

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“.

Всяки 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
Копане 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 криптовалута	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 ВІР-34	332
Сигнализация и активиране на ВІР-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
Заключение	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 и стейт 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 „Хммм! 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 четиримесечно 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 кралица за създаване на потомство, в мравешката колония няма централна власт или лидер. Високоинтелигентното и сложно поведение, което проявява милионната 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.