



Оглавление

Предисловие	10
Вступление	12
Благодарности	15
О книге	17
Кому адресована эта книга	17
Структура книги	18
Соглашения об оформлении кода	19
Прочие онлайн-ресурсы	20
От издательства	20
Об авторе	21
Глава 1. Введение в Биткоин	22
Что такое Биткоин?	22
Общая картина	25
Проблемы современных денег	32
Подход, предлагаемый технологией Биткоин	36
Где можно использовать биткоины?	39
Другие криптовалюты	46
Итоги	48
Глава 2. Криптографические хеш-функции и цифровые подписи	49
Электронная таблица учета жетонов на булочки	50
Криптографические хеши	55
Упражнения	65

Цифровые подписи	67
Повторение	83
Упражнения	85
Итоги	86
Глава 3. Адреса	88
Раскрыты привычки потребления булочек	89
Замена имен открытыми ключами	90
Укорачивание открытых ключей	94
Избегание дорогостоящих опечаток	98
Возвращаемся к конфиденциальности	107
Повторение	108
Упражнения	111
Итоги	113
Глава 4. Кошельки	114
Первая версия кошелька	115
Резервное копирование закрытых ключей	120
Иерархически детерминированные кошельки	124
Назад к резервному копированию	132
Расширенные открытые ключи	137
Создание защищенных закрытых ключей	141
Математика открытого ключа	144
Умножение публичного ключа	145
Повторение	152
Упражнения	154
Итоги	156
Глава 5. Транзакции	157
Проблемы в старой системе	158
Платежи с использованием транзакций	159
Язык сценариев	171
Необычные виды платежей	177
Дополнительные элементы в транзакциях	189
Вознаграждение и создание монет	190
Доверие к Лизе	192
Повторение	195
Упражнения	197
Итоги	199

Глава 6. Блокчейн	200
Лиза может удалять транзакции	201
Построение блокчейна	201
Легкие кошельки	213
Деревья Меркла	224
Безопасность легких кошельков	233
Повторение	236
Упражнения	239
Итоги	242
Глава 7. Доказательство работы	243
Клонирование Лизы	244
Принуждение к честному получению счастливых чисел	255
Майнеры должны уйти	264
Корректировка сложности	268
Какой вред могут принести майнеры?	273
Комиссионные отчисления за транзакции	283
Повторение	290
Упражнения	294
Итоги	295
Глава 8. Одноранговая сеть	296
Общая папка	297
Создание одноранговой сети	298
Как общаются соседние узлы?	301
Сетевой протокол	303
Оставляем в прошлом систему жетонов на булочки	316
Инициализация сети	319
Запуск собственного полного узла	332
Повторение	343
Упражнения	346
Итоги	348
Глава 9. И снова о транзакциях	349
Временная блокировка транзакций	350
Временная блокировка выходов	357
Сохранение данных в блокчейне Биткоин	365
Замена ожидающих транзакций	371
Разные типы подписей	376

Повторение	377
Упражнения	379
Итоги	381
Глава 10. SegWit	382
Проблемы, решаемые с помощью segwit	383
Решения	393
Экономия пропускной способности	411
Совместимость кошельков	412
Еще раз о типах платежей	413
Ограничения блоков	415
Повторение	419
Упражнения	422
Итоги	424
Глава 11. Апгрейды Биткоин	425
Форки в Биткоин	426
Повторение транзакции	438
Механизмы обновления	441
Повторение	456
Упражнения	458
Итоги	460
Приложение А. Использование bitcoin-cli	462
Взаимодействие с bitcoind	462
Графический интерфейс пользователя	464
Знакомство с bitcoin-cli	465
Начало работы	466
Приложение Б. Решения упражнений	477
Приложение В. Веб-ресурсы	495