзакций, осуществляемых в мире сегодня, и полностью зависима от финансовых институтов, которые извлекают огромные прибыли из этой зависимости.

Биткойн с самого начала был спроектирован для электронных транзакций, и это его сильная сторона. Он позволяет осуществлять мгновенные электронные транзакции из любой точки мира, на любую сумму, без необходимости доверяться другой стороне или какой-либо зависимости от третьей стороны. Когда цифровые валюты достигнут критической массы, наши сегодняшние сомнения покажутся глупыми.

Часть II

Как работает биткойн

Глава шестая

Асимметричные ключи

По своей сути биткойн – это открытый протокол. Говоря «протокол», я имею в виду, что биткойн – это набор правил, которому должны соответствовать биткойн-программы. Говоря «открытый», я имею в виду, что протокол, или набор правил, находятся в публичном доступе, и любой может их проверить. Этот протокол позволяет биткойн-программам (которые мы обычно называем биткойн-клиентами) связываться друг с другом через интернет стандартизированным способом.

Тогда первым вопросом будет, если биткойн – открытый протокол, или набор правил, что удерживает людей от написания программ, нарушающих правила. Ответ – ничего. Кто угодно может написать программу, которая использует биткойн-протокол и связывается с другими биткойн-программами через интернет и пытается «нарушить правила» в свою пользу, однако клиенты, которые не соответствуют протоколу, просто игнорируются другими клиентами.

В качестве аналогии представьте игроков в шахматы по почте, когда игроки находятся в разных местах и их ходы отправляются в письмах. Оба игрока знают, как выглядит доска целиком, и любой из них может ходить, как захочет, если его ход соответствует шахматным правилам. В противном случае другой игрок игнорирует или отвергает этот ход. Тот же принцип лежит в основе биткойна: любой из «игроков» (биткойн-клиентов) точно знает, как выглядит «доска» (блокчейн), и может самостоятельно проверить по другим источникам, что любой «ход» другого (транзакция) является верным.

Если мы хотим понять биткойн на более глубоком, чем аналогия, уровне, то мы должны уяснить идею асимметричного шифрования (также известного как шифрование с открытым ключом). Асимметричное шифрование – это ключевой элемент биткойна, и без него биткойн не мог бы существовать. Идея асимметричного шифрования не нова, и фактически оно является составной частью безопасности многих программных систем. Мы используем асимметричное шифрование каждый раз, когда посещаем безопасный (SSL) сайт, например, сайт интернет-банка.

Прежде чем я объясню, что такое асимметричное шифрование, давайте представим такую задачу. Скажем, Алиса в Австралии хочет отправить письмо Бобу в Англию. Содержимое письма – большой секрет. Как Алисе послать письмо Бобу без риска, что по дороге кто-нибудь прочитает это письмо? Без асимметричной криптографии достичь этого можно только единственным способом, когда Алиса и Боб изначально понимают, как закодировать письмо. Тогда письмо будет зашифровано, и Боб будет знать, как его расшифровать, когда он его получит. Но что если у Алисы и Боба нет заранее подготовленного ключа для шифра; что если Боб никогда до этого не встречал Алису? В таких обстоятельствах без асимметричного шифрования Алиса не сможет безопасно отослать письмо Бобу.

Таким образом, это приводит нас к асимметричной криптографии и тому способу, которым она решает эту задачу. Некоторое время назад несколько талантливых математиков разработали способ, при помощи которого можно генерировать пары ключей, математически связанных друг с другом. В этом контексте можно представлять ключ как очень большое число – число с

несколькими сотнями цифр[6]. Эти ключи называются «открытый ключ» и «закрытый ключ», или вместе – асимметричные ключи. Оказывается, у этих ключей есть несколько очень полезных свойств!

Используя открытый ключ, можно зашифровать сообщение таким образом, что его будет возможно расшифровать только закрытым ключом. Таким образом, Боб может теперь сгенерировать пару ключей и передать всему миру свой открытый ключ, поскольку из него невозможно[7] получить его закрытый секретный ключ. Если Алиса хочет послать Бобу безопасное сообщение, она просто должна зашифровать содержимое своего письма открытым ключом Боба при помощи известного алгоритма, и Боб сможет расшифровать сообщение своим закрытым ключом, который он не показывает никому другому.

Вы используете технологию асимметричной криптографии каждый день, когда используете Wi-Fi, Bluetooth или безопасные вебсайты, где данные зашифрованы, чтобы предотвратить то, что называется атакой «человек в середине». Другими словами, асимметричная криптография используется, чтобы предотвратить перехват вашей беседы, письма или транзакции кем-либо еще.

Итак, теперь мы знаем, как Алиса может безопасно послать письмо Бобу, но, когда Боб получит письмо, как он может быть уверен, что письмо отправила Алиса, а не кто-нибудь другой? Оказывается, асимметричные ключи могут решить и эту проблему. Алиса также генерирует пару ключей: открытый и закрытый ключ. Как и Боб, Алиса раскрывает свой открытый ключ всему миру. Алиса может подписать содержимое письма «цифровой подписью», используя свой закрытый ключ. Затем, используя открытый ключ Алисы, Боб может определить, что письмо действительно было подписано Алисой, поскольку никто другой не может подписать письмо без доступа к закрытому ключу Алисы. Таким образом, письмо Алисы может прочитать только Боб, и Боб может удостовериться, что письмо написала именно Алиса.

Это очень полезная и мощная идея – она до сих пор впечатляет меня сегодня, несмотря на повседневное ее использование. Вы можете оценить ее полезность для военных коммуникаций, и, на самом деле, многие годы Соединенные Штаты пытались остановить экспорт программ, которые используют сильную асимметричную криптографию.

---

[6] Стоит остановиться и задуматься, насколько астрономически велико число, состоящее из нескольких сотен цифр. Это на много порядков больше, чем число атомов в наблюдаемой вселенной.

[7] Как мы уже заметили в третьей главе, нет ничего по-настоящему «невозможного» в мире криптографии, однако на практике некоторые вещи рассматриваются как достаточно сложные, чтобы для всех практических целей мы считали их невозможными.

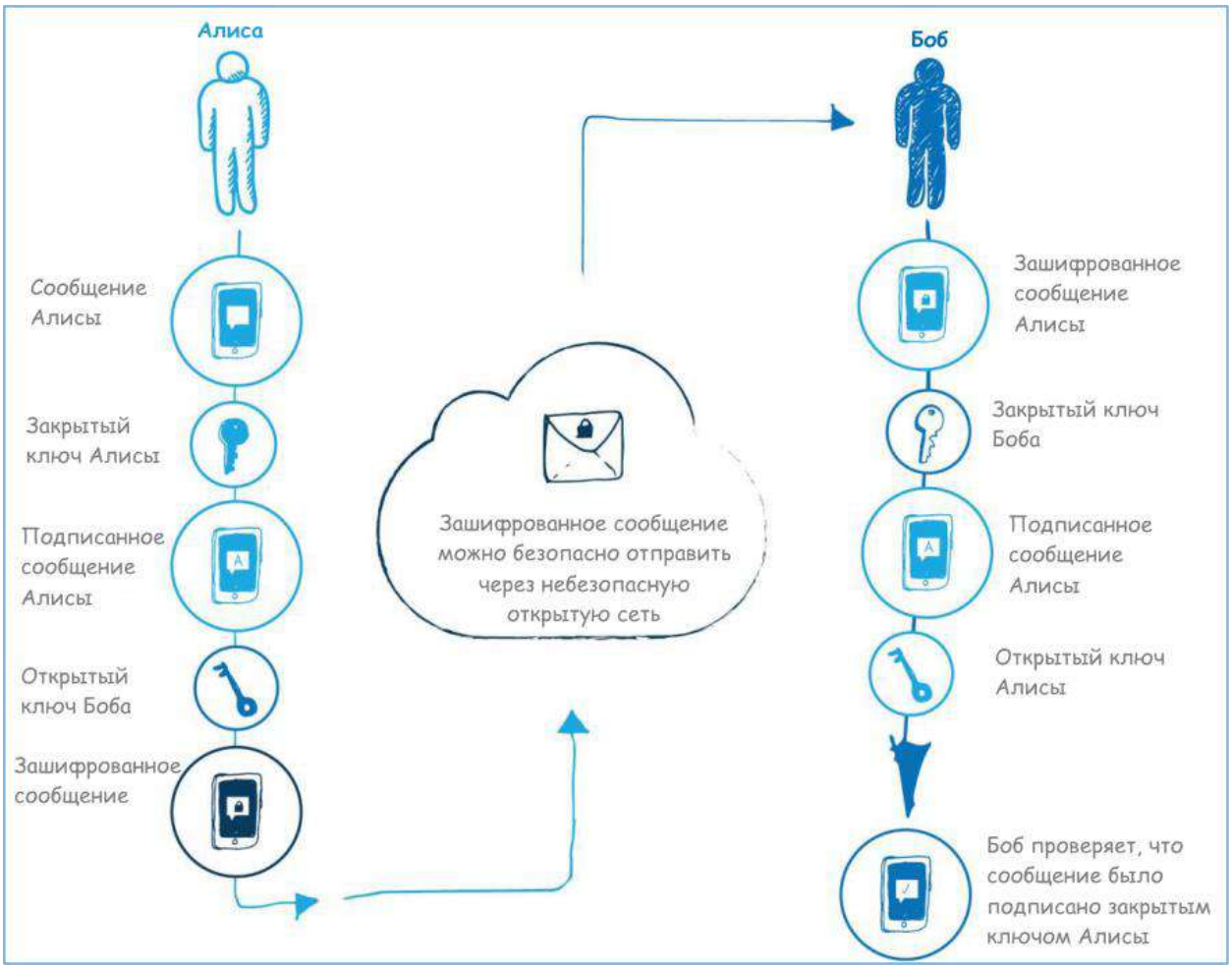


Рис. 2. Асимметричное шифрование. Алиса посылает подписанное зашифрованное сообщение Бобу.

Теперь, когда мы понимаем принцип работы асимметричной криптографии, как это относится к биткойну? Помните, в Главе третьей мы проводили аналогию и говорили, что в некоторых отношениях биткойн работает по принципу чековой книжки? Мы говорили, что один пользователь послал биткойны на биткойн-адрес другого пользователя, и что транзакция была подписана отправителем транзакции. Это и есть та точка, где все начинает соединяться: дело в том, что биткойн-адрес – это производная открытого ключа.

Давайте рассмотрим наш изначальный пример с чековой книжкой более подробно, поскольку теперь мы понимаем идею открытого ключа. У меня есть 50 биткойнов на моем мобильном телефоне, и я хотел бы отправить их на мобильный телефон моего друга Джо. Сперва Джо нажимает кнопку на своем телефоне, чтобы сгенерировать новый биткойн-адрес. Хотя, на самом деле, он создает пару асимметричных ключей. Закрытый ключ хранится на телефоне Джо, а производная от открытого ключа (биткойн-адрес) отображается на экране и затем пересылается мне. Используя биткойн-адрес Джо, я начинаю транзакцию на своем телефоне, указывая сумму, которую хочу отправить ему. Затем я подписываю эту транзакцию цифровой подписью, используя мой закрытый ключ, и отправляю транзакцию в интернет. Помните, мы говорили, что выписать

чек – это то же самое, что написать в банк письмо, разрешающее банку выделить средства с моего счета указанному человеку. В случае с биткойном, транзакция, в сущности, является публичным объявлением о передаче контроля над XBT 50, зарегистрированными на мой адрес, биткойн-адресу, который я указываю. Только мой закрытый ключ позволяет мне разрешить передачу биткойнов на адрес Джо, и я даю это разрешение, когда подписываю транзакцию цифровой подписью.

Когда транзакция отправлена, Джо может подтвердить в биткойн-сети, что у него есть право потратить эти биткойны – транзакция окончательная. Разумеется, несмотря на все эти технические шаги, все это происходит автоматически, за кулисами, посредством нажатия нескольких кнопок на телефоне.

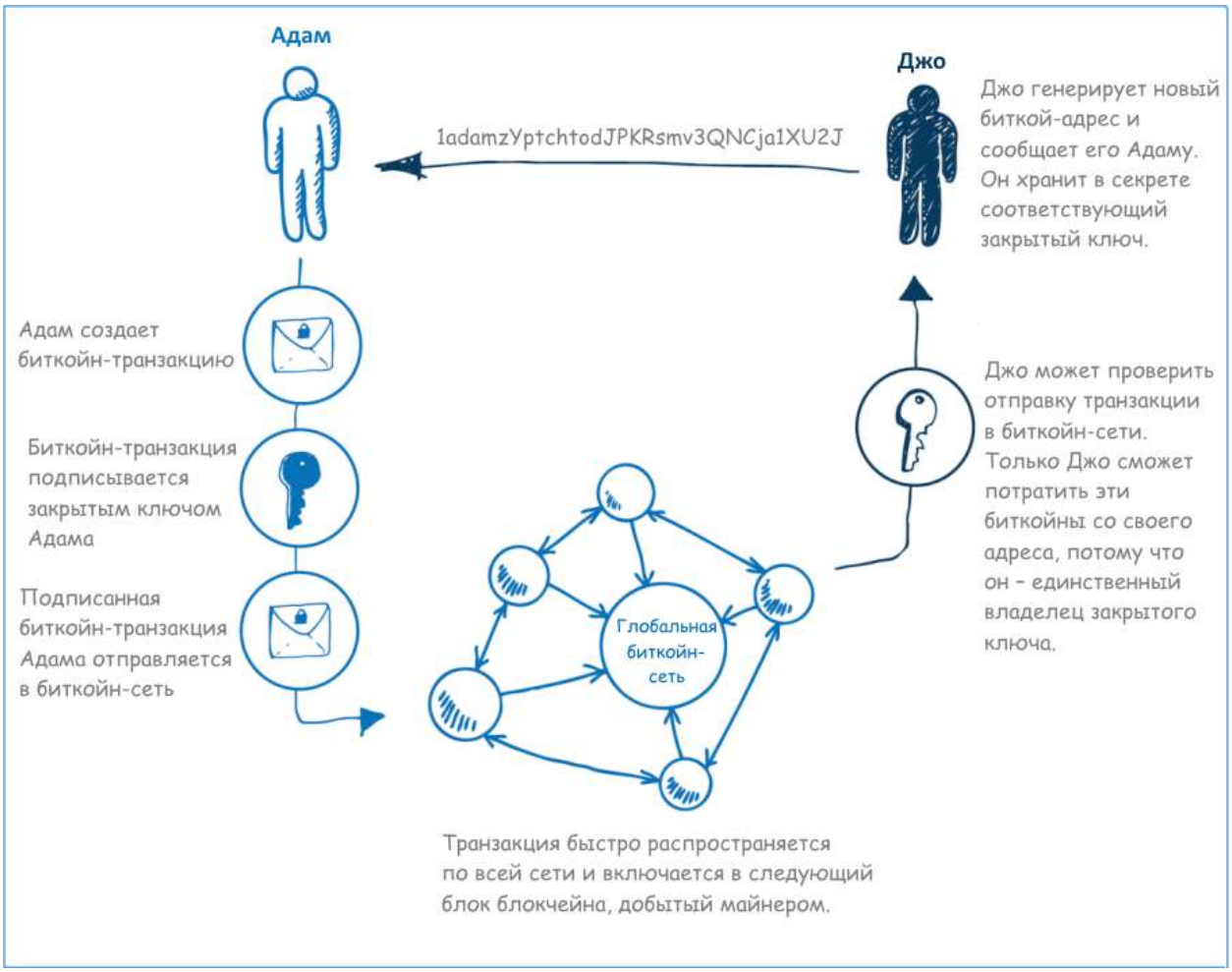


Рис. 3. Адам посылает Джо биткойны через биткойн-сеть

Глава седьмая

Хеширование

В Главе четвертой мы рассмотрели, как биткойны генерируются и вводятся в экономику. Мы объяснили, что биткойны генерируются примерно каждые десять минут в ходе решения математической задачи. В этой главе мы рассмотрим более подробно, как это работает. Чтобы разобраться в добыче биткойна, нам нужно познакомиться с другой идеей из компьютерных наук: это хеширование, или криптографический хеш.

Хеширование – это очень интересная концепция, которая, как и асимметричная криптография, является одной из ключевых идей в сфере безопасности программного обеспечения. Как мы делали ранее, давайте начнем с представления задачи. Если у меня есть компьютерная система, как я мог бы безопасно хранить пароль каждого пользователя таким образом, что если система будет скомпрометирована, то пользовательские пароли – не будут? Другими словами, по очевидным причинам это плохая идея – хранить базу данных, содержащую тысячи или миллионы пользовательских паролей.

Решение этой задачи включает в себя криптографический хеш. Процесс хеширования получает нечто на вход, например, пароль, и пропускает эти входные данные через алгоритм, который выводит большое число, называемое «хеш». Хеш определяют две отличительные особенности. Во-первых, для одних и тех же входных данных процесс хеширования всегда возвращает одинаковый результат. Например, если вы вводите пароль, который пропускается через алгоритм хеширования, генерирующий определенное число, то каждый раз будет генерироваться одно и то же число. Во-вторых, хеширование – это однонаправленный процесс. Невозможно взять значение хеша и при помощи обратной разработки раскрыть, что было на входе. Эти два свойства и определяют криптографический хеш. Если бы процесс был обратим, он назывался бы не хешированием, а старым добрым шифрованием/дешифрованием, и это совершенно другая тема.

Оказывается, процесс хеширования значений имеет множество полезных особенностей в приложении к компьютерным наукам. Одной из задач, которые мы предлагали выше, была задача о безопасном хранении пользовательских паролей в системе. Вместо того, чтобы хранить пароль пользователя, мы сперва хешируем его пароль[8] и храним значение хеша. Когда пользователь пытается в следующий раз войти в систему при помощи пароля, нам не нужно знать, каким был его пароль, мы только должны знать, что пароль совпадает с тем, что был введен в прошлый раз. Другими словами, если хеш введенного пароля совпадает с хешем, хранящимся в базе данных, мы знаем, что пользователь ввел правильный пароль – хотя мы не знаем, и не хотим знать, что это был за пароль. Если позже наша система будет скомпрометирована, атакующий получит только список хешей паролей, необратимых и не имеющих никакой ценности.

Если вы похожи на меня, этот процесс покажется вам очаровательным, но вы, вероятно, спросите себя – если пароли хешируются, как же получается, что если вы забыли пароль к определенной системе, то компания может выслать вам его по электронной почте. Это очень

[8] Процесс хеширования пользовательского пароля немного более сложен, и включает добавление к паролю случайного значения, известного как «соль». Таким образом, если у двух человек будет одинаковый пароль, это обеспечивает разные значения хеша, делая систему более безопасной.

хороший вопрос. Это означает, что пароли не хешируются, и эта система крайне небезопасна. Печально, но многие системы сегодня допускают это. Это одна из причин, по которым нужно использовать разные пароли для каждой из систем, к которым вы имеете доступ. Когда в новостях обнаруживается, что система была «хакнута» и тысячи паролей скомпрометированы, это случается потому, что проектировщики системы не смогли обеспечить безопасность пользовательских паролей с помощью техники хеширования, которая повсеместно считается наилучшим подходом.

Ради интереса заметим, что, если вы забыли пароль к системе, которая надлежащим образом хеширует пароли пользователей, правильный подход – это сброс пароля системой, когда пароль заменяется каким-нибудь временным значением, что позволяет вам поменять его на что-нибудь другое, когда вы войдете в систему. Однако, надо заметить, что такой подход не гарантирует, что система на самом деле хеширует пароли.

Теперь, каким образом все это относится к добыче биткойна? Ну, мы сказали, что обратная разработка хеша невозможна. Технически говоря, теоретически она возможна посредством того, что называется атака «грубой силой» – перебор всех возможных входных комбинаций до тех пор, пока не получится такой же хеш. Однако, на практике количество комбинаций астрономически велико, что делает такую атаку невозможной в практических целях. Также нужно заметить, что разные входные значения могут выдать в результате одинаковое значение хеша, это явление называется коллизией и случается крайне редко, если использовать правильный алгоритм хеширования, так что для нашего обсуждения здесь это неважно.

Теперь давайте предположим, что есть только миллион возможных значений хеша, число между нулем и миллионом. В реальности, конечно, мы знаем, что возможно гораздо больше миллиона значений хеша, но давайте продолжим с миллионом, чтобы проиллюстрировать мою мысль. Таким образом, шансы правильно угадать верные входные данные для данного хеша будут один к миллиону. Имея достаточное количество попыток и достаточное время, в конце концов я найду исходные данные, которые после хеширования дадут значение, которое я пытаюсь подобрать.

Давайте предположим, что процесс проб и ошибок занимает двадцать четыре часа чтобы найти совпадение (современный домашний компьютер сделает миллион итераций меньше, чем за секунду, но давайте оставим двадцать четыре часа для нашего примера). Помня, что в нашем примере мы сказали, что все значения хеша – это числа между нулем и миллионом, давайте предположим, что вместо нахождения входных данных, которые дадут определенное значение хеша, мы хотели бы найти входные данные, хеширование которых даст число, меньшее или равное 10. То есть, мы хотим найти любой вход, который даст в результате значение хеша 1, 2, 3, 4, 5, 6, 7, 8, 9 или 10. В этом случае в десять раз более вероятно, что полученное нами значение хеша подойдет, поэтому наш компьютер найдет совпадение в среднем в десять раз быстрее – теперь потребуется примерно 2,4 часа вместо 24 часов.

Если бы я хотел создать задачу, которая будет решаться быстрее, скажем, решаться за 10 минут, я бы поднял ограничение до любого хеша между 1 и 150. Задача теперь в 150 раз проще, чем в первом примере, и быстрый подсчет покажет, что такая задача должна решаться нашим (медленным) компьютером примерно за 10 минут. Что случится, если второй, настолько же мощный компьютер подключится к попыткам найти решение задачи? Теперь ее можно будет

решить в два раза быстрее. Если я хочу, чтобы решение все равно занимало 10 минут, я должен буду сделать задачу в два раза труднее, задав условие, что значение хеша должно быть теперь меньше 75, а не 150. По мере того, как все больше компьютеров подключаются к решению задачи, и они все эффективнее начинают решать задачу, мы делаем ее более сложной, задавая меньший диапазон приемлемых значений хеша.

И, если вы до сих пор не догадались, это и есть задача, которую биткойн-сеть предлагает биткойн-майнерам. Разница, конечно, в том, что существует гораздо больше миллиона комбинаций, числа так велики, что их так просто и не назовешь. Все биткойн-майнеры мира в то время, пока я пишу этот текст, коллективно обрабатывают примерно 350 000 000 000 000 000 входных значений в секунду в попытке найти то самое значение, хеш которого попадет в определенный диапазон значений хеша.

Биткойн-сеть регулярно оценивает сложность задачи, и, если задача решается быстрее или медленнее, чем за установленный интервал 10 минут, тогда задача соответствующим образом подстраивается посредством расширения или сокращения диапазона приемлемых значений хеша. Из всех компьютеров мира, пытающихся решить задачу, только первый решивший получает биткойны «в награду», и процесс начинается заново. Следующий вопрос тогда: как остальная биткойн-сеть подтверждает, что задача была решена, и каким образом в этом процессе генерируются биткойны? Первый вопрос простой. Компьютер, который решил задачу, объявляет об этом решении биткойн-сети, и другие компьютеры проверяют решение. Хотя обратная разработка входного значения для данного диапазона значений хеша – это медленный процесс проб и ошибок, но как только решение найдено, его легко проверить, просто пропустив предложенное решение через алгоритм хеширования и убедившись, что результирующее значение хеша попадает в заданный диапазон. Затем добытые биткойны выдаются на определенный майнером адрес, вводя новые биткойны в экономику. Так же, как монархи в старину выпускали тэлли под налоги, которые никогда не будут собраны, и банки выпускали банкноты под средства, которых у них не было, биткойн-сеть медленно генерирует новые биткойны. Ключевая разница между биткойном и другими системами, однако, состоит в том, что во всех предыдущих системах частота генерации валюты устанавливалась по прихоти монарха, правительства, банка или, в последние времена, контролируемого правительством центрального банка. Частота генерации биткойна устанавливается алгоритмически, и не может быть предметом манипуляций участников рынка – она предопределена. Частота генерации определяется биткойн-протоколом, и со временем понижается, пока в конце концов биткойны не перестанут генерироваться вообще. Для любой даты в прошлом или будущем можно подсчитать примерное количество биткойнов в обращении.

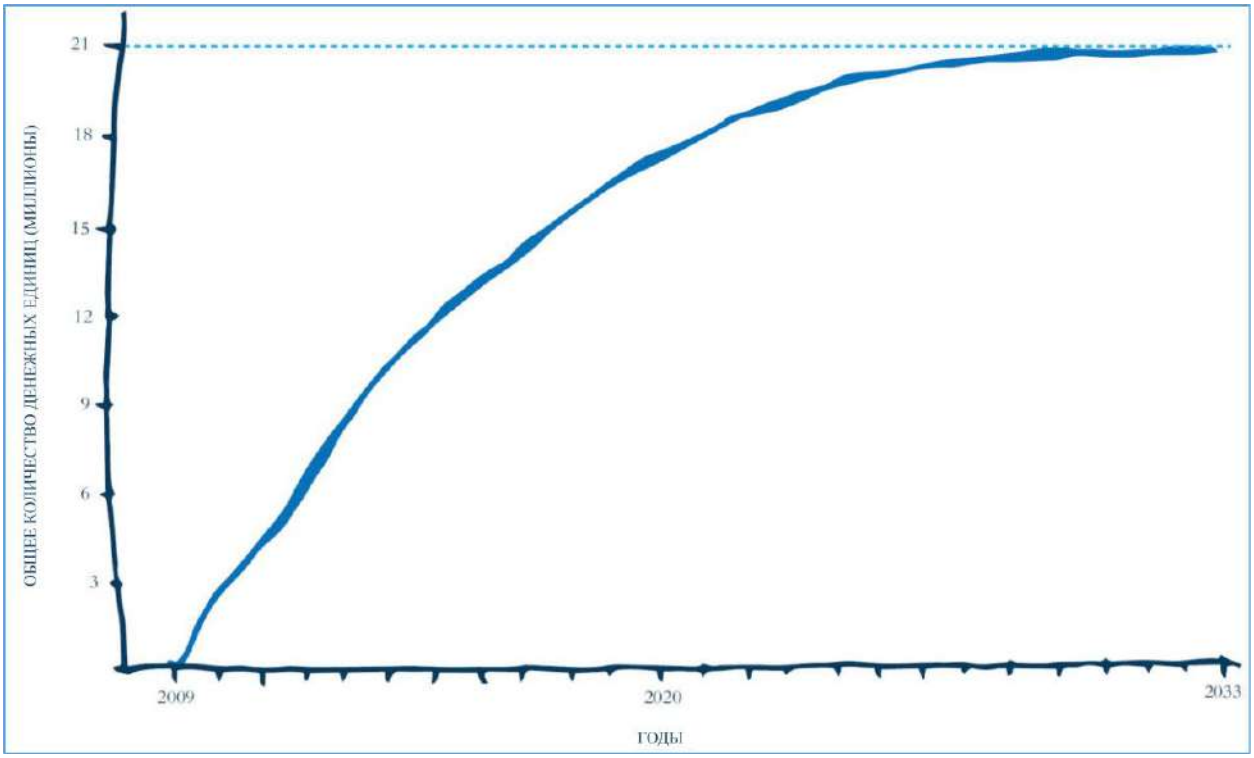


Рис. 4. Распределение биткойнов по времени

Глава восьмая

Децентрализация

Давайте ненадолго возьмем паузу на предыдущем направлении мысли, и обратимся к децентрализации. Децентрализация – относительно недавняя концепция в компьютерном знании, которая находит все больше применений за последнее десятилетие. Одним из первых примеров децентрализации стал пиринговый (P2P) файлообмен. За прошедшие годы существовало много его реализаций, наиболее распространенной из которых сейчас является сеть торрентов. Если вы незнакомы с торрентами, позвольте дать краткое введение. Традиционный метод загрузки файлов из интернета довольно прост. Один компьютер (сервер) хранит файл, который вам нужен, а другой компьютер (клиент) запрашивает этот файл с сервера, и сервер передает файл клиенту. Эта модель до сих пор преобладает сегодня, и большую часть времени, которое вы проводите в интернете, работает так, как описано. Кстати, эта модель называется клиент-серверной. Однако, у нее есть некоторые ограничения. Одно из этих ограничений состоит в том, что файл нельзя загрузить быстрее, чем позволит сервер. Обычно это не проблема, но что если есть миллион человек, которые хотят загрузить с сервера один и тот же файл? Пропускная способность сервера ограничена, вследствие чего этот ограниченный канал должен быть поделен между всеми людьми, загружающими файл. Кстати, отдельный сервер не может поддерживать миллион соединений, так что понадобится ферма из серверов, содержащих файл, что приведет к большим затратам для владельца серверов, или маленькой скорости для клиентов, загружающих файл.

Здесь может помочь распределенная пиринговая сеть. Она работает следующим образом: скажем, у меня есть файл, который я хочу сделать доступным для других людей. Используя P2P-программу этот файл делится на сотни частей (точный размер и количество частей зависит от многих факторов). Теперь люди могут загружать файл с моего компьютера по одной части за раз, в любом порядке. Пропускная способность с моей стороны невелика, так что изначально это будет довольно медленно для тех нескольких человек, которые попытаются загрузить этот файл с моего компьютера. Если кто-либо другой получил от меня одну из частей файла, остальные люди могут теперь загрузить эту часть либо с меня, либо с другого участника сети. Со временем все больше и больше народу загружает одни части файла с моего компьютера, а другие – с компьютеров других людей, до тех пор, пока первоначальный файл не окажется распределен между компьютерами множества людей. Если приходит кто-то новый и хочет загрузить этот файл, программа будет одновременно загружать файл со множества разных компьютеров, возможно, никогда больше не соединяясь с моим компьютером, на котором файл находился изначально – в сущности, в этот момент я могу вообще выключить свой компьютер, и при условии, что в интернете находится полная копия файла, люди будут продолжать его загрузку беспрепятственно. Эта система показала себя очень успешной для файлов, пользующихся большим спросом. В последнее время мы можем видеть, что децентрализованный подход применяется в программных продуктах, для которых он изначально не задумывался, и наиболее свежим примером является блокчейн.

Глава девятая

Блокчейн

Мы рассмотрели и обсудили три основные идеи из области компьютерных наук, лежащие в основе биткойна: асимметричную криптографию, криптографический хеш и пиринговые сети. Хоть эти идеи и интересны, они не революционны в контексте биткойна. Все эти вещи уже применялись в различных вариантах долгое время. Однако, то, что связывает их воедино – это фундаментально новая идея, являющаяся основой биткойна. Эта идея известна как блокчейн.

Блокчейн – это децентрализованный открытый гроссбух: давайте попробуем в этом разобраться. В случае обычного бизнеса, или скажем лучше, банка, гроссбухом называют набор записей, который содержит подробности пользовательских транзакций и балансы счетов. В современных банках эти записи хранятся в больших программных системах. Как вы, вероятно, можете догадаться, это большие устойчивые системы, которые должны поддерживать миллионы пользователей, ежедневно осуществляющих миллионы транзакций. Возможно, вам уже знакомы некоторые из симптомов тех трудностей, которые испытывают банки с надежным управлением столь большими наборами данных. Например, вам не удавалось загрузить с интернет-портала вашего банка историю транзакций ранее некоторого периода в прошлом. Или, возможно, вы замечали, что некоторые транзакции не сразу появляются в истории, пока они не будут обработаны ночью. Все эти и другие похожие странности являются компромиссами, необходимыми для того, чтобы банки могли управлять этими (часто древними) системами, содержащими огромные объемы данных.

Мы сказали, что блокчейн – это децентрализованный открытый гроссбух. Мы знаем, что такое гроссбух: это набор записей, содержащих подробности пользовательских транзакций и балансы счетов. Теперь давайте объясним, что мы имеем в виду под «децентрализованным» и «открытым». В отличие от банка этот гроссбух не хранится на центральном сервере, контролируемом каким-либо человеком или организацией. Блокчейн-гроссбух доступен публично и хранится локально множеством клиентов, его можно свободно загрузить из интернета. В это может быть трудно поверить, но вы поняли правильно: вся история любых биткойн-транзакций, сделанных кем угодно по всему миру с самого появления биткойна (12 января 2009 года) публично доступна для просмотра любому человеку, к тому же, на большинстве компьютеров или ноутбуков, где есть биткойн-программы, хранятся копии этого гроссбуха. Вероятно, у вас появилось много вопросов, например, как это возможно, или почему это вообще хорошая идея. Давайте начнем с того, как это возможно. Конечно, это большой объем данных, но не невозможно большой. Финансовые записи занимают очень немного места, и объективно глядя, все записи о биткойн-транзакциях с самого начала на момент написания этого текста занимают тот же объем места, что и дюжина, или около того, фильмов в HD-качестве. Если вы загрузите биткойн-клиент, который хранит локальную копию блокчейна, потребуется много времени, чтобы начать в первый раз, когда вы его запустите, поскольку он загружает полную копию блокчейна. Другое дело, что хранение полной копии блокчейна на всех компьютерах мира не является абсолютно необходимым. Это определенно невозможно на мобильных устройствах, и сейчас в тренде биткойн-клиенты, которые хранят локально только важные вещи, а не весь блокчейн. Тем не менее, это иллюстрирует мое утверждение о том, что блокчейн публично доступен всему миру, и фактически существует множество сайтов, которые упрощают навигацию по истории всех биткойн транзакций, сделанных кем угодно и когда угодно.

Вас, возможно, несколько обеспокоит тот момент, что, если вы будете использовать биткойн, вся история когда-либо сделанных вами транзакций будет публично доступна. Это только частично правда, и мы обсудим этот момент далее, в главе об анонимности. Публичный гроссбух содержит только биткойн-адреса и суммы. В нем нет какой-либо личной или опознаваемой информации. Другими словами, если я посылаю 50 биткойнов с адреса А моему другу Джо с адресом Б, весь мир видит, что 50 биткойнов отправлены с адреса А на адрес Б, но никто не может определить, что адрес А принадлежит мне и адрес Б принадлежит Джо. Так что, когда я гляжу на блокчейн, все, что я вижу – это балансы адресов и транзакции с одного адреса на другой – ничто из этой информации не ставит под удар конфиденциальность людей, осуществляющих эти транзакции.

Другой момент, который необходимо понять, и который мы еще не обсуждали, состоит в том, что в отличие от электронной почты, где вы можете иметь только один адрес, или, по крайней мере, небольшое количество адресов, количество биткойн-адресов, которые могут быть у человека, не ограничено. Фактически это поощряется, и большинство биткойн клиентов настроены по умолчанию таким образом, чтобы каждая транзакция использовала новый адрес. Давайте еще раз рассмотрим пример отправки 50 биткойнов моему другу Джо, сейчас мы уже знаем немного больше. Когда я прошу Джо сказать мне его биткойн-адрес, он, как правило, не называет мне адрес, содержащий всю сумму его богатства, а создаст абсолютно новый адрес, на котором вообще нет биткойнов, и я отправляю 50 биткойнов на этот новый адрес. Биткойн-программы не требуют от вас управления балансом каждого адреса индивидуально, они могут показать вам общий баланс всех адресов, которые вы когда-либо создавали. Если взглянуть на дело с моей стороны, вряд ли у меня есть адрес, содержащий точную сумму денег, которую я хочу отослать Джо. Например, у меня может быть биткойн-адрес А, на котором есть 30 биткойнов, и биткойн-адрес Б, с 35 биткойнами. В нашем примере программа автоматически сгенерирует транзакцию, которая возьмет 30 биткойнов с адреса А, потом 20 – с адреса Б, отправит эти 50 биткойнов на адрес Джо, а также отправит оставшиеся 15 биткойнов на новый адрес В, который она автоматически сгенерировала для меня. И у Джо, и у меня могут быть сотни или тысячи адресов, содержащих маленькие суммы денег, которые вместе составляют наше полное биткойн-состояние. Ни один из нас не может видеть адресов другого, кроме тех, которые используются в транзакции.

Исключением из этого правила будет случай, когда я получаю одну транзакцию на большую сумму денег, скажем, миллион долларов в биткойнах. Если после этого я захочу потратить 1 биткойн с этого адреса, получатель сможет увидеть, что я имею в своем распоряжении около миллиона долларов в биткойнах, что я не хотел бы раскрывать. Достаточно сказать, что для счастливчиков, оказавшихся в таком положении, существуют техники, позволяющие скрыть это богатство, разбрасывающие деньги по множеству адресов – современные программы делают этот процесс тривиальным.

Теперь, когда мы знаем, что такое блокчейн, как он на самом деле работает? Вопрос, возможно, стоит сформулировать так: как мы можем обеспечить непротиворечивую запись транзакций в децентрализованном окружении? Первое, что нужно понять о блокчейне, это то, что он называется блокчейном потому, что состоит из цепочки последовательных блоков. Блок – это группа транзакций. Угадайте, с какой частотой генерируются блоки? Примерно раз в 10 минут.

Наверное, вы начали понимать, что существует связь между блокчейном и добычей биткойна, и если вы предположили это, вы правы.

Глава десятая

Добыча биткойна

Помните, в Главе четвертой мы сказали, что добыча биткойна помимо введения биткойнов в экономику преследует также две других цели. Она обеспечивает обработку платежей и безопасность сети. Давайте теперь рассмотрим, каким образом эти задачи выполняются в процессе добычи биткойна. Выше мы упоминали, что, когда транзакция начата, она отправляется в биткойн-сеть. Что это означает на самом деле? Биткойн-клиенты (т.е. программы) пытаются соединиться со множеством других биткойн-клиентов, которые называют «пиры». Обычно каждый отдельный клиент соединен с 10-20 другими пирами. Некоторые из этих пиров – обычные пользователи, осуществляющие транзакции, и небольшое число этих пиров могут быть майнерами. Когда биткойн-клиент получает сведения о биткойн-транзакции, они передаются от клиента к клиенту до тех пор, пока через короткий промежуток времени не будут получены одним или несколькими биткойн-майнерами.

Биткойн-майнеры делают еще кое-что помимо решения хеш-задачи и введения биткойнов в экономику: они обеспечивают важную функцию создания блокчейна, по одному блоку за раз. Когда биткойн-майнер получает сведения о транзакции, сперва проверяется ее подлинность, и затем она записывается в блок локально, на компьютере биткойн-майнера. Если биткойн-майнер успешно решил задачу, решение задачи включается в блок как его часть, вместе со всеми транзакциями, созданными за прошедшие 10 минут. Затем блок закрывается и распространяется по интернету, и процесс начинается заново. Любой другой в сети может независимо проверить, что транзакции в блоке подлинные и что решение хеш-задачи, известное также как «доказательство работы», верно. Любые последующие майнеры, которые решили задачу, игнорируются, их блоки больше не подходят, и процесс начинается заново. Таким образом блокчейн – это последовательность блоков, содержащих транзакции за данный десятиминутный период. Каждый блок математически связан с предыдущим блоком, так что можно тривиальным (для компьютера!) образом проверить весь блокчейн на достоверность, не анализируя при этом отдельные транзакции.

И это приводит нас к третьей цели, которой достигают биткойн-майнеры: безопасности сети. Действия, предпринимаемые для решения криптографической хеш-задачи, служат не только интересам майнера, они также нужны для защиты от нечестных майнеров, расходующих деньги дважды, что называют «двойной тратой». Если взять более ранний пример, где я посылаю 50 биткойнов Джо, пусть взамен Джо присылает мне книгу, которую я у него купил (по сегодняшним ценам это была бы довольно дорогая книга). В то же время, что если я попробую отправить те же самые 50 биткойнов другому человеку, перед тем, как первая транзакция успела стать обработанной и проверенной? Предполагая, что я уже получил товар от Джо, будет проблематично, если биткойн-сеть каким-то образом примет мой платеж другому участнику и позже отклонит изначальный платеж, который я отправил Джо. Децентрализованная добыча биткойна решает эту проблему.

Когда я отправляю транзакцию для Джо в биткойн-сеть, Джо почти мгновенно сможет ее увидеть (обычно через несколько секунд). В это время транзакция видна, но еще не включена в блок майнером. Если это транзакция с небольшой суммой, или транзакция между участниками, которые доверяют друг другу, видимость транзакции в сети будет обычно считаться приемлемой,

однако, при определенных усилиях с моей стороны, все еще возможно дважды потратить средства, отправив в сеть другую транзакцию, которая использует те же самые средства – но для транзакций с небольшой суммой требуемые усилия, вероятно, не будут стоить затраченного времени (к тому же, разумеется, есть еще и риск быть пойманным). По прошествии приблизительно 10 минут мы можем ожидать, что моя транзакция будет теперь официально включена биткойн-майнером в последний блок блокчейна. В этом момент транзакция имеет «одно подтверждение». Теперь, если вы примете во внимание, что в мире тысячи специальных компьютеров, добывающих биткойн, вероятность, что я сумею обмануть Джо и дважды потратить свои средства, и успешно добыть блок, который отвергнет транзакцию для Джо, очень мала. Для транзакций со средними или большими суммами обычно считается благоразумным подождать 3-6 подтверждений, или, другими словами, подождать, когда будут добыты 3-6 последовательных блоков (от 30 до 60 минут), чтобы быть абсолютно уверенным в транзакции. Чтобы успешно осуществить двойную трату, в этом случае нужно будет успешно добыть подряд 6 блоков, отклоняющих транзакцию. И чтобы достичь этого, нужно контролировать примерно 50 % от общей вычислительной мощности биткойн-сети. Как вы можете видеть, это делает попытку двойной траты крайне сложной и дорогой, что прежде всего перевешивает, в общем случае, любые преимущества двойной траты. Вы также можете видеть, что по мере того, как растет биткойн-сеть, увеличивается количество майнеров и возрастает трудность хеш-задачи, двойная трата становится еще более сложной для нечестного майнера. Именно так биткойн-майнеры обеспечивают безопасность сети.

Резюмируя, добыча биткойна обеспечивает три вещи: обработку транзакций, безопасность сети и ввод биткойнов в экономику. Это изящная система.

Глава одиннадцатая

Стимул майнера

Настало время указать на тот факт, что у майнера есть выбор, включать или не включать транзакцию в блок. Майнер может отклонять все транзакции, если хочет, и просто решать хеш-задачу. Это называется «добыча пустого блока» и время от времени случается. Тогда вопрос в том, зачем майнеру вообще беспокоиться о том, чтобы включать транзакции в блок? Есть несколько причин. Во-первых, по сравнению с работой, которую майнер делает, пытаясь решить хеш-задачу, включение транзакций в блок – это тривиальная операция, которая почти ничего не требует от его компьютера. Во-вторых, транзакции включаются в блокчейн в интересах биткойн-сообщества. Если майнеры не будут включать транзакции в блокчейн, биткойн не будет работать, а если он не будет работать, то биткойны ничего не будут стоить. Если же биткойн ничего не будет стоить, тогда майнеры будут тратить все свои усилия на добычу чего-то, что ничего не стоит. Вы можете возразить, что для сообщества хорошо, чтобы майнеры включали транзакции в блок, но для индивидуального майнера убыточно тратить ресурсы на обработку транзакций. Это отчасти верно, но, как я заметил в начале абзаца, необходимые усилия ничтожны. Существует также и третий момент. Майнеры не могут брать комиссию за включение транзакции в блок, но люди, осуществляющие транзакции, могут добровольно предложить комиссию. Майнеры тогда могут отклонять транзакции, которые вообще не включают комиссии, или отклонять транзакции с комиссией ниже определенной величины. Какова же обычная комиссия сегодня? В большинстве случаев она нулевая. В сегодняшней экономике стимулом майнера в первую очередь являются биткойны, которые он получает за успешно добытый блок. Транзакции включаются в блок по доброй воле майнеров в интересах роста биткойн-экономики и роста биткойна. В некоторых случаях биткойн-клиенты автоматически включают небольшую комиссию (не больше нескольких центов), чтобы удостовериться, что транзакции не будут отклонены майнерами и с большей вероятностью будут включены в следующий добытый блок.

С течением времени количество биткойнов, получаемых за успешно добытый блок, будет постепенно уменьшаться, пока, примерно в 2140 году, награда за добычу блока не окажется нулевой. Ожидается, что за этот долгий период времени, пока вознаграждение за блок как стимул для добычи биткойна постепенно уменьшается, этот стимул будет постепенно частично заменяться и, в конце концов, будет вытеснен стимулом в виде комиссий за транзакции.

Благодаря тому факту, что биткойн-экономика – это открытый рынок, и что комиссии за транзакции добровольны, величина комиссии всегда будет определяться спросом и предложением, что создаст конкурентоспособный рынок с низкими комиссиями за транзакцию.

Глава двенадцатая

TL;DR

TL;DR: известное сленговое выражение, означающее «слишком длинно; не читал». Это краткое резюме в конце длинного текста, содержащее его сокращенную версию. Однако, к сожалению, если вы открыли эту главу, не прочитав предыдущие главы второй части, где в общих чертах описаны ключевые принципы компьютерных наук, лежащие в основе биткойна, тогда вам будет трудно понять эту главу, и в своем понимании биткойна в дальнейшем вы останетесь на уровне сравнений по аналогии. Если вы прочитали Часть II, то эта глава нужна, чтобы собрать все эти идеи вместе в ясное понимание биткойна.

Сперва мы узнали, что асимметричная криптография – это технология, лежащая в основе закрытых и открытых ключей; используя это отношение, мы можем математически проверить достоверность биткойн-транзакции, подписанной закрытым ключом отправителя. Затем мы узнали о криптографическом хеше, который является необратимым алгоритмом, применяемым к некоторым данным. Методом проб и ошибок (более квадрильона попыток в секунду) майнеры в биткойн-сети пытаются вычислить криптографический хеш для случайных данных до тех пор, пока результирующее значение хеша не попадет в предзаданный диапазон – задача, спроектированная таким образом, чтобы решаться в среднем за десять минут всей биткойн-сетью. Трудность этой задачи с одной стороны защищает сеть от «двойных трат», а с другой стороны контролирует поставку биткойна. В дополнение биткойн-майнеры также обрабатывают транзакции, формирующие блок. Если майнер успешно добудет блок (решив криптографическую хеш-задачу), этот блок будет распознан биткойн-сетью и навсегда включен в блокчейн – открытый децентрализованный гроссбух биткойна. Это кратчайшее описание того, как работает эта сложная и изящная система.

Часть III

Более широкий взгляд

Глава тринадцатая

Mt. Gox

Если вы ничего не знали о биткойне до прочтения этой книги, вы все равно могли слышать название «Mt. Gox» благодаря основным медиа. Mt. Gox составил интересную часть истории биткойна, так что стоит разобраться, что случилось. Mt. Gox – это обанкротившаяся японская биткойн-биржа, запущенная французом по имени Марк Карпелес.

До 2013 года биткойн был мало известен за пределами горстки людей, разбросанной по всему миру. Тогда он еще не стал мейнстримом и не был предметом обсуждения правительств крупных государств. Если в те времена вы хотели купить биткойн, у вас был весьма ограниченный выбор. В те годы Mt. Gox безоговорочно был крупнейшим биткойн-обменником в мире, утверждавшим, что держит более, чем 80 % рынка торговли биткойном. Я полагаю, это было близко к истине, поскольку в тот период альтернатив было немного.

Поскольку Mt. Gox контролировал подавляющее большинство биткойн-торгов, а большинство людей очень мало понимали в биткойне, название «Mt. Gox» стало почти синонимом биткойна как такового. Кстати, есть известная история о том, почему Mt. Gox стал называться «Mt. Gox». Видимо, когда создавался сайт, изначальный владелец уже купил доменное имя *mtgox.com* для другого проекта, над которым он работал, связанного с карточной игрой «Magic: The Gathering». Поэтому доменное имя означало «Magic The Gathering Online eXchange». Позже он отказался от идеи этого сайта, и доменное имя использовалось для биткойн-биржи, известной как «Mt. Gox». Через некоторое время первый владелец продал большую часть своей компании Марку Карпелесу.

Теперь я думаю, что в ранние дни Mt. Gox, возможно, никто не предполагал, что сайт столь вырастет – может и да, но я сомневаюсь, что они могли предполагать невероятный рост биткойна в начале 2013 года. По разным причинам биткойн начал процветать, выведя цену одного биткойна примерно с 10 до примерно 250 долларов всего за несколько месяцев. В дальнейшем цена выросла до почти 1000 долларов к концу года. И куда шли люди, чтобы купить биткойн? Одним из немногих мест, где они могли это сделать, был обменник Mt. Gox.

Я хочу подчеркнуть, что у меня нет никакой инсайдерской информации о том, что делал или чего не делал Mt. Gox; я знаю о Mt. Gox только как их клиент, а также из обсуждений с коллегами по индустрии. В начале 2013 года мой бизнес-партнер Адриан и я использовали Mt. Gox чтобы купить себе биткойн. Поскольку большую часть нашей карьеры мы занимались разработкой программных систем для финансовых институтов, платформа Mt. Gox показалась нам непрофессиональной и дилетантской. Открытие и верификация наших аккаунтов заняла у них несколько недель, их клиентская служба работала плохо, а сайт не обновлялся долгое время. К тому же ходили рассказы об отказах систем Mt. Gox под сравнительно большой нагрузкой и сообщения о том, что их «хакнули» и люди потеряли деньги. Определенно это был тип финансовой системы, которому я не стал бы доверять свои деньги. При этом мы собирались купить биткойн. Наша стратегия была такова: мы депонировали относительно небольшие суммы денег, покупали биткойн, немедленно его выводили, и повторяли этот цикл снова. Таким образом, в случае каких-либо проблем с Mt. Gox наши потери ограничивались бы суммой последнего депозита. К несчастью для многих других клиентов Mt. Gox, они не использовали подобный подход. К середине 2013 года стало очевидно, что у Mt. Gox неприятности, поскольку

они приостановили вывод денег, и вскоре после этого компания объявила о банкротстве, признавая потерю почти всех биткойнов, которые они хранили для клиентов, что к моменту их банкротства составляло приблизительно полмиллиарда американских долларов, или около 7 % всех биткойнов в обращении.

По любой шкале это событие было катастрофой для биткойна в целом. Это было катастрофой для всех, имевших биткойн-счета, и катастрофой для репутации биткойна, который многим виделся провальным сам по себе благодаря плохому управлению Mt. Gox. Я не знаю, почему Mt. Gox потерял деньги. В одном из своих объявлений они подозревали, что деньги украдены, но в конечном счете это просто спекуляция на тему того, как так получилось – суть в том, что люди потеряли из-за этого много денег.

Сожалея о тех, кого затронул коллапс Mt. Gox, нужно заметить, что объявление об их банкротстве было в некотором роде желанным. Их задержки и приостановка вывода денег, длившаяся много месяцев вызывала новые проблемы для биткойн-сообщества, и очень плохую репутацию в прессе. Mt. Gox был тикающей часовой бомбой. Их коллапс позволил начать с чистого листа другим компаниям, гораздо более надежным, чем Mt. Gox, и вести биткойн вперед.

Также можно заметить, что в какой-то степени именно плохо организованная платформа Mt. Gox привела нас к идее создания собственной биткойн-биржи, Independent Reserve. Мы знали, что для того, чтобы биткойн в конечном счете был успешным, нужна была стабильная, устойчивая платформа, на которой люди могут покупать биткойн, и Mt. Gox таковой не являлся.

Глава четырнадцатая

Silkroad

Если вы не слышали о коллапсе Mt. Gox в 2014 году, то, возможно, вы слышали о Silkroad. Кстати, название «шелковый путь» изначально относится к последовательности торговых путей, соединявших Азию и Европу на протяжении многих периодов истории. Они назывались так благодаря выгодной торговле китайским шелком, осуществлявшейся вдоль путей, и значительно поспособствовали развитию торговли между двумя частями света.

«Шелковый путь», о котором мы говорим, однако, был сайтом специального типа. Он был особенным, потому что к нему не было доступа из обычного браузера. Доступ к нему можно было получить только используя специальную программу под названием «Tor»[9], которая делала пользователя анонимным, позволяя людям заходить на сайт так, чтобы их невозможно было отследить. Сайт Silkroad был в сущности рынком, где вы могли покупать и продавать товары. Благодаря тому факту, что он был настроен с явно выраженной целью анонимизировать пользователей, товары на продажу были большей частью предметами черного рынка, которых не было на обычных сайтах, где власти могли отслеживать активность. Поэтому преобладающими видами продуктов, доступных на Silkroad были запрещенные наркотики, лекарства, отпускаемые только по рецепту, огнестрельное оружие и другие незаконные товары.

Silkroad использовал биткойн в качестве валюты, поскольку биткойн можно было переводить между участниками рынка анонимно[10]. К сожалению, это ухудшило репутацию биткойна, поскольку СМИ сделали ложный вывод о том, что раз Silkroad использует биткойн в качестве валюты, то и все пользователи биткойна – это пираты и наркоторговцы с Silkroad. В октябре 2013 года ФБР смогло выследить администраторов сайта, и сайт был остановлен[11]. Что произошло с ценой на биткойн? Случился небольшой спад, и затем она продолжила расти. Причина этого в том, что огромное большинство пользователей биткойна не были пиратами и наркоторговцами, и тот факт, что биткойн продолжил расти, несмотря на отсутствие Silkroad, является тому подтверждением.

Из этого мы можем извлечь несколько уроков. Во-первых, все валюты в определенной степени используются и будут использоваться для незаконных целей – это доказательство их пригодности в качестве валюты. В ноябре 2013 года, отвечая на запрос сената Соединенных Штатов, Агентство по борьбе с финансовыми преступлениями подчеркнуло, что любое незаконное использование биткойна незначительно по сравнению с 1,6 триллиона долларов США «глобального криминального дохода» в 1999 году.

Также стоит заметить, что любые сделки, осуществленные на Silkroad между анонимными участниками, по крайней мере не привели к росту насилия в обществе, в противоположность насилию, которое иногда связано со сделками с использованием наличных, осуществляющимися на улице.

---

[9] «Tor» - это аббревиатура для «The Onion Router» (луковый роутер), этот проект изначально разрабатывался для ВМС США, и был спроектирован для зашифрованной и анонимной онлайн-коммуникации. Сейчас это программное обеспечение широко используется в интернете чтобы обеспечить анонимность для людей, желающих сохранить конфиденциальность онлайн.

[10] Более серьезное обсуждение этой темы см. в Главе восемнадцатой – «Анонимность»

[11] Silkroad с тех пор уже заменили другие анонимные черные рынки, разросшиеся за счет его падения

Глава пятнадцатая

Другие цифровые валюты

Биткойн – не единственная цифровая валюта, хотя он был первой и наиболее успешной на международном уровне, и занимает подавляющую долю рынка (98 %) в смысле капитализации по сравнению с другими цифровыми валютами. Биткойн впервые заработал в 2009 году, и до 2011 года не было никаких альтернативных цифровых валют, наподобие Лайткойна, который в значительной степени является клоном биткойна с незначительными изменениями нескольких настроек.

Я верю, что разработчики некоторых из этих ранних валют имели добрые намерения, однако сегодня в мире существует более 500 «альтернативных биткойну» цифровых валют, о которых большинство людей (включая меня) никогда не слышали, и я полагаю, что добрая часть из них, является ничем иным, как схемой, предназначенной для принесения прибыли разработчику.

Другое дело, что несмотря на то, что биткойн стал огромным эволюционным шагом в истории денег, он все еще несовершенен, и неизбежно, что протокол биткойна будет со временем совершенствоваться (как это уже происходило), и что потенциально новые цифровые валюты могут быть жизнеспособны одновременно с биткойном, или в конечном счете заменят биткойн. Идея блокчейна по существу здравая, и большинство цифровых валют, если не все, базируются на тех же основных принципах, что и биткойн.

Глава шестнадцатая

Как обезопасить ваш биткойн

Мы уже упоминали, что у биткойна и у физических денег есть общие свойства. Однако, биткойн имеет ряд особенностей, которые позволяют защитить его от случайной потери или кражи способом, недоступным для обычных денег.

Для начала, вы можете сделать резервную копию кошелька. Это означает именно то, что сказано: так же, как вы делаете резервные копии фотографий или писем, вы можете создать копию вашего цифрового кошелька и хранить ее в разных местах. Это простейший способ защитить ваши биткойны от случайной потери. Если вы потеряете телефон с биткойн-кошельком, или если откажет диск компьютера, вы сможете восстановить все свои деньги из резервной копии. Еще лучше то, что вам даже не надо делать резервную копию после каждой транзакции. Большинство современных биткойн-кошельков спроектированы таким образом, что, если вы сделали копию, даже если там не было средств в тот момент, когда была сделана копия – деньги, полученные в будущем, все равно будут восстановлены, так что вам нужно сделать резервную копию кошелька только один раз. Некоторые кошельки спроектированы так, что вы даже можете генерировать новые адреса, и все равно достаточно скопировать кошелек только один раз[12].

Резервные копии защищают ваш кошелек от случайной потери данных, но они не защищают вас от воров. Впрочем, кошельки легко шифруются и могут быть защищены паролем. Тогда, если кто-нибудь украдет ваш кошелек с биткойнами на нем, он не сможет их потратить без вашего пароля. Тем временем, вы можете восстановить ваш кошелек из резервной копии и для безопасности перевести деньги в новый кошелек. Тогда, даже если воры смогут угадать ваш пароль, биткойны будут уже отправлены на новый адрес, и ваш старый кошелек станет абсолютно бесполезным для них. Все эти вещи не требуют владения специальными навыками, они обычно являются составной частью большинства биткойн-программ и ими очень легко пользоваться даже новичку.

Эти возможности великолепно подходят для защиты средств в разумных объемах, однако, имея дело с большими суммами биткойнов, скажем, эквивалентных миллиону долларов, мы можем захотеть принять дополнительные предосторожности. В конце концов, что если атакующий получит доступ к нашему компьютеру и установит программу-шпион, тайно записывающую пароли, которые вы набрали? История показывает, что нет предела хитрым и бесчестным техникам, которые могут выдумать воры, когда речь идет о краже денег. Достаточно вспомнить некоторые известные ограбления казино в Лас-Вегасе и вещи, на которые люди шли, когда на кону стояли большие суммы денег. Однако, биткойн предоставляет великолепные возможности, когда речь идет о безопасности. Один из способов защиты большой суммы биткойнов называется «заморозка». Идея заморозки в этом контексте означает хранение биткойнов на компьютере или другом устройстве, никак не соединенном с интернетом. Компьютер или мобильный телефон, соединенный с интернетом, потенциально может быть взломан кем угодно из любого места мира, если найдена уязвимость. Но храня биткойны на компьютере, который не соединен с интернетом, вы немедленно ограничиваете потенциальные угрозы только теми, которые исходят от людей, имеющих физический доступ к этому компьютеру.

[12] Такие кошельки называются «иерархически детерминированными» или «HD-кошельками».

Конечно, кошелек на этом компьютере должен быть зашифрован и защищен надежным паролем. Современные программы легко обеспечивают возможность хранения биткойнов в заморозке.

У биткойна есть еще более продвинутые средства безопасности, такие как адреса с «множественной сигнатурой» (в просторечии известные как «мульти-сиг» адреса). Во всех до сих пор приведенных нами примерах мы описывали, как я посылаю 50 биткойнов своему другу Джо в транзакции, подписанной соответствующим закрытым ключом, который находится у меня. В случае с мульти-сиг адресами транзакция может быть сконфигурирована таким образом, что для подписи будут необходимы два разных человека, или три человека, или двое из трех людей, или любая комбинация подписей, которую вы можете представить. Например, у вас может быть биткойн-кошелек, который требует **обе** подписи – вашу и вашего бизнес-партнера, чтобы отправить транзакцию, или только **одну из** подписей. Или, возможно, у вас есть совет директоров, и транзакция должна быть подписана любыми тремя из семи директоров. Это очень мощные средства, позволяющие обезопасить биткойн способами, недоступными для физических денег.

Последний метод обеспечения безопасности биткойн-кошелька, о котором мы будем говорить, называется «бумажный кошелек», и это наиболее примитивное из всех устройств для обеспечения безопасности биткойна. Вы можете просто распечатать ваш закрытый ключ на бумаге, и в случае ЭМИ[13], который разрушит все ваши электронные устройства, вы сможете восстановить средства, используя распечатанный закрытый ключ. Конечно, можно пойти еще дальше, и напечатать половину закрытого ключа на одном листе, а другую половину – на другом, и хранить их в различных безопасных местах – возможности бесконечны.

[13] «ЭМИ» или «электромагнитный импульс» - это краткий сильный выброс энергии, который может вызывать потерю данных, хранящихся на дисках компьютера, без возможности восстановления. Он может возникнуть естественным образом, например, вследствие удара молнии, или благодаря человеку, как форма оружия.

Глава семнадцатая

Умные контракты

До сих пор в этой книге мы обсуждали наиболее распространенный и простой тип транзакции – участник А посылает деньги участнику Б. Мы рассмотрели, как этот процесс осуществляется с помощью биткойна, а также некоторые великолепные преимущества биткойна в сравнении с обычной валютой. Однако, пользуясь этим примером, мы только чуть царапнули по поверхности того, что биткойн и технология блокчейн могут действительно достичь. Введем идею «умных контрактов». Биткойн способен создавать сложные транзакции, вовлекающие множество участников. Давайте рассмотрим пример.

Пусть, скажем, производитель автомобилей делает новую машину. В процессе ее создания генерируется новый биткойн-адрес, на который депонируется символическая сумма биткойнов (т. е. 0,0001), и эта транзакция записывается в блокчейн. Этот открытый адрес производитель присваивает машине. Закрытый ключ затем выдается продавцу, который может хранить его на своем мобильном телефоне, так что его телефон вдобавок служит ключом от машины, позволяя ему открыть и завести машину.

Когда продавец собирается продать машину покупателю, транзакция записывается таким образом, что деньги переводятся продавцу, а машина переводится покупателю – как адрес, к которому он может получить доступ с мобильного телефона. Оба участника должны подписать транзакцию, чтобы она стала действительной и была включена в блокчейн. Когда транзакция завершена, покупатель может «представить» свой телефон машине через NFC[14], и машина распознает нового владельца и включит зажигание. В этом примере транзакция между двумя участниками происходит одновременно, и, таким образом, ни один из участников не должен доверяться другому. Более того, покупатель может просмотреть всю историю транзакций для машины в блокчейне, чтобы убедиться, что она настоящая, и удостовериться, что продавец действительно является владельцем машины.

Давайте расширим этот пример. Что если покупатель не может позволить себе купить машину, и ему нужно занять денег, чтобы сделать покупку. Биткойн-транзакция может быть построена таким образом, что кредитор имеет право собственности на машину до тех пор, пока либо оговоренная сумма не будет выплачена ему в пределах определенного промежутка времени, и тогда машина переводится должнику, либо должник теряет залог, и кредитор остается собственником машины.

Идея многостороннего соглашения не нова, банки одалживали деньги во все времена. Однако, при использовании биткойна и технологии блокчейн, процесс становится гораздо более эффективным, и участники в меньшей степени должны доверяться друг другу, чтобы выполнить условия контракта, которые соблюдаются автоматически биткойн-сетью. Интересно взглянуть, какие новые возможности использования биткойна и блокчейна люди откроют завтра.

[14] NFC (Near Field Communication) – коммуникация ближнего поля, технология, все шире использующаяся в современных телефонах и дающая возможность обмена данными между устройствами, находящимися в непосредственной близости друг к другу.

Глава восемнадцатая

Анонимность

Один из больших вопросов, которые возникли в отношении биткойна, – являются ли транзакции анонимными и, если они анонимны, не будет ли биткойн способствовать отмыванию денег и другим преступлениям. Ответ здесь – и да, и нет. Давайте рассмотрим этот вопрос более пристально.

Пусть, скажем, я покупаю нечто большое стоимостью в миллионы долларов у незнакомого мне человека, и он дает мне новый биткойн-адрес, на который я должен перевести 10 000 биткойнов. В этот момент транзакция анонимна. Если предположить, что другой участник сгенерировал абсолютно новый адрес, у меня нет возможности определить, кто он такой, и никто не может связать получение 10 000 биткойнов с этим человеком. Если этот человек будет хранить эти средства и никогда их не потратит, то он останется анонимным. В какой-то момент, однако, незнакомец скорее всего захочет потратить свои 10 000 биткойнов, или, возможно, обменять их на фиатную валюту[15]. Теперь если наш незнакомец найдет другого незнакомца на улице и продаст свои 10 000 биткойнов за миллион долларов наличными, все по-прежнему останется весьма анонимным. Однако обычно, особенно в случае больших сумм, этому человеку нужно будет потратить эти деньги при помощи законного бизнеса или обменять в заслуживающем доверия обменнике. В этих точках, в частности при обмене валюты, в процессе открытия счета требуется строгая проверка личности для соблюдения норм AML/CTF[16], применяемых в традиционном финансовом секторе. Как только деньги начинают проводиться по обычным каналам, для исследователя становится возможным соединить точки и проследить историю транзакций. Итак, анонимен ли биткойн? Он может быть таковым в той же степени, в какой анонимны наличные деньги. Наличность тоже может быть анонимной, но, если в один прекрасный день вы придете в банк с миллионом долларов наличными, власти могут удивленно поднять брови.

---

[15] «Фиатная валюта» - это деньги, которые государство объявляет законным платежным средством, но которые не обеспечены физическими ценностями. Ценность фиатных денег выводится из отношений между спросом и предложением, а не из ценности материала, из которого они сделаны.

[16] AML/CTF (Anti Money Laundering / Counter Terrorism Financing) – противодействие отмыванию денег и финансированию терроризма – это набор законных требований, которым должны следовать банки и другие финансовые институты, чтобы удостовериться, что их клиенты не используют деньги в незаконных целях. Поскольку биткойн-биржи наряду с биткойном имеют дело и с традиционными валютами, от них обычно также требуется следовать различным процедурам проверки личности их клиентов и уведомлять о подозрительных транзакциях.

Глава девятнадцатая

Регулирование

Многие мировые правительства сейчас задают себе вопрос, должен ли биткойн считаться законным платежным средством, и если так, должен ли он регулироваться, и если да, то до какой степени.

По моему мнению, ответ заключается в том, что биткойну нужно сбалансированное и тщательно продуманное регулирование. Регулирование, которое не подавляет новую индустрию, но, в то же самое время, защищает потребителей от противозаконных действий. Другой момент, который нужно принять во внимание, состоит в том, что мы не можем взять вчерашние законы, применявшиеся к абсолютно другой финансовой парадигме, и использовать их для биткойна. Биткойн работает фундаментально отличным от обычной валюты способом, и необходимо разработать такое регулирование, которое поддерживает децентрализованную цифровую модель.

Тогда возникает вопрос о том, как должно выглядеть подобное регулирование? Я полагаю, что абсолютно необходимо разрешить биткойн и другие цифровые валюты в качестве легального платежного средства, идея валюты, выпущенной государством, в один прекрасный день может оказаться пережитком прошлого. Правительства и экономики должны использовать эту новую мировую валюту и наблюдать, как расцветает торговля, поскольку люди могут проводить транзакции по всему миру в мгновение ока, без задержек из-за устаревших и работающих со скрипом банковских систем. Даже без учета биткойна, как разработчик программных систем, который провел много лет, создавая программы для финансовых институтов, я могу сказать, что большинство систем, которые я видел, по-настоящему древние. Это большие ЭВМ, созданные более тридцати лет назад, которым нужны специальные (действительно старые) инженеры, чтобы их обслуживать. Это одна из причин, по которым банки медленно принимают новые технологии, поскольку их системы не готовы к обновлению.

Принятие биткойна может привести к росту торговли по всему миру, возможно, даже вывести целые государства из нищеты, превращая их в цветущие экономики.

Где, по моему мнению, регулирование *необходимо*, так это в финансовых учреждениях, хранящих биткойн для других людей, подобно банкам. Мы уже были свидетелями первого великого финансового краха биткойна с падением Mt. Gox, и не далее, чем за неделю до того, как я пишу эти строки, мы видели, как Bitstamp, европейская биткойн-биржа, потеряла биткойнов на пять миллионов долларов из своих цифровых хранилищ. К их чести, большинство их средств хранилось безопасным образом в заморозке, и они восполнили балансы держателей счетов. Это подчеркивает, однако, что без некоторого надзора за мерами безопасности, которые предпринимают эти организации, потребители не смогут доверять учреждениям, ответственным за хранение их биткойнов.

Важно подчеркнуть, что это не уязвимость биткойна самого по себе, это только признак незрелости финансового сектора биткойна. За двенадцать месяцев, прошедшие с краха Mt. Gox, мы могли видеть, как вся индустрия предпринимает большие шаги в усовершенствовании безопасности, и несомненно будет продолжать это делать. Сильный, стабильный и безопасный

финансовый сектор биткойна соответствует всеобщим интересам – и сбалансированный уровень регулирующего надзора в этой области не принесет ничего дурного.

Для регуляторов важно помнить, что поскольку биткойн является новой индустрией, он движется очень быстрыми шагами, и все время развиваются новые методы. Было бы шагом назад для регуляторов, если бы при ограниченном понимании развивающейся индустрии они требовали бы невозможного для исполнения инструкций, или создавали бы инструкции, вредные для роста биткойна. Наилучшим ходом для них на настоящий момент будет держаться на шаг позади и внимательно наблюдать, делая нужные шаги по мере созревания индустрии. Этот принцип, вероятно, применим ко многим областям.

Глава двадцатая

Хронология

Множество событий значительно изменили лицо биткойна, от изначальной отправной точки в конце 2008 года, до цветущей индустрии, которой он стал сейчас. Далее следуют некоторые из ключевых моментов в этой хронологии.

Октябрь 2008 года. Опубликована анонимная статья, озаглавленная «Биткойн: пиринговая система электронных денег», описывающая по существу то, чем стал биткойн. Статья была опубликована человеком, использующим псевдоним *Сатоши Накамото*.

Январь 2009 года. Добыт первый блок блокчейна, также называемый генезис-блоком, стала публично доступна версия 0.1 биткойн-программы (включая исходный код). Программа была написана анонимно, и из-за довольно нестандартного стиля программирования, совмещенного со строгим теоретическим ноу-хау и полнотой, долгое время были популярны спекуляции на тему была ли она написана академическим ученым с небольшим опытом программирования, или возможно командой таких людей.

Тогда же, 12 января 2009 **года** произошла первая биткойн-транзакция – от Сатоши Накамото к Хэлу Финни

Октябрь 2009 года. Вебсайт New Liberty Standard опубликовал кажущийся ему подходящим обменный курс биткойна на тот момент, основанный на формуле, которая включала стоимость электричества, необходимого для работы компьютера, добывающего биткойн. Предложенный ими обменный курс был USD 1 = XBT 1309.03.

Февраль 2010 года. Появилась первая биткойн-биржа под названием «The Bitcoin Market». Эта биржа продержалась недолго, и закрылась из-за проблем с мошенничеством немногим более года спустя.

Май 2010 года. Программист из США по имени Laszlo купил несколько пицц в Jercos за 10 000 биткойнов. Цена пиццы была 25 долларов (эквивалент цены биткойна в 0,0025 доллара).

Июль 2010 года. Биткойн был упомянут на известном IT-вебсайте Slashdot, что вызвало десятикратное увеличение цены менее, чем за неделю. Цена выросла с 0,008 до 0,08 доллара. В том же месяце Джед МакКалеб запустил Mt. Gox, прочитав о биткойне на Slashdot. Интересно отметить, что Джед МакКалеб сказал позднее, в 2011 году после продажи Mt. Gox:

«*Я создал Mt. Gox ради интереса, после того, как прочитал о биткойне прошлым летом. Заниматься этим было интересно и весело. Я все еще уверен, что у биткойна прекрасное будущее. Но чтобы действительно сделать Mt. Gox таким, каким он может быть, требуется больше времени, чем у меня есть сейчас. Так что я решил передать эстафету кому-нибудь, кто имеет больше возможностей, чтобы вывести сайт на следующий уровень.*»

Другими словами, МакКалеб работал над Mt. Gox в одиночку несколько недель или месяцев в свободное время – все получилось благодаря тому, что у него было хобби, и биткойн не обладал реальной ценностью в то время. Он признал этот факт в тот момент, когда продал сайт. Сравните это с современной биржей, такой как Independent Reserve, разработка которой командой профессиональных программистов заняла более 18 месяцев, включая предусмотренные в

системе меры для обеспечения ее безопасности, масштабируемости, стабильности и надежности. Неудивительно, что без обширной переработки Mt. Gox не был способен поддерживать многомиллионную индустрию в будущем.

Другой интересной вещью, произошедшей в июле 2010 года было то, что в этом месяце кто-то придумал способ использования GPU (графического процессора), чтобы добывать биткойн быстрее, чем это было возможно с использованием обычного способа добычи на центральном процессоре.

Глобальная частота обработки хешей биткойн-сетью достигла теперь 1 гигахеша (GH), или 1 000 000 000 (1 миллиарда) хешей в секунду.

Август 2010 года. В биткойн-протоколе была обнаружена и затем использована уязвимость. Это привело к созданию более чем 184 миллиардов биткойнов, сгенерированных в одной транзакции. В течение нескольких часов проблема была обнаружена и уязвимость исправлена. История транзакций от данной транзакции и далее была навсегда удалена. Это был единственный большой дефект безопасности, найденный и использованный за всю историю биткойна.

Ноябрь 2010 года. Капитализация рынка биткойна в первый раз превысила миллион долларов США. Цена биткойна на Mt. Gox достигла 50 центов.

Декабрь 2010 года. Глобальная частота обработки хешей биткойн-сетью в первый раз превысила 100 GH.

Февраль 2011 года. Открылся Silkroad, сетевой черный рынок, использующий биткойн как форму платежа. В том же месяце курс биткойна на Mt. Gox впервые достиг паритета с долларом.

Март 2011 года. Джед МакКалеб продал Mt. Gox Марку Карпелесу.

Апрель 2011 года. О биткойне в первый раз написали традиционные медиа, TIME опубликовал статью под названием «Онлайн-валюта может бросить вызов правительствам и банкам».

Июнь 2011 года. Цена биткойна на Mt. Gox впервые превысила 10 долларов. В том же месяце Mt. Gox начал показывать признаки проблем, в их системе была найдена серьезная брешь в безопасности, приведшая к компрометации личных данных более чем 60 000 пользователей, а также к мошенническим заявкам на сотни тысяч биткойнов, что вызвало резкое падение цены до 1 цента.

В июне также произошла крупнейшая кража биткойнов в истории. Были украдены 25 000 000 биткойнов стоимостью более четверти миллиона долларов США.

В том же месяце WikiLeaks начал принимать пожертвования в биткойнах.

Июль 2011 года. Всего через месяц после проблем с безопасностью у Mt. Gox польская биткойн-биржа, на тот момент третья по величине в мире, потеряла 17 000 биткойнов своих клиентов.

Август 2011 года. Еще одна биткойн-компания, обрабатывавшая биткойн-транзакции, потеряла более 150 000 биткойнов стоимостью на тот момент более 2 миллионов долларов США.

В то время случалось множество подобных инцидентов. Как можно видеть, это была неприятная история для биткойна, так что стоит уделить время анализу того, что означает «потеря», и почему это продолжало происходить. Необходимо заметить, что во всех этих случаях (исключая уязвимость, обнаруженную в августе 2010 года) проблема была не в биткойне самом по себе, а в некомпетентности людей, управлявших компаниями, на которых была возложена ответственность по хранению биткойнов для других людей. В тот период, как в значительной степени и сейчас, эти компании никак не регулировались, но люди доверяли им биткойны на миллионы долларов.

В основе биткойн-кошелька, в котором хранятся чьи-либо биткойны, лежит файл или набор файлов на компьютере. Чтобы защитить эти файлы, нужно сделать их резервную копию и зашифровать их как описано в главе «Как обезопасить ваш биткойн». Организация, ответственная за биткойны стоимостью в миллионы долларов в сущности должна выполнить ту же задачу, однако применяемые методы должны быть какими-то более надежными (сравните защиту денег в вашем кошельке с банковским хранилищем, с золотом в Форт-Ноксе – по мере того, как возрастает ответственность, уровень безопасности также должен повышаться). Если файлы, в которых хранятся закрытые ключи для биткойн-кошелька повреждены или изменены (например, из-за отказа оборудования), или вор получил доступ к компьютеру и украл файлы, то биткойны потеряны.

Сегодня происходит меньше подобных инцидентов с безопасностью, но угроза все равно сохраняется, вот почему компании и частные лица должны помнить об этом.

Октябрь 2011 года. Бывший сотрудник Google создает «Litecoin» - альтернативную биткойну валюту.

Май 2012 года. Более, чем половина биткойн-транзакций за месяц были вызваны онлайн-игрой SatoshiDICE.

Июнь 2012 года. В Сан-Франциско, США, основан известный онлайн-кошелек Coinbase.

Ноябрь 2012 года. Награда за добычу биткойна впервые уменьшена наполовину – вознаграждение за добычу блока опустилось с 50 XBT до 25 XBT (это случилось при добыче блока 210 000).

Популярная платформа онлайн-блогов «Wordpress» начинает принимать платежи в биткойнах.

Декабрь 2012 года. «Bitcoin Central» – первая биткойн-биржа, лицензированная как европейский банк, – начинает работу в европейском нормативно-правовом сегменте.

Январь 2013 года. Выпущены первые ASIC (Application Specific Integration Circuit – интегральная схема специального назначения) – машины для добычи биткойна. Так же, как GPU опередили CPU, ASIC сейчас является наиболее мощной и эффективной из доступных машин – это специальное оборудование, предназначенное только для добычи биткойна.

BitPay, базирующаяся в США компания по обработке биткойн-платежей, объявила, что число транзакций их продавцам превысило 10 000.

Февраль 2013 года. Цена биткойна достигла наибольшей высоты, превысив значение 31,91 доллара, зафиксированное на Mt. Gox за 601 день до этого в июне 2011 года.

Март 2013 года. Произошло раздвоение блокчейна, вызванное различным поведением двух разных версий биткойн-программ. Это значило, что пользователи с старой версией программы видели одни транзакции, тогда как пользователи с новой версией видели другой набор транзакций. Раздвоение было быстро исправлено биткойн-майнерами, возвратившимися к более ранней версии программы. Цена биткойна временно упала в этот период, но он быстро снова окреп до цены перед ветвлением.

К концу месяца цена выросла еще больше, и общая капитализация рынка биткойна в первый раз превысила миллиард долларов США.

Апрель 2013 года. Цена продолжила впечатляющий рост в апреле, достигнув 250 долларов. Потенциальным катализатором беспрецедентного роста называли кипрский финансовый кризис. После пика цена стабилизировалась на уровне 120 долларов на следующие несколько месяцев.

Май 2013 года. Нечто, внушившее мне интерес во время моего исследования – ESEA, компания из США, занимающаяся компьютерными играми, использовала компьютеры пользователей с помощью тщательно разработанной вредоносной программы, чтобы тайно добывать себе биткойн. Они были пойманы и получили коллективный иск на миллионы долларов. Это, конечно, не единственный пример подобной активности. В одном из мест, где я раньше работал, сотрудник был уволен за тайное использование мощных компьютеров компании для добычи биткойна.

Вероятно, менее интересно, но более важно, что в том же месяце в Сан-Диего, США был открыт первый биткойн-банкомат.

Также Coinbase получил за май более 5 миллионов долларов из средств инвесторов, наибольшая инвестиция в биткойн-индустрию на тот момент.

Июнь 2013 года. В Сиднее, Австралия была основана наша компания, Independent Reserve, перед этим мы провели шесть месяцев, анализируя биткойн и биткойн-рынок, чтобы понять, как наилучшим образом встроиться в новую экономику. Мы решили, что в Австралии нужна надежная биткойн-биржа, чтобы создать твердую основу, которую другие бизнесы, связанные с биткойном, могли бы использовать как базис для собственных предложений.

Август 2013 года. Федеральный судья в США классифицировал биткойн как легальное платежное средство. В то же время немецкое правительство узаконило биткойн, объявив цифровые валюты «единицей расчета». Также в августе биткойн появился на блумбергских терминалах с кодом валюты XBT.

Сентябрь 2013 года. Глобальная вычислительная мощность биткойн-сети впервые достигла 1 пентахеша или 1 000 000 000 000 000 (1 квадриллиона) хешей в секунду.

Октябрь 2013 года. Печально известный сайт Silkroad был закрыт ФБР. Вместо предсказанного скептиками коллапса рынка цена биткойна ненадолго упала, но после продолжила расти, поскольку стало очевидно, что большая часть транзакций не была связана с Silkroad, и Silkroad был относительно небольшим игроком в биткойн-экономике.

В том же месяце глобальный инвестиционный банк Merill Lynch назвал биткойн потенциально «*основным платежным средством в электронной коммерции, способным стать серьезным конкурентом традиционным системам перевода денег*».

В октябре же крупнейший китайский поисковик Baidu стал первым сервисом такого рода, принимающим биткойн.

Ноябрь 2013 года. Глава Федерального Резерва США, Бен Бернанке, публично объявил, что биткойн «*может иметь долгосрочную перспективу, особенно если инновации предложат быструю, более безопасную и более эффективную платежную систему*». Сенат США, проведший слушания по вопросу биткойна, также осторожно высказался в пользу цифровых валют, а Сеть по борьбе с финансовыми преступлениями объявила биткойн новаторским и полезным, предупредив, что преждевременное регулирование может задушить инновации. Они также указали критикам, что любое нелегальное использование биткойна было незначительным в сравнении с 1,6 триллиона долларов «глобального криминального дохода» в 1999 году. Позитивные результаты слушаний в сенате вызвали в ноябре рост цены биткойна до 1242 долларов.

В то же время предприниматель-миллиардер сэр Ричард Брэнсон объявил на CNBC, что его компания «Virgin Galactic», занимающаяся коммерческими космическими полетами, будет принимать платежи в биткойнах. Он назвал биткойн «волнующей новой валютой». Компания уже получила первый платеж стоимостью примерно 250 000 долларов.

В этот момент истории биткойна он используется для перевода большего количества денег, чем Western Union, примерно 245 миллионов долларов в месяц.

Декабрь 2013 года. Один из электромобилей Tesla Model S Илона Маска (PayPal, SpaceX, Tesla, SolarCity) был продан в США за биткойны. Цена машины в то время была примерно 103 000 долларов.

Однако, в то время, как биткойн расцветал на западе, на востоке Центральный банк Китая запретил финансовым учреждениям обрабатывать биткойн-транзакции, что вызвало падение цены до примерно 500 долларов. Это постановление вынудило Baidu прекратить принимать платежи в биткойнах.

Январь 2014 года. Глобальная вычислительная мощность в первый раз достигла 10 пентахешей.

Март 2014 года. Британское налоговое управление заявило, что биткойн должен рассматриваться в качестве валюты для выполнения транзакций.

Июнь 2014 года. Expedia, одно из крупнейших туристических агентств в мире, начинает принимать биткойн-платежи.

Глобальная вычислительная мощность сети достигает 100 пентахешей.

Июль 2014 года. Dell, один из крупнейших производителей компьютеров в мире, начинает принимать биткойн-платежи.

Сентябрь 2014 года. PayPal, одна из крупнейших компаний по обработке платежей, дает торговцам возможность принимать платежи в биткойнах.

Октябрь 2014 года. В Сиднее запущен Independent Reserve, наиболее продвинутая и безопасная на тот момент биткойн-биржа в Австралии.

Ноябрь 2014 года. Австралийский сенат начинает изучение вопроса использования биткойна и цифровых валют в Австралии.

Декабрь 2014 года. Microsoft, один из крупнейших производителей программного обеспечения в мире, начинает принимать биткойн для некоторых онлайн-покупок.

Январь 2015 года. Нью-Йоркская фондовая биржа и консорциум международных банков инвестируют 75 миллионов долларов в биткойн-индустрию.

Август 2015 года. Сенат Австралии выпускает рекомендации по результатам изучения вопроса цифровых валют, требуя рассматривать биткойн как обычные деньги в целях налогообложения, а также применить к цифровым валютам законы против отмывания денег. Этот итог воспринят биткойн-индустрией Австралии как весьма позитивный шаг по направлению к узакониванию молодой валюты.

Послесловие Адриана Пржеложны

Я надеюсь, что вам доставило удовольствие прочтение книги Адама, также как и мне понравилось время, проведенное за редактированием и завершением его рукописи. Мы с Адамом последние 14 лет работали совместно над таким количеством разных проектов, что часто мне казалось, что он здесь, рядом со мной, работает над этой книгой, спорит о некоторых формулировках или пытается убедить меня, что его интерпретация неясного грамматического правила более верна, чем моя.

Пока я работал над книгой, я раздумывал, включать ли дополнительные главы и расширять ли некоторые секции. Я знаю, что Адам, вероятно, написал бы больше, если бы у него был шанс, но я решил, что лучше будет сохранить книгу близкой к оригиналу, чтобы продемонстрировать работу и мысли самого Адама. Это показалось мне более важным, чем добавление еще одной главы, скажем, «Побочные цепочки» или «Будущее биткойна», и, по моему мнению, эта книга достаточно сильна как есть, она не нуждается в дополнительном содержимом.

Мне жаль, что Адам не может видеть свои амбиции реализованными, а свою книгу изданной. Я знаю, что он был бы горд видеть этот проект завершенным. Это была кульминация многих часов работы над текстом, многих лет исследований и тяжелой работы в ИТ и биткойн-индустрии, давшей ему знания и понимание для написания этой книги.

Я знаю, что ему доставила бы радость эта публикация, которая оставит его след в истории на многие годы.

Адриан Пржеложны