



Оглавление

Предисловие	10
Вступление	12
Благодарности	15
О книге	17
Кому адресована эта книга	17
Структура книги	18
Соглашения об оформлении кода	19
Прочие онлайн-ресурсы	20
От издательства	20
Об авторе	21
Глава 1. Введение в Биткоин	22
Что такое Биткоин?	22
Общая картина	25
Проблемы современных денег	32
Подход, предлагаемый технологией Биткоин	36
Где можно использовать биткоины?	39
Другие криптовалюты	46
Итоги	48
Глава 2. Криптографические хеш-функции и цифровые подписи	49
Электронная таблица учета жетонов на булочки	50
Криптографические хеши	55
Упражнения	65

Цифровые подписи	67
Повторение	83
Упражнения	85
Итоги	86
Глава 3. Адреса	88
Раскрыты привычки потребления булочек	89
Замена имен открытыми ключами	90
Укорачивание открытых ключей	94
Избегание дорогостоящих опечаток	98
Возвращаемся к конфиденциальности	107
Повторение	108
Упражнения	111
Итоги	113
Глава 4. Кошельки	114
Первая версия кошелька	115
Резервное копирование закрытых ключей	120
Иерархически детерминированные кошельки	124
Назад к резервному копированию	132
Расширенные открытые ключи	137
Создание защищенных закрытых ключей	141
Математика открытого ключа	144
Умножение публичного ключа	145
Повторение	152
Упражнения	154
Итоги	156
Глава 5. Транзакции	157
Проблемы в старой системе	158
Платежи с использованием транзакций	159
Язык сценариев	171
Необычные виды платежей	177
Дополнительные элементы в транзакциях	189
Вознаграждение и создание монет	190
Доверие к Лизе	192
Повторение	195
Упражнения	197
Итоги	199

Глава 6. Блокчейн	200
Лиза может удалять транзакции	201
Построение блокчейна	201
Легкие кошельки	213
Деревья Меркла	224
Безопасность легких кошельков	233
Повторение	236
Упражнения	239
Итоги	242
Глава 7. Доказательство работы	243
Клонирование Лизы	244
Принуждение к честному получению счастливых чисел	255
Майнеры должны уйти	264
Корректировка сложности	268
Какой вред могут принести майнеры?	273
Комиссионные отчисления за транзакции	283
Повторение	290
Упражнения	294
Итоги	295
Глава 8. Одноранговая сеть	296
Общая папка	297
Создание одноранговой сети	298
Как общаются соседние узлы?	301
Сетевой протокол	303
Оставляем в прошлом систему жетонов на булочки	316
Инициализация сети	319
Запуск собственного полного узла	332
Повторение	343
Упражнения	346
Итоги	348
Глава 9. И снова о транзакциях	349
Временная блокировка транзакций	350
Временная блокировка выходов	357
Сохранение данных в блокчейне Биткоин	365
Замена ожидающих транзакций	371
Разные типы подписей	376

Повторение	377
Упражнения	379
Итоги	381
Глава 10. SegWit	382
Проблемы, решаемые с помощью segwit	383
Решения	393
Экономия пропускной способности	411
Совместимость кошельков	412
Еще раз о типах платежей	413
Ограничения блоков	415
Повторение	419
Упражнения	422
Итоги	424
Глава 11. Апгрейды Биткоин	425
Форки в Биткоин	426
Повторение транзакции	438
Механизмы обновления	441
Повторение	456
Упражнения	458
Итоги	460
Приложение А. Использование bitcoin-cli	462
Взаимодействие с bitcoind	462
Графический интерфейс пользователя	464
Знакомство с bitcoin-cli	465
Начало работы	466
Приложение Б. Решения упражнений	477
Приложение В. Веб-ресурсы	495

*Посвящается любви всей моей жизни —
жене Линнее.*

Умной, верной, настоящей.

И биткоинерам всего мира



Предисловие

В чем разница между системой Биткоин и аналогами денег, которые используются в многопользовательских играх? Все они определяются программно, создаются из ничего и могут иметь ценность, сопоставимую с традиционными валютами. Случайному наблюдателю они кажутся почти одинаковыми.

Но есть важные различия в том, как они реализованы, что оказывает влияние на все аспекты соответствующих систем: если игровые валюты реактивно банят пользователей, уличенных в мошенничестве, то Биткоин действует упреждающе, предотвращая различные виды мошенничества, делая их невозможными, непрактичными или менее выгодными, чем честное поведение.

Книга «Грокаем технологию Биткоин» точно описывает, как это достигается. Когда вы познакомитесь с хеш-функциями, цифровыми подписями, доказательствами работы и многими другими понятиями, то увидите, что технология Биткоин весьма эффективно предотвращает мошенничество, не требуя глобального запрета на активность какого-либо пользователя.

Здесь приведено множество преимуществ этой ключевой особенности. Когда вы узнаете об адресах, кошельках, майнерах и узлах, то увидите, что в ситуации, когда никто не имеет реальной возможности обманывать, можно разрешить всем участвовать в каждой части протокола, не ставя никого в положение безграничного доверия. И поскольку никто не сможет воспользоваться своим положением, отпадает необходимость в идентификации личности. «Грокаем технологию Биткоин» наглядно демонстрирует, как любой может использовать публичную цепочку блоков (блокчейн), сохраняя определенную степень конфиденциальности.

Децентрализованная система, которая не использует идентификацию личности или не зависит от доверия других участникам, в корне отличается

от привычных систем, знакомых большинству из нас. Калле Розенбаум активно использует эту особенность, начиная объяснение каждого аспекта Биткоина с примера централизованной системы, эксплуатирующей доверие или зависящей от идентификации и понятной любому читателю. Затем он постепенно превращает эту базовую систему в децентрализованную и псевдонимную систему, не требующую выражения доверия и реализованную с использованием технологии Биткоин. Благодаря пошаговым объяснениям с четкими определениями и превосходными иллюстрациями, даже самые узкоспециальные темы становятся доступными для заинтересованного непрофессионала.

Технология Биткоин нуждается в книгах, таких как «Грокаем технологию Биткоин», но ей также нужны активные пользователи, которые читают эти книги и разбираются в технических принципах, на которых она основана. В течение первых дней, которые, как я надеюсь, продолжатся долгой историей использования биткоинов, пользователей часто просят оценить предлагаемые изменения в системе — изменения, которые могут повлиять на безопасность и конфиденциальность их электронных кошельков. Прочитав эту книгу, вы поймете, как система предотвращает мошенничество, и сможете гарантировать, что будущие изменения сохранят эту важную особенность и ее многочисленные преимущества.

*Дэвид А. Хардинг (David A. Harding),
соавтор документации для Биткоин*



Вступление

Биткоин изменил мир.

Мир стал свидетелем крупных достижений, способствовавших улучшению качества жизни людей, в том числе изобретения вакцины, электричества, радио, автомобиля и Интернета. Некоторые из этих технологий начинались как игры для богатых, но в конечном счете получили массовое распространение и стали приносить огромную пользу жителям Земли. Биткоин вскоре встанет с ними в один ряд. Именно это и кажется мне в нем самым захватывающим.

Мне повезло жить в социально стабильном обществе. Проводя финансовые операции, я не боюсь, что кто-то постучится в мою дверь. Я никогда не чувствовал, что нужно как можно быстрее потратить деньги, потому что гиперинфляция съест мой обед. Но из-за этого мне трудно было понять важность Биткоин. Технология Биткоин¹ интересует меня больше с теоретической стороны, но когда я слышу от менее удачливых людей, живущих под властью репрессивных или некомпетентных режимов, о том, как Биткоин улучшает их жизнь, все становится более чем реальным. Биткоин даст людям возможность отказаться от системы, которая держит их в заложниках.

Сатоши Накамото (Satoshi Nakamoto), так называет себя человек (или группа людей), пожелавший не раскрывать свою личность, опубликовавший в октябре 2008 года научную статью в списке рассылки, посвященном

¹ Здесь и далее: *Биткоин* (с прописной буквы): концепция и протокол первой децентрализованной криптовалюты, использующей технологию блокчейн. Криптовалютный токен *биткоин* (со строчной): валюта сама по себе. — *Примеч. ред.*

криптографии. Статья называлась «Bitcoin: A Peer-to-Peer Electronic Cash System» (см. приложение В). В своей статье Накамото описывает важные части технологии Биткоин, первой системы электронных (цифровых) денег, в которой отсутствует центральный орган эмиссии или обработки транзакций. В январе 2009 года Накамото опубликовал первую программу, реализующую эту систему. В то время технология Биткоин не привлекла широкого внимания, кроме узкого круга экспертов в области криптографии. Но по мере того как система доказывала свои возможности, круг интересующихся расширялся. Однако пока голос противников Биткоин звучит громче, чем голос сторонников, как часто бывает с новаторскими технологиями. По состоянию на 2019 год уже сотни миллионов людей знают о Биткоин и десятки миллионов используют эту систему.

Когда я начал изучать Биткоин в 2013 году, мне потребовалось много времени, чтобы получить достаточно полное понимание технологии. И не потому, что я несообразительный, а потому что Биткоин — сложная система. Это не просто новомодная база данных, а смесь экономики, математики, технологий и антропологии.

В 2015 году я начал вести блог о Биткоин, и, думаю, издательству Manning понравились мои статьи, потому что компания прислала мне электронное письмо с предложением написать книгу о «блокчейне». Поскольку моя страсть — Биткоин, а не только блокчейн, чрезмерно раскрученное слово, обозначающее базу данных для Биткоин, — я выразил свою благодарность и сказал, что мне было бы интереснее написать книгу о Биткоин. Я несколько лет искал свое место в биткоин-сообществе, и эта возможность показалась мне подходящей. Я начал работу над проектом, но он оказался намного сложнее и занял больше времени, чем я ожидал.

Первоначально эта книга задумывалась как типичный технический обзор Биткоин, но оказалось трудно описать одну тему без передачи всех нюансов. Начало книги получилось бы слишком сложным. Стало ясно, что нужен какой-то иной подход. Я обсудил это с женой, и у нас появилась идея концептуального описания Биткоин с нуля. Книга начинается с действительно простой системы электронных таблиц, понятной каждому, и эта система постепенно превращается в Биткоин. В каждой главе описываются некоторые проблемы в текущей системе, и затем решаются добавлением технологии, рассматриваемой в этой главе.

Рукопись «Grokking Bitcoin» будет выпущена под лицензией Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) вскоре после публикации печатной версии. Выпуск версии под

открытой лицензией был моим требованием, которое я выдвинул, перед тем как взяться за эту книгу. Это мой способ внести свой вклад в биткоин-сообщество, давшее мне так много за эти годы. Я и издательство Manning надеюсь, что те, кто не сможет позволить себе купить эту книгу, смогут прочитать ее свободно распространяемую версию. Однако благотворительность — не единственная причина. Мы также надеемся, что эта версия сделает книгу более заметной, дав потенциальным читателям возможность ознакомиться с ее содержимым. Если можете себе это позволить, пожалуйста, купите красивую печатную версию. Издательство Manning и я потратили много времени и сил на создание этой книги, и мы будем очень признательны за ваш вклад!

Я надеюсь, вам понравится книга «Грокаем технологию Биткоин» настолько же, насколько я страдал, работая над ней!



Благодарности

Я должен сказать спасибо многим людям, без которых эта книга была бы невозможна.

В первую очередь хочу поблагодарить свою жену Линнею за наши обсуждения и ее безоговорочную поддержку. Ты лучшая!

Кристина Тейлор (Christina Taylor), мой дорогой редактор из Manning, спасибо, что не давали мне расслабиться. Работа, работа и еще раз работа. Спасибо также вам, Берт Бейтс (Bert Bates), за ваш ценный вклад в педагогику.

Я также хочу поблагодарить других сотрудников издательства Manning за их профессионализм: Озрена Харловича (Ozren Harlovic), Ребекку Райнхарт (Rebecca Rinehart), Кэндис Гиллхулли (Candace Gillhoolley), Ану Ромак (Ana Romac), Майкла Стивенса (Michael Stephens), Эрин Туи (Erin Twohey), Кристофера Кауфмана (Christopher Kaufmann), Матко Хрватина (Matko Hrvatin) и Грега Уайлда (Greg Wild). Отдельное спасибо фантастической команде из технического отдела: Чаку Ларсону (Chuck Larson), иллюстратору; Ребекке Деуэль-Гальегос (Rebecca Deuel-Gallegos), редактору; Кевину Каллахану (Kevin Callahan), наборщику; Тиффани Тейлор (Tiffany Taylor), корректору; а также Лори Вайдерт (Lori Weidert), выпускающему редактору.

Хочу поблагодарить Джонатана Йогенфорса (Jonathan Jogenfors) и Понта Линдблома (Pontus Lindblom) за обзор некоторых глав, охватывающих их области знаний.

Многие люди на различных интернет-форумах оказали значительную помощь мне в моих исследованиях. Особенно помогли Дэвид А. Хардинг (David A. Harding), Питер Уилль (Pieter Wuille) и Марк Эрхардт (Mark

«Murch» Erhardt). Спасибо вам за беседы в Twitter и отличные ответы на Bitcoin Stack Exchange (см. веб-ресурс 2 в приложении C).

В обсуждении условий открытой публикации этой книги мне помогал Андреас М. Антонопулос (Andreas M. Antonopoulos). Вашу поддержку в этом деле трудно переоценить. Спасибо! Также спасибо за аналогию с «вегетарианским рестораном», использованную в главе 11. И спасибо за увлекательные беседы с вами; вы стали для меня главным источником вдохновения.

Я писал эту книгу, используя AsciiDoctor — язык разметки текста. Спасибо вам, Дэн Аллен (Dan Allen), за ваш тяжелый труд над AsciiDoctor; это невероятно удобный язык.

Книга преодолела три раунда рецензирования с разными научными редакторами. Их отзывы и замечания были чрезвычайно полезны для проверки идей и выявления пробелов. Спасибо вам: Ян Гойвертс (Jan Goyvaerts), Макс Хамбер (Max Humber), Ирина Романенко (Iryna Romanenko), Жан-Франсуа Морин (Jean-François Morin), Аль Кринкер (Al Krinker), Джоэл Котарски (Joel Kotarski), Маркус Бекманн (Markus Beckmann), Кристофер Бейли (Christopher Bailey), Витон Витанис (Viton Vitanis), Паоло Фрейли (Paolo Freuli), Томо Хельман (Tomo Helman), Марчелло Сери (Marcello Seri), Мацей Дроздовски (Maciej Drozdowski), Цицерон Зандона (Cicero Zandona), Барнаби Норман (Barnaby Norman), Фрэнсис Буонтемпо (Frances Buontempo), Гленн Свонк (Glenn Swonk) и Серхио Фернандес Гонсалес (Sergio Fernandez Gonzalez).

Спасибо также всем читателям программы раннего доступа Manning Early Access Program (MEAP), которые делились своими мыслями, предложениями и вопросами на форуме издательства Manning, а также спасибо Аруну Сурье (Aruna Surya) за советы и предложения, присланные по электронной почте.

Если я кого-то не упомянул, прошу извинить меня — и вам тоже спасибо.



0 книге

Основная цель этой книги — помочь вам решить, доверяете ли вы технологии Биткоин. На пути к этой цели вы подробно познакомитесь с множеством понятий, таких как цифровые подписи, доказательство работы и одноранговые сети. Попутно мы достигнем некоторых промежуточных целей:

- ★ установим кошелек с биткоинами на свой смартфон и разберемся, как все это работает;
- ★ изучим технические аспекты Биткоин;
- ★ рассмотрим варианты хранения личных ключей, в зависимости от количества биткоинов в кошельке и желаемого уровня безопасности и удобства;
- ★ запустим полноценный узел для участия в финансовых транзакциях без третьих сторон;
- ★ познакомимся с необычными заявлениями жуликов, обманщиков и аферистов, сопровождающими успехи Биткоин. Будьте внимательны!

Кому адресована эта книга

Эта книга адресована всем, кто хочет понять технологию Биткоин на глубоком концептуальном уровне. Книга не требует навыков программирования, но базовое представление о некоторых технических понятиях пригодится — например, о базах данных, компьютерных сетях, компьютерных программах и веб-серверах. Нелишними будут и некоторые знания математики, но это, конечно, не обязательно.

Структура книги

Эта книга состоит из 11 глав и трех приложений.

- ★ Глава 1 предлагает обзор Биткоин. Здесь вы узнаете, что такое технология Биткоин, почему она так важна и как работает.
- ★ Глава 2 рассматривает криптографические аспекты: хеш-функции и цифровые подписи. Это основные строительные блоки, знание которых понадобится в остальной части книги. Здесь также закладывается основа системы фиктивных денег на примере таблицы жетонов на булочки, которую мы будем развивать в главах 2–8.
- ★ Глава 3 охватывает адреса. Пересылая биткоины, вы должны указать биткоин-адрес получателя. Что такое биткоин-адреса, зачем они нужны, как создаются и используются?
- ★ Глава 4 рассказывает, как биткоин-кошелек следит за вашими секретными ключами и как сгенерировать несколько секретных ключей из одного огромного случайного числа, называемого начальным числом, или сидом. Здесь также подробно обсуждаются вопросы резервного копирования.
- ★ Глава 5 исследует анатомию транзакций в Биткоине, как транзакции получают цифровую подпись и обрабатываются.
- ★ Глава 6 рассматривает технологию блокчейн (blockchain): базу данных для хранения транзакций. Здесь мы посмотрим, как устроена цепочка блоков и как она позволяет использовать так называемые легкие кошельки.
- ★ Глава 7 охватывает вопросы доказательства работы, которое используется для выбора того, кто добавит новую транзакцию в цепочку блоков. Этот процесс, называемый майнингом, обеспечивает безопасность биткоинов в цепочке блоков — блокчейне.
- ★ Глава 8 исследует сеть Биткоин. Биткоин не имеет центрального органа управления, и вы узнаете, как можно организовать подобное с использованием одноранговой сети. Здесь также рассказывается, как стать активным членом сети Биткоин, запустив свой узел.
- ★ Глава 9 вновь возвращается к транзакциям, чтобы рассказать о дополнительных возможностях, важных для разных применений.
- ★ Глава 10 вводит понятие протокола SegWit. В 2017-м в технологию Биткоин было добавлено серьезное усовершенствование, повышающее надежность транзакций, эффективность верификации и пропускную способность блокчейна, и в этой главе мы узнаем все подробности.

- ★ Глава 11 рассматривает ситуации софт-форка и хард-форка, то есть разделения версий криптовалюты, и того, как Биткоин может безопасно модернизироваться путем софт-форка с использованием тщательно разработанного плана развертывания.

Советую обязательно прочитать главы 2–8, в которых мы последовательно с самого начала будем строить систему жетонов, или токенов, на булочки. Каждая глава добавляет в систему технологию для решения конкретной проблемы, и к концу главы 8 мы создадим сеть Биткоин. Главы 9, 10 и 11 можно читать не по порядку, но рекомендую особенно внимательно прочитать главу 11, потому что она охватывает суть Биткоин. Поняв, о чем рассказывает глава 11, вы грокнете Биткоин.

Время от времени я буду использовать некоторые обзорные рисунки из главы 1, как во вступительных разделах к главам, так и внутри самих глав, чтобы вы не заблудились. Легко потерять представление об общей картине и цели текущей темы; ищите заголовки со значком перископа «На чем мы остановились?»



Все главы, кроме главы 1, включают упражнения. Я добавил их, чтобы вы могли оценить свои знания и навыки. Каждый блок упражнений делится на разделы с простыми, помогающими быстро проверить знание некоторых фактов, и более сложными, требующими более скрупулезных рассуждений, упражнениями. Называются они «Для разминки» и «Придется пораскинуть мозгами». Некоторые упражнения в разделах «Придется пораскинуть мозгами» действительно очень сложные, поэтому, если вам не удастся их выполнить, обратитесь к приложению В за ответами.

Соглашения об оформлении кода

В книге очень мало примеров программного кода. Его практически нет. Но в главе 8 и в приложении А приводятся несколько команд для ОС Linux. Команды начинаются со знака доллара и пробела, как показано ниже:

```
$ cd ~/.bitcoin
```

Длинные команды, не уместяющиеся в одну строку, будут разбиты на несколько строк с использованием символа обратного слеша \ и отступа в следующей строке на четыре пробела, например:

```
$ ./bitcoin-cli getrawtransaction \
    30bca6feaf58b811c1c36a65c287f4bd393770c23a4cc63c0be00f28f62ef170 1
```

Обратные слешы используются для записи команд в нескольких строках большинством интерпретаторов командной строки для Linux, поэтому команды из книги можно напрямую копировать в окно терминала. Длинные строки, которые выводятся командами, не разбиваются с использованием обратного слеша; они просто переносятся и снабжаются значком стрелки, обозначающим перенос, как показано ниже:

```
{ "result": "0000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f",  
  "error": null, "id": "1" }
```

Во всей книге данные оформляются моноширинным шрифтом, например: 7af24c99. Я обычно не указываю кодировку явно (десятичные числа, шестнадцатеричные строки, строки base64, строки base58 и т. д.), потому что часто это очевидно из контекста.

Прочие онлайн-ресурсы

Если у вас есть вопросы о Биткоин, на которые вы не нашли здесь ответов, рекомендую обратиться на сайт Bitcoin Stack Exchange (приложение В), где качество ответов определяется голосованием читателей.

Также советую посетить сайт Bitcoin Developer Reference (веб-ресурс 3), где можно найти исчерпывающую документацию о Биткоин.

Исходный код Bitcoin Core (веб-ресурс 4) является наиболее точным источником информации. Это эталонная реализация протокола Биткоин, и чтение такого исходного кода иногда является единственным способом найти необходимые ответы.

От издательства

Ваши замечания, предложения, вопросы отправляйте по адресу comp@piter.com (издательство «Питер», компьютерная редакция).

Мы будем рады узнать ваше мнение!

На веб-сайте издательства www.piter.com вы найдете подробную информацию о наших книгах.

Об авторе



Калле Розенбаум (Kalle Rosenbaum) занимается разработкой программного обеспечения вот уже 20 лет. Его увлечение Биткоином началось в 2013 году и продолжается до сих пор. В 2015-м Калле основал консалтинговую компанию по технологии Биткоин и с тех пор работает в этой отрасли. Он также ведет блог, где разъясняет различные технические вопросы, связанные с Биткоином, такие как усовершенствование механизма распространения блоков, боковые цепочки и транзакции «replace-by-fee» (замена за плату). Его блог служит целью помочь себе и другим извлекать выгоду.

1

Введение в Биткоин



Эта глава охватывает следующие темы:

- ✓ знакомство с технологией Биткоин;
 - ✓ оплата биткоинами;
 - ✓ проблемы, решаемые технологией Биткоин.
-

Цель этой книги — дать достаточный объем сведений о технологии Биткоин, чтобы вы смогли принять обоснованное решение о том, как можно использовать ее для улучшения личной жизни или бизнеса. Надеюсь, вы узнаете достаточно, чтобы решить, доверяете ли вы Биткоин или нет (надеюсь, что первое). Начиная движение к этой цели, я буду предполагать, что вы знаете, что означают следующие термины:

- ★ компьютерная программа;
- ★ база данных;
- ★ компьютерная сеть;
- ★ веб-сервер.

Если какой-то из этих терминов вам не знаком, не волнуйтесь. Отыщите его определение либо продолжайте чтение — я думаю, что вы не будете испытывать особых затруднений.

Что такое Биткоин?

Биткоин — это система электронных (цифровых) денег, которая позволяет людям обмениваться биткоинами (денежная единица в системе Биткоин)

между собой, не прибегая к услугам банков или какой-либо другой доверенной третьей стороны. Биткоины похожи на обычные банкноты и монеты, но это исключительно электронная валюта, и операции с ней осуществляются через Интернет. Валюта Биткоин не привязана ни к какой *фиатной валюте*, такой как доллар США или китайский юань; она имеет свободный плавающий обменный курс по отношению к большинству фиатных валют. Вы можете покупать и продавать биткоины за бумажные валюты онлайн, используя одну из нескольких бирж, например kraken.com, bitstamp.net или localbitcoins.com.

КАК ПРАВИЛЬНО?

Система называется *Биткоин (Bitcoin)*, и ее название записывается с заглавной буквы *Б (В)*. Денежная единица называется *биткоин (bitcoin)* и записывается с маленькой буквы *б (b)*. Часто для обозначения биткоинов используется значок ₿ и аббревиатуры *ВТС* и *ХВТ*. В этой книге я буду использовать аббревиатуру *ВТС*.

Никакие компании или правительства не контролируют систему Биткоин. Ее работу круглосуточно обеспечивают тысячи компьютеров по всему миру, объединенных в *сеть Биткоин*, как показано на рис. 1.1. Вам не нужно нигде регистрироваться — чтобы использовать Биткоин, достаточно иметь доступ в Интернет и компьютерную программу, например мобильное приложение.

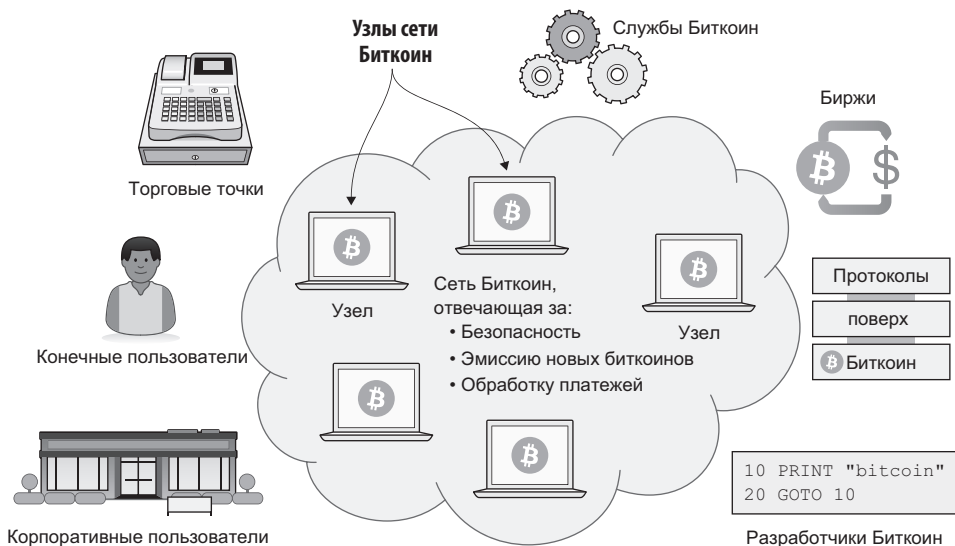


Рис. 1.1. Сеть Биткоин и ее экосистема

Любой желающий может использовать или участвовать в сети Биткоин без специального разрешения со стороны банка или другого подобного учреждения. Благодаря *свободной* природе Биткоин, за последние годы появилось много родственных технологий. Участников этой биткоин-экосистемы можно грубо разделить на несколько групп:

- ★ *Конечные пользователи* — люди, использующие Биткоин для своих повседневных нужд, например для хранения сбережений, покупок, игры на бирже или заработка.
- ★ *Корпоративные пользователи* — компании, использующие Биткоин для решения своих бизнес-задач, например для выплаты заработной платы работникам в других странах или в случаях, аналогичных конечным пользователям.
- ★ *Торговые точки* — например, рестораны или книжные магазины, принимающие платежи в биткоинах.
- ★ *Службы Биткоин* — компании, предоставляющие клиентам услуги, связанные с Биткоин, такие как пополнение счета мобильного телефона, услуги анонимного доступа, денежные переводы или выплата чаевых.
- ★ *Биржи* — коммерческие службы, которые люди могут использовать для обмена местной валюты на биткоины и обратно.
- ★ *Протоколы поверх Биткоин* — системы, действующие «поверх» Биткоин и выполняющие определенные задачи, например протоколы платежных сетей, специализированные маркеры и децентрализованные биржи.
- ★ *Разработчики Биткоин* — люди, работающие (часто бесплатно) над компьютерными программами с открытым исходным кодом, которыми пользуются участники сети Биткоин.

Задача сети Биткоин заключается в обработке платежей в биткоинах, ведении учета того, кто чем владеет, защите от несанкционированных модификаций и эмиссии новых биткоинов с заранее установленной скоростью. Сеть состоит из тысяч компьютеров, разбросанных по всему миру. Мы называем эти компьютеры *узлами Биткоин*, или просто *узлами*. Любой из участников, упомянутых выше, тоже может активно участвовать в работе биткоин-сети, запустив собственный биткоин-узел. Вы тоже должны будете запустить свой узел, если не хотите доверять другим предоставление вам финансовой информации.



КАКИЕ АСПЕКТЫ НЕ ИНТЕРЕСУЮТ БИТКОИН

Сеть Биткоин не проводит различий между пользователями. Никто не находится в более привилегированном положении, чем другие. Неважно, кто они и чем занимаются, все участвуют в работе сети на общих условиях.

Общая картина

Сеть Биткоин — это сеть из компьютеров, на которых установлено программное обеспечение Биткоин. Эта сеть проверяет и подтверждает платежи между пользователями Биткоин.

Предположим, что Алиса хочет заплатить Бобу 1 BTC. Платеж начинается с того, что Алиса создает транзакцию и отправляет ее в сеть Биткоин, как показано на рис. 1.2. Здесь я изобразил в общих чертах четыре этапа и каждый из них объясню в следующих разделах. Рисунок 1.2 появится также во введении к главам 2–8, где я также укажу, какую часть рисунка мы будем рассматривать в той или иной главе.

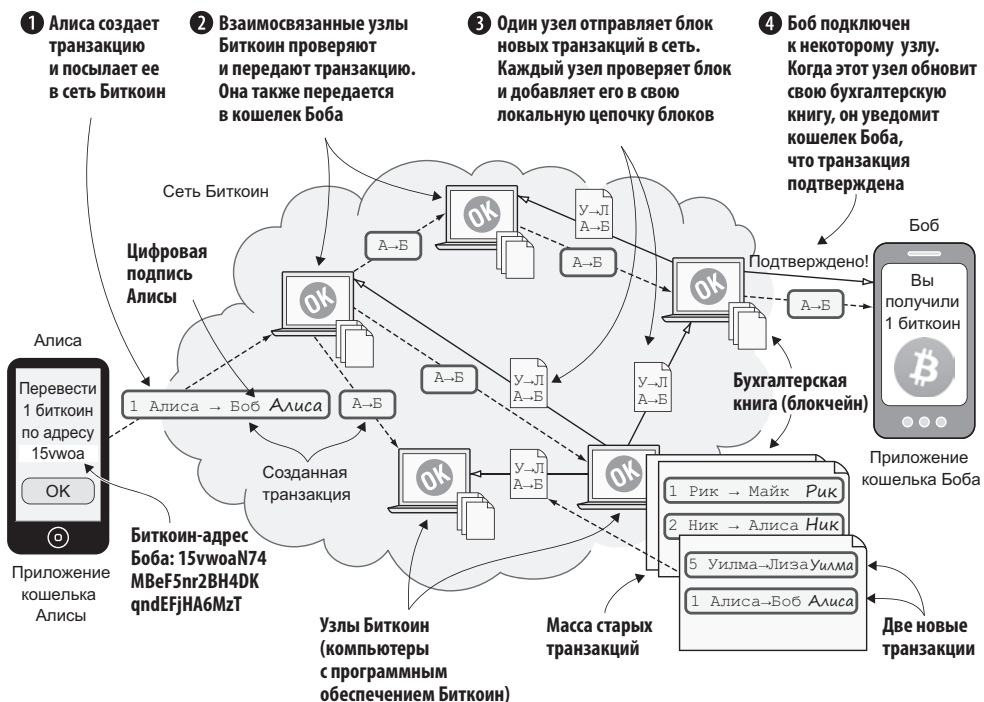


Рис. 1.2. Выполнение платежа в сети Биткоин. Платеж обрабатывается в четыре этапа

Теперь посмотрим, как обрабатывается платеж на пути от Алисы к Бобу:

- 1** Алиса создает транзакцию, которая переводит 1 биткоин Бобу, подписывает ее и посылает в сеть Биткоин.

- ❷ Компьютеры в сети — узлы Биткоин — проверяют, действительно ли у Алисы есть деньги и является ли транзакция подлинной. Затем они передают транзакцию своим соседям, которые называют *пирами*.
- ❸ Каждый компьютер обновляет свою копию *цепочки блоков Биткоин (блокчейн)*, или *консенсусный реестр*, добавляя в нее информацию о новом платеже.
- ❹ Сеть уведомляет Боба, что он получил 1 биткоин.



**Я ДУМАЛ,
ЧТО БИТКОИН
ПОДДЕРЖИВАЕТ
АНОНИМНОСТЬ!**

Биткоин не использует имен или другую личную информацию. Я указал здесь имена участников только ради упрощения.

Обратите внимание, что в действительности Алиса *не посылает* 1 биткоин Бобу, а просит сеть переместить 1 биткоин из кошелька Алисы в кошелек Бобу внутри цепочки блоков (блокчейне) Биткоин.

Цепочка блоков (блокчейн) Биткоин — это база данных, копия которой хранится на каждом компьютере в сети Биткоин. Представьте, что блокчейн — это большая бухгалтерская книга, в котором зафиксированы все транзакции, выполнявшиеся когда-либо.

В следующих четырех разделах мы подробно разберем каждый этап.

Шаг ❶: транзакции

Шаг ❶ (рис. 1.3) — Алиса просит сеть перевести 1 биткоин Бобу. Для этого она посылает транзакцию в сеть Биткоин. Транзакция содержит инструкции о том, как перевести деньги, и цифровую подпись, подтверждающую, что именно Алиса просит перевести деньги.

Транзакция Биткоин — это блок данных, определяющий:

- ★ сумму перевода (1 биткоин);
- ★ биткоин-адрес получателя перевода (биткоин-адрес Боба, 15vwoaN74MBeF5nr2BH4DKqndEFjHA6MzT);
- ★ *цифровую подпись* (созданную с помощью закрытого ключа Алисы).



ТРАНЗАКЦИЯ

Транзакция — это платеж. Эти два термина взаимозаменяемы. Подробнее о транзакциях рассказывается в главах 5 и 9.



Рис. 1.3. Алиса создает транзакцию, подписывает ее и посылает одному или нескольким узлам в сети Биткоин

Цифровая подпись создается на основе транзакции и огромного секретного числа, называемого *закрытым ключом*, известного только Алисе. В результате получается цифровая подпись, которую может создать только владелец закрытого ключа.

Приложение мобильного кошелька Алисы подключается к одному или нескольким узлам в сети Биткоин и посылает им созданную транзакцию.

ЦИФРОВЫЕ ПОДПИСИ

Подробнее о цифровых подписях рассказывается в главе 2.

Шаг ②: сеть Биткоин

Алиса посылает транзакцию одному или нескольким узлам Биткоин. На этапе ② (рис. 1.4) каждый такой узел проверяет действительность транзакции и передает ее своим пирам. Для этого он обращается к локальной копии блокчейна (цепочки блоков) и убеждается, что:

- ★ биткоин, который пытается потратить Алиса, действительно существует;
- ★ цифровая подпись Алисы действительна.

Если все проверки пройдены, узел пересылает транзакцию своим пирам в сети Биткоин. Такая пересылка называется *ретрансляцией*. Спустя какое-то время транзакция Алисы пройдет через всю сеть и каждый узел проверит ее по пути. Блокчейн пока не обновляется; это следующий шаг.

ОШИБОЧНЫЕ ТРАНЗАКЦИИ

Ошибочные транзакции просто уничтожаются. Они не уходят дальше первого узла.

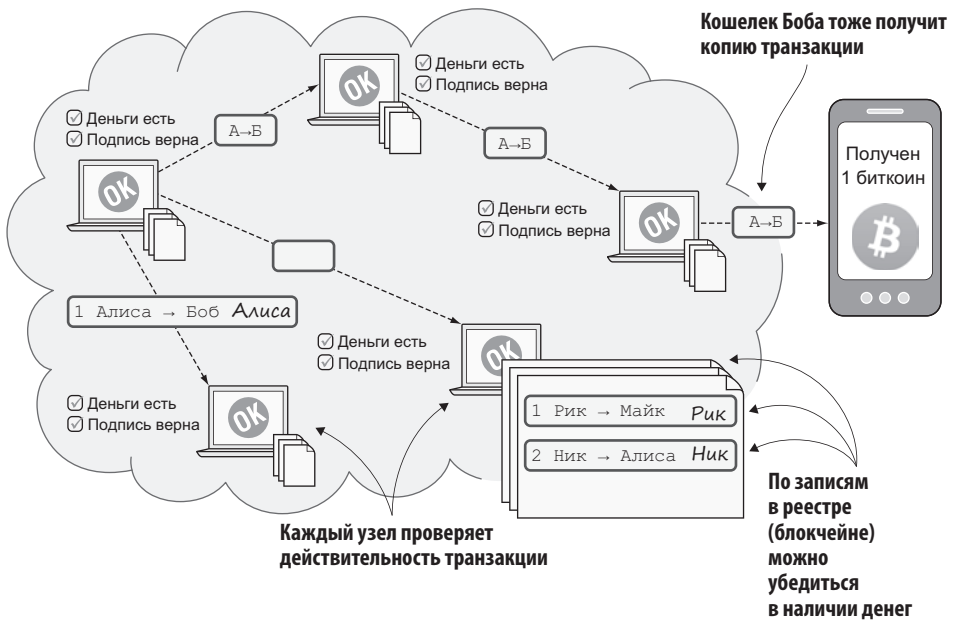


Рис. 1.4. Алиса посылает транзакцию узлу в сети. Узел проверяет транзакцию и пересылает ее другим узлам. В какой-то момент транзакция будет получена всеми узлами сети

Шаг ③: блокчейн

На шаге ③ узлы обновляют свои локальные копии цепочки блоков (блокчейна) Биткоин, добавляя транзакцию Алисы. Блокчейн содержит историческую информацию обо всех предыдущих транзакциях; время от времени в него добавляются новые транзакции, такие как транзакция Алисы.

БЛОКЧЕЙН

Название *блокчейн* (цепочка блоков) описывает структуру консенсусного реестра. Консенсусный реестр организован как последовательность блоков, составленных в цепочку так, чтобы легко было обнаружить любые изменения. Подробнее об этом рассказывается в главе 6.

Добавление транзакции Алисы в блокчейн выполняется не так просто, как может показаться. Транзакция Алисы не единственная в сети Биткоин.

Одновременно могут выполняться тысячи транзакций. Если все узлы будут обновлять свои копии блокчейна при получении каждой транзакции, копии недолго будут оставаться копиями, потому что на разные узлы транзакции могут приходить в разном порядке, как показано на рис. 1.5.

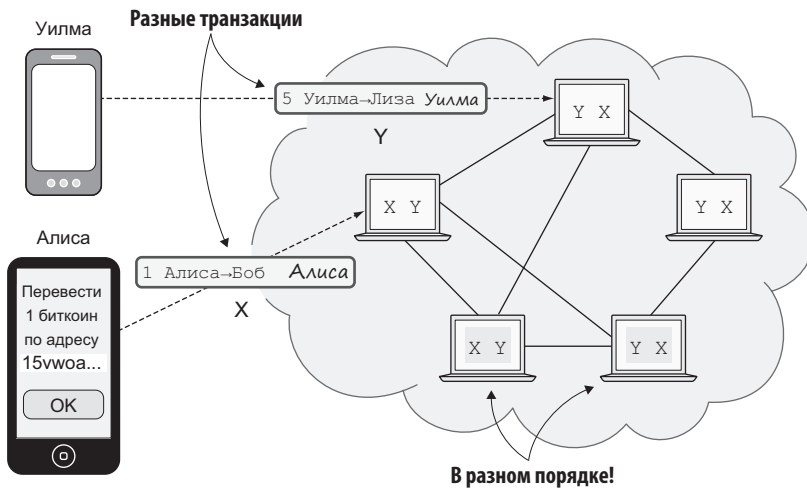


Рис. 1.5. На разные узлы транзакции поступают в разном порядке. Если все узлы будут записывать транзакции в блокчейн в порядке их поступления, блокчейны на разных узлах будут отличаться

Для упорядочения транзакций один узел берет на себя инициативу, говоря: «Я хочу добавить эти две транзакции в блокчейн в порядке Y, X!» Это сообщение, известное как *блок*, отправляется лидером (рис. 1.6) точно так же, как Алиса отправляет транзакцию.

Получив новый блок, узлы обновляют свои копии блокчейна и передают блок своим пирам. Транзакция Алисы — одна из транзакций в блоке и теперь становится частью блокчейна.

Почему узел может пожелать взять на себя инициативу? Узел, берущий инициативу, вознаграждается вновь отчеканенными биткоинами и комиссией за транзакции, которые он включает в блок.

Сможет ли любой узел все время брать на себя инициативу и получать вознаграждение? Нет, не сможет. Чтобы взять на себя инициативу, узел должен

**ДОБАВЛЯТЬ НОВЫЕ
ТРАНЗАКЦИИ МОЖНО
ТОЛЬКО В КОНЕЦ
БЛОКЧЕЙНА**

Новые транзакции всегда добавляются в конец блокчейна — он растет только с конца.

решить сложную задачу. Для этого требуется много времени и электроэнергии, а значит, лидеры будут возникать нечасто. Задача настолько сложна, что большинство узлов в сети даже не пытаются браться за нее. Узлы, делающие такую попытку, называют *майнерами*¹, потому что они добывают новые монеты, подобно тому как золотоискатель добывает золото. Более подробно мы обсудим этот процесс в главе 7.

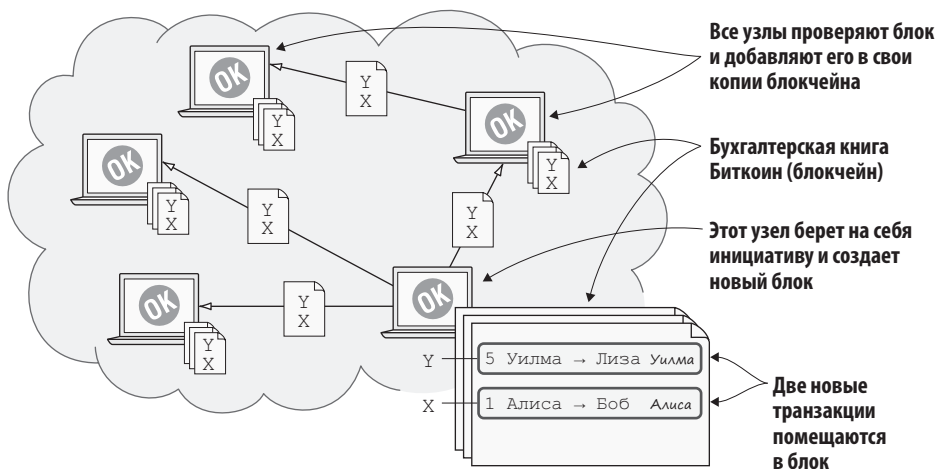


Рис. 1.6. Один из узлов берет на себя инициативу и определяет порядок добавления транзакций. Другие узлы проверяют блок и обновляют свои копии блокчейна

Шаг 4: кошельки

Боб и Алиса являются пользователями сети Биткоин, и им обоим нужна компьютерная программа для взаимодействия с сетью. Такая программа называется *биткоин-кошелек*. Существует несколько типов биткоин-кошельков для разных устройств, таких как мобильные телефоны и настольные компьютеры, и даже существуют специализированные аппаратные кошельки.

ЧТО ДЕЛАЕТ КОШЕЛЕК

Типичный биткоин-кошелек:

- управляет ключами;
- следит за входящими/исходящими биткоинами;
- посылает биткоины.

¹ В переводе с англ. *miner* (майнер) — добытчик. — Примеч. пер.

Перед шагом ④ процесса оплаты узлы в сети обновляют свои локальные копии блокчейна. Теперь сеть должна уведомить Алису и Боба о том, что транзакция прошла, как показано на рис. 1.7.

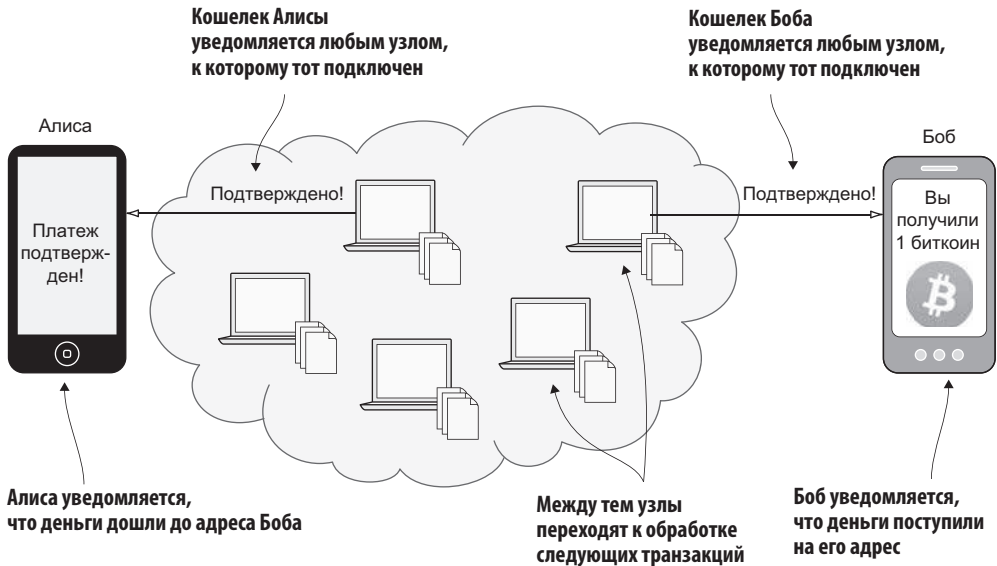


Рис. 1.7. Кошелек Боба просит узел сообщить об операциях с биткоин-адресом Боба. Алиса послала платеж по адресу Боба, а узел только что записал транзакцию в блокчейн, о чем уведомляет кошелек Боба

Кошелек Боба подключен к некоторым узлам сети Биткоин. Когда в блокчейн добавляется транзакция, касающаяся Боба, узлы, к которым подключен кошелек Боба, уведомят его об этом. Кошелек Боба отобразит сообщение, что он получил 1 биткоин. Алиса тоже использует кошелек. Ее кошелек также будет уведомлен о выполнении транзакции.

Помимо отправки и получения транзакций, кошельки Алисы и Боба также управляют их закрытыми ключами. Как отмечалось выше, закрытый ключ используется для создания цифровых подписей биткоин-адреса. Алиса создала свою цифровую подпись с помощью одного из своих закрытых ключей. Когда позже Боб захочет потратить деньги, которые получил на свой биткоин-адрес, сгенерированный с использованием его закрытого ключа, он должен будет создать транзакцию и подписать ее цифровой подписью этим закрытым ключом.

Проблемы современных денег

Технология Биткоин не получила бы такого распространения, если бы не решала насущных проблем. Биткоин решает некоторые проблемы, свойственные традиционным финансовым системам. Давайте рассмотрим некоторые наиболее широко обсуждаемые группы проблем.

Дискриминация

Люди, имеющие счета в банках и доступ к банковским услугам, таким как онлайн-платежи или кредиты, оказываются в более привилегированном положении. По данным Всемирного банка, около 38% населения мира не имеет банковских счетов (см. веб-ресурс 6 в приложении В). Цифры постепенно улучшаются, но многие люди по-прежнему могут использовать только наличные.

Без банковского счета и основных банковских услуг, таких как онлайн-платежи, люди не могут распространить свой бизнес за пределы своих стран и регионов. Продавец не может предлагать товары или услуги в Интернете для увеличения своей клиентской базы. Человеку, живущему в сельской местности, возможно, придется провести в дороге полдня, чтобы оплатить счет за коммунальные услуги или пополнить свой мобильный счет.

Такая дискриминация в отношении людей, имеющих и не имеющих банковские счета, обусловлена несколькими факторами:

- ★ для некоторых банковские услуги слишком дороги;
- ★ чтобы пользоваться банковскими услугами, нужны документы, например удостоверение личности, которого у многих нет;
- ★ в банковских услугах может быть отказано людям с определенными политическими взглядами или тем, кто ведет определенный бизнес. Людям также может быть отказано в обслуживании из-за этнической принадлежности, национальности, сексуальных предпочтений или цвета кожи.

ПРОБЛЕМЫ

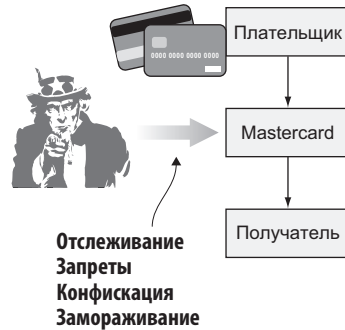
☐ Дискриминация

Проблемы конфиденциальности

Говоря об электронных платежах, например, с использованием кредитных карт или банковских переводах, нельзя не упомянуть о проблемах с конфи-

денциальностью, характерных для традиционных денег. Сотрудники банков легко могут:

- ★ отслеживать платежи;
- ★ запрещать платежи;
- ★ замораживать активы;
- ★ конфисковывать средства со счетов.



Вы можете сказать: «Мне нечего скрывать, а правительству нужны эти инструменты для борьбы с преступностью». Проблема в том, что никто не знает, как правительство будет выглядеть через пять лет и как это правительство определяет преступность. Новые законы — часто результат выборов. После следующих выборов ваше правительство может принять закон, позволяющий замораживать средства граждан, разделяющих вашу политическую точку зрения. В некоторых странах это уже происходит.

Есть много примеров, когда власть использовалась, чтобы лишить кого-либо возможности совершать сделки. Например, в 2010 году попала под санкции некоммерческая организация WikiLeaks. Тогда, после давления со стороны правительства США на крупные платежные сети Visa и Mastercard (см. веб-ресурс 7), были заблокированы все пожертвования через традиционные каналы. В 2013 году мы также видели, как Кипр конфисковал 47,5% всех банковских депозитов, превышающих 100 тысяч евро, в рамках программы финансового спасения (веб-ресурс 8).

ПРОБЛЕМЫ

- ☐ Дискриминация
- ☐ Проблемы конфиденциальности

Обратите внимание, что эта проблема обычно не затрагивает банкноты и монеты. Пока есть наличные деньги, люди могут торговать свободно и в частном порядке. В некоторых странах, например в Швеции, объем наличности постепенно сокращается, то есть вскоре вы не сможете купить даже жевательную резинку, чтобы где-то не зафиксировалась информация об этой транзакции.

Инфляция

Под *инфляцией* подразумевается снижение покупательной способности денег (рис. 1.8).

Большинство валют подвержено инфляции, одни больше, другие меньше. Например, в 2007–2008 годах зимбабвийский доллар упал примерно на

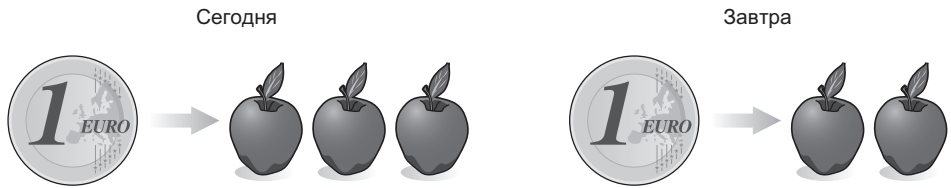


Рис. 1.8. Инфляция

10²³%, достигнув пика в 80 миллиардов процентов в месяц, державшегося в течение нескольких месяцев в 2008 году. Это почти 100% среднесуточный уровень инфляции, то есть цены примерно удваивались каждый день.

Подобные экстремальные проявления инфляции называются *гиперинфляцией* и обычно обусловлены ростом денежной массы. Правительства иногда увеличивают денежную массу, стремясь изъять ценности у населения и покрыть такие расходы, как государственный долг, война или социальное обеспечение. При чрезмерном использовании этого инструмента риск гиперинфляции возрастает многократно.

ПРОБЛЕМЫ

- ☐ Дискриминация
- ☐ Проблемы конфиденциальности
- ☐ Инфляция

Быстрый рост денежной массы, скорее всего, приведет к обесцениванию национальной валюты. Это, в свою очередь, заставит людей обменивать местную валюту на товары или валюты других стран, которые лучше справляются с удержанием цен, что еще больше способствует снижению стоимости местной валюты. Ситуация может обостриться до крайности, как в Зимбабве. Результат катастрофичен для людей, поскольку они видят, что их сбережения превращаются практически в ничто. В табл. 1.1 перечислены примеры недавних гиперинфляций.

Таблица 1.1. Некоторые примеры недавних гиперинфляций. Источник: Википедия

Страна	Год	Наибольшая инфляция в месяц (%)
Зимбабве	2007–2008	$4,19 \times 10^{16}$
Югославия	1992–1994	313×10^6
Перу	1990	397
Украина	1992–1994	285
Венесуэла	2012–	120

Зимбабве показала пример одного из самых экстремальных случаев инфляции за всю историю, но даже сегодня некоторые страны страдают от очень высокой инфляции. Одна из них — Венесуэла, где в 2016 году ее валюта, боливар, претерпела инфляцию в 254%, а в 2017 году — около 1088%. В 2018 году прогнозируется ошеломляющий уровень инфляции в 1 370 000%.

Границы

Перемещать ценности через национальные границы, используя национальную (*фиатную*) валюту, сложно, дорого, а иногда даже незаконно. Если вы решите отправить тысячу шведских крон (SEK) из Швеции человеку на Филиппинах, то сможете воспользоваться услугами, например, Western Union. Когда я исследовал этот вопрос, 1000 шведских крон стоили 5374 филиппинских песо (PHP), или 109 долларов США (табл. 1.2).

Таблица 1.2. Стоимость перевода 5374 филиппинских песо из Швеции на Филиппины

Отправка из	Получение в	Получено фактически	Комиссионные	Комиссионные (%)
Банк	Банк	5109 PHP	265 PHP	4,9%
Банк	Наличные	4810 PHP	564 PHP	10,5%
Кредитная карта	Наличные	4498 PHP	876 PHP	16,3%

Если у получателя есть банковский счет, открытый для получения международных денежных переводов, вы сможете обойтись комиссией 4,9%. Но если получатель ограничен возможностью получать только наличные, тогда комиссия может удвоиться, а то и утроиться до 10,5% или 16,3%, в зависимости от скорости перевода и удобства его получения.

В отличие от международных переводов, перемещение фиатной валюты в пределах государства обычно удобнее. Например, наличные можно передать непосредственно получателю или перевести с помощью какого-либо мобильного приложения, созданного специально для национальной валюты. Пока вы остаетесь в пределах одной страны и одной валюты, фиатные деньги обычно довольно удобны в обращении.

ПРОБЛЕМЫ

- ☐ Дискриминация
- ☐ Проблемы конфиденциальности
- ☐ Инфляция
- ☐ Границы

Подход, предлагаемый технологией Биткоин

Биткоин предлагает модель, принципиально отличающуюся от модели традиционных финансовых институтов. Рассмотрим основные различия.

Децентрализация

Вместо централизованной организации, например Федеральной резервной системы США, контроль биткоинов осуществляется тысячами компьютеров, или узлов. Ни один узел или группа узлов не имеет больше привилегий или обязательств, чем любой другой. Это равенство между узлами делает систему Биткоин *децентрализованной*, в противовес централизованным системам, таким как банки или поисковая система Google (рис. 1.9).

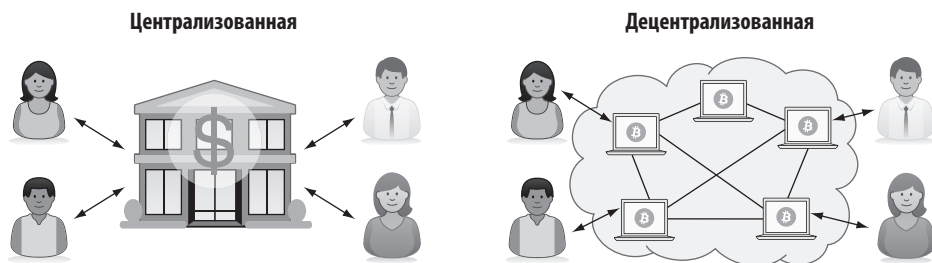


Рис. 1.9. Централизованная и децентрализованная услуги

В централизованной системе услуга контролируется одним субъектом, например банком. Этот субъект может решать, кто получит услугу и что ему разрешено делать. Например, онлайн-видеосервис может предлагать видеофильмы только людям, проживающим в определенном географическом местоположении.

В децентрализованной системе с несколькими тысячами узлов, разбросанными по всему миру, очень сложно контролировать, кто и как использует систему. Независимо от того, где они проживают, кем являются или кому отправляют деньги, система Биткоин

РЕШЕННЫЕ ПРОБЛЕМЫ

- ☒ Дискриминация
- ☒ Проблемы конфиденциальности
- ☐ Инфляция
- ☐ Границы

будет одинаково относиться ко всем пользователям. В системе Биткоин нет центрального органа управления, который можно использовать для цензуры платежей, отказа в обслуживании или конфискации средств.

Как уже отмечалось, система Биткоин не ограничивает доступ к своим услугам, а значит, вам не нужно ни у кого спрашивать разрешения на участие в ней. Любой, у кого есть компьютер и подключение к Интернету, может настроить узел Биткоин и играть активную роль в сети — никаких вопросов не задается и никакой регистрации не требуется.

Изменение правил Биткоин практически невозможно без общего согласия. Если узел не подчиняется правилам, остальные узлы его просто игнорируют. Например, одно из правил гласит, что денежная масса в системе Биткоин ограничена 21 миллионом биткоинов. Этот предел почти невозможно изменить из-за децентрализации; никто не сможет, угрожая или давая взятки, изменить правила.

Ограниченная денежная масса

Поскольку денежная масса в системе Биткоин не может превысить 21 миллиона биткоинов, люди могут быть уверены, что, владея 1 биткоином, они *всегда* будут владеть, по крайней мере, одной 21-миллионной частью всех биткоинов. Эта особенность не встречается ни в одной фиатной валюте, где решения об эмиссии очень часто принимаются компанией или государством. Биткоин устойчив к высокой инфляции, потому что нет возможности увеличить денежную массу по чьему-либо желанию.

РЕШЕННЫЕ ПРОБЛЕМЫ

- ☒ Дискриминация
- ☒ Проблемы конфиденциальности
- ☒ Инфляция
- ☐ Границы

Денежная масса в системе Биткоин пока не достигла предела. Согласно *заранее установленному* графику, она растет с уменьшающейся скоростью и в конечном счете прекратит расти примерно к 2140 году (рис. 1.10).

На момент написания этих строк в обращении находилось около 17 миллионов биткоинов, а текущий ежегодный прирост составлял примерно 4%. Этот прирост уменьшается вдвое каждые четыре года.

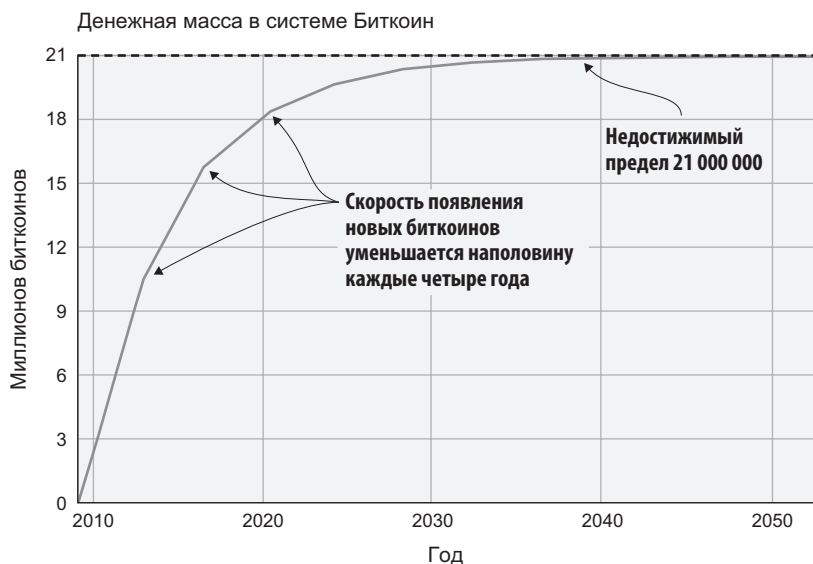


Рис. 1.10. С течением времени количество биткоинов достигнет своего предела, примерно равного 21 миллиону. Увеличение в последние 100 лет перед 2140 годом будет едва заметно

Отсутствие границ

Поскольку Биткоин — это система, управляемая обычными компьютерами, подключенными к Интернету, она имеет такой же глобальный характер. То есть любой человек, имеющий подключение к Интернету, может отправлять деньги другим людям по всему миру, как показано на рис. 1.11.

РЕШЕННЫЕ ПРОБЛЕМЫ

- ☒ Дискриминация
- ☒ Проблемы конфиденциальности
- ☒ Инфляция
- ☒ Границы

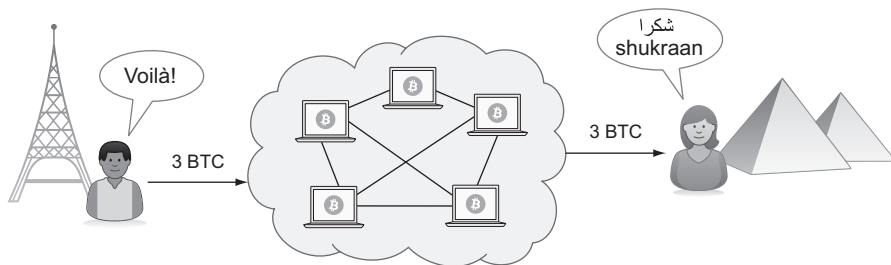


Рис. 1.11. Биткоин не имеет границ

Нет никакой разницы между отправкой биткоина кому-то находящемуся в одной комнате с вами или на другом континенте. Суть от этого не меняется: деньги отправляются непосредственно получателю, который видит платеж почти мгновенно. Получатель может быть *уверен*, что не более чем через час деньги будут принадлежать ему. Как только деньги осядут в кошельке, перевод нельзя отменить без согласия получателя.

Где можно использовать биткоины?

К настоящему моменту мы затронули несколько общих вариантов использования биткоинов. В этом разделе мы подробнее рассмотрим эти и некоторые другие варианты. Трудно предсказать, какие варианты мы увидим в будущем, поэтому будем придерживаться того, что известно сейчас.

Сбережение

Одна из интересных особенностей биткоинов заключается в том, что безопасность хранения денег зависит от безопасности хранения набора закрытых ключей: секретных данных, которые понадобятся, когда вы захотите потратить свои деньги. Вы сами выбираете, как хранить свои закрытые ключи. Можете записать их на бумаге или хранить в электронном виде с помощью мобильного приложения, чтобы упростить к ним доступ. Также можете запомнить свои личные ключи. Эти ключи — все, что нужно, чтобы тратить деньги. Держите их в тайне.



Сбережение — привлекательный вариант использования биткоинов. Самый простой способ сберечь деньги — создать закрытый ключ, записать его на листе бумаги и запереть в сейфе. Этот лист бумаги теперь является вашим сберегательным счетом, вашим сберегательным кошельком. Затем вы можете перевести биткоины в свой кошелек. Пока закрытый ключ хранится в безопасности, ваши деньги тоже будут пребывать в безопасности. На выбор есть множество различных схем сбережения, и вы легко найдете приемлемый для себя баланс между безопасностью и удобством. Например, вы можете хранить ключи в незашифрованном виде в мобильном телефоне для удобного доступа или хранить их в зашифрованном виде в хранилище с вооруженной охраной.

Трансграничные платежи

Как уже отмечалось, перевод денег из одной страны в другую стоит дорого (скажем, 15%), особенно если деньги переводятся в бедную страну, а у получателя нет банковского счета. В последнее время растет популярность использования биткоинов для обхода этой дорогой и медлительной устаревшей системы. Обычно дешевле обменять шведские кроны на биткоины в Швеции, переслать биткоины на Филиппины, а затем обменять биткоины на филиппинские песо.

Некоторые компании предлагают подобную услугу: вы платите шведские кроны компании, а компания выплачивает деньги филиппинскими песо вашему другу (рис. 1.12). Вы даже не узнаете, что за кулисами используются биткоины. Такие компании обычно берут несколько процентов за услугу, но это все равно дешевле, чем традиционные услуги по переводу денег.



Рис. 1.12. Компания, предлагающая услугу денежных переводов, использует биткоины для передачи денег из Швеции на Филиппины

Конечно, если получатель может свободно использовать биткоины в своей стране, потребность в посреднике, берущем деньги за услуги, отпадает сама собой. Вы можете сами послать биткоины своему другу напрямую. В этом вся прелесть системы Биткоин. Биржи и другие обслуживающие компании — это всего лишь мосты, соединяющие старый мир с новым миром Биткоин.

Покупки

Наиболее очевидный вариант использования системы Биткоин — это покупки. Отсутствие границ и безопасность Биткоин делают ее идеальной для онлайн-платежей за товары и услуги.



Выполняя традиционные онлайн-платежи, вы отправляете данные своей дебетовой карты продавцу и *надеетесь*, что продавец снимет ровно ту сумму, с которой вы согласились. Вы также *надеетесь*, что продавец предпримет все меры безопасности при обработке данных вашей дебетовой карты. Вполне возможно, что эти данные он сохранит в базе данных. Только представьте: при оплате каждой покупки дебетовой картой информация о карте будет сохраняться в базе данных продавца. Вполне вероятно, что *одна* из баз данных будет взломана, а данные украдены. Чем больше продавцов сохранит ваши данные, тем выше риск.

В системе Биткоин эта проблема отсутствует, потому что вы не посылаете конфиденциальную информацию продавцу или кому-либо еще. Вы переводите сумму, которую согласились перевести, и больше ничего.

Спекуляции на курсах

Мир полон людей, желающих быстро разбогатеть. Биткоин может привлекать их *волатильностью* цен или динамикой курса. Глядя на историю цен на биткоины, изображенную на рис. 1.13, представляется заманчивым купить биткоины по низкой цене и продать по высокой.

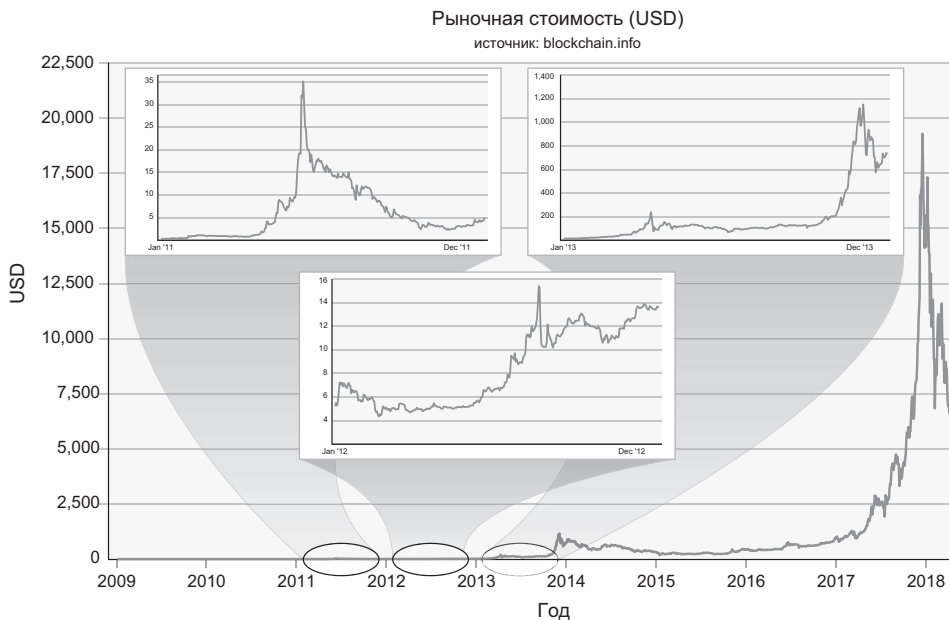


Рис. 1.13. Цены в долларах США (USD) за всю историю Биткоин

В ноябре 2013 года за несколько недель цена биткоина поднялась с примерно 100 долларов США до более чем 1100. Это явно был так называемый *пузырь*, в котором люди боялись упустить значительную прибыль и покупали, повышая цену до тех пор, пока она в конечном итоге не начала снова падать. Падение до 50% от пикового значения было столь же быстрым, как и рост. Та же картина повторилась в конце 2017 года, но с большим размахом. Это случалось уже много раз. Подобные колебания редко бывают вызваны какими-либо конкретными новостями или технологическим прогрессом и чаще возникают из-за спекуляций. Игра на курсах может быть захватывающей, если вы можете позволить себе проиграть, но она больше похожа на лотерею, чем на реальный заработок. Иногда правительство или крупная корпорация делает негативное заявление о Биткоин, порожающее страх на рынке, но эти события, как правило, оказывают ограниченное влияние на стоимость самих монет.

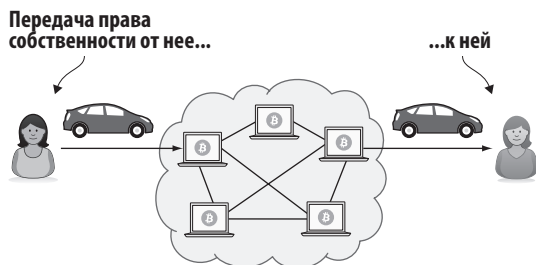
Волатильность цены на биткоин противоречит утверждениям о том, что он обладает неинфляционным свойством; падение рыночной стоимости на 50% выглядит вполне себе инфляционным. Биткоин все еще относительно нов, и множество краткосрочных спекуляций вызывает волатильность. Но биткоин растет, и все больше людей и организаций начинают использовать его для хранения своих богатств, поэтому он, вероятно, стабилизируется в долгосрочной перспективе, и его дефляционное свойство проявится со временем.

Безвалютное использование

Биткоин — цифровая валюта, но эту форму денег можно использовать не только как деньги. В этом разделе описываются два основных способа использования, но есть и другие, в том числе еще не изобретенные.

Право собственности

Биткоин позволяет внедрять в платежи небольшие фрагменты данных. Этими данными может быть, например, номер кузова автомобиля. Когда автомобиль покидает завод, производитель может перевести небольшую сумму в бит-



коинах новому владельцу автомобиля, указав номер шасси. Этот платеж будет представлять передачу права собственности на автомобиль.

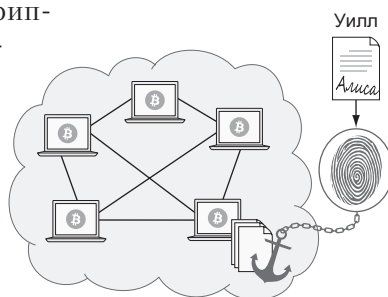
Платежи в биткоинах являются открытыми записями, но они никак не связаны с людьми. Они привязаны к длинным цепочкам цифр, называемым *открытыми ключами*, которые подробно описываются в главе 2. Производитель автомобилей может опубликовать свой открытый ключ на своем веб-сайте, в газетах и в рекламных объявлениях, чтобы связать ключ с личностью производителя. После этого любой сможет убедиться, что производитель передал право собственности на автомобиль новому владельцу. Новый владелец сможет доказать, что владеет автомобилем, с помощью своего закрытого ключа, соответствующего открытому ключу, посредством которого производитель передал право собственности.

Новый владелец может продать автомобиль кому-то другому и передать право собственности, отправив ту же сумму в биткоинах, которую получил от производителя, на открытый ключ нового владельца. Широкая публика сможет проследить, как менялось право собственности на автомобиль от производителя, через открытый ключ каждого владельца.

Доказательство существования

Используя тот же метод хранения данных в биткоин-платеже для передачи права собственности на автомобиль, можно доказать, что документ существовал до определенного момента времени.

Цифровой документ имеет *сигнатуру*: криптографический хеш, который любой может вычислить по документу. Создание другого документа с той же сигнатурой практически невозможно. Эту сигнатуру можно прикрепить к платежу в биткоинах. Куда уходят деньги, не имеет значения; важно, что сигнатура сохранится в блокчейне Биткоин. Таким способом можно «привязать» документ к блокчейну.



Платежи в биткоинах являются открытыми записями, поэтому любой сможет убедиться в существовании документа до момента оплаты, рассчитав сигнатуру документа и сравнив его с сигнатурой, хранящейся в блокчейне.

Как оцениваются биткоины?

Как рассказывалось в разделе «Игра на курсах», цена биткоина может сильно колебаться. Но как эта цена определяется? Существует несколько бирж, торгующих биткоинами, большинство из которых проводят торги в Интернете. Они напоминают фондовые биржи, где встречаются интересы пользователей, желающих продать и купить биткоины.



Разные рынки могут иметь разные цены, в зависимости от спроса и предложения. Например, в таких странах, как Венесуэла, где правительство пытается помешать развитию рынка биткоинов, предложение невелико. А спрос высок, потому что люди стремятся избавиться от своей гиперинфляционной валюты. Эти факторы приводят к росту цен на биткоины на этом рынке, по сравнению, например, с рынками США и Европы, где люди могут торговать более свободно.

В каких случаях биткоины не могут использоваться

Биткоин имеет много достоинств, но его можно использовать не во всех ситуациях. По крайней мере пока.

Микроплатежи

Транзакция в системе Биткоин обычно должна включать комиссию за обработку. Величина комиссии зависит не от суммы, а от размера транзакции в байтах, потому что цена обработки транзакции в сети Биткоин в основном зависит от ее размера (в байтах). Транзакции с большой суммой ничуть не больше (в байтах) транзакции с маленькой суммой, поэтому комиссия за обработку обеих транзакций примерно одинакова. Комиссия за транзакцию также зависит от спроса и предложения на доступное пространство в блокчейне. Блокчейн не может обрабатывать более 12 Мбайт транзакций