

УДК 004.738.5:336.74Bitcoin
ББК 32.971.35+65.262.6с
А72

Антонопулос А. М.

А72 Осваиваем биткойн / пер. с англ. А. В. Снастина. – М.: ДМК Пресс, 2018. – 428 с.: ил.

ISBN 978-5-94074-965-3

Второе издание бестселлера включает подробное введение в самую известную криптовалюту – биткойн, а также в лежащую в ее основе технологию блокчейна. Приведено описание технических основ биткойна и других валют, описание децентрализованной сети биткойн, пиринговой архитектуры, жизненного цикла транзакций и принципов обеспечения безопасности. Показаны методики разработки блокчейн-приложений с многочисленными примерами кода.

Книга будет интересна разработчикам, инженерам, архитекторам программных и прочих систем, а также всем, кто хочет глубже узнать о криптовалютах и блокчейн-технологиях.

УДК 004.738.5:336.74Bitcoin
ББК 32.971.35+65.262.6с

Authorized Russian translation of the English edition of Mastering Bitcoin, 2nd Edition ISBN 9781491954386 © 2017 Andreas M. Antonopoulos LLC.

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.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

ISBN 978-1-491-95438-6 (англ.)
ISBN 978-5-94074-965-3 (рус.)

Copyright © 2017 Andreas M. Antonopoulos LLC
© Оформление, издание, перевод, ДМК Пресс, 2018

Содержание

Предисловие	14
Благодарности	19
 Глава 1. Введение.....	 24
Что такое биткойн	24
История создания биткойна	27
Варианты использования биткойнов, пользователи и их истории	29
Начинаем обучение	30
Выбор биткойн-кошелька	31
Сразу переходим к делу	33
Получаем свой первый биткойн.....	35
Поиск информации о текущей стоимости биткойна.....	36
Отправка и получение биткойна.....	37
 Глава 2. Как работает биткойн.....	 40
Транзакции, блоки, майнинг и блокчейн	40
Общий обзор биткойн-системы	40
Покупка чашки кофе	41
Транзакции биткойна	43
Входные и выходные данные транзакции.....	43
Цепочки транзакций	44
Получение сдачи.....	45
Общие формы транзакций	46
Создание транзакции	47
Формирование правильных входных данных.....	48
Формирование выходных данных	49
Добавление транзакции в реестр	51
Майнинг биткойнов	52
Майнинг транзакций в блоках.....	54
Расходование транзакции.....	56
 Глава 3. Bitcoin Core: эталонная реализация.....	 58
Среда разработки биткойна.....	59

Компиляция Bitcoin Core из исходных кодов	60
Выбор версии Bitcoin Core	60
Конфигурирование компилируемой версии Bitcoin Core	61
Сборка выполняемых файлов Bitcoin Core	64
Запуск узла Bitcoin Core.....	65
Самый первый запуск Bitcoin Core.....	67
Конфигурирование узла Bitcoin Core	67
Прикладной программный интерфейс (API) Bitcoin Core	72
Получение информации о состоянии клиента Bitcoin Core	73
Обработка и расшифровка транзакций	74
Исследование блоков.....	76
Использование программного интерфейса Bitcoin Core.....	77
Прочие клиенты, библиотеки и инструментальные пакеты	80
C/C++.....	80
JavaScript	80
Java.....	81
Python.....	81
Ruby	81
Go	81
Rust.....	81
C#	81
Objective-C.....	82
Глава 4. Ключи и адреса	83
Введение.....	83
Криптография с открытым ключом и криптовалюта	84
Секретный ключ и открытый ключ.....	85
Секретные ключи.....	86
Открытые ключи	88
Криптография с использованием эллиптических кривых.....	89
Генерация открытого ключа	91
Биткойн-адреса	93
Форматы кодирования Base58 и Base58Check.....	94
Форматы ключей	99
Реализация ключей и адресов на языке Python	105
Усовершенствованные ключи и адреса.....	108
Зашифрованные секретные ключи (BIP-38).....	109
Адреса скриптов Pay-to-Script Hash (P2SH) и адреса мультиподписей	110
«Престижные» адреса.....	112

Глава 5. Кошельки	121
Общий обзор технологии кошельков	121
Недетерминированные кошельки (со случайным выбором ключей)	122
Детерминированные кошельки (с источником)	123
HD-кошельки (BIP-32/BIP-44)	123
Источники и мнемонические коды (BIP-39)	125
Оптимальные практические методики технологии кошельков	125
Практическое использование биткойн-кошелька	126
Подробности технологии кошельков	128
Мнемонические кодовые слова (BIP-39).....	128
Создание HD-кошелька из источника.....	134
Использование расширяемого открытого ключа в веб-магазине	139
 Глава 6. Транзакции	 146
Введение.....	146
Транзакции в подробностях	146
Транзакции – что внутри	147
Входные и выходные данные транзакции.....	148
Выходные данные транзакции	150
Входные данные транзакции.....	153
Оплата транзакций.....	156
Добавление сумм оплаты в транзакции	160
Скрипты транзакций и язык Script	161
Неполнота по Тьюрингу	162
Верификация без сохранения состояния.....	162
Формирование структуры скрипта (Lock + Unlock).....	162
Скрипт Pay-to-Public-Key-Hash (P2PKH)	167
Цифровые подписи (ECDSA).....	169
Как работают цифровые подписи	170
Проверка цифровых подписей	172
Типы хэш-значений подписи (SIGHASH)	172
Математическое обоснование алгоритма ECDSA	175
Важность фактора случайности в цифровых подписях.....	176
Биткойн-адреса, балансы и прочие абстракции	177
 Глава 7. Более сложные транзакции и скрипты	 181
Введение.....	181
Мультиподписи.....	181
Скрипт Pay-to-Script-Hash (P2SH).....	183

Адреса P2SH	186
Преимущества механизма P2SH.....	186
Погашающий скрипт и проверка корректности	187
Запись выходных данных (RETURN)	188
Блокировки по времени (timelocks)	190
Блокирование транзакции по времени (nLocktime)	190
Check Lock Time Verify (CLTV)	191
Относительные блокировки по времени.....	193
Относительные блокировки по времени, устанавливаемые полем nSequence	194
Относительные блокировки по времени с применением параметра CSV	196
Median-Time-Past.....	196
Защита блокировок по времени от нелегального получения отчислений.....	197
Скрипты с управлением потоком выполнения (условные выражения).....	198
Условные выражения с применением оператора VERIFY	200
Использование средств управления потоком выполнения в скриптах	201
Пример сложного скрипта	202
Глава 8. Сеть биткойна	205
Архитектура пиринговой сети.....	205
Типы и роли узлов	206
Расширенная биткойн-сеть	207
Сеть Bitcoin Relay Network.....	209
Обследование биткойн-сети.....	211
Полноценные узлы	215
Взаимная «инвентаризация»	216
Узлы с упрощенной проверкой платежей (SPV).....	218
Фильтр Блума	221
Как работает фильтр Блума	221
Как SPV-узлы применяют фильтры Блума.....	225
SPV-узлы и приватность.....	227
Зашифрованные и защищенные соединения	227
Tor Transport.....	227
Аутентификация и шифрование в пиринговой сети	228
Пулы транзакций	229
Глава 9. Блокчейн	231
Введение.....	231

Структура блока	233
Заголовок блока	233
Идентификаторы блока: хэш-значение заголовка блока и высота блока	234
Первичный блок	235
Связывание блоков в структуру данных блокчейна	236
Деревья Меркле	237
Деревья Меркле и упрощенная верификация платежей (SPV)	244
Тестовые структуры блокчейна в биткойн-системе	244
Testnet – «песочница» для тестирования биткойнов	245
Segnet – тестовая сеть для функции Segregated Witness	247
Regtest – локальная структура данных блокчейна	247
Использование тестовых структур блокчейна для разработки	248

Глава 10. Майнинг и консенсус	249
Введение	249
Экономика биткойна и создание валюты	251
Децентрализованный консенсус	253
Независимая верификация транзакций	254
Узлы майнинга	256
Объединение транзакций в блоки	257
Coinbase-транзакция	258
Вознаграждение coinbase и отчисления за транзакции	260
Структура coinbase-транзакции	261
Данные coinbase	262
Формирование заголовка блока	264
Майнинг блока	265
Алгоритм доказательства выполнения работы (PoW)	266
Представление целевого значения	272
Изменение целевого значения для регулирования уровня сложности	273
Успешный майнинг блока	276
Проверка корректности нового блока	276
Формирование и выбор цепочек блоков	278
Разветвления структуры данных блокчейна	279
Майнинг и конкуренция в хэш-вычислениях	287
Решение с расширением диапазона дополнительных значений nonce	289
Пулы майнинга	290
Атаки на механизм консенсуса	295
Изменение правил консенсуса	299
Устойчивые разветвления	299
Устойчивые разветвления: ПО, сеть, майнинг и цепочка	301

Разделение майнеров и уровень сложности.....	303
Спорные устойчивые разветвления.....	303
Неустойчивые разветвления	304
Критика неустойчивых разветвлений	306
Оповещение о неустойчивом разветвлении с помощью поля версии блока	307
Оповещение и активация по стандарту BIP-34.....	307
Оповещение и активация по стандарту BIP-9.....	308
Разработка программного обеспечения для механизма консенсуса	311
Глава 11. Обеспечение безопасности биткойн-системы	313
Основы обеспечения безопасности	313
Разработка защищенных биткойн-систем	315
Основа доверительных отношений	316
Наиболее эффективные практические методики защиты пользователей.....	317
Физические средства хранения биткойнов.....	318
Аппаратные кошельки	319
Разумный баланс защиты и рисков	319
Диверсификация рисков.....	319
Мультиподпись и управление	320
Жизнеспособность	320
Резюме.....	321
Глава 12. Приложения блокчейна.....	322
Введение.....	322
Базовые элементы	323
Приложения, создаваемые из базовых элементов.....	325
Цветные монеты.....	326
Использование цветных монет	327
Выпуск цветных монет.....	327
Транзакции цветных монет.....	328
Counterparty	331
Каналы платежей и каналы состояний	332
Каналы состояний – основные концепции и терминология.....	333
Пример простого канала платежей.....	335
Создание каналов без доверительных отношений.....	338
Асимметричные отменяемые обязательства	341
Контракты Hash Time Lock Contracts (HTLC)	346
Каналы платежа с маршрутизацией (Lightning Network)	347

Простой пример работы Lightning Network.....	348
Механизмы передачи и маршрутизации в сети Lightning Network.....	351
Преимущества сети Lightning Network	354
Резюме.....	355

Приложение А. Статья о биткойне Сатоши Накамото 356

Биткойн – пиринговая система электронных денег	356
Введение.....	357
Транзакции	357
Сервер меток времени	359
Доказательство выполнения работы.....	359
Сеть.....	360
Стимул	361
Требуемое дисковое пространство.....	362
Упрощенная верификация платежей.....	363
Объединение и разделение сумм транзакций	364
Приватность.....	364
Вычисления.....	365
Резюме.....	368
Ссылки.....	369
Лицензия	369

Приложение Б. Операторы, константы и символы скриптового языка для транзакций Script 371

Приложение В. Предложения по улучшению биткойна (Bitcoin Improvement Proposals) 377

Приложение Г. Функция Segregated Witness (Segwit)..... 383

Зачем нужен механизм Segregated Witness	384
Как работает механизм Segregated Witness	385
Неустойчивое разветвление (обратная совместимость)	386
Примеры использования выходных данных Segregated Witness в транзакциях	386
Обновление ПО для использования Segregated Witness.....	390
Новый алгоритм подписи в механизме Segregated Witness.....	394
Экономические стимулы для использования механизма Segregated Witness	394

Приложение Д. Bitcore	398
Список функциональных возможностей Bitcore.....	398
Примеры использования библиотеки Bitcore	398
Предварительные сведения	398
Примеры кошелька, использующего bitcore-lib.....	399
 Приложение Е. Библиотека rusoin, утилиты ku и tx	 401
Утилита для работы с ключами ku (Key Utility)	401
Утилита для работы с транзакциями (tx).....	407
 Приложение Ж. Команды проводника биткойна bx.....	 410
Примеры практического использования команд проводника bx.....	412
 Предметный указатель.....	 415
Об авторе	427