Содержание

Посвящается моей маме Терезе (1946–2017).
Она научила меня любить книги
и не принимать на веру мнение авторитетов.
Спасибо, мама!

Предисловие

Как я писал книгу о биткойне

Про биткойн я впервые услышал в середине 2011 года. Первое впечатление было приблизительно таким: «Пфф! Деньги для умников-ботаников», – и я забыл об этом на следующие шесть месяцев, не оценив важности этого явления. Впоследствии подобную реакцию я часто видел у многих умнейших людей, знакомых мне, и это немного утешает. Когда я встретился с биткойном во второй раз при обсуждении в списке рассылки, я решил прочитать документ с техническим описанием, написанный Сатоши Накамото (Satoshi Nakamoto), чтобы изучить авторитетный источник и понять, о чем вообще идет речь. До сих пор помню тот момент, когда я прочитал эти девять страниц, когда осознал, наконец, что биткойн – это не просто цифровые деньги, а сеть доверия, которая могла бы также стать основой для гораздо большего. Осознание того, что «биткойн – это не деньги, а децентрализованная сеть доверия», стало исходным пунктом для четырехмесячного исследования, во время которого я жадно поглощал каждый фрагмент информации о биткойне, который мне попадался. Эта тема овладела моим умом, я полностью увлекся ею, не отходя от компьютера по 12 и более часов в сутки, читал, писал, программировал, изучал все, что мог. Из этого состояния отрешенности от действительности я вышел, похудев на 20 фунтов (около 9 кг) из-за недостаточно полноценного питания, твердо решив вплотную заняться работой с биткойном.

Два года спустя, после создания нескольких небольших стартапов, использующих разнообразные сервисы и продукты, связанные с технологией биткойна, я решил, что пришло время для того, чтобы написать свою первую книгу. Биткойн как неисчерпаемый источник вдохновения занимал все мои мысли, эта технология стала самой значимой со времени появления Интернета. Настало время поделиться моей увлеченностью, моими знаниями об этой великолепной технологии с более широкой аудиторией.

Для кого предназначена эта книга

Эта книга предназначена в основном для программистов-кодеров. Если вы можете писать программы на каком-либо языке программирования, то из этой книги вы узнаете, как работают криптографические валюты, как их использовать и как разрабатывать программное обеспечение (ПО) для работы с ними. Кроме того, несколько первых глав можно рассматривать как подробное введение в технологию биткойна для тех, кто не занимается программированием, но пытается понять внутреннее устройство и функционирование биткойна и криптографических валют.

Почему на обложке изображены насекомые?

Муравей-листорез относится к биологическим видам, демонстрирующим чрезвычайно сложное поведение в колонии социальных насекомых (суперорганизме), но каждый отдельный муравей действует в соответствии с набором простых правил, соответствующих принципам социального взаимодействия и основанных на обмене химическими ароматическими веществами (феромонами). Цитата из Википедии: «Муравьи-листорезы образуют самые крупные и самые сложные сообщества живых организмов на Земле, если не считать людей». В действительности муравьи-листорезы не едят листья, но используют их для разведения особого вида грибов, являющегося основным источником питания для колонии. Вы понимаете? Муравьи занимаются сельскохозяйственным производством!

Несмотря на то что муравьи образуют кастовое сообщество и у них имеется матка-королева для производства потомства, все же у них нет централизованного органа управления или лидера всей муравьиной колонии. Высокий интеллект и разумное поведение, демонстрируемое многомиллионной колонией, является так называемым эмерджентным свойством (emergent property), системным эффектом, возникающим или проявляющимся как следствие взаимодействия отдельных членов социальной сети.

Природа наглядно показывает, что децентрализованные системы могут быть весьма гибкими и проявлять эмерджентную (приобретенную, а не врожденную) сложность и невероятную изощренность поведения без обязательного наличия в них центрального органа управления, иерархии или сложных составных частей.

Биткойн – это чрезвычайно разумная и изощренная децентрализованная сеть доверия, которая может поддерживать огромное количество финансовых процессов. При этом каждый узел сети биткойн следует нескольким простым математическим правилам. Такое взаимодействие множества узлов как раз и приводит к формированию разумного поведения при отсутствии, казалось бы, неизбежной сложности или доверия к отдельно взятому узлу. Подобно муравьиной колонии, сеть биткойн является гибкой сетью простых узлов, соблюдающих простые правила, и эти узлы, объединенные в сеть, могут делать удивительные вещи без какой-либо централизованной координации.

Условные обозначения и соглашения, принятые в книге

В книге используются следующие типографские соглашения:

Курсив

Используется для смыслового выделения важных положений, новых терминов, имен команд и утилит, а также имен и расширений файлов и каталогов.

Моноширинный шрифт
: Используется для листингов программ, а также в обычном тексте для обозначения имен переменных, функций, типов, объектов, баз данных, переменных среды, операторов, ключевых слов и других программных конструкций и элементов исходного кода.

Моноширинный полужирный шрифт
: Используется для обозначения команд или фрагментов текста, которые пользователь должен ввести дословно без изменений.

Моноширинный курсив
: Используется для обозначения в исходном коде или в командах шаблонных меток-заполнителей, которые должны быть заменены соответствующими контексту реальными значениями.


Такая пиктограмма обозначает совет или рекомендацию.


Такая пиктограмма обозначает указание или примечание общего характера.


Эта пиктограмма обозначает предупреждение или особое внимание к потенциально опасным объектам.

Отзывы и пожелания

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв прямо на нашем сайте www.dmkpress.com, зайдя на страницу книги, и оставить комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу dmkpress@gmail.com, при этом напишите название книги в теме письма.

Если есть тема, в которой вы квалифицированы, и вы заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу http://dmkpress.com/authors/publish_book/ или напишите в издательство по адресу dmkpress@gmail.com.

Скачивание исходного кода примеров

Скачать файлы с дополнительной информацией для книг издательства «ДМК Пресс» можно на сайте www.dmkpress.com или www.дмк.рф на странице с описанием соответствующей книги.

Список опечаток

Хотя мы приняли все возможные меры для того, чтобы удостовериться в качестве наших текстов, ошибки все равно случаются. Если вы найдете ошибку

в одной из наших книг — возможно, ошибку в тексте или в коде, — мы будем очень благодарны, если вы сообщите нам о ней. Сделав это, вы избавите других читателей от расстройств и поможете нам улучшить последующие версии этой книги.

Если вы найдете какие-либо ошибки в коде, пожалуйста, сообщите о них главному редактору по адресу dmkpress@gmail.com, и мы исправим это в следующих тиражах.

Нарушение авторских прав

Пиратство в Интернете по-прежнему остается насущной проблемой. Издательства «ДМК Пресс» и Packt очень серьезно относятся к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в Интернете с незаконно выполненной копией любой нашей книги, пожалуйста, сообщите нам адрес копии или веб-сайта, чтобы мы могли применить санкции.

Пожалуйста, свяжитесь с нами по адресу электронной почты dmkpress@gmail.com со ссылкой на подозрительные материалы.

Мы высоко ценим любую помощь по защите наших авторов, помогающую нам предоставлять вам качественные материалы.

Адреса биткойн-систем и транзакций в книге

Почти все адреса биткойн-систем, транзакций, ключей, QR-кодов и данных блокчейна, используемых в этой книге, являются реальными. Это означает, что вы можете просматривать структуры данных блокчейна, изучать транзакции, предлагаемые как примеры, использовать их в собственных скриптах и программах и т. д.

Но следует отметить, что секретные ключи, использованные для формирования адресов, либо опубликованы в этой книге, либо уже «засвечены» (таким образом, секретными уже не являются). И если вы отправите деньги на любой из этих адресов, то деньги будут безвозвратно потеряны или в некоторых случаях кто-то, прочитавший данную книгу, сможет присвоить их, воспользовавшись опубликованными здесь секретными ключами.

Не посылайте деньги по какому-либо адресу, приведенному в этой книге. Деньги будут присвоены другим читателем или исчезнут безвозвратно.

Как связаться с автором

С автором книги Андреасом М. Антонопулосом можно связаться через его личный сайт: https://antonopoulos.com/.

Информация о книге «Mastering Bitcoin», а также о платформе Open Edition и переводах книги на другие языки доступна на сайте: https://bitcoinbook.info/.

Автор в соцсети Facebook: https://facebook.com/AndreasMAntonopoulos.

Автор в Twitter: https://twitter.com/aantonop.

Автор в Linkedin: https://linkedin.com/company/aantonop.

Автор благодарит всех, кто поддерживает его работу ежемесячными безвозмездными взносами.

Страница автора на сайте Patreon: https://patreon.com/aantonop.

Благодарности

Эта книга представляет собой результат труда многих людей, внесших свой вклад. Я благодарен за всю помощь, которую я получил от друзей, коллег и даже совершенно незнакомых людей, подключившихся к моей работе над полноценной технической книгой о криптографических валютах и биткойне.

Невозможно отделить технологию биткойна от биткойн-сообщества, поэтому книга о технологии биткойна появилась во многом благодаря биткойн-сообществу, которое вдохновляло, поддерживало и поощряло мою работу от начала до конца. Эта книга, как ничто другое, позволила мне стать частью замечательного сообщества на два года, за что я безмерно ему благодарен. Очень трудно назвать по именам всех людей, с которыми я беседовал на конференциях, мероприятиях, семинарах, неформальных встречах, вечеринках и небольших частных собраниях, а также всех, кто общался со мной через Twitter, Reddit, на форуме bitcointalk.org и на GitHub, в общем, всех, кто так или иначе оказал влияние на эту книгу. Все идеи, аналогии, вопросы, ответы и объяснения, которые вы найдете в этой книге, были в той или иной степени предложены, проверены или улучшены с помощью сообщества. Спасибо всем за поддержку, без вас эта книга не появилась бы на свет. Я бесконечно благодарен вам.

Разумеется, путь к написанию книг начался гораздо раньше. Моим первым языком (в школе) был греческий, поэтому пришлось пройти коррективный курс английского письменного на первом курсе университета. Я выражаю благодарность Диане Кордас (Diana Kordas), моему преподавателю английского письменного, которая помогла мне обрести уверенность и прочные навыки в течение того года. Позже, уже как профессионал, я развил свои навыки технического писателя, публикуя статьи о центрах данных в журнале Network World. Благодарю Джона Дикса (John Dix) и Джона Галланта (Jon Gallant), предоставивших мне первую рабочую должность обозревателя-колумниста в Network World, редактора Майкла Куни (Michael Cooney) и коллегу Джона Тилл Джонсон (Johna Till Johnson), которые редактировали мои обзоры и готовили их к публикации. 500 слов в неделю в течение четырех лет дали мне достаточный опыт, и я окончательно решил заняться написанием книг.

Спасибо также тем, кто поддержал меня, когда я предложил свою книгу издательству O'Reilly. Отдельная благодарность Джону Галланту (John Gallant), Грегори Нессу (Gregory Ness), Ричарду Стиннену (Richard Stiennon), Джоелю Снайдеру (Joel Snyder), Эдаму Б. Ливайну (Adam B. Levine), Сандре Гиттлин (Sandra Gittlen), Джону Диксу (John Dix), Джоне Тилл Джонсон (Johna Till Johnson), Роджеру Веру (Roger Ver) и Йону Матонису (Jon Matonis). Особая благодарность Ричарду Кэгэну (Richard Kagan) и Таймону Маттошко (Tymon Mattoszko) за обзоры и рецензии ранних версий книги и Мэтью Тэйлору (Matthew Taylor) за редактуру и корректуру.

Спасибо Крикет Лью (Cricket Liu), автору книги DNS и BIND, который представил меня издательству O'Reilly. Также благодарю Майкла Лукидеса (Michael Loukides) и Элисон Макдоналд (Allyson MacDonald) из O'Reilly, которые в течение нескольких месяцев помогали моей книге появиться на свет. Элисон проявила особое терпение и такт, когда сроки выпуска книги оказывались под угрозой и повседневная жизнь с ее проблемами вмешивалась в издательские планы. За работу над вторым изданием благодарю Тимоти МакГоверна (Timothy McGovern) за общее руководство процессом, Ким Кофер (Kim Cofer) за внимательное и тщательное редактирование, а также Ребекку Панцер (Rebecca Panzer) за создание иллюстраций для множества новых схем.

Черновые наброски нескольких первых глав были самыми трудными, потому что биткойн – трудная тема сама по себе. Когда я начинал описывать один аспект технологии биткойна, неизбежно приходилось распутывать целый клубок взаимосвязанных аспектов. Приходилось многократно останавливать работу в слегка подавленном настроении, когда я безуспешно пытался упростить для понимания и доступно изложить такую обширную техническую тему. В конце концов, я решил рассказать историю биткойна с помощью рассказов людей, использующих технологию биткойна, и работать над книгой стало заметно легче. Я благодарю своего друга и наставника Ричарда Кэгэна (Richard Kagan), который помог распутать этот клубок проблем и преодолеть сложные моменты застоя. Спасибо Памеле Морган (Pamela Morgan), которая проверяла первые черновики каждой главы как в первом, так и во втором издании и задавала сложные вопросы, чтобы книга стала лучше. Также благодарю разработчиков из группы San Francisco Bitcoin Developers Meetup, Таарика Льюиса (Taariq Lewis) и Дениз Терри (Denise Terry) за помощь в проверке первого чернового материала. Спасибо Эндрю Ноглеру (Andrew Naugler) за дизайн инфографики.

Во время написания книги я открыл доступ к первым черновикам на сервисе GitHub и предложил всем желающим их прокомментировать. В ответ было получено более ста замечаний, предложений, исправлений и дополнений. Благодарю всех откликнувшихся на мое предложение, а их полный список можно посмотреть ниже, в разделе «Первый черновик (вклад сообщества на GitHub)». Особая благодарность – добровольным редакторам на GitHub Мин Т. Нгуену (Minh T. Nguyen) (1-е издание) и Уиллу Биннсу (Will Binns) (2-е издание), которые без устали регулировали, управляли и обрабатывали предложения, сообщения об ошибках и неточностях, а также исправляли ошибки непосредственно на GitHub.

После создания чернового варианта книги она прошла через несколько этапов технического редактирования и рецензирования. Спасибо Крикет Лью (Cricket Liu) и Лорне Ланц (Lorne Lantz) за тщательное рецензирование, комментарии и поддержку.

Несколько разработчиков, использующих технологию биткойна, прислало примеры кода, отзывы, комментарии и всячески поддерживало мою работу. Спасибо Амиру Тааки (Amir Taaki) и Эрику Воскуилу (Eric Voskuil) за предо-

ставленные фрагменты кода для примеров и множество полезных замечаний, Крису Клеешульте (Chris Kleeschulte) за материал, включенный в приложение по Bitcore, Виталику Бутерину (Vitalik Buterin) и Ричарду Киссу (Richard Kiss) за помощь с математикой эллиптических кривых и предоставление фрагментов кода, Гэвину Андресену (Gavin Andresen) за исправления, комментарии и поддержку, Михалису Каргакису (Michalis Kargakis) за комментарии, предложения и описание btcd, Робину Инге (Robin Inge) за поиск опечаток и ошибок, что несомненно улучшило печатное издание. При работе над вторым изданием я снова получил огромную помощь от многих разработчиков Bitcoin Core, в том числе от Эрика Ломброзо (Eric Lombrozo), открывшего тайны Segregated Witness, от Люка-младшего (Luke-Jr), который помог улучшить главу о транзакциях, от Джонсона Лау (Johnson Lau), рецензировавшего Segregated Witness и другие главы, и от многих других. Благодарю Джозефа Пуна (Joseph Poon), Тадже Драйа (Tadge Dryja) и Олаолува Осантокана (Olaoluwa Osuntokun), которые предоставили описание сети Lightning Network, рецензировали мои материалы, отвечали на вопросы, которые вызывали у меня затруднения.

Своей любовью к печатному слову и к книгам я обязан моей матери Терезе, вырастившей меня в доме, в котором книжные полки и шкафы стояли буквально у каждой стены. Моя мама купила мне самый первый компьютер в 1982 году, хотя сама считала себя технофобом. Мой отец, Менелаос, инженер-строитель, который недавно опубликовал свою первую книгу в возрасте 80 лет, научил меня логическому и аналитическому мышлению и любви к науке и технике.

Спасибо всем за поддержку на протяжении всего этого пути.

Первый черновик (вклад сообщества на GitHub)

Многие люди внесли свой вклад, предлагая комментарии, исправления и дополнения в самую первую черновую версию книги на GitHub. Благодарю всех за участие в создании этой книги.

Ниже приведен список самых активных участников процесса подготовки первой версии книги на GitHub с указанием в скобках идентификаторов их учетных записей:

- Алекс Уотерс (Alex Waters, alexwaters);
- Эндрю Доналд Кеннеди (Andrew Donald Kennedy, grkvlt);
- bitcoinctf;
- Брайан Гмырек (Bryan Gmyrek, physicsdude);
- Кейси Флинн (Casey Flynn, cflynn07);
- Чэпмэн Шуп (Chapman Shoop, belovachap);
- Кристи Д'Анна (Christie D'Anna, avocadobreath);
- Коди Скотт (Cody Scott, Siecje);
- coinradar;
- Крэджин Годли (Cragin Godley, cgodley);
- dallyshalla;

- Диего Виола (Diego Viola, diegoviola);
- Дирк Якель (Dirk Jäckel, biafra23);
- Димитрис Цапакидис (Dimitris Tsapakidis, dimitris-t);
- Дмитрий Маракасов (Dmitry Marakasov, AMDmi3);
- drstrangeM;
- Эд Айкхолт (Ed Eykholt, edeykholt);
- Эд Лиф (Ed Leafe, EdLeafe);
- Эдвард Поснак (Edward Posnak, edposnak);
- Элиас Родригес (Elias Rodrigues, elias19r);
- Эрик Воскуил (Eric Voskuil, evoskuil);
- Эрик Уинчелл (Eric Winchell, winchell);
- Эрик Вальстрём (Erik Wahlström, erikwam);
- effectsToCause (vericoin);
- Эстебан Ордано (Esteban Ordano, eordano);
- ethers;
- fabienhinault;
- Франк Хёгер (Frank Höger, francyi);
- Гаурав Рана (Gaurav Rana, bitcoinsSG);
- genjix;
- halseth;
- Хольгер Шинцель (Holger Schinzel, schinzelh);
- Иоаннис Керувим (Ioannis Cherouvim, cherouvim);
- Айш От, младший (Ish Ot Jr., ishotjr);
- Джеймс Эддисон (James Addison, jayaddison);
- Джеймсон Лопп (Jameson Lopp, jlopp);
- Джейсон Бистерфельдт (Jason Bisterfeldt, jbisterfeldt);
- Хавьер Рохас (Javier Rojas, fjrojasgarcia);
- Джереми Бокобца (Jeremy Bokobza, bokobza);
- JerJohn15;
- Джо Бауэрс (Joe Bauers, joebauers);
- joflynn;
- Джонсон Лау (Johnson Lau, jl2012);
- Джонатан Кросс (Jonathan Cross, jonathancross);
- Jorgeminator;
- Кай Баккер (Kai Bakker, kaibakker);
- Май-Суан Чиа (Mai-Hsuan Chia, mhchia);
- Marzig (marzig76);
- Максимилиан Райхель (Maximilian Reichel, phramz);
- Михалис Каргакис (Michalis Kargakis, kargakis);
- Микаэль С. Ипполито (Michael C. Ippolito, michaelcippolito);
- Михаил Руссу (Mihail Russu, MihailRussu);
- Мин Т. Нгуен (Minh T. Nguyen, enderminh);
- Нагарай Хубли (Nagaraj Hubli, nagarajhubli);

- Nekomata (nekomata-3);
- Роберт Ферс (Robert Furse, Rfurse);
- Ричард Кисс (Richard Kiss, richardkiss);
- Рубен Александер (Ruben Alexander, hizzvizz);
- Сэм Ричи (Sam Ritchie, sritchie);
- Сергей Котляр (Sergej Kotliar, ziggamon);
- Сейичи Учида (Seiichi Uchida, topecongiro);
- Симон де ла Рувьер (Simon de la Rouviere, simondlr);
- Стефан Усте (Stephan Oeste, Emzy);
- takaya-imai;
- Тьяго Аррaис (Thiago Arrais, thiagoarrais);
- venzen;
- Уилл Биннс (Will Binns, wbnns);
- wintercooled;
- wjx;
- Войцех Лангиевич (Wojciech Langiewicz, wlk);
- yurigeorgiev4.

Глава 1

Введение

Что такое биткойн

Биткойн (bitcoin) – это набор концепций и технологий, которые формируют основу цифровой денежной экосистемы. Денежные единицы, называемые биткойнами, используются для хранения и передачи ценности в денежном выражении между членами биткойн-сети. Пользователи биткойн-системы обмениваются информацией друг с другом, используя для этого протокол биткойна, работающий в основном через Интернет, хотя могут применяться и любые другие транспортные сетевые протоколы. Стек протоколов биткойна, доступный в виде ПО с открытыми исходными кодами, может быть реализован на многочисленных типах устройств, в том числе на ноутбуках и смартфонах, что существенно увеличивает массовую доступность этой технологии.

Пользователи могут передавать биткойны по сети, чтобы выполнять с ними практически те же операции, что с традиционными денежными средствами, в том числе покупать и продавать товары, пересылать деньги людям и организациям или предоставлять кредит. Биткойны можно покупать, продавать и обменивать на другие валюты на специализированных валютных биржах. В некотором смысле биткойн является идеальной формой денег для Интернета благодаря скорости операций с ним, защищенности и безграничности области его применения.

В отличие от обычных денежных единиц, биткойн абсолютно виртуален. Не существует ни физических денежных знаков, ни даже цифровых денежных знаков для биткойна. Воображаемые денежные единицы участвуют в транзакциях, которые передают какие-либо ценности (в стоимостном выражении) от отправителя к получателю. Пользователи биткойна владеют ключами, которые позволяют им подтверждать обладание биткойнами в биткойн-сети. С помощью этих ключей пользователи могут подписывать (заверять) транзакции для получения доступа к своей валюте и ее расходования посредством передачи новому владельцу. Ключи часто хранятся в цифровом кошельке на компьютере или смартфоне каждого пользователя. Обладание ключом, с помощью которого можно заверить транзакцию, является единственным предваритель-

ным условием для операций с биткойнами, при этом управление полностью передается каждому пользователю.

Биткойн представляет собой распределенную пиринговую (peer-to-peer) (или одноранговую) систему. Это означает, что в ней нет «центрального» сервера или какого-либо пункта управления. Биткойны создаются с помощью процесса, называемого майнингом (mining), который подразумевает конкуренцию в поиске решений для математической задачи при обработке транзакций биткойнов. Любой член биткойн-сети (то есть любой, использующий устройство, на котором работает полный стек протоколов биткойна) может выступить в роли майнера (miner), используя вычислительные мощности своего компьютера для проверки и фиксации транзакций. В среднем через каждые 10 минут кто-то побеждает в состязании за право подтверждения корректности транзакций, выполненных за эти прошедшие 10 минут, и вознаграждается за это новым биткойном. По существу, майнинг биткойнов способствует децентрализации функций клиринга и выпуска денежных знаков центральным банком и фактически исключает необходимость в каком-либо центральном банке.

Протокол биткойна включает встроенные алгоритмы, которые управляют функцией майнинга в сетевой среде. Сложность вычислительной задачи, которую обязательно должны выполнить майнеры, регулируется динамически, поэтому в среднем через каждые 10 минут кто-то достигает успеха вне зависимости от количества майнеров (и от количества обрабатываемых задач), конкурирующих в текущий момент. Кроме того, протокол предусматривает уменьшение наполовину скорости создания новых биткойнов через каждые 4 года и ограничивает общее количество созданных биткойнов фиксированной величиной, которая не должна превышать сумму в 21 миллион единиц. Таким образом, количество биткойнов, находящихся в обращении, весьма точно описывается легко прогнозируемой кривой, которая достигнет значения 21 миллион к 2140 году. Благодаря такому уменьшению скорости «эмиссии» в течение длительного интервала времени биткойн представляет собой дефляционную валюту. Более того, биткойн не подвержен инфляции в форме «печатания» новых денежных купюр сверх предполагаемой эмиссионной нормы.

Если заглянуть поглубже, то биткойн также можно определить как название протокола, пиринговой сети и новой технологии распределенной обработки данных. Биткойн как денежная единица действительно представляет собой самое первое практическое приложение этой новой технологии. Биткойн является суммарным результатом многолетних исследований в области криптографии и распределенных систем и включает четыре главные инновации, объединенные в единственную в своем роде мощную комбинацию. Основными компонентами технологии биткойна являются:

- децентрализованная пиринговая сеть (протокол биткойна);
- общедоступный реестр транзакций (блокчейн (blockchain));
- набор правил для независимой проверки (валидации) транзакций и эмиссии (выпуска) денежных единиц (правила консенсуса);

- механизм для достижения глобального децентрализованного (распределенного) консенсуса при проверке корректности (валидации) блокчейна (алгоритм доказательства выполнения работы, Proof-of-Work algorithm).

Как разработчик я считаю биткойн системой, очень похожей на «Интернет денег» (Internet of money), то есть на сеть для распространения ценностей и для защиты права владения цифровыми активами, функционирующую на основе распределенных вычислений. При этом роль биткойна гораздо более значимая, чем кажется на первый взгляд.

В этой главе мы начнем изучение некоторых основных концепций и определений, познакомимся с необходимым программным обеспечением (ПО) и попробуем использовать биткойн для простых транзакций. В следующих главах будут рассматриваться более глубокие уровни технологии, которая сделала возможным появление биткойна, а также внутренние функциональные возможности и особенности сети и протокола биткойна.

Цифровые деньги до биткойна

Появление жизнеспособных цифровых денег тесно связано с разработками в области криптографии. Поэтому вполне естественно считать основополагающей главной задачей использование битов для представления стоимостной ценности, которую можно обменивать на товары и услуги. Все желающие пользоваться цифровыми деньгами должны ответить на три ключевых вопроса:

1. Могу ли я быть уверенным в том, что цифровые деньги достоверны (и законны) и не являются поддельными (фальшивыми)?
2. Могу ли я быть уверенным в том, что цифровые деньги можно потратить только один раз (эта проблема известна под названием «двойное расходование» (double spending))?
3. Могу ли я быть уверенным в том, что никто другой не сможет заявить, что эти деньги принадлежат ему, а не мне?

Организации, ведающие выпуском бумажных денег, ведут непрерывную борьбу с проблемой подделки купюр, используя для этого всё более сложные степени защиты бумаги и технологии печати. Бумажные деньги решают проблему двойного расходования очень просто, потому что один и тот же лист бумаги не может находиться в двух местах одновременно. Разумеется, и привычные всем нам деньги часто можно хранить и передавать в цифровой форме. В этих случаях проблемы подделки и двойного расходования устраняются с помощью процедуры клиринга (безналичных взаимных расчетов) всех электронных транзакций в централизованной системе компетентных органов, осуществляющих общий мониторинг всех денежных средств, находящихся в обращении. Для цифровых денег, которые не могут воспользоваться преимуществами невидимой типографской краски или голографических полосок, криптография предлагает основное средство для создания уверенности в законности объявляемой пользователем ценности. Точнее говоря, криптографические цифровые подписи позволяют пользователю заверить (собственной подписью) цифровые активы или транзакцию, подтверждающую

право владения этим активом. При использовании соответствующей архитектуры цифровые подписи также могут применяться для устранения проблемы двойного расходования.

С началом более широкой доступности и более глубокого понимания методов криптографии в конце 1980-х гг. многие исследователи попытались использовать криптографию для создания цифровых валют. Самые первые проекты в этой области генерировали цифровые деньги, обычно обеспечиваемые национальной валютой или драгоценными металлами, например золотом.

Несмотря на то что эти первые цифровые деньги действительно функционировали, они оставались в рамках централизованных систем, поэтому представляли собой легкую мишень для нападений государственных органов и хакеров. Первые цифровые деньги использовали централизованную расчетную палату для регулирования выполнения всех транзакций с регулярными интервалами точно так же, как в обычной банковской системе. К сожалению, в большинстве случаев эти находящиеся в ранней стадии становления цифровые деньги привлекали особое внимание встревоженных правительственных органов и в конечном итоге уничтожались в судебном порядке. Иногда крах цифровых валют становился заметным явлением, когда поддерживающие их компании внезапно ликвидировались. Чтобы стать устойчивыми к воздействиям противников, будь то официальные правительственные органы или криминальные элементы, децентрализованные цифровые деньги должны были непременно избавиться от единственной уязвимой для атак точки. Биткойн является именно такой системой, децентрализованной по своей сущности изначально и свободной от каких-либо центральных органов авторизации или пунктов управления, которые можно атаковать и вывести из строя.

История создания биткойна

Биткойн был создан в 2008 году, о чем сообщала статья «Bitcoin: A Peer-to-Peer Electronic Cash System»[1], опубликованная под псевдонимом Сатоши Накамото (Satoshi Nakamoto) (см. приложение А). Накамото объединил несколько более ранних инноваций, таких как b-money и HashCash, для создания полностью децентрализованной электронной системы денежных расчётов, в основе которой не имелось какого бы то ни было центрального органа авторизации для эмиссии денежных единиц или для регулирования и проверки корректности транзакций. Главным нововведением стало использование распределенной системы вычислений (названной алгоритмом доказательства выполнения работы, Proof-of-Work algorithm) для проведения всеобщих «выборов» через каждые 10 минут, что позволяло в децентрализованной сети достигать консенсуса (consensus) по текущему состоянию транзакций. Такой подход изящно решил

[1] «Bitcoin: A Peer-to-Peer Electronic Cash System», Satoshi Nakamoto (https://bitcoin.org/bitcoin.pdf).

проблему двойного расходования, при возникновении которой одна денежная единица может быть потрачена дважды. До этого проблема двойного расходования была явным недостатком цифровых денег и решалась операциями клиринга всех транзакций через центральную расчётную палату.

Биткойн-сеть начала свою работу в 2009 году на основе реализации, описанной в статье Накамото и с тех пор многократно улучшенной многими другими программистами. Реализация алгоритма доказательства выполнения работы (майнинга), обеспечивающего защиту и жизнеспособность биткойна, постоянно наращивала свою мощь и в настоящее время превосходит суммарную вычислительную мощность самых лучших суперкомпьютеров мира. Общая рыночная стоимость биткойна временами превышает сумму в 20 миллиардов долларов США в зависимости от текущего курса обмена биткойна на доллар. До сего момента самой крупной транзакцией, проведенной в биткойн-сети, была сумма в 150 миллионов долларов США, переведенная мгновенно и обработанная без каких-либо отчислений.

Сатоши Накамото отстранился от активной деятельности в апреле 2011 года и передал ответственность за разработку программного кода и развитие сети преуспевающей группе добровольцев. Настоящее имя человека или группы людей, придумавших биткойн, остается неизвестным. В любом случае, ни Сатоши Накамото, ни кто-либо другой не пытался лично управлять всей биткойн-системой в целом. Функциональность биткойн-системы основана на совершенно ясных математических принципах, на открытых исходных кодах и на консенсусе (согласовании) между членами системы. Само по себе это изобретение стало прорывом и уже породило новую область науки на стыке таких дисциплин, как распределенная обработка данных, экономика и эконометрика (математическая экономика).

Решение проблемы распределенной обработки данных

Изобретение Сатоши Накамото, кроме всего прочего, представляет собой практическое и совершенно новое решение одной из задач распределенной обработки данных, известной под названием «Задача византийских генералов». Краткое объяснение задачи: попытаться согласовать образ действий или состояние системы посредством обмена информацией в ненадежной и потенциально опасной сетевой среде. Решение Сатоши Накамото, использующее концепцию доказательства выполнения работы для достижения консенсуса без центрального органа управления, заслуживающего доверия, является настоящим прорывом в области распределенной обработки данных, а область применения этого решения не ограничивается финансовой сферой. Эту технологию можно применять для достижения консенсуса в децентрализованных сетях для доказательства честности и корректности процедур голосования при выборах, результатов тиражей лотерей, реестров имущества (активов, фондов и т. п.), цифровых нотариальных свидетельств и многого другого.

Варианты использования биткойнов, пользователи и их истории

Биткойн – это инновация в древней технологии денежного оборота. По своей сути деньги просто обеспечивают обмен разнообразными ценностями между людьми. Поэтому, чтобы полностью понять биткойн и его практическое применение, мы начнем знакомство с этой технологией с точки зрения людей, использующих ее. Каждый из упомянутых ниже людей и соответствующих рассказов о них показывает один или несколько конкретных вариантов использования. Мы будем возвращаться к ним на протяжении всей книги:

Розничная торговля дешевыми товарами в Северной Америке
: Алиса (Alice) живет в области залива в Северной Калифорнии. Она услышала о биткойне от своих друзей-технарей и хочет использовать его. Мы будем следить за тем, как Алиса изучает биткойн, зарабатывает несколько биткойнов, затем тратит несколько биткойнов на чашку кофе в кафе Боба в Пало Алто. Эта история познакомит нас с программным обеспечением, с процедурами обмена и с основными простыми транзакциями с точки зрения потребителя розничных товаров.

Розничная торговля дорогостоящими товарами в Северной Америке
: Кэрол (Carol) – владелица художественной галереи в Сан-Франциско. Она продает дорогостоящие картины за биткойны. В этой истории будет описана опасность атак типа 51 процент при достижении консенсуса для розничных продавцов дорогостоящих товаров.

Услуги по офшорному контракту
: Боб (Bob), владелец кафе в Пало Алто, создает новый веб-сайт. Он заключил контракт с веб-разработчиком Гопешем (Gopesh), который живет в Бангалоре (Индия). Гопеш согласен получить оплату в биткойнах. Эта история демонстрирует возможности биткойна в области аутсорсинга, при получении услуг по контракту и при выполнении международных денежных переводов.

Веб-магазин
: Габриэль (Gabriel) – предприимчивый юноша из Рио-де-Жанейро, организовал небольшой веб-магазин, в котором продаются футболки, кофейные кружки и наклейки с логотипом биткойна. Габриэль слишком молод, чтобы открыть личный счет в банке, но родители всячески поощряют его тягу к предпринимательству.

Благотворительная деятельность, пожертвования
: Эухения (Eugenia) – директор детского благотворительного учреждения на Филиппинах. Недавно она узнала при биткойн и хочет воспользоваться им для охвата новой крупной группы зарубежных и местных жертвователей,

чтобы организовать сбор средств для своей благотворительной деятельности. Кроме того, она изучает способы применения биткойна для быстрой передачи денежных средств нуждающимся. Эта история продемонстрирует использование биткойна для организации сбора денежных средств без учета различий валют и государственных границ, а также использование общедоступного реестра для честного ведения дел в благотворительных организациях.

Импорт/экспорт
Мохаммед (Mohammed) – импортер электроники в Дубаи. Он пытается использовать биткойн для покупки электроники в США и Китае для импорта в ОАЭ, чтобы ускорить процедуру оплаты импортируемых товаров. Эта история покажет, как можно использовать биткойн для крупных международных бизнес-платежей, связанных с материальными товарами.

Майнинг биткойнов
Цзин (Jing) – студент, изучающий компьютерную инженерию в Шанхае. Он собрал стойку с блоками майнинга для зарабатывания биткойнов, используя свои инженерные навыки и знания для обеспечения прибыли. В этой истории будет рассматриваться «промышленная» основа биткойна: специализированное оборудование, применяемое для защиты биткойн-сети и для генерации новых денежных единиц.

В каждой из этих историй фигурируют реальные люди, предприятия и организации, использующие в настоящее время биткойн для создания новых рынков, новых отраслей промышленности и современных эффективных решений проблем глобальной экономики.

Начинаем обучение

Биткойн (bitcoin) – это протокол, доступ к которому можно получить с помощью клиентского приложения, говорящего на языке этого протокола. Биткойн-кошелек (bitcoin wallet) представляет собой наиболее часто используемый пользовательский интерфейс к биткойн-системе, точно так же, как веб-браузер является наиболее часто используемым пользовательским интерфейсом к протоколу HTTP. Существует множество реализаций и вариантов биткойн-кошельков, подобно множеству вариантов веб-браузеров (например, Chrome, Safari, Firefox, Internet Explorer, Яндекс-браузер). У каждого есть свой любимый браузер (я за Mozilla Firefox) и свой «отрицательный герой» (я против Internet Explorer), так и биткойн-кошельки различаются по качеству, производительности, защищенности, уровню секретности (приватности) и надежности. Существует также эталонная реализация протокола биткойна, известная как Satoshi Client или Bitcoin Core, производная от исходной реализации, написанной Сатоши Накамото.

Выбор биткойн-кошелька

Биткойн-кошельки являются наиболее активно разрабатываемыми приложениями в экосистеме биткойна. Здесь существует жесткая конкуренция, и, несмотря на то что очередной новый кошелек, возможно, разрабатывается прямо сейчас, несколько кошельков, появившихся в прошлом году, уже не имеет активной поддержки. Многие кошельки предназначены для конкретных платформ или для специальных вариантов использования, некоторые больше подходят для начинающих, тогда как другие предоставляют полный набор функциональных возможностей для более опытных пользователей. Выбор кошелька абсолютно индивидуален и зависит от способа использования и практического опыта пользователя. Таким образом, невозможно порекомендовать конкретное название или конкретный проект кошелька. Тем не менее можно провести классификацию биткойн-кошельков в соответствии с поддерживаемыми платформами и функциональными возможностями и внести определенную ясность в информацию о различных типах существующих кошельков. Хорошо, что перемещение денег между кошельками производится просто, дешево и быстро, поэтому лучше всего попробовать несколько разных кошельков, чтобы выбрать тот, который больше всего соответствует вашим требованиям.

По поддерживаемым платформам можно классифицировать биткойн-кошельки следующим образом:

- *кошелек для десктопа (desktop wallet)* – первый тип биткойн-кошелька, созданный как эталонная реализация, и многие пользователи работают с кошельками для десктопа (настольного компьютера), выбирая их за функциональные возможности, автономность и полноту управления, которые предлагает этот тип кошельков. Но работа под управлением операционных систем общего назначения, таких как Windows и MacOS, имеет свои недостатки, связанные с недостаточной защищенностью, так что десктоп-платформы зачастую не могут обеспечить надлежащий уровень защиты и соответствующую конфигурацию;
- *мобильный кошелек (mobile wallet)* – наиболее часто используемый тип биткойн-кошелька. Работающие под управлением операционных систем для смартфонов, таких как Apple iOS и Android, эти кошельки чаще всего являются наилучшим выбором для новых пользователей. Многие из них спроектированы таким образом, чтобы обеспечить максимальную простоту использования, но есть и полнофункциональные мобильные кошельки для опытных пользователей;
- *веб-кошелек (web wallet)* – доступен через веб-браузер, а сам пользовательский кошелек хранится на сервере, принадлежащем третьей стороне. Это похоже на организацию веб-почты, полностью основанной на использовании стороннего сервера. Некоторые из этих сервисов используют для работы код на стороне клиента, выполняемый в браузере пользователя, что позволяет сохранить управление ключами биткойна

в руках пользователя. Но большинство сервисов предлагает компромисс, принимая на себя управление ключами биткойна в обмен на простоту использования. И всё же я не рекомендую хранить большой объем биткойнов на сторонних системах;

- *аппаратный кошелек (hardware wallet)* – устройство, обеспечивающее защиту биткойн-кошелька, хранящегося на специализированных аппаратных средствах. Такое устройство может работать вместе с десктопным веб-браузером, обмениваясь данными через порт USB или через ближнюю бесконтактную связь (near-field-communication (NFC)) на мобильном устройстве. Благодаря обработке всех операций с биткойнами на специализированной аппаратуре этот тип кошельков считается очень хорошо защищенным и вполне подходящим для хранения крупных сумм в биткойнах;
- *бумажный кошелек (paper wallet)* – ключи, управляющие биткойном, также могут быть распечатаны для долговременного хранения. Это называют бумажным кошельком, несмотря на то что печать может производиться и на других материалах (дерево, металл и т. д.). Бумажные кошельки предлагают низкотехнологичные, но весьма защищенные средства хранения биткойнов в течение длительного времени. Офлайн-хранилище также часто называют «холодильным хранением» (cold storage).

Другой способ классификации биткойн-кошельков – по степени их независимости (возможности автономного функционирования) и по способу их взаимодействия с биткойн-сетью:

- *полноценный клиент (full client)*, или *«полноценный узел» (full node)*, – это клиент, который хранит полную хронологию транзакций биткойнов (каждую транзакцию, когда-либо выполненную любым пользователем), управляет кошельками пользователей и может непосредственно начать выполнение транзакций в биткойн-сети. Полноценный клиент имеет дело со всеми аспектами протокола и способен независимо проверять корректность всей структуры блокчейна и любой транзакции. Полноценный клиент потребляет довольно-таки существенные ресурсы компьютера (например, более 125 Гб дисковой памяти, 2 Гб оперативной памяти), но при этом обеспечивает полную автономию и независимую верификацию транзакций;
- *упрощенный клиент (lightweight client)* – также известен под названием «клиент с упрощенной проверкой платежей» (simple-payment-verification (SPV) client), соединяется с полноценным узлом биткойн-сети (описанным выше) для доступа к информации о транзакциях биткойнов, но хранит пользовательский кошелек локально и независимо создает, проверяет и пересылает транзакции. Упрощенные клиенты взаимодействуют с биткойн-сетью напрямую, без каких-либо посредников;

- *клиент с прикладным программным интерфейсом (API) стороннего производителя (third-party API client)* – взаимодействует с биткойн-сетью через систему прикладных программных интерфейсов (API) стороннего производителя (третьей стороны) вместо прямого соединения с биткойн-сетью. Кошелек может храниться у самого пользователя или на сторонних серверах, но все транзакции выполняются через посредника (третью сторону).

Многие биткойн-кошельки попадают сразу в несколько групп классификации, поскольку в них объединены различные классификационные характеристики, но наиболее часто встречаются три комбинации: настольный (десктоп) полноценный клиент, мобильный упрощенный кошелек и веб-кошелек с прикладным программным интерфейсом от стороннего производителя. Чаще всего границы между описанными выше категориями слабо различимы, так как многие кошельки работают на нескольких платформах и могут взаимодействовать с сетью разнообразными способами.

В этой книге мы рассмотрим использование разнообразных загружаемых биткойн-клиентов, от эталонной реализации (Bitcoin Core) до мобильных и веб-кошельков. В некоторых примерах потребуется применение эталонной реализации Bitcoin Core, которая, будучи полноценным клиентом, кроме того, предоставляет прикладные программные интерфейсы (API) к кошельку, сети и сервисам выполнения транзакций. Если вы намерены глубже исследовать программные интерфейсы в биткойн-системе, то вам необходима работающая эталонная реализация Bitcoin Core или один из альтернативных клиентов (см. раздел «Альтернативные клиенты, библиотеки и инструментальные пакеты разработчика» в главе 3).

Сразу переходим к делу

Алиса, с которой мы познакомились немного раньше, в разделе «Варианты использования биткойнов, пользователи и их истории», – пользователь с минимумом технических знаний. Она совсем недавно узнала о биткойне от своего друга Джо (Joe). Как-то на вечеринке Джо в очередной раз с энтузиазмом рассказывал о биткойне всем присутствующим и даже предлагал продемонстрировать работу с ним. Заинтригованная его рассказом, Алиса спросила, с чего начать использование биткойна. Джо ответил, что для новичков лучшим выбором будет мобильный кошелек, и порекомендовал несколько предпочтительных, с его точки зрения, вариантов. Алиса загрузила программу Mycelium для платформы Android и установила ее на своем мобильнике.

Когда Алиса впервые запускает Mycelium, то, как и большинство биткойн-кошельков, это приложение автоматически создает новый кошелек для нового пользователя. Алиса видит на экране этот кошелек, выглядящий так, как показано на рис. 1.1 (примечание: не посылайте биткойны на адрес из этого примера, вы потеряете их навсегда).

Рис. 1.1 ❖ Мобильный кошелек Mycelium

Самая важная часть изображения на показанном экране – биткойн-адрес (bitcoin address) Алисы, который выглядит как длинная строка букв и цифр: `1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK`. Справа от биткойн-адреса кошелька расположен QR-код, особая форма штрихового кода, содержащая ту же информацию в формате, который может быть отсканирован видеокамерой смартфона. QR-код представляет собой квадрат с рисунком, составленным из черных и белых точек. Алиса может скопировать биткойн-адрес или QR-код в буфер обмена простым касанием (tapping) изображения QR-кода или кнопки **Receive** (Принять). В большинстве кошельков касание QR-кода также увеличивает его изображение, чтобы упростить его сканирование камерой смартфона.

Биткойн-адреса начинаются с цифр 1 или 3. Как и адреса электронной почты, биткойн-адреса можно сообщать другим пользователям биткойн-системы, которые воспользуются ими для пересылки биткойнов непосредственно в ваш кошелек. С точки зрения безопасности распространение своего биткойн-адреса не связано с каким-либо риском. Биткойн-адрес можно публиковать везде без угрозы для своей учетной записи. В отличие от адресов электронной почты, новые биткойн-адреса можно создавать без ограничений, и все они будут направлять денежные средства в ваш кошелек. В действительности многие новейшие версии кошельков автоматически создают новый адрес для каждой очередной транзакции в целях обеспечения максимальной секретности. Кошелек – это просто набор адресов и ключей, открывающих доступ к хранящимся в нем денежным средствам.

Теперь Алиса готова к получению цифровых денег. Прикладная программа кошелька случайным образом сгенерировала секретный ключ (private key) (более подробно секретный ключ будет описан в разделе «Секретные ключи» главы 4) вместе с соответствующим ему биткойн-адресом. В этот момент ее биткойн-адрес неизвестен в биткойн-сети и не «зарегистрирован» в какой-либо части биткойн-системы. Этот биткойн-адрес – пока просто число, соответствующее ключу, который Алиса может использовать для управления доступом к своим денежным средствам. Биткойн-адрес сгенерирован кошельком автономно без обращения или регистрации на каком-либо сервисе. В действительности большинство кошельков не устанавливает никакой связи между биткойн-адресом и какой-либо внешней идентифицируемой информацией, включая данные, подтверждающие личность пользователя. До того момента, когда этот адрес определяется как получатель денежных единиц в результате транзакций, зафиксированных в реестре биткойна, он является просто частью огромного набора возможных адресов, допустимых в биткойн-системе. Только после связывания такого адреса с некоторой транзакцией он становится частью списка известных адресов в биткойн-сети.

Итак, Алиса готова начать практическое использование своего нового биткойн-кошелька.

Получаем свой первый биткойн

Первой и зачастую самой сложной задачей для новых пользователей является получение хотя бы нескольких биткойнов. В отличие от иностранных валют, невозможно купить биткойны в банке или в пункте обмена валют.

Биткойн-транзакции необратимы. Трансферы в большинстве электронных платежных сетевых систем, таких как кредитные карты, дебетовые карты, PayPal и банковские счета, являются обратимыми. Для любого продавца биткойнов это различие создает вполне реальную опасность, состоящую в том, что покупатель может отозвать свой электронный платеж после того, как получит биткойны, то есть, в сущности, обманет продавца. Чтобы как-то уменьшить риск, компании, принимающие обычные электронные платежи в обмен на биткойны, обычно требуют от покупателей пройти процедуры проверки подлинности личности и подтверждения платежеспособности, которые могут продолжаться от нескольких дней до нескольких недель. Это означает, что как новый пользователь вы не имеете возможности мгновенно купить биткойны с помощью кредитной карты. Но немного терпения и творческого мышления – и такой способ вам не понадобится.

Ниже описаны некоторые методы получения биткойнов новыми пользователями:

- найдите друга (знакомого), у которого есть биткойны, и купите у него несколько единиц. Многие пользователи биткойн-систем начинали именно таким способом, потому что он наименее сложный. Найти лю-

дей с биткойнами можно на неформальной встрече местной группы биткойн-пользователей, о которых сообщается на сайте Meetup.com;
- воспользуйтесь надежным сервисом, например localbitcoins.com, чтобы найти продавца в вашем регионе и купить биткойны за наличные с оплатой при личной встрече;
- заработайте биткойны, продавая продукцию или услуги. Если вы программист, продавайте свои навыки и умения. Если вы парикмахер, стригите людей за биткойны;
- воспользуйтесь биткойн-банкоматом в вашем городе. Биткойн-банкомат – это устройство, которое принимает наличные деньги и пересылает биткойны в ваш биткойн-кошелек на смартфоне. Найти ближайший биткойн-банкомат можно с помощью онлайновой карты на сайте Coin ATM Radar (http://coinatmradar.com);
- воспользуйтесь обменным пунктом биткойнов, связанным с вашим банковским счетом. Сейчас во многих странах существуют обменные пункты, поддерживающие рынок покупателей и продавцов, обменивающих биткойны на местную валюту. В списках обменных курсов, например BitcoinAverage (https://bitcoinaverage.com), часто указываются обменные пункты, обменивающие биткойны на конкретную валюту.

Одним из преимуществ биткойна перед другими платежными системами, если использовать его правильно, является то, что биткойн обеспечивает гораздо бóльшую секретность для пользователей. Приобретение, хранение и расходование биткойнов не требуют разглашения личной информации и своих идентификационных данных или передачи таких данных кому бы то ни было. Но там, где биткойн имеет дело с обычными системами, например с валютными биржами или обменными пунктами, часто применяются государственные или международные законодательные нормы. Для обмена биткойнов на денежные единицы вашей страны от вас наверняка потребуют подтвердить свою личность и доказать подлинность банковской информации. Пользователи должны знать о том, что после одной операции с биткойнами, при которой была идентифицирована их личность, все последующие транзакции биткойнов будут так же легко идентифицироваться и прослеживаться. Это одна из причин, по которой многие пользователи предпочитают иметь учетные записи, предназначенные специально для обменных операций и не связанные напрямую с их кошельками.

Алисе рассказал о биткойнах ее друг, поэтому у нее есть возможность без затруднений приобрести свой первый биткойн. Далее мы увидим, как она покупает биткойн у своего друга Джо и как Джо пересылает этот биткойн в кошелек Алисы.

Поиск информации о текущей стоимости биткойна

Прежде чем Алиса сможет купить биткойн у Джо, они должны договориться об обменном курсе (exchange rate) между биткойном и долларами США. При этом у всех новичков возникает вполне естественный вопрос: «Кто устанавливает цену биткойна?» Короткий ответ: цена устанавливается рынком.

Биткойн, как и большинство других валют, имеет плавающий обменный курс (floating exchange rate). Это означает, что цена биткойна по отношению к любой другой валюте постоянно изменяется в зависимости от спроса и предложения на различных рынках, где имеет хождение биткойн. Например, «цена» биткойна в долларах США вычисляется отдельно на каждом рынке на основе самых последних операций по обмену биткойнов на доллары США. Таким образом, цена может изменяться несколько раз в секунду, и эти изменения следуют непрерывно. Информационные валютные сервисы объединяют данные о ценах с нескольких рынков и вычисляют средневзвешенное (с учетом объемов операций) значение, представляющее общерыночный обменный курс для конкретной пары валют (например, BTC/USD).

Существуют сотни приложений и веб-сайтов, на которых можно узнать текущий рыночный обменный курс. Ниже перечислены наиболее известные и посещаемые веб-сайты:

- Bitcoin Average (http://bitcoinaverage.com) – сайт предлагает легкочитаемый простой обзор средневзвешенных обменных курсов для каждой валюты;
- CoinCap (http://coincap.io) – сервис предоставляет списки рыночных оценок (капитализации) и обменные курсы для сотен криптовалют, включая и биткойн;
- Chicago Mercantile Exchange Bitcoin Reference Rate (http://www.cmegroup.com/trading/cf-bitcoin-reference-rate.html) – ставка-ориентир (reference rate), которая может использоваться для институциональной и договорной ставки, являющейся частью данных об инвестиционных выплатах CME.

Помимо разнообразных сайтов и приложений, большинство биткойн-кошельков автоматически вычисляет соотношение между биткойном и другими валютами. Джо воспользуется своим кошельком для автоматического преобразования цены перед отправкой биткойна Алисе.

Отправка и получение биткойна

Алиса решила поменять 10 долларов США на биткойн, чтобы не слишком рисковать своими деньгами при использовании этой новой для нее технологии. Она отдала Джо 10 долларов наличными, открыла свой кошелек (приложение Mycelium) и нажала кнопку **Receive** (Принять). После этого появился QR-код, представляющий первый биткойн-адрес Алисы.

Далее Джо нажал кнопку **Send** (Отправить) в своем кошельке на смартфоне, после чего появился экран с двумя полями ввода:

- биткойн-адрес получателя;
- отправляемая сумма в биткойнах (BTC) или в местной валюте (USD).

В поле ввода для биткойн-адреса есть маленькая пиктограмма, выглядящая как QR-код. Это позволяет Джо сканировать штриховой код с помощью видеокамеры смартфона, чтобы не вводить вручную достаточно длинный и слож-

ный биткойн-адрес Алисы. Касанием значка QR-кода Джо активизирует камеру смартфона и сканирует QR-код с экрана смартфона Алисы.

Теперь у Джо есть биткойн-адрес Алисы, определенный как получатель. Джо вводит сумму 10 долларов США, и кошелек выполняет автоматическое преобразование с учетом самого свежего обменного курса, полученного с онлайн-сервиса. На тот момент обменный курс составляет 100 долларов США за биткойн, так что 10 долларов равны 0.10 биткойна (BTC), или 100 миллибиткойнам (mBTC), как показано на снимке с экрана мобильного кошелька Джо (см. рис. 1.2).

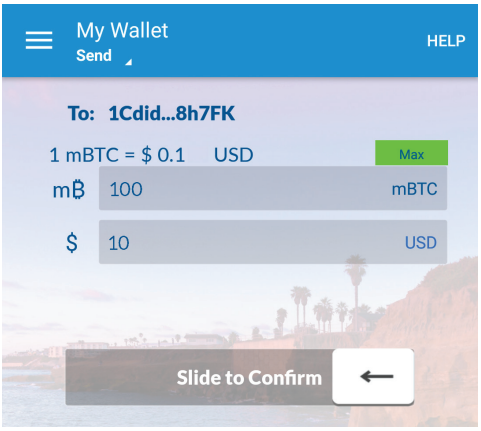

Рис. 1.2 ❖ Экран отправки денег мобильного биткойн-кошелька Airbitz

Затем Джо внимательно проверяет, правильно ли он ввел передаваемую сумму, поскольку после передачи денег ошибку исправить будет уже невозможно. После тщательнейшей проверки адреса и суммы Джо нажимает кнопку **Send** (Отправить), чтобы начать транзакцию. Мобильный биткойн-кошелек Джо создает транзакцию, которая передает 0.10 BTC на адрес, указанный Алисой, изымая денежные средства из кошелька Джо и подписывая текущую транзакцию с помощью секретных ключей Джо. Биткойн-сеть оповещается о том, что Джо выполнил авторизацию процедуры передачи определенной денежной суммы на новый адрес Алисы. Так как транзакция передается по пиринговому (peer-to-peer) протоколу, она быстро распространяется по биткойн-сети. Менее чем за секунду большинство надежно связанных между собой узлов этой сети принимает информацию о совершаемой транзакции и впервые видит адрес Алисы.

Тем временем кошелек Алисы постоянно «прослушивает» все транзакции, объявляемые в биткойн-сети, в поисках транзакции, целевой адрес которой совпадает с адресами кошельков Алисы. Через несколько секунд кошелек Джо завершает проведение транзакции, а в кошельке Алисы появляется оповещение о получении 0.10 биткойна (BTC).

Подтверждения

Сначала адрес Алисы обозначается в транзакции, выполняемой Джо, как «Unconfirmed» (Неподтвержденный). Это означает, что транзакция уже распространена по сети, но пока еще не записана в реестр транзакций биткойна, известного как блокчейн (blockchain). Для подтверждения транзакция обязательно должна быть включена в блок и добавлена в структуру данных блокчейна, а эта операция выполняется в среднем каждые 10 минут. В более привычных финансовых терминах такая операция называется клирингом (clearing). Более подробно операции распространения, проверки (валидации) и клиринга (подтверждения) будут рассматриваться в главе 10.

Теперь Алиса стала законной владелицей 0.10 биткойна, которые она может расходовать. В следующей главе мы рассмотрим ее первую покупку на биткойны и более подробно разберемся в технологиях, являющихся основой механизмов транзакций и распространения информации по сети.