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

Для Аманды.
Только после встречи с тобой я стал жить в раю.
– Дейв

Содержание

От издательства

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 на нашем сайте www.dmkpress.com, зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу dmkpress@gmail.com; при этом укажите название книги в теме письма.

Если вы являетесь экспертом в какой-либо области и 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.

Список опечаток

Хотя мы приняли все возможные меры для того, чтобы обеспечить высокое качество наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг, мы будем очень благодарны, если вы сообщите о ней главному редактору по адресу dmkpress@gmail.com. Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательство «ДМК Пресс» очень серьезно относится к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконной публикацией какой-либо из наших книг, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

Ссылку на подозрительные материалы можно прислать по адресу электронной почты dmkpress@gmail.com.

Мы высоко ценим любую помощь по защите наших авторов, благодаря которой мы можем предоставлять вам качественные материалы.

Отзывы о книге «Осваиваем Биткойн», третье издание

«Книга “Осваиваем Биткойн” очень полезна для каждого, кому хочется или требуется понять технологию биткойна и концепции его протоколов».

– Рене Пикхардт (René Pickhardt), разработчик Bitcoin Lightning Network

«Окунитесь в увлекательный мир Биткойна с книгой “Осваиваем Биткойн”. Это надежное пособие, которое поможет разобраться в тонкостях данной цифровой валюты. Если вы разработчик, инвестор или просто интересуетесь будущим денег, эта содержательная книга станет для вас путеводителем, который предоставит необходимые знания и поможет чувствовать себя уверенно в эпоху интернета денег».

– Жорж Лесмес (Jorge Lesmes), старший директор NTT DATA

«Спустя почти десятилетие после выхода в свет третье издание книги “Осваиваем Биткойн” закрепило за ней роль основного источника технического образовательного контента по теме биткойна. Ни одна другая книга не является столь же всеобъемлющей и актуальной».

– Олаолува Осунтокун (Olaoluwa Osuntokun), технический директор Lightning Labs

«Всесторонний обзор всего, что происходит в системе Биткойн, и как все это сочетается друг с другом».

– Марк «Мурч» Эрхардт (Mark «Murch» Erhardt), биткойн-инженер Chaincode Labs

Предисловие

Как была написана книга о Биткойне

Впервые я (Андреас) узнал о Биткойне в середине 2011 года. Первой моей реакцией было что-то вроде «Ха! Деньги умников!», и еще полгода я просто игнорировал это явление, не понимая его важности. Некоторым утешением может служить тот факт, что подобную реакцию можно было наблюдать у многих моих умнейших знакомых. Во второй раз я столкнулся с Биткойном в одном из обсуждений списка рассылки. Тогда я решил прочитать техническое описание, написанное Сатоши Накамото (Satoshi Nakamoto), и разобраться в сути дела. До сих пор помню момент, когда я закончил читать эти девять страниц и осознал, что биткойн – это не просто цифровая валюта, а доверительная сеть, способная стать основой для многого другого, помимо собственно денег. С осознанием факта, что «это не столько деньги, сколько децентрализованная доверительная сеть», я приступил к четырехмесячному исследованию Биткойна и начал впитывать каждый крохотный обрывок информации о нем, который только мог найти. На волне энтузиазма я проводил по 12 и более часов в день у экрана, читая, записывая, кодируя и изучая как можно больше. Я вышел из этого погружения похудевшим более чем на 20 фунтов (примерно 9 кг) из-за неправильного питания, с твердым намерением посвятить себя дальнейшей работе над Биткойном.

Спустя два года, после создания нескольких небольших стартапов для изучения различных услуг и продуктов на основе биткойна, я понял, что настало время написать свою первую книгу. Биткойн оказался той темой, которая вызвала у меня бурный творческий подъем и поглотила все мои мысли; это самая захватывающая технология, с которой я столкнулся после появления интернета. Настало время поделиться своей страстью к этой удивительной технологии с широким кругом читателей.

Целевая аудитория

Эта книга рассчитана в основном на программистов. Если вы умеете пользоваться языком программирования, эта книга научит вас работать с криптовалютами, использовать их и разрабатывать программное обеспечение для работы с ними. Первые несколько глав также можно использовать в качестве углубленного введения в биткойн для тех, кто не является кодером и пытается понять внутреннее устройство Биткойна и криптовалют.

Почему на обложке букашки?

Муравей-листорез – это биологический вид, который обладает очень сложным поведением в составе колонии-суперорганизма. При этом каждый отдельный муравей живет в соответствии с набором простых правил, обусловленных социальным взаимодействием и обменом химическими запахами (феромонами). По данным Википедии: «Как и люди, муравьи-листорезы образуют самые большие и сложные социальные живые сообщества на Земле». В действительности муравьи-листорезы не едят листья, а используют их для выращивания грибка в качестве основного источника пищи для обитателей своей колонии. Представляете? Эти муравьи занимаются сельским хозяйством!

Хотя муравьи живут в кастовом обществе и имеют королеву для производства потомства, в их колонии нет центральной власти или лидера. Высокоинтеллектуальное и совершенное поведение многомиллионной колонии – это эмерджентное свойство, возникающее в процессе взаимодействия особей внутри социальной сети.

Природа наглядно показывает: децентрализованные системы могут быть жизнеспособными. Они могут формировать эмерджентную сложность и невероятную развитость без необходимости в центральном руководстве, иерархии или сложных элементах.

Биткойн – это чрезвычайно сложная децентрализованная доверительная сеть, которая способна поддерживать огромное количество финансовых процессов. При этом каждый узел в сети Биткойн соблюдает всего лишь несколько простых правил. Взаимодействие между множеством узлов – именно это обеспечивает формирование такого продуманного поведения, а не сложность или доверие к какому-либо отдельному узлу. Подобно муравейнику, сеть Биткойн – это жизнестойкая система простых узлов, подчиняющихся простым правилам. Вместе они способны совершать удивительные вещи без какой-либо централизованной координации.

Условные обозначения, используемые в этой книге

В этой книге используются следующие типографские нормы:

Курсив
: Обозначает новые термины, URL-адреса, адреса электронной почты, имена и расширения файлов.

`Моноширинный шрифт`
: Используется в листингах программ, а также внутри абзацев для обозначения таких элементов программы, как имена переменных или функций, базы данных, типы данных, переменные среды, операторы и ключевые слова.

`Моноширинный полужирный шрифт`
: Показывает команды или другой текст, который должен быть набран пользователем вручную.

Моноширинный курсив
: Обозначает текст для замены на значения, вводимые пользователем, или на значения из контекста.


Этот элемент обозначает совет или рекомендацию.


Этот элемент обозначает общее примечание.


Этот элемент обозначает предупреждение или оповещение о потенциальной опасности.

Примеры кода

Все фрагменты кода могут быть воспроизведены на большинстве операционных систем с минимальным набором компиляторов и интерпретаторов для соответствующих языков. В случае необходимости приводятся базовые инструкции по установке и пошаговые примеры вывода этих инструкций.

Некоторые фрагменты кода и его выходные результаты были переформатированы для печати. Во всех этих случаях строки разделены символом обратной косой черты (\), за которым следует символ новой строки. При расшифровке примеров следует удалить эти два символа и снова соединить строки, чтобы получить идентичный результат, как показано в примере.

Во всех фрагментах кода по возможности используются реальные значения и вычисления, так что можно переходить от примера к примеру и видеть те же результаты в любом коде, который вы будете писать для вычисления тех же значений.

Использование примеров кода

Эта книга призвана помочь вам в вашей работе. Как правило, если в книге предлагаются примеры кода, их можно использовать в своих программах и документации. Вам не нужно обращаться за разрешением, если только вы не воспроизводите значительную часть кода. Например, написание программы, использующей несколько фрагментов кода из этой книги, не требует разрешения. Продажа или распространение примеров из книг O'Reilly требует разрешения. Для ответа на вопрос со ссылкой на эту книгу и цитированием примера кода разрешение не требуется. Включение значительного количества примеров из этой книги в документацию вашего продукта требует разрешения.

Мы ценим, но не требуем указания авторства. Авторство обычно включает название, автора, издателя и ISBN. Например: «Mastering Bitcoin, 3rd ed., by Andreas M. Antonopoulos and David A. Harding (O'Reilly). Copyright 2024 David Harding, ISBN 978-1-098-15009-9».

Некоторые издания этой книги распространяются под лицензией с открытым исходным кодом, например CC-BYNC, и в этом случае применяются условия этой лицензии.

Если вы считаете, что использование примеров кода выходит за рамки добросовестного использования или вышеуказанного разрешения, свяжитесь с нами по адресу permissions@oreilly.com.

Изменения относительно предыдущего издания книги

Особое внимание в третьем издании уделено переработке текста второго издания 2017 года и сохранившегося текста первого издания 2014 года. Кроме того, было добавлено множество концепций, актуальных для разработки современного Биткойна в 2023 году:

Глава 4
: Мы перегруппировали информацию об адресах таким образом, чтобы работать со всеми данными в историческом порядке. Мы добавили новый раздел по P2PK (где под «адресом» подразумевался IP-адрес), обновили предыдущие разделы по P2PKH и P2SH, а также добавили новые разделы по segwit/bech32 и taproot/bech32m.

Прежние главы 6 и 7
: Структура глав 6 «Транзакции» и 7 «Расширенные транзакции» была переработана и дополнена. Теперь это четыре новые главы: глава 6 «Транзакции» (структура транзакций), глава 7 «Авторизация и аутентификация», глава 8 «Цифровые подписи» и глава 9 «Плата за транзакции».

Глава 6
: Мы добавили почти полностью новую версию текста, описывающего структуру транзакций.

Глава 7
: Мы добавили новый текст о MAST, P2C, мультиподписях без скриптов, а также о taproot и tapscript.

Глава 8
: Мы пересмотрели текст о ECDSA и добавили новое описание подписей Шнорра, мультиподписей и пороговых подписей.

Глава 9
: Мы добавили почти полностью новый текст о комиссионных сборах, функциях повышения комиссионных сборов RBF и CPFP, пиннинге транзакций, ретрансляции пакетов и политике исключений для CPFP.

Глава 10
: Мы добавили текст о передаче компактных блоков, существенно обновили описание фильтров bloom с лучшим описанием проблем конфиденциальности, а также написали новый текст о компактных блочных фильтрах.

Глава 11
: Добавлен текст о технологии Signet.

Глава 12

Добавлен текст о BIP8 и коде активации Speedy Trial.

Приложения

Мы удалили специфические библиотечные приложения. После приложения с оригинальным техническим описанием мы добавили новое приложение с описанием того, чем реализация и свойства биткойна отличаются от предложенных в техническом описании.

Адреса и транзакции Биткойна в этой книге

Биткойн-адреса, транзакции, ключи, QR-коды и данные блокчейна, используемые в этой книге, по большей части реальны. Это означает, что вы можете просматривать блокчейн, изучать транзакции, приведенные в качестве примеров, извлекать их с помощью собственных скриптов или программ и т. д.

Однако имейте в виду, что закрытые ключи для построения адресов либо напечатаны в книге, либо «сожжены». Это означает, что если вы отправите деньги на любой из этих адресов, они будут либо навсегда потеряны, либо, как вариант, любой читатель книги сможет забрать их, используя напечатанные в ней закрытые ключи.

НЕ ОТПРАВЛЯЙТЕ ДЕНЬГИ НИ ПО ОДНОМУ ИЗ АДРЕСОВ, УКАЗАННЫХ В ЭТОЙ КНИГЕ. Ваши деньги достанутся другому читателю или будут утеряны навсегда.

Как связаться с авторами

Обратиться к Андреасу М. Антонопулосу можно через его персональный сайт: https://antonopoulos.com.

Подпишитесь на Андреаса в Facebook: https://facebook.com/AndreasMAntonopoulos.

Подпишитесь на Андреаса в Twitter: https://twitter.com/aantonop.

Подпишитесь на Андреаса в LinkedIn: https://linkedin.com/company/aantonop.

Большое спасибо всем спонсорам Андреаса, которые поддерживают его работу ежемесячными пожертвованиями. Вы можете посмотреть его страницу на Patreon здесь: https://patreon.com/aantonop.

Информация о книге «Осваиваем Биткойн», а также об открытом издании и переводах Андреаса доступна на сайте https://bitcoinbook.info.

Связаться с Дэвидом А. Хардингом можно через его личный сайт: https://dtrt.org.

Благодарности за первое и второе издания

Андреас М. Антонопулос

Эта книга является результатом труда и усилий многих людей. Я благодарен за помощь, которую мне оказали друзья, коллеги и даже совершенно незнакомые

люди, которые присоединились ко мне в стремлении написать исчерпывающе полную техническую книгу о криптовалютах и Биткойне.

Как невозможно разграничить технологию Биткойн и сообщество биткойна, так и это издание является в равной степени продуктом этого сообщества и книгой о технологии. С самого начала и до самого конца моя работа над этой книгой получала ободрение, поддержку и благодарность от всего биткойн-сообщества. Более того, эта книга позволила мне в течение двух лет оставаться частью замечательного сообщества, и я не могу не поблагодарить вас за то, что вы приняли меня в него. Слишком много людей, чтобы называть их по именам, – тех, кого я встречал на конференциях, мероприятиях, семинарах, сборах, посиделках в пиццерии и небольших личных встречах, а также многих, кто общался со мной в Twitter, на reddit, на bitcointalk.org и на GitHub, – всех, кто оказал влияние на эту книгу. Каждая идея, сравнение, вопрос, ответ и объяснение, которые вы найдете в этой книге, были в какой-то момент поддержаны, проверены или улучшены благодаря общению с сообществом. Спасибо всем вам за поддержку; без вас эта книга не увидела бы свет. Я бесконечно вам благодарен.

Разумеется, путь автора начинается задолго до выхода первой книги. Моим родным языком (и языком обучения в школе) был греческий, поэтому на первом курсе университета мне пришлось посещать коррекционный курс английского языка. Я благодарен Диане Кордас (Diana Kordas), моему преподавателю английского, которая помогала мне в тот год обрести уверенность и навыки. Позже, став профессионалом, я совершенствовал свои навыки написания технических статей по тематике центров обработки данных, работая в журнале Network World. Я благодарен Джону Диксу (John Dix) и Джону Галланту (John Gallant), которые предоставили мне первую работу в качестве обозревателя в Network World, а также моему редактору Майклу Куни (Michael Cooney) и моей коллеге Джоне Тилл Джонсон (Johna Till Johnson), которые занимались правкой моих колонок и делали их пригодными для публикации. Написание 500 слов в неделю в течение четырех лет позволило мне получить достаточно опыта, чтобы в конце концов задуматься об авторстве.

Также выражаю благодарность тем, кто поддержал меня во время подачи заявки на издание книги в O'Reilly своими рекомендациями и рецензиями. В частности, спасибо Джону Галланту (John Gallant), Грегори Нессу (Gregory Ness), Ричарду Стиннону (Richard Stiennon), Джоэлу Снайдеру (Joel Snyder), Адаму Левину (Adam B. Levine), Сандре Гитлен (Sandra Gittlen), Джону Диксу (John Dix), Джоне Тилл Джонсон (Johna Till Johnson), Роджеру Веру (Roger Ver) и Джону Матонису (Jon Matonis). Особая благодарность Ричарду Кагану (Richard Kagan) и Тимону Маттошко (Tymon Mattoszko), которые рецензировали ранние версии заявки, а также Мэтью Тейлору (Matthew Taylor), который выполнил техническое редактирование и форматирование текста заявки.

Благодарю Крикета Лю (Cricket Liu), автора книги «*DNS и BIND*» в O'Reilly, который познакомил меня с издательством. Спасибо также Майклу Лоукидесу (Michael Loukides) и Эллисон Макдональд (Allyson MacDonald) из O'Reilly, которые в течение нескольких месяцев работали над этой книгой. Эллисон была особенно терпелива в моменты срыва сроков и задержек с выпуском, когда жизнь вносила коррективы в запланированный нами график. Выражаю благодарность Тимоти Макговерну (Timothy McGovern) за руководство работами

при выпуске второго издания, Ким Кофер (Kim Cofer) за терпеливую редактуру, а также Ребекке Панцер (Rebecca Panzer) за иллюстрации к многочисленным новым рисункам.

Самыми трудными были несколько черновиков первых глав, потому что тема Биткойна является сложной для последовательного изучения. Каждый раз, когда я дергал за одну из нитей технологии Биткойн, мне приходилось распутывать всю тему. То и дело я останавливался и впадал в уныние в поисках простого объяснения темы и понятного изложения такого сложного технического материала. Я благодарен своему другу и наставнику Ричарду Кагану (Richard Kagan), который помог разобраться с историей и преодолеть моменты писательского кризиса. Выражаю благодарность разработчикам из группы San Francisco Bitcoin Developers Meetup, а также Таарику Льюису (Taariq Lewis) и Дениз Терри (Denise Terry) за помощь в проверке предварительных версий. Также выражаю особую благодарность Эндрю Науглеру (Andrew Naugler) за дизайн инфографики.

В процессе работы над книгой я выложил первые черновики на GitHub и предложил аудитории высказать свои замечания. Было получено более сотни комментариев, предложений, исправлений и дополнений. Этот вклад и моя благодарность за него подробно описаны в разделе «Черновик ранней версии (вклад GitHub)». В первую очередь я искренне благодарен моим добровольным редакторам на GitHub Мингу Т. Нгуену (Ming T. Nguyen, 1-е издание) и Уиллу Биннсу (Will Binns, 2-е издание), которые без устали курировали, принимали и обрабатывали предложения, сообщения о проблемах, а также исправляли ошибки на GitHub.

После завершения работы над книгой она прошла несколько этапов технического рецензирования. Благодарю Крикета Лю (Cricket Liu) и Лорна Ланца (Lorne Lantz) за их тщательную проверку, комментарии и поддержку.

Несколько разработчиков биткойна предоставили примеры кода, обзоры, комментарии и полезные советы. Спасибо Амиру Тааки (Amir Taaki) и Эрику Воскуилу (Eric Voskuil) за примеры кода и множество замечательных комментариев; Крису Клешульте (Chris Kleeschulte) за информацию о Bitcore; Виталику Бутерину (Vitalik Buterin) и Ричарду Киссу (Richard Kiss) за помощь с расчетами эллиптических кривых и вклад в код; Гэвину Андресену (Gavin Andresen) за исправления, комментарии и поддержку; Михалису Каргакису (Michalis Kargakis) за комментарии, вклад и запись btcd; а также Робину Инге (Robin Inge) за исправления, внесенные в улучшение второго издания. При подготовке второго издания мне вновь оказали значительную поддержку многие разработчики Bitcoin Core, в том числе Эрик Ломброзо (Eric Lombrozo), который раскрыл суть сегрегированного свидетельства, Люк Дашжр (Luke Dashjr), который помог улучшить главу о транзакциях, Джонсон Лау (Johnson Lau), который рецензировал сегрегированное свидетельство и другие главы, и многие другие. Я благодарен Джозефу Пуну (Joseph Poon), Тадге Драйе (Tadge Dryja) и Олаолуве Осунтокуну (Olaoluwa Osuntokun), которые объясняли суть Lightning Network, рецензировали мои работы и отвечали на вопросы, когда я оказывался в затруднительном положении.

Своей любовью к словесности и книгам я обязан моей маме Терезе, которая вырастила меня в доме, где все стены были уставлены книгами. Мама также ку-

пила мне мой первый компьютер в 1982 году, хотя я сам считал себя технофобом. Мой отец Менелаос, инженер-строитель, который недавно опубликовал свою первую книгу в возрасте 80 лет, был тем, кто научил меня логическому и аналитическому мышлению, а также любви к науке и инженерии.

Спасибо всем, кто поддерживал меня на всех этапах этого пути.

Благодарности за третье издание

Дэвид А. Хардинг

Знакомство с неинтерактивным протоколом подписи Шнорра, которое начинается с описания интерактивного протокола идентификации Шнорра в разделе «Подписи Шнорра», было написано под сильным впечатлением от введения в эту тему в книге «Подписи Борроммеанского кольца» (Borrommean Ring Signatures, 2015), написанной Грегори Максвеллом (Gregory Maxwell) и Эндрю Поэлстрой (Andrew Poelstra). Я глубоко признателен каждому из них за всю их бескорыстную помощь в течение последнего десятилетия.

Неоценимую техническую помощь в работе над черновиками этой книги оказали Хорхе Лесмес (Jorge Lesmes), Олаолува Осунтокун (Olaoluwa Osuntokun), Рене Пикхардт (René Pickhardt) и Марк Эрхардт (Mark «Murch» Erhardt). В частности, невероятно глубокая и содержательная рецензия Мерча, как и его готовность оценить несколько итераций одного и того же текста, позволили поднять качество этой книги выше моих самых смелых ожиданий.

Я также выражаю глубокую благодарность Джимми Сонгу (Jimmy Song) за его предложение принять участие в этом проекте, моему соавтору Андреасу (Andreas) за разрешение обновить его бестселлер, Анджеле Руфино (Angela Rufino) за сопровождение моего авторского процесса в O'Reilly, а также всем остальным сотрудникам O'Reilly, благодаря которым работа над третьим изданием стала приятным и продуктивным опытом.

В заключение, я просто не представляю, как можно выразить благодарность всем участникам проекта Bitcoin, которые помогали мне в моей жизни – от создания программ, которые я использую, до обучения их работе и помощи в передаче тех крох знаний, которые я приобрел. Вас очень много, и я не смогу перечислить все ваши имена, но я часто думаю о вас и знаю, что мой вклад в эту книгу был бы невозможен без всей вашей помощи.

Черновик ранней версии (вклад GitHub)

Многие авторы предложили свои комментарии, исправления и дополнения к черновому варианту ранней версии, размещенной на GitHub. Спасибо всем за ваш вклад в создание этой книги.

Ниже приведен список известных участников GitHub, в скобках указан их учетный идентификатор GitHub:

- Abdussamad Abdurrazzaq (AbdussamadA);
- Adán SDPC (aesedepece);
- Akira Chiku (achiku);
- Alex Waters (alexwaters);

- Andrew Donald Kennedy (grkvlt);
- Andrey Esaulov (andremaha);
- andronoob;
- AnejaBK;
- Appaji (CITIZENDOT);
- ariesunny;
- Arthur O'Dwyer (Quuxplusone);
- bargitta;
- Basem Alasi (Bamskki);
- bisqfan;
- bitcoinctf;
- blip151;
- Bryan Gmyrek (physicsdude);
- Carlos Sims (simsbluebox);
- Casey Flynn (cflynn07);
- cclauss;
- Chapman Shoop (belovachap);
- chrisd95;
- Christie D'Anna (avocadobreath);
- Cihat Imamoglu (cihati);
- Cody Scott (Siecje);
- coinradar;
- Cragin Godley (cgodley);
- Craig Dodd (cdodd);
- dallyshalla;
- Dan Nolan (Dan-Nolan);
- Dan Raviv (danra);
- Darius Kramer (dkrmr);
- Darko Janković (trulex);
- David Huie (DavidHuie);
- didongke;
- Diego Viola (diegoviola);
- Dimitris Tsapakidis (dimitris-t);
- Dirk Jäckel (biafra23);
- Dmitry Marakasov (AMDmi3);
- drakos (Jolly-Pirate);
- drstrangeM;
- Ed Eykholt (edeykholt);
- Ed Leafe (EdLeafe);
- Edward Posnak (edposnak);
- Elias Rodrigues (elias19r);
- Eric Voskuil (evoskuil);
- Eric Winchell (winchell);
- Erik Wahlström (erikwam);
- effectsToCause (vericoin);
- Esteban Ordano (eordano);
- ethers;
- Evlix;
- fabienhinault;
- Fan (whiteath);
- Felix Filozov (ffilozov);
- Francis Ballares (fballares);
- François Wirion (wirion);
- Frank Höger (francyi);
- Gabriel Montes (gabmontes);
- Gaurav Rana (bitcoinsSG);
- genjix;
- Geremia;
- Gerry Smith (Hermetic);
- gmr81;
- Greg (in3rsha);
- Gregory Trubetskoy (grisha);
- Gus (netpoe);
- halseth;
- harelw;
- Harry Moreno (morenoh149);
- Hennadii Stepanov (hebasto);
- Holger Schinzel (schinzelh);
- Ioannis Cherouvim (cherouvim);
- Ish Ot Jr. (ishotjr);
- ivangreene;
- James Addison (jayaddison);
- Jameson Lopp (jlopp);
- Jason Bisterfeldt (jbisterfeldt);
- Javier Rojas (fjrojasgarcia);
- Jordan Baczuk (JBaczuk);
- Jeremy Bokobza (bokobza);
- JerJohn15;
- jerzybrzoska;
- Jimmy DeSilva (jimmydesilva);
- Jo Wo (jowo-io);
- Joe Bauers (joebauers);
- joflynn;
- Johnson Lau (jl2012);
- Jonathan Cross (jonathancross);
- Jorgeminator;
- jwbats;
- Kai Bakker (kaibakker);
- kollokollo;
- krupawan5618;
- kynnjo;
- Liangzx;
- lightningnetworkstores;
- lilianrambu;

- Liu Yue (lyhistory);
- Lobbelt;
- Lucas Betschart (lclc);
- Matt Wesley (MatthewWesley);
- Magomed Aliev (30mb1);
- Mai-Hsuan Chia (mhchia);
- Marco Falke (MarcoFalke);
- María Martín (mmartinbar);
- Marcus Kiisa (mkiisa);
- Mark Erhardt (Xekyo);
- Mark Pors (pors);
- Martin Harrigan (harrigan);
- Martin Vseticka (MartyIX);
- Marzig (marzig76);
- Matt McGivney (mattmcgiv);
- Matthijs Roelink (Matthiti);
- Maximilian Reichel (phramz);
- MG-ng (MG-ng);
- Michalis Kargakis (kargakis);
- Michael C. Ippolito (michaelcippolito);
- Michael Galero (mikong);
- Michael Newman (michaelbnewman);
- Mihail Russu (MihailRussu);
- mikew (mikew);
- milansismanovic;
- Minh T. Nguyen (enderminh);
- montvid;
- Morfies (morfies);
- Nagaraj Hubli (nagarajhubli);
- Nekomata (nekomata-3);
- nekonenene;
- Nhan Vu (jobnomade);
- Nicholas Chen (nickycutesc);
- Ning Shang (syncom);
- Oge Nnadi (ogennadi);
- Oliver Maerz (OliverMaerz);
- Omar Boukli-Hacene (oboukli);
- Óscar Nájera (Titan-C);
- Parzival (Parz-val);
- Paul Desmond Parker (sunwukonga);
- Philipp Gille (philippgille);
- ratijas;
- rating89us;
- Raul Siles (raulsiles);
- Reproducibility Matters (TheCharlatan);
- Reuben Thomas (rrthomas);
- Robert Furse (Rfurse);
- Roberto Mannai (robermann);
- Richard Kiss (richardkiss);
- rszheng;
- Ruben Alexander (hizzvizz);
- Sam Ritchie (sritchie);
- Samir Sadek (netsamir);
- Sandro Conforto (sandroconforto);
- Sanjay Sanathanan (sanjays95);
- Sebastian Falbesoner (theStack);
- Sergei Tikhomirov (s-tikhomirov);
- Sergej Kotliar (ziggamon);
- Seiichi Uchida (topecongiro);
- shaysw;
- Simon de la Rouviere (simondlr);
- simone-cominato;
- sindhoor7;
- Stacie (staciewaleyko);
- Stephan Oeste (Emzy);
- Stéphane Roche (Janaka-Steph);
- takaya-imai;
- Thiago Arrais (thiagoarrais);
- Thomas Kerin (afk11);
- Tochi Obudulu (tochicool);
- Tosin (tkuye);
- Vasil Dimov (vasild);
- venzen;
- Vlad Stan (motorina0);
- Vijay Chavda (VijayChavda);
- Vincent Déniel (vincentdnl);
- weinim;
- wenxiaolong (QingShiLuoGu);
- wenzhenxiang;
- Will Binns (wbnns);
- wintercooled;
- wjx;
- wll2007;
- Wojciech Langiewicz (wlk);
- Yancy Ribbens (yancyribbens);
- yjjnls;
- Yoshimasa Tanabe (emag);
- yuntai;
- yurigeorgiev4;
- Zheng Jia (zhengjia);
- Zhou Liang (zhouguoguo).

Об авторах

Андреас М. Антонопулос (Andreas M. Antonopoulos) – известный технический специалист и опытный предприниматель, который стал одним из самых известных и уважаемых представителей сферы Биткойн. Будучи прекрасным оратором, преподавателем и писателем, Андреас излагает сложные темы доступным и понятным языком. В качестве консультанта он оказывает помощь стартапам в определении, оценке и управлении рисками в сфере безопасности и бизнеса.

Андреас вырос вместе с интернетом, создав свою первую компанию, раннюю электронную доску объявлений (Bulletin Board System, BBS) и систему доступа в интернет, еще будучи подростком в своем доме в Греции. Он получил степень в области компьютерных наук, передачи данных и распределенных систем в Университетском колледже Лондона (University College London, UCL), который недавно вошел в десятку лучших университетов мира. После переезда в США Андреас стал соучредителем и руководителем успешной исследовательской компании в области технологий, а также консультантом десятков руководителей компаний из списка Fortune 500 по вопросам сетевых технологий, безопасности, центров обработки данных и облачных вычислений. Более двухсот его статей по вопросам безопасности, облачных вычислений и центров обработки данных были опубликованы в печати и распространены по всему миру. Он имеет два патента в области сетевых технологий и безопасности.

В 1990 году Андреас занялся преподаванием различных дисциплин в области ИТ в частной, профессиональной и академической среде. Он оттачивал свое ораторское мастерство перед аудиториями самого разного размера – от пяти руководителей в зале заседаний до тысяч человек на крупных конференциях. За его плечами более четырехсот выступлений. Он считается харизматичным оратором и преподавателем мирового класса. В 2014 году он был назначен преподавателем Университета Никосии – первого в мире университета, предлагающего степень магистра в области цифровых валют. В этой роли он помогал разрабатывать учебную программу и преподавал курс «Введение в цифровые валюты», предлагаемый в качестве массового открытого онлайн-курса в университете.

Будучи предпринимателем в сфере Биткойн, Андреас основал несколько биткойн-компаний и запустил несколько проектов с открытым исходным кодом. Он выступает в качестве советника нескольких биткойн- и криптовалютных компаний. Он широко публикуется в журналах и блогах, посвященных Биткойну, является постоянным ведущим популярного подкаста Let's Talk Bitcoin, а также часто выступает на конференциях по технологиям и безопасности по всему миру.

Дэвид А. Хардинг (David A. Harding) – технический писатель, который специализируется на создании документации для программного обеспечения с открытым исходным кодом. Он является соавтором еженедельного новостного бюллетеня *Bitcoin Optech* (2018–2023), учебников *21.co Bitcoin Computer* (2015–2017) и документации для разработчиков Bitcoin.org (2014–2015). Он также является членом грантового комитета Brink.dev (2022–2023) и бывшим членом его правления (2020–2022).

Колофон

Животное на обложке книги «Осваиваем Биткойн» – это муравей-листорез (Atta colombica). Муравей-листорез (простое название) – это зонтичный муравей из тропиков Южной и Центральной Америки, а также Мексики и юга Соединенных Штатов. Как и люди, муравьи-листорезы образуют самые большие и сложные сообщества животных на планете. Они получили свое название за то, что жуют листья, которые служат питанием в их грибковом хозяйстве.

Крылатые муравьи – как самцы, так и самки совершают массовый выход из гнезда для брачного полета, известного как ревоада (revoada). Самки спариваются с несколькими самцами, чтобы собрать 300 млн сперматозоидов, необходимых для создания колонии. Самки также хранят кусочки мицелия родительского грибного сада в инфрабуккальном кармане, расположенном в ротовой полости; они будут использовать его для создания собственных грибных садов. Опустившись на землю, самка теряет крылья и устраивает подземное гнездо для своей колонии. Успех новых королев невелик: лишь 2,5 % создают долгоживущую колонию.

Когда колония созревает, муравьи делятся на касты в зависимости от размера, каждая из которых выполняет различные функции. Обычно выделяют четыре касты: минимы – самые маленькие рабочие, которые ухаживают за молодняком и грибными садами; миноры, чуть крупнее минимов, являются первой линией обороны колонии, патрулируют окрестности и нападают на врагов; медиа – общие фуражиры, которые обрывают листья и приносят их фрагменты в гнездо; и майоры – самые крупные рабочие муравьи, которые действуют как солдаты, защищая гнездо от вторжения. Недавние исследования показали, что майоры также расчищают основные кормовые тропы и переносят громоздкие предметы обратно в гнездо.

Многие из животных, обитающих на обложках книг издательства O'Reilly, находятся под угрозой исчезновения; все они важны для мира.

Иллюстрация для обложки выполнена Карен Монтгомери (Karen Montgomery) на основе изображения из книги «Зарубежные насекомые» (*Insects Abroad*).

Глава 1

Введение

Биткойн – это совокупность концепций и технологий, которые составляют основу экосистемы цифровых денег. Единицы валюты, называемые биткойн, используются для хранения и передачи стоимости между участниками сети Биткойн. Пользователи этой сети общаются друг с другом посредством биткойн-протокола, в основном через интернет, хотя можно использовать и другие информационные сети. Стек протоколов Биткойна, доступный в виде программного обеспечения с открытым исходным кодом, может быть запущен на различных вычислительных устройствах, включая ноутбуки и смартфоны, что обеспечивает широкую доступность технологии.

В этой книге денежная единица называется «биткойн» (bitcoin) со строчной буквы «б», а система называется «Биткойн» (Bitcoin) с прописной буквы «Б».

Пользователи могут переводить биткойны по сети для выполнения практически всех операций, которые можно совершать с обычными валютами, включая покупку и продажу товаров, отправку денег частным лицам или организациям, а также выдачу кредитов. Биткойн можно покупать, продавать и обменивать на другие валюты на специализированных валютных биржах. Биткойн можно смело назвать идеальной формой интернет-денег, поскольку эта валюта работает быстро, безопасно и не знает границ.

В отличие от традиционных денег, биткойн полностью виртуален. Не существует ни физических монет, ни даже их цифровых версий. Монеты подразумеваются при совершении транзакций, в ходе которых стоимость передается от отправителя к получателю. Пользователи Биткойна контролируют ключи, с помощью которых можно подтвердить право собственности на биткойн в сети Биткойн. С помощью этих ключей можно подписывать транзакции с целью разблокировать их стоимость и потратить путем передачи новому владельцу. Ключи часто хранятся в цифровом кошельке на любом пользовательском компьютере или смартфоне.

Единственным условием для проведения операций с биткойнами является владение ключом, который дает возможность подписывать транзакции, – именно это передает полный контроль каждому пользователю.

Биткойн – это распределенная одноранговая (peer-to-peer) система. У нее отсутствует центральный сервер или центр управления. Единицы биткойна

получаются в результате процесса под названием «майнинг» (англ. mining – буквально «добыча»), который подразумевает многократное выполнение вычислительных задач, связанных со списком последних транзакций в сети Биткойн. Любой участник сети Биткойн может выступать в роли майнера, используя свои вычислительные устройства для безопасного проведения транзакций. Каждый майнер Биткойна в среднем за 10 минут может повысить безопасность прошедших транзакций, а в качестве вознаграждения он получает как совершенно новые биткойны, так и комиссионные за прошедшие транзакции. В сущности, майнинг биткойнов обеспечивает децентрализацию функций центрального банка по выпуску валюты и клирингу, заменяя собой необходимость в существовании какого-либо центрального банка.

Протокол Биткойна включает в себя встроенные алгоритмы для регулирования функции майнинга в сети. Сложность вычислительной задачи, которую должны выполнить майнеры, регулируется динамически, так что в среднем каждые 10 минут кто-то добивается успеха, независимо от того, сколько майнеров (и какой объем обработки) конкурируют в каждый момент времени. Протокол также постепенно уменьшает количество создаваемых биткойнов, что ограничивает общее количество биткойнов, которое когда-либо будет создано, фиксированной суммой чуть менее 21 млн монет. В результате количество биткойнов в обращении следует легкопредсказуемой кривой, по которой каждые четыре года в обращение поступает половина оставшихся монет. К моменту выпуска примерно 1 411 200 блоков, который предположительно произойдет в 2035 году, будет выпущено 99 % всех когда-либо существовавших биткойнов. Вследствие сокращения темпов эмиссии биткойна в долгосрочной перспективе эта валюта имеет дефляционный характер. Кроме того, никто не заставит вас принять биткойны, выпущенные сверх ожидаемого уровня эмиссии.

Помимо этого, Биткойн – это еще и название протокола, одноранговой сети и инновационной технологии распределенных вычислений. Биткойн опирается на десятилетия исследований в области криптографии и распределенных систем. Он включает в себя как минимум четыре ключевых новшества, собранных воедино в уникальную и мощную комбинацию. Биткойн – это:

- децентрализованная одноранговая (пиринговая) сеть (протокол Биткойн);
- общедоступный реестр транзакций (блокчейн);
- набор правил для независимой проверки (валидации) транзакций и эмиссии денежных средств (правила консенсуса);
- механизм достижения глобального децентрализованного консенсуса на действующем блокчейне с алгоритмом доказательства выполнения работы (Proof-of-Work).

С точки зрения разработчика, Биткойн можно рассматривать как подобие интернета денег, сеть для распространения ценностей и защиты прав собственности на цифровые активы с помощью распределенных вычислений. Биткойн – это нечто намного большее, чем может показаться на первый взгляд.

В этой главе речь идет о начале работы с объяснением некоторых основных концепций и терминов, о получении необходимого программного обеспечения и об использовании Биткойна для простых транзакций. В следующих

главах начнется изучение технологических уровней, обеспечивающих работу, а также внутренних механизмов сети и протокола Биткойна.

Цифровые валюты до Биткойна

Появление жизнеспособных цифровых денег тесно связано с развитием криптографии. Это неудивительно с учетом фундаментальных проблем при использовании битов для представления стоимости, которую можно обменять на товары и услуги. Три основных вопроса, с которыми сталкиваются пользователи цифровых денег:

- можно ли доверять подлинности денег, не являются ли они фальшивыми?
- можно ли быть уверенным в возможности потратить цифровые деньги только один раз (проблема, известная как doublespend – «двойная трата»)?
- можно ли быть уверенным, что больше никто, кроме меня, не сможет предъявить права на эти деньги?

Эмитенты бумажных денег постоянно решают проблему фальшивок, применяя все более сложные виды бумаги и технологии печати. Физические деньги легко решают проблему двойной траты, поскольку одна и та же бумажная купюра не может находиться в двух местах одновременно. Безусловно, обычные деньги также часто хранятся и передаются в цифровом виде. В этих случаях проблемы подделки и двойной траты решаются с помощью клиринга всех электронных транзакций через центральные структуры, которым известна вся валюта, находящаяся в обращении. Для цифровых денег, не имеющих аналогов в виде специальных чернил или голографических полос, основанием для доверия к легитимности заявления пользователя о ценности служит криптография. В частности, криптографические цифровые подписи дают пользователю возможность подписать цифровой актив или транзакцию, подтверждая его право собственности на него. При соответствующей архитектуре цифровые подписи также можно использовать для решения проблемы двойной траты.

По мере того как в конце 1980-х годов криптография становилась все более доступной и понятной, многие специалисты пытались использовать ее для создания цифровых денег. В рамках этих ранних проектов выпускались цифровые валюты, обычно обеспеченные национальной денежной системой или драгоценным металлом, например золотом.

Несмотря на работоспособность этих ранних цифровых валют, они имели централизованный характер и, как следствие, легко подвергались внешним атакам со стороны правительств и хакеров. Подобно традиционной банковской системе, ранние цифровые валюты использовали центральный расчетный аппарат для урегулирования всех транзакций через определенные промежутки времени. Некоторые из них потерпели впечатляющий крах при внезапной ликвидации материнской компании. Для защиты от вмешательства недоброжелателей, будь то законные правительства или преступные сообщества, нужна децентрализованная цифровая валюта, исключающая возможность единой точечной атаки. Биткойн – именно такая система, децентрализованная по своей сути и не имеющая никаких центральных органов власти или точек контроля, которые могли бы быть атакованы или дискредитированы.

История Биткойна

Впервые концепция Биткойна была описана в 2008 году в статье под названием «Биткойн: пиринговая система электронных денег» («Bitcoin: A Peer-to-Peer Electronic Cash System»)[1]. Материал был подписан псевдонимом Сатоши Накамото (Satoshi Nakamoto) (см. приложение А). В своей работе Накамото объединил несколько ранее сделанных изобретений, таких как цифровые подписи и система Hashcash, для создания полностью децентрализованной системы электронных денег. Эта система не нуждается в централизованном управлении для эмиссии валюты, расчетов и подтверждения транзакций. Ключевым новшеством стало использование распределенной системы вычислений – алгоритма «proof-of-work» («доказательство работы») – для проведения глобальной лотереи в среднем каждые 10 минут, что дает децентрализованной сети возможность прийти к консенсусу относительно состояния транзакций. Тем самым достигается эффективное решение проблемы двойной траты, при которой одна валютная единица может быть потрачена дважды. Ранее эта проблема считалась слабым местом цифровых валют и устранялась за счет клиринга всех транзакций через центральный расчетный центр.

Сеть Биткойн была запущена в 2009 году на основе эталонной разработки, созданной Накамото и впоследствии доработанной многими другими программистами. Количество и мощность систем, выполняющих алгоритм доказательства работы (proof-of-work, то есть майнинг) для обеспечения безопасности и устойчивости сети Биткойн, росли в геометрической прогрессии. В настоящее время их совокупная вычислительная мощность превышает общее количество вычислительных операций лучших суперкомпьютеров мира.

В апреле 2011 года Сатоши Накамото исчез из публичного пространства, возложив ответственность за разработку кода и сети на быстро растущую группу добровольных помощников. Кто именно создал биткойн, до сих пор остается невыясненным. Однако ни Сатоши Накамото, ни кто-либо другой не имеет единоличного контроля над системой Биткойн, поскольку ее работа основана на полностью прозрачных математических правилах, открытом исходном коде и общем согласии между участниками. Это изобретение само по себе является революционным и уже породило новую научно-техническую отрасль в области распределенных вычислений, экономики и эконометрики.

Решение проблемы распределенных вычислений

Изобретение Сатоши Накамото также является практически новым решением проблемы распределенных вычислений, известной как «проблема (задача) византийских генералов» (Byzantine Generals' Problem). Суть проблемы заключается в попытке договориться между несколькими субъектами без лидера о порядке действий путем обмена информацией по ненадежной и потенциально взломанной сети. Решение Сатоши Накамото, использующее концепцию доказательства работы для получения консенсуса *без привлечения центральной доверенной инстанции*, стало прорывом в области распределенных вычислений.

[1] «Bitcoin: A Peer-to-Peer Electronic Cash System», Satoshi Nakamoto.

Приступая к работе

Биткойн – это протокол, доступ к которому можно получить при помощи приложения с поддержкой этого протокола. По аналогии с веб-браузером, который является наиболее распространенным пользовательским интерфейсом для протокола HTTP, «биткойн-кошелек» (Bitcoin wallet) является наиболее распространенным пользовательским интерфейсом для системы Биткойн. Как и в примере со множеством веб-браузеров (например, Chrome, Safari и Firefox), существует множество реализаций и брендов биткойн-кошельков. И точно так же, как мы выбираем свои любимые браузеры, биткойн-кошельки могут отличаться по качеству, производительности, безопасности, конфиденциальности и надежности. Кроме того, имеется эталонная реализация протокола Биткойн, известная как «Bitcoin Core». Она создана на основе исходной концепции, разработанной Сатоши Накамото.

Выбор биткойн-кошелька

Биткойн-кошельки входят в число наиболее активно разрабатываемых приложений в экосистеме Биткойн. Здесь царит высокая конкуренция, и даже если прямо сейчас разрабатывается новый кошелек, несколько прошлогодних могут уже не поддерживаться. Выбор кошелька в значительной степени основан на личных предпочтениях, он определяется сферой применения и опытом пользователя. Поэтому нет смысла рекомендовать какой-либо определенный бренд или кошелек. Тем не менее можно классифицировать биткойн-кошельки в соответствии с их платформой и функциями, чтобы внести некоторую ясность относительно всех существующих типов кошельков. Стоит попробовать несколько разных вариантов, пока не найдется подходящий под конкретные нужды.

Разновидности биткойн-кошельков

Биткойн-кошельки в зависимости от платформы можно условно разделить на следующие категории.

Кошелек для настольных компьютеров
: Кошелек для ПК стал первым типом биткойн-кошелька, созданным в качестве эталонного варианта. Многие пользователи работают с кошельками для ПК по причине предлагаемых ими возможностей, автономности и управляемости. Однако запуск на распространенных операционных системах, таких как Windows и macOS, связан с определенными недостатками в плане обеспечения безопасности, поскольку эти платформы часто оказываются незащищенными и плохо настроенными.

Мобильный кошелек
: Мобильный кошелек можно назвать наиболее распространенным типом биткойн-кошелька. Эти приложения работают на операционных системах смартфонов, таких как Apple iOS и Android, и зачастую представляют собой

оптимальный выбор для начинающих. Многие из этих кошельков рассчитаны на простоту и удобство использования, но есть и полнофункциональные мобильные кошельки для опытных пользователей. Чтобы не загружать и не хранить большие объемы данных, многие мобильные кошельки получают информацию с удаленных серверов. Это снижает уровень конфиденциальности, поскольку позволяет третьим лицам получать сведения о ваших адресах и балансах биткойнов.

Веб-кошелек
: Доступ к веб-кошелькам открывается через веб-браузер, а сам кошелек находится на сервере стороннего оператора. Это похоже на веб-почту, поскольку полностью зависит от использования стороннего сервера. Некоторые из этих сервисов используют клиентский код, запускаемый в браузере пользователя, что дает возможность сохранить контроль над ключами Биткойна в руках владельца, хотя его зависимость от сервера все равно ставит конфиденциальность под угрозу. Однако большинство из подобных систем лишают пользователей контроля над ключами Биткойна в обмен на простоту использования. Хранить большие суммы биткойнов в сторонних системах нежелательно.

Аппаратные устройства подписи
: Аппаратные кошельки представляют собой оборудование для хранения ключей и подписывания транзакций с помощью специализированного аппаратного и микропрограммного обеспечения. Обычно они подключаются к настольному, мобильному или веб-кошельку через USB-кабель, беспроводной интерфейс ближнего поля (NFC) или камеру для работы с QR-кодами. Поскольку все операции с биткойном выполняются на специализированном оборудовании, такие кошельки менее уязвимы для различных типов атак. Иногда аппаратные устройства подписи называют «аппаратными кошельками», но для отправки и получения транзакций их нужно использовать в связке с полнофункциональным кошельком. Безопасность и конфиденциальность, обеспечиваемые этим кошельком в связке, играют решающую роль при использовании аппаратного устройства подписи.

Полнофункциональная или облегченная версия

Биткойн-кошельки можно также классифицировать по степени их автономности и способу взаимодействия с сетью Биткойн:

Полноценный узел (клиент)
: Полноценный узел (клиент) – это программа для проверки всей истории транзакций биткойна (каждая транзакция каждого пользователя, за все время). Опционально полноценные клиенты могут также хранить подтвержденные ранее транзакции и предоставлять данные другим программам Биткойна как на этом же компьютере, так и через интернет. Полноценный клиент использует значительные компьютерные ресурсы – примерно столько же, сколько часовой просмотр потокового видео за каждый день транзакций Биткойна, но при этом он обеспечивает пользователям полную автономность.

Облегченный клиент

Облегченный клиент, или клиент с упрощенной проверкой платежей (Simplified-Payment-Verification, SPV), подключается к полноценному клиенту либо другому удаленному серверу для получения и отправки информации о транзакциях биткойна, но в то же время обеспечивает локальное хранение пользовательского кошелька, частичную проверку получаемых транзакций и независимое создание исходящих транзакций.

Сторонний API-клиент

Сторонний API-клиент предназначен для взаимодействия с сетью Биткойн через систему API сторонних разработчиков, а не путем прямого подключения. Кошелек может храниться у пользователя или на сторонних серверах, но при этом клиент полностью доверится удаленному серверу, который будет передавать ему точную информацию и защищать его конфиденциальность.

Биткойн является одноранговой (пиринговой – peer-to-peer, P2P) сетью. Полноценные узлы (клиенты) сети – это равноправные пользователи (пиры): каждый из них индивидуально проверяет достоверность всех подтвержденных транзакций и может предоставлять данные своему пользователю с максимальной степенью достоверности. Облегченные кошельки и другое программное обеспечение являются *клиентами*: каждый клиент зависит от одного или нескольких пиров, которые предоставляют ему достоверные данные. Биткойн-клиенты могут выполнять вторичную проверку некоторой части получаемых ими данных и устанавливать соединения с несколькими пирами для уменьшения зависимости от подлинности отдельного пира, но в конечном итоге безопасность клиента зависит от надежности его пиров.

Кто контролирует ключи

Очень важным аспектом является вопрос о том, *кто контролирует ключи*. Как будет показано в последующих главах, доступ к биткойнам контролируется «секретными ключами» (private keys), которые похожи на очень длинные PIN-коды. Если вы единственный, кто имеет право распоряжаться этими секретными ключами, значит, вы контролируете свои биткойны. И наоборот, если контроль над ними вам не принадлежит, вашими биткойнами управляет третье лицо, которое в конечном итоге контролирует ваши средства от вашего имени. Программное обеспечение для управления ключами разделяется на две важные категории по принципу контроля: *кошельки*, где ключи и денежные средства вы контролируете, и счета в хранилищах, где ключами управляет третья сторона. Чтобы особо отметить этот момент, один из авторов (Андреас) придумал такую фразу: *Твои ключи – твои монеты* (Your keys, your coins). *Не твои ключи – не твои монеты*.

Если совместить все эти классификации, можно выделить несколько основных типов биткойн-кошельков, среди которых наиболее распространены три: полнофункциональные кошельки (сетевые узлы) для настольных компьютеров (вы контролируете ключи), облегченные мобильные кошельки (вы контролируете ключи) и веб-аккаунты сторонних разработчиков (вы не контролируете ключи). Границы между различными категориями иногда размыты, поскольку программы работают на разных платформах и могут по-разному взаимодействовать с сетью.