

АНДРЕАС АНТОНОПУЛОС

СТАНЕТЕ БИТКОЙН ЕКСПЕРТ
ПРОГРАМИРАНЕ НА ОТВОРЕНИЯ БЛОКЧЕЙН

София, 2019

Преводът е направен по изданието:

Mastering Bitcoin, Second Edition

by Andreas M. Antonopoulos

Published by O'Reilly Media, Inc.

Authorized Bulgarian translation of the English edition of *Mastering Bitcoin, 2E* ISBN 9781491954386

© 2017 Andreas M. Antonopoulos, LLC.

All rights reserved.

This translation is published and sold by permission of O'Reilly Media, Inc., which owns or controls all rights to publish and sell the same.

Логото на О'Райли е регистрирана търговска марка на „О'Райли Медия“. „Станете биткойн експерт“, изображението на корицата и свързаното с книгата търговско оформление са търговски марки на „О'Райли Медия“.

Всички права на български език запазени. Нито една част от тази книга не може да бъде възпроизвеждана или предавана под каквато и да е форма и по какъвто и да било начин без изричното съгласие на „Изток-Запад“.

© Издателство „Изток-Запад“, 2019

© Боян Костов, превод

© Ранди Камър, оформление на корицата

© Дейвид Футато, вътрешно оформление

© Ребека Демарест, илюстрации

ISBN 978-619-01-0450-6

Андреас М. Антонопулос

СТАНЕТЕ БИТКОЙН ЕКСПЕРТ

ПРОГРАМИРАНЕ НА ОТВОРЕНИЯ БЛОКЧЕЙН

Превод от английски

Боян Костов



Beijing Boston Farnham Sebastopol Tokyo **O'REILLY®**

Посветена на майка ми Тереза (1946–2017)

Тя ме научи да обичам книгите и да не се подчинявам сляпо на властта.

Благодаря ти, мамо!

СЪДЪРЖАНИЕ

Предговор	13
Кратък речник	23
1 Въведение	35
Какво е биткойн?	35
История на биткойн	38
Биткойн употреби, потребители и техните истории	39
Първи стъпки	41
Избиране на биткойн портфейл	41
Бърз старт	44
Вашият първи биткойн	46
Откриване на текущата цена на биткойн	47
Изпращане и получаване на биткойн	48
2 Как работи биткойн	51
Трансакции, блокове, добив и блокчейн	51
Биткойн: общ преглед	52
Купуване на чаша кафе	52
Биткойн трансакции	54
Входове и изходи на трансакции	54
Вериги от трансакции	55
Получаване на ресто	56
Често срещани форми на трансакции	57
Изграждане на трансакция	59
Намиране на правилните входове	59
Създаване на изходи	61
Добавяне на трансакцията към счетоводната книга	62
Добив на биткойн	64
Копаене на трансакции в блокове	65
Изхарчване на трансакцията	67

3 Bitcoin Core: референтна имплементация	69
Среда за разработка на биткойн	70
Компилиране на Bitcoin Core от изходния код	71
Избиране на версия на Bitcoin Core	72
Конфигуриране на програмата за компилиране на Bitcoin Core	73
Компилиране на изпълнимите файлове на Bitcoin Core	76
Администриране на възел с Bitcoin Core	77
Първоначално стартиране на Bitcoin Core	79
Конфигуриране на възел с Bitcoin Core	79
Приложно-програмен интерфейс (API) на Bitcoin Core	84
Получаване на информация за състоянието на клиента Bitcoin Core	85
Анализиране и декодиране на трансакции	86
Анализиране на блокове	88
Използване на програмния интерфейс на Bitcoin Core	89
Алтернативни клиенти, библиотеки и инструменти	93
C/C++	93
JavaScript	93
Java	93
Python	94
Ruby	94
Go	94
Rust	94
C#	94
Objective-C	94
4 Ключове, адреси	95
Въведение	95
Криптография с публични ключове и криптовалuti	96
Частни и публични ключове	97
Частни ключове	98
Публични ключове	101
Криптография с елиптични криви	101
Генериране на публичен ключ	104

Биткойн адреси	106
Кодиране с Base58 и Base58Check	108
Формати на ключовете	112
Имплементация на ключове и адреси в Python	119
Усъвършенствани ключове и адреси	123
Криптирани частни ключове (BIP-38)	123
Pay-to-Script Hash (P2SH) и адреси с мултиподписи	124
Персонализирани (vanity) адреси	126
Книжни портфейли	132
5 Портфейли	137
Преглед на технологията на портфейла	137
Недетерминистични портфейли	138
Детерминистични портфейли	139
Йерархични детерминистични (HD) портфейли (BIP-32/BIP-44)	140
Семена и мнемонични кодови думи (BIP-39)	141
Най-добри практики за портфейли	142
Използване на биткойн портфейл	143
Технологията на биткойн портфейла в детайли	144
Мнемонични кодови думи (BIP-39)	144
Създаване на йерархичен детерминистичен портфейл от семе	151
Използване на разширен пуличен ключ в уеб магазин	157
6 Трансакции	163
Въведение	163
Трансакции в детайли	163
Трансакции – зад кулисите	164
Изходи и входи на трансакции	165
Изходи на трансакции	167
Входи на трансакции	170
Такси за трансакции	174
Добавяне на такси към трансакции	177

Скриптове за трансакции и езикът Скрипт	179
Нецялостност по Тюринг	180
Верификация без съхранение на състоянието (stateless)	180
Изграждане на скриптове (заклучващ + отключващ)	181
Pay-to-Public-Key-Hash (P2PKH)	185
Цифрови (ECDSA) подписи	188
Как работят цифровите подписи	189
Верификация на подписа	190
Видове хешове на подпис (SIGHASH)	191
ECDSA математика	194
Значението на случайния принцип при подписите	195
Биткойн адреси, баланси и други абстракции	196
7 Усъвършенствани трансакции и скриптове	201
Въведение	201
Мултиподписи	201
Pay-to-script-Hash (P2SH)	203
P2SH адреси	206
Предимства на P2SH	207
Осребряващ скрипт и валидиране	207
Запис на несвързани с плащане данни	
върху изход с оператор RETURN	208
Времева блокировка	210
Времева блокировка на трансакция (nLocktime)	211
Check Lock Time Verify (CLTV)	212
Относителни времеви блокировки	214
Относителни времеви блокировки с nSequence	215
Относителни времеви блокировки с CSV	217
Median-Time-Past	217
Защита с времева блокировка срещу кражба на такси	218
Скриптове за управление на потока от данни (условни клаузи)	219
Условни клаузи с операционни кодове VERIFY	221
Използване на управление на потока от данни в скриптове	222
Пример за сложен скрипт	223

8 Биткойн мрежата	227
Архитектура на мрежа тип „peer-to-peer“	227
Типове и роли на възли	228
Разширената биткойн мрежа	229
Биткойн предавателни мрежи (Relay Networks)	232
Откриване на мрежата	233
Пълни възли	237
Обмен на „инвентар“	238
Възли за опростена проверка на плащане (SPV)	240
Блум филтри	243
Как работят блум филтрите	244
Как възлите за опростена проверка на плащане използват блум филтри	247
Възли за опростена проверка на плащане и поверителност	249
Криптирани и автентифицирани връзки	249
Tor транспорт	250
Peer-to-Peer автентификация и криптиране	250
Басейни с трансакции	251
9 Блокчейн	253
Въведение	253
Структура на блок	254
Блоков хедър	255
Идентификатори на блока: хеш на блоковия хедър и височина на блока	256
Първичният блок	257
Свързване на блокове в блокчейн	258
Дърво на Меркел	259
Дървета на Меркел и опростена проверка на плащане (SPV)	266

Тестовите блокчейни на биткойн	267
Testnet – тестовата площадка на биткойн	267
Segnet – testnet за отделен свидетел	269
Regtest – локалният блокчейн	270
Използване на тестовите блокчейни за разработка	271

10 Добив на биткойн и консенсус 273

Въведение	273
Икономика на биткойн и създаване на валута	275
Децентрализиран консенсус	276
Независима верификация на трансакции	278
Добивни възли	280
Агрегиране на трансакции в блокове	281
Coinbase трансакция	282
Coinbase възнаграждение и такси	284
Структура на coinbase трансакция	285
Coinbase данни	286
Създаване на блоков хедър	288
Добив на блок	290
Алгоритъм на доказателство-за-работа	290
Представяне на целта	297
Промяна на целта за коригиране на сложността	298
Успешен добив на блок	300
Валидиране на нов блок	301
Асемблиране и избор на вериги от блокове	302
Блокчейн разклонение (fork)	304
Добив на биткойн и надпревара между хеширащи мощности	311
Решение с допълнителни стойности на еднократен код (nonce)	314
Басейни за добив на биткойн	314
Консенсусни атаки	319
Промяна на консенсусните правила	323
Твърдо (окончателно) разклонение	323

Твърдо разклонение: софтуер, мрежа, добив и верига	325
Разделяне на копачи и сложност	327
Спорни твърди разклонения	328
Меко (частично) разклонение	329
Критика на меките разклонения	330
Сигнализация с блокова версия на меко разклонение	331
Сигнализация и активиране на BIP-34	332
Сигнализация и активиране на BIP-9	333
Разработка на консенсусен софтуер	336
11 Биткойн сигурност	339
Принципи на сигурност	339
Разработване на защитени биткойн системи	340
Коренът на доверието	342
Най-добри практики за защита на потребителите	343
Физическо съхранение на биткойн	344
Хардуерни портфейли	345
Балансиране на риска	345
Диверсифициране на риска	345
Мултиподписи и управление	346
Оцеляване	346
Заклучение	346
12 Блокчейн приложения	347
Въведение	347
Градивни блокове (примитиви)	348
Приложения от градивни блокове	351
Colored coins („цветни“ монети)	351
Използване на „цветни“ монети	352
Емитиране на „цветни“ монети	353
Трансакции с „цветни“ монети	354
Counterparty	357
Канали за плащане истейт канали	358

Стейт канали – основни понятия и терминология	359
Пример за прост канал за плащане	361
Създаване на канали без нужда от доверие (trustless)	364
Асиметрични отменяеми обвързвания	367
Hash Time Lock Contracts (HTLC)	372
Маршрутизирани канали за плащане (Светкавична мрежа)	373
Пример за проста Светкавична мрежа	374
Светкавична мрежа: транспорт и маршрутизация	377
Ползи от Светкавичната мрежа	379
Заклучение	381

Приложения

А. „Бялата книга за биткойн“ от Сатоши Накамото	383
Б. Оператори, константи и символи на езика Биткойн Скрипт	397
В. Предложения за подобрене на биткойн	403
Г. Отделен свидетел	413
Д. Bitcore	429
Е. Pуcoin, ku и tx	433
Ж. Команди на Bitcoin Explorer (bx)	443

Показалец	447
------------------	------------

Написването на книгата за биткойн

За пръв път се сблъсках с биткойн в средата на 2011 г. Непосредствената ми реакция беше нещо от сорта на „Хмм! Смешни пари!“ и аз ги пренебрегнах в продължение на още шест месеца, без да успея да схвана важността им. Това е реакция, която съм виждал отново и отново сред мнозина от най-умните ми познати, което ми носи известна утеха. Втория път, когато се натъкнах на биткойн – в един дискуссионен форум, реших да прочета написаната от Сатоши Накамото „Бяла книга“, за да проуча най-достоверния източник и да видя за какво всъщност става дума. Все още си спомням момента, в който приключих с прочитането на тези девет страници и разбрах, че биткойн не е просто цифрова валута, а мрежа на доверие, която може да осигури основа за далеч повече от обикновени валути. Осъзнаването, че „това не са пари, а децентрализирана мрежа на доверие“, ме накара да се впусна в четиринадесетно пътешествие, по време на което поглъщах всяка частица информация за биткойн, която успях да намеря. Бях обсебен и очарован, прекарвах 12 и повече часа на ден пред монитора, като четях, пишех, програмирах и учех колкото е възможно повече.

Излязох от това дисоциативно състояние отслабнал с 10 килограма поради липсата на редовно хранене, но решен да се посветя на работата си върху биткойн.

Две години по-късно, след като създадох няколко малки стартап компании, за да проуча различни услуги и продукти, свързани с биткойн, реших, че е време да напиша първата си книга. Биткойн беше темата, която събуди креативността ми и превзе мислите ми; това беше най-вълнуващата технология, с която се бях сблъсквал след появата на интернет. Беше настъпило време да споделя страстта си към тази невероятна технология с по-широка аудитория.

Целева публика

Тази книга е предназначена предимно за програмисти. Ако можете да използвате език за програмиране, тя ще ви научи как функционират криптографските валути, как да ги използвате и как да разработвате софтуер, който работи с тях. Първите няколко глави обаче са задълбочено въведение в света на

биткойн, подходящо и за непрограмисти – онези, които се опитват да разберат биткойн и криптовалутите в дълбочина.

Защо на корицата има буболечки?

Мравката листорез е вид, който проявява изключително сложно поведение в суперорганизма на колонията, но всяка отделна мравка работи, следвайки набор от прости правила, управлявани от социално взаимодействие и обмен на химически аромати (феромони). Според „Уикипедия“: „Наред с хората, мравките създават най-големите и най-сложните животински общества на Земята“. Мравките листорези всъщност не ядат листа, а по-скоро ги използват за отглеждане на гъби, които са основен източник на храна за колонията. Схващате ли? Тези мравки се занимават със земеделие!

Въпреки че мравките образуват основано на касти общество и имат краллица за създаване на потомство, в мравешката колония няма централна власт или лидер. Високоинтелигентното и сложно поведение, което проявява многомилионната колония, е емергентно свойство*, породено от взаимодействието на индивиди в социална мрежа.

Природата демонстрира, че децентрализираните системи могат да бъдат устойчиви и да развият емергентна комплексност и невероятна усъвършенстваност, без да се нуждаят от централна власт, йерархия или сложни компоненти.

Биткойнът е изключително сложна децентрализирана мрежа на доверие, която може да поддържа безкрайно много финансови процеси. Всеки възел** в биткойн мрежата обаче следва няколко прости математически правила. Взаимодействието между много възли е това, което води до емергентност на сложно поведение, а не някаква вродена комплексност или доверие в някой отделен възел. Подобно на мравешката колония, биткойн мрежата е еластична мрежа от прости възли, следващи прости правила, които заедно могат да правят невероятни неща без каквато и да е централна координация.

* Емергентност е случайното и неочаквано възникване (формиране) на ново качество в сложна система, което не произтича от качествата на съставните ѝ елементи.

** Възелът (наричан още връх, точка и нод; от англ. node) е основен елемент на всяка структура от данни, представляващ отделно устройство (например компютър), част от по-голяма мрежа.

Конвенции, използвани в тази книга

В тази книга се използват следните типографски конвенции:

Курсив

Обозначава нови термини, URL* адреси, имейл адреси, имена на файлове и разширения на файлове.

Разширен и смален (Constant width)

Използва се за програмни регистри, както и за обозначаване на програмни елементи като имена на променливи или функции, бази данни, типове данни, променливи на средата, команди и ключови думи.

Разширен, смален и удебелен (Constant width bold)

Обозначава команди или друг текст, който трябва да бъде написан буквално от потребителя.

Разширен, смален и в курсив (Constant width italic)

Обозначава текст, който трябва да бъде заменен с предоставени от потребителя стойности или със стойности, определени от контекста.



Тази икона означава пояснение.



Тази икона означава бележка.



Тази икона означава предупреждение.

* Унифицираният локатор на ресурси (URL) е стандартизиран указател за мрежовия адрес на даден ресурс, например документ или страница в интернет.

Примерни кодове

Дадените примери са на Python и C++ и използват текстовия интерфейс на Юникс-подобна операционна система като Линукс или тази на Макинтош (macOS). Всички кодови фрагменти са достъпни в хранилището на GitHub (<https://github.com/bitcoinbook/bitcoinbook>) в поддиректорията за кодове (*code*) на главното хранилище. Разклонете кода от книгата, изпробвайте примерните кодове или ни пратете корекции чрез GitHub.

Всички кодови фрагменти могат да бъдат възпроизведени на повечето операционни системи с минимум инсталации на компилатори и интерпретатори за съответните езици. Където е необходимо, предоставяме базови инструкции за инсталиране и постъпкови примери за резултата от тези инструкции.

Някои от кодовите фрагменти и изходни кодове са преформатирани за печат. Във всички такива случаи редовете са разделени с обратно наклонена черта (\), последвана от символ за нов ред. Когато преписвате примерите, премахнете тези два знака и съединете отново редовете, и би трябвало да получите идентични резултати като показаното в примера.

Всички кодови фрагменти използват реални стойности и изчисления, когато е възможно, така че да можете да конструирате пример след пример и да виждате същите резултати във всеки код, който записвате, стига да използвате същите стойности за калкулациите. Частните ключове и съответните публични ключове и адреси например са реални. Всички примерни трансакции, блокове и референции към блокчейна са въведени в същинския блокчейн и са част от публичната счетоводна книга (регистър), така че можете да ги прегледате на всяка биткойн система.

Използване на примерни кодове

Тази книга е тук, за да ви помогне да свършите работата си. Като цяло, ако в тази книга се предлага примерен код, можете да го използвате във вашите програми и документация. Не е нужно да се свързвате с нас за разрешение, освен ако не възпроизвеждате значителна част от кода. Написването на програма, която използва няколко фрагмента код от тази книга например, не изисква разрешение. Продажбата или разпространението на компактдиск с примери от книгите на „О’Райли“ изисква разрешение. Отговорът на въпрос, при който цитирате тази книга и цитирате примерен код, не изисква разрешение. Включването на значително количество примерен код от тази книга в документацията на ваш продукт обаче изисква разрешение.

Приветстваме, но не се нуждаем от признание. Признанието обикновено включва заглавието, автора, издателя и ISBN. Например: „Станете биткойн

експерт“ от Андреас М. Антонопулос („О’Райли“). Авторско право 2017 Андреас М. Антонопулос, 978-1-491-95438-6.

Някои издания на тази книга се предлагат под лиценз с отворен код, като например CC-BY-NC (<https://creativecommons.org/licenses/by-nc/4.0/>), в който случай се прилагат условията на този лиценз.

Ако смятате, че използването на примерите с код не спазва правилата за честна употреба или даденото по-горе разрешение, можете да се свържете с нас на адрес permissions@oreilly.com.

Биткойн адреси и трансакции в тази книга

Биткойн адресите, трансакциите, ключовете, QR кодовете и блокчейн данните, използвани в тази книга, са реални в по-голямата си част. Това означава, че можете да разглеждате блокчейна, да разглеждате предложените като примери трансакции, да ги извличате със собствени скриптове или програми и т.н.

Имайте предвид обаче, че частните ключове, използвани за изграждане на адреси, или са отпечатани в тази книга, или са „изгорени“. Това означава, че ако изпратите пари на някой от тези адреси, парите ви ще бъдат загубени завинаги, а в някои случаи всеки, който прочете книгата, може да ги използва с помощта на отпечатаните тук частни ключове.



НЕ ИЗПРАЩАЙТЕ ПАРИ НА НИКОЙ ОТ АДРЕСИТЕ В ТАЗИ КНИГА. Вашите пари ще бъдат взети от друг читател или ще бъдат загубени завинаги.

О’Райли Сафари



„Сафари“ (преди „Safari Books Online“) е платформа за обучение и справки на членски принцип за частни предприятия, държавни организации, педагози и обикновени потребители.

Членовете ѝ имат достъп до хиляди книги, учебни видеоклипове, пътеки на обучение, интерактивни уроци и подобрени списъци от над 250 издатели, включително „О’Райли Медия“, „Харвард Бизнес Ревю“, „Прентис Хол Профешънъл“, „Адисън-Уесли Профешънъл“, „Майкрософт Прес“, „Самс“, „Кю“, „Пичпит Прес“, „Адоуби“, „Фокал Прес“, „Сиско Прес“, „Джон Уайли & Сонс“, „Сингрес“, „Морган Кауфман“, „Ай Би Ем Редбукс“, „Пакт“, „Адоуби Прес“, „Еф Ти Прес“, „Апрес“, „Манинг“, „Ню Райдърс“, „МакГроу-Хил“, „Джоунс & Бартлет“, „Корс Текнолоджи“ и много други.

За повече информация посетете <http://oreilly.com/safari>.

Как да се свържете с нас

Моля, адресирайте коментарите и въпросите относно тази книга до издателя:

O'Reilly Media Inc.
1005 Gravenstein Highway North
Sebastopol, CA 95472
800-998-9938 (в САЩ или Канада)
707-829-0515 (международен или местен)
707-829-0104 (факс)

За да коментирате или зададете технически въпроси относно тази книга, изпратете имейл на bookquestions@oreilly.com.

За повече информация относно нашите книги, курсове, конференции и новини вижте нашия уебсайт на <http://www.oreilly.com>.

Намерете ни във фейсбук: <http://facebook.com/reilly>

Следвайте ни в твитър: <http://twitter.com/reillymedia>

Гледайте ни в ютюб: <http://www.youtube.com/reillymedia>

Контакт с автора

Можете да се свържете с мен, Андреас М. Антонопулос, на моя личен сайт: <https://antonopoulos.com/>

Информация за „Станете биткойн експерт“, както и свободно достъпното издание и преводи може да намерите на: <https://bitcoinbook.info/>

Следвайте ме във фейсбук: <https://facebook.com/AndreasMAntonopoulos>

Следвайте ме в твитър: <https://twitter.com/aantonop>

Следвайте ме в линкдин: <https://linkedin.com/company/aantonop>

Много благодаря на всички мои спонсори, които подкрепят работата ми чрез месечни дарения. Можете да проследите страницата ми в Патреон тук: <https://patreon.com/aantonop>

Благодарности

Тази книга е резултат от усилията и приноса на много хора. Благодарен съм за цялата помощ, която получих от приятели, равнопоставени партньори и дори напълно непознати, които се присъединиха към мен в това усилие да напиша техническа книга-еталон за криптовалутите и биткойн.

Невъзможно е да се направи разграничение между технологията на биткойна и биткойн общността, и тази книга е не по-малко продукт на тази общност, отколкото книга за технологията. Работата ми върху тази книга беше

окуражавана, приветствана, подкрепяна и възнаградена от цялата биткойн общност от самото начало до самия край. Повече от всичко, тази книга ми позволи в продължение на две години да бъде част от тази чудесна общност и не мога да ви благодаря достатъчно, че ме приехте в нея. Има твърде много хора, които трябва да спомена по име – хора, които срещях на конференции, събития, семинари, срещи в пицарии и малки частни събирания, както и много хора, с които комуникирах посредством туитър, reddit, bitcoin-talk.org и GitHub и които оказаха влияние върху тази книга. Всяка идея, аналогия, въпрос, отговор и обяснение, които откривате в тази книга, в някакъв момент бяха вдъхновени, проверени или подобрени вследствие на взаимоотношенията ми с общността. Благодаря ви за подкрепата; без вас тази книга не би се случила. Аз съм ви вечно благодарен.

Разбира се, моето пътуване към превръщането ми в писател започва много преди първата ми книга. Първият ми език (и образование) беше гръцкият, така че през първата си година в университета трябваше да положа курс по английски език. Дълга благодарности на моята учителка по английски Даяна Кордас, която ми помогна да изградя увереност и умения през тази първа година. По-късно, вече професионалист, развих уменията си в сферата на техническата литература по темата за центровете за данни, пишейки за списание „Нетуърк Уърлд“. Дълга благодарности на Джон Дикс и Джон Галънт, които ме назначиха на първата ми работа, свързана с писане, като журналист в „Нетуърк Уърлд“; на моя редактор Майкъл Куни и колежката ми Джона Тил Джонсън, които редактираха моите статии и ги правеха подходящи за публикуване. Писането на 500 думи на седмица в продължение на четири години ми осигури достатъчно опит, за да обмисля в крайна сметка дали да не стана писател.

Благодаря и на онези, които ме подкрепиха, когато изпратих предложението си за тази книга на „О’Райли“, като предоставиха препоръки и прегледаха предложението. Благодаря по-конкретно на Джон Галънт, Грегъри Нес, Ричард Стийнън, Джоел Снайдер, Адам Б. Левин, Сандра Гитлен, Джон Дикс, Джона Тил Джонсън, Роджър Вър и Джон Матонис. Специални благодарности на Ричард Кейган и Тимон Матошко, които прегледаха ранните версии на предложението, и на Матю Тейлър, който го редактира.

Благодаря на Крикет Лу, автор на издадената от „О’Райли“ „DNS and BIND“, който ме запозна с О’Райли. Благодаря също така на Майкъл Лукидис и Алисън Макдоналд от „О’Райли“, които работиха в продължение на цели месеци, за да помогнат за осъществяването на тази книга. Алисън беше особено търпелива, когато животът се намеси в плановите ни и бяха пропуснати крайни срокове, и всичко се забави. За второто издание благодаря на Тимъти Макгавърн за начина, по който ръководеше процеса, на Ким Кофър за търпеливото редактиране и на Ребека Панцер за илюстриране на многото нови диаграми.

Първите няколко чернови на първите няколко глави бяха най-трудни, защото темата биткойн не е никак лесна за разнищване. Всеки път, когато издърпах някоя нишка от технологията на биткойн, трябваше да разплитам всичко. Няколкократно блокирах и се отчайвах в борбата си да направя темата лесна за разбиране и да изградя разказ около такъв крайно технически въпрос. В крайна сметка реших да разкажа историята на биткойн чрез историите на хората, използващи биткойн, и цялата книга стана много по-лесна за написване. Дълга благодарности на моя приятел и наставник Ричард Кейган, който ми помогна да разкажа историята и да преодолее моментите, в които блокирах. Благодаря на Памела Морган, която прегледа ранните чернови на всяка глава от първото и второто издание на книгата и зададе трудните въпроси, с които ми помогна да ги направя по-добре. Благодаря също така на разработчиците от групата San Francisco Bitcoin Developers Meetup (вижте <https://www.meetup.com/>), както и на Тарик Люис и Денис Тери за това, че помогнаха за проверката на първоначалното съдържание на книгата. Благодаря и на Андрю Ноглър за дизайна на информационните графики.

По време на разработването на книгата публикувах предварително издание – чернова на GitHub и помолих посетителите да споделят с мен своите съвети и коментари. В отговор на това получих повече от сто коментара, предложения, корекции и различни други приноси. Благодаря на всички съдействали поименно в „Предварително издание (съдействали на GitHub)“ на страница 21. Преди всичко, моите искрени благодарности на моите редактори доброволци от GitHub Мин Т. Нгуен (първо издание) и Уил Бинс (второ издание), които работеха неуморно, за да обработват, управляват и решават заявки за теглене, издават доклади и извършват корекции на грешки в GitHub.

След като книгата бе завършена, тя премина през няколко кръга на технически преглед. Благодаря на Крикет Лиу и Лоум Ланц за задълбочения им анализ, коментари и подкрепа.

Няколко разработчици на биткойн предоставиха примерни кодове, коментари, забележки и насърчения. Благодаря на Амир Таки и Ерик Воскуил за примерните кодови фрагменти и многото страхотни коментари; на Крис К्लешулте за предоставянето на приложението за Bitcore; на Виталик Бутерин и Ричард Кис за помощта с математиката на елиптичните криви и за кодовите примери; на Гавин Андресън за корекциите, коментарите и насърченията; на Михалис Каргакис за коментарите и за помощта с имплементацията btcd; и на Робин Инг за списъка с печатни грешки, с помощта на който подобрихме второто издание. За второто издание отново получих доста помощ от много разработчици на Bitcoin Core, включително Ерик Ломброзо, който демистифицира Отделения свидетел, Люк Дашър, който помогна за подобряването на главата за трансакциите, Джонсън Лау, който прегледа някои глави, вклю-

чително тази за Отделения свидетел, и много други. Дълга благодарности на Джоузеф Пуун, Тадеус „Тадж“ Драйджа и Олаолуа Осунтокун, които ми обясниха Светкавичната мрежа, преглеждаха написаното от мен и отговаряха на въпросите ми, когато изпадах в затруднение.

Дълга любовта си към думите и книгите на моята майка Тереза, която ме отгледа в къща със стени, заети от горе до долу с книги. Майка ми също така купи първия ми компютър през 1982 г., въпреки че е самообявил се технофоб. Баща ми Менелаос, строителен инженер, който току-що публикува първата си книга на 80-годишна възраст, беше този, който ме научи на логическо и аналитично мислене и любов към науката и инженерството.

Благодаря ви, че ме подкрепяхте по време на това пътуване.

Предварително издание (съдействали на GitHub*)

Много хора допринесоха, предлагайки коментари, корекции и допълнения към предварително издание на GitHub. Благодаря на всички за техния принос към тази книга.

Следва списък на всички, които ни оказаха впечатляващо съдействие в GitHub, включително тяхното GitHub потребителско име в скоби:

- Алекс Уотърс (alexwaters)
- Андрю Доналд Кенеди (grkvlt)
- bitcoinctf
- Брайън Гмирек (physicsdude)
- Кейси Флин (cflynn07)
- Чапман Шуп (belovachap)
- Кристи Д'Ана (avocadobreath)
- Коуди Скот (Siecje)
- coinradar
- Крейгин Годли (cgodley)
- dallyshalla
- Диего Виола (diegoviola)
- Дърк Йакел (biafra23)
- Димитрис Цапакидис (dimitris-t)
- Дмитрий Маракасов (AMDmi3)
- drstrangeM
- Ед Ейкхолт (edeykholt)
- Ед Лийфи (EdLeafe)
- Едуард Поснак (edposnak)
- Елиас Родригес (elias19r)
- Ерик Воскуил (evoskuil)
- Ерик Уинчел (winchell)
- Ерик Уолстром (erikwam)
- effectsToCause (vericoins)

* GitHub е уеб-базирана услуга за разполагане на софтуерни проекти и техни съвместни разработки (най-вече с общодостъпен или отворен код) върху отдалечен интернет сървър в софтуерно хранилище.

- effectsToCause (vericoiñ)
- Естебан Ордано (eordano)
- ethers
- fabienhinault
- Франк Хьогер (francyi)
- Горав Рана (bitcoinsSG)
- genjix
- halseth
- Холгер Шинцел (schinzelh)
- Йоанис Черувим (cherouvim)
- Иш От Джуниър (ishotjr)
- Джеймс Адисън (jayaddison)
- Джеймсън Лоп (jlopp)
- Джейсън Бистърфелд (jbisterfeldt)
- Хавиер Рохас (fjrojasgarcia)
- Джереми Бокобза (bokobza)
- JerJohn15
- Джо Бауърс (joebauers)
- joflynn
- Джонсън Лау (jl2012)
- Джонатан Крос (jonathancross)
- Jorgeminator
- Кай Бакър (kaibakker)
- Май-Хсуан Чиа (mhchia)
- Марциг (marzig76)
- Максимилиан Райхел (phramz)
- Михалис Каргакис (kargakis)
- Майкъл С. Иполито (michaelcippolito)
- Михаил Русу (MihailRussu)
- Мин Т. Нгуен (enderminh)
- Нагарай Хубли (nagarajhubli)
- Некомата (nekomata-3)
- Робърт Фърс (Rfurse)
- Ричард Кис (richardkiss)
- Рубен Александър (hizzvizz)
- Сам Ричи (sritchie)
- Сергей Котлиар (ziggamon)
- Сейчи Учида (topecongiro)
- Симон де ла Рувиер (simondlr)
- Стивън Оесте (Emzy)
- takaya-imai
- Тиаго Араис (thiagoarraiz)
- venzen
- Уил Бинс (wbnnns)
- wintercooled
- wjx
- Войчек Лангиевич (wlk)
- yurigeorgiev4