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 Арраис (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-