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

6 Блокчейн

Эта глава охватывает следующие темы:

- ✓ улучшение защищенности электронной таблицы;
- ✓ легкие кошельки;
- ✓ снижение требований к пропускной способности кошельков.

В главе 5 мы обсудили транзакции, которые позволяют любому проверить все сделки, зафиксированные в электронной таблице. Но осталось еще кое-что, чего не могут проверяющие: удаление и цензурирование транзакций Лизой. Как противостоять цензуре, мы обсудим в главах 7 и 8, а в этой главе посмотрим, как лишить Лизу возможности тайком удалять или подменять транзакции.

С этой целью мы заменим электронную таблицу цепочкой блоков — *блокчейном* (рис. 6.1). Блокчейн содержит транзакции, защищенные от подмены путем хеширования и подписания набора транзакций остроумным способом. Этот способ позволяет с легкостью представить криптографическое подтверждение мошенничества, если Лиза удалит или подменит транзакцию. Все проверяющие хранят свои копии блокчейна и могут выполнить его полную проверку, чтобы убедиться, что Лиза не удалила уже подтвержденные транзакции.

В этой главе также представлен легкий кошелек, или кошелек с *упрощенной проверкой платежей* (Simplified Payment Verification, SPV), который будет доверять проверку блокчейна кому-то другому — полному узлу — для экономии пропускной способности и места в памяти. Блокчейн предлагает такую возможность, но она имеет свою цену.

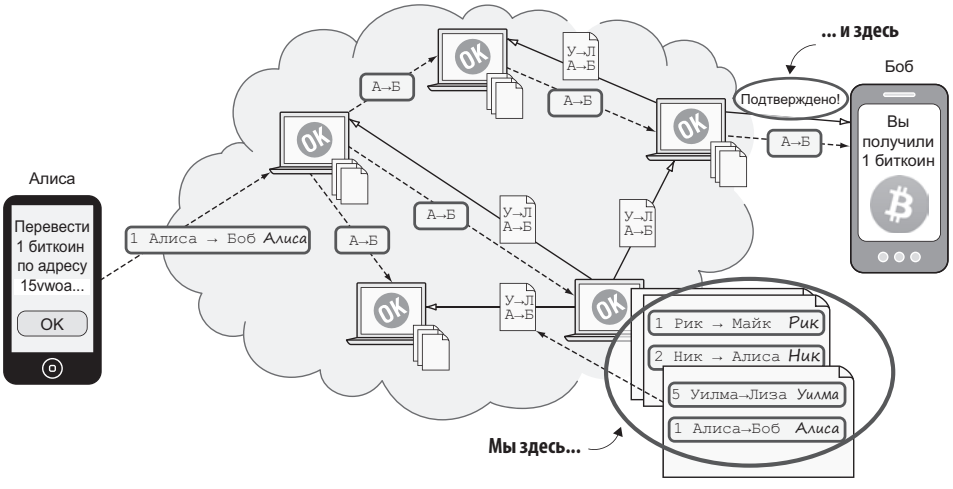


Рис. 6.1. Блокчейн в Биткоин

Лиза может удалять транзакции

Как уже не раз отмечалось, Лиза может удалять транзакции. Например, она может купить булочку в кафе, съесть ее и удалить транзакцию. Конечно, Лиза никогда так не поступит, потому что она самый надежный человек в мире, но не все ее коллеги знают или верят в это. Предположим, что она действительно удалила транзакцию, как показано на рис. 6.2.

Позже, когда в кафе заметят пропажу транзакции, они не смогут доказать, что транзакция Лизы когда-либо присутствовала в электронной таблице. И Лиза не сможет доказать, что ее там не было. Это весьма неприятная ситуация. Разбирательства, когда слово выступает против слова, могут оказаться длительными и дорогостоящими, возможно, с участием адвокатов, полиции, страховых компаний и следователей.

Можно ли доказать, что транзакция была в свое время подтверждена? Лизе нужен какой-то способ, позволяющий опубликовать транзакции и их порядок, чтобы исключить возможность их изменения.

Построение блокчейна

Возможность удаления транзакций обусловлена тем, что никто не сможет доказать, что список транзакций изменялся. Можно ли как-то изменить систему, чтобы получить возможность доказать, что Лиза вмешивалась в историю транзакций?

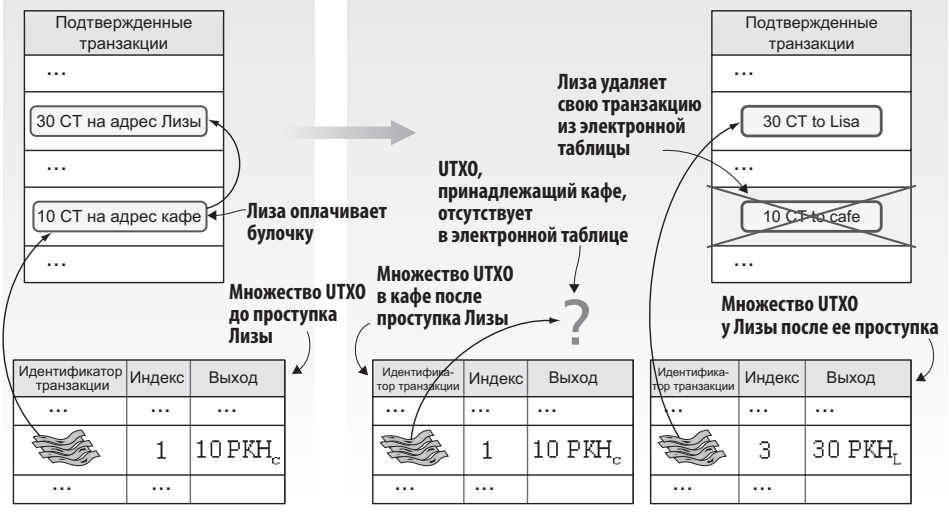


Рис. 6.2. Лиза купила булочку и отменила свою транзакцию. Фактически она украла булочку! В кафе и у Лизы теперь разное множество UTXO

Среди сотрудников нашлись разработчики, предложившие избавиться от электронной таблицы и заменить ее цепочкой блоков — блокчейном (рис. 6.3).

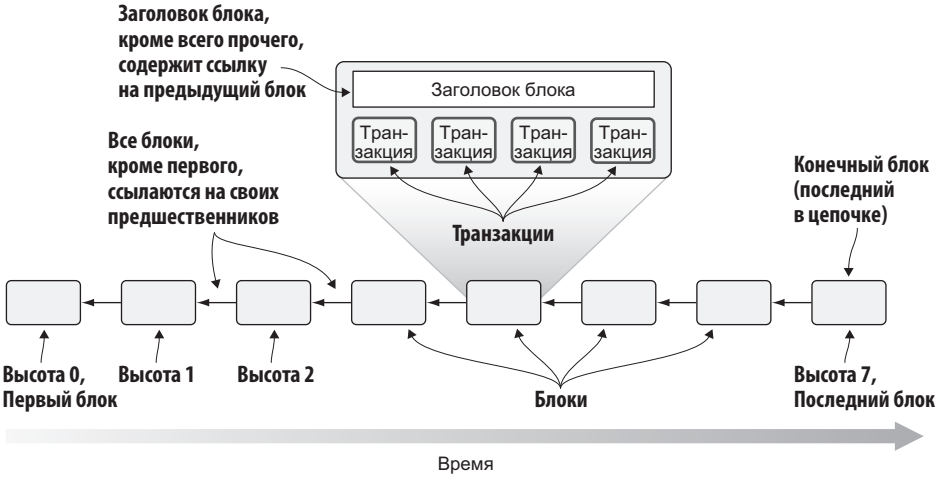


Рис. 6.3. Блокчейн — это цепочка блоков. Блоки содержат группы транзакций, и каждый из них ссылается на предыдущий

Каждый блок в блокчейне ссылается на предыдущий блок и имеет неявную *высоту*, которая указывает, насколько далеко он находится от первого блока. Первый блок имеет высоту 0, второй — высоту 1 и т. д. На рис. 6.3 *конечный*, или последний, блок в блокчейне находится на высоте 7, то есть блокчейн включает 8 блоков. Каждые 10 минут Лиза помещает последние неподтвержденные транзакции в новый блок и делает его доступным для всех, кому это интересно.

ДЛИНА БЛОКЧЕЙНА

Блокчейн в Биткоин содержит сотни тысяч блоков. На момент написания этих строк конечный блок имел высоту 550 836.

Блокчейн хранит транзакции точно так же, как электронная таблица. Но при этом каждый блок имеет *заголовок* для защиты целостности содержащихся в нем транзакций и предшествующих ему блоков. Предположим, что блокчейн на рис. 6.3 вырос и теперь содержит 20 блоков, поэтому конечный блок находится на высоте 19. На рис. 6.4 показано, что содержат последние несколько блоков в блокчейне.

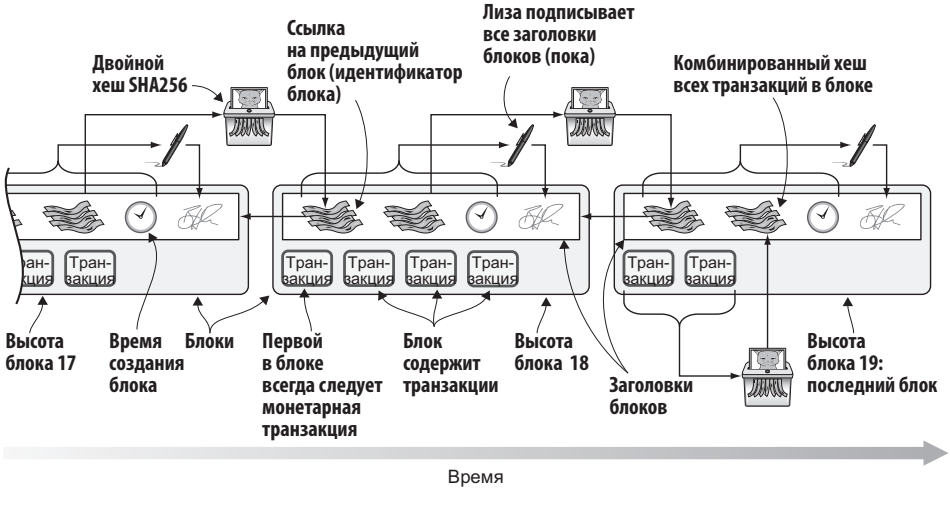
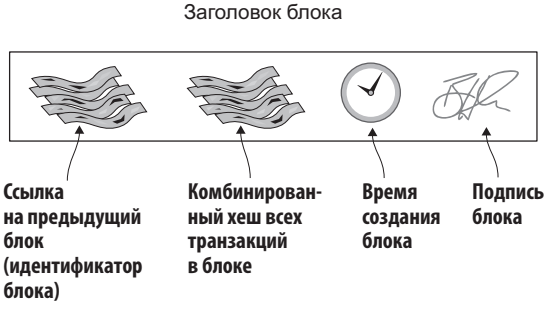


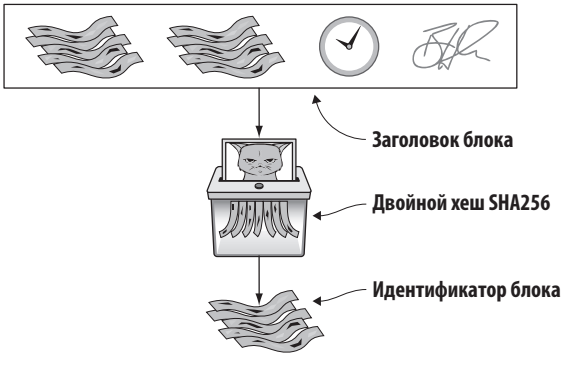
Рис. 6.4. Заголовок каждого блока защищает целостность транзакций в нем и во всех предшествующих блоках

Каждый блок содержит одну или несколько транзакций и заголовок. Заголовок блока включает:

- двойной хеш SHA256 заголовка предыдущего блока;
- комбинированный хеш транзакций в блоке, *корень дерева Меркла* (merkle root);
- время создания блока;
- подпись Лизы для заголовка блока.



Хеш заголовка блока служит идентификатором блока, так же как хеш транзакции служит идентификатором транзакции (txid). Время от времени я буду называть хеш заголовка блока *идентификатором блока*.



Первый левый элемент заголовка блока — это идентификатор предыдущего блока в блокчейне. Вот почему эта структура называется *цепочкой* блоков (блокчейном). Хеши предыдущих заголовков блоков образуют цепочку.

Второй элемент слева — это комбинированный хеш транзакций. Это *корень дерева Меркла*. Мы поговорим об этом элементе в последующих разделах в этой главе, а пока просто отмечу, что все транзакции в блоке хешируются в одно хеш-значение, которое записывается в заголовок блока. Нельзя изменить какую-либо транзакцию в блоке, не изменив корень дерева Меркла.

Третий элемент слева — время создания блока. Это время не является точным и даже не всегда увеличивается от блока к блоку. Но оно достаточно точное в человеческом понимании.

Четвертый элемент — подпись блока, оставленная Лизой, являющаяся своеобразной печатью «одобрено», которую может проверить каждый. Подпись Лизы доказывает, что она одобрила блок, и ее можно использовать как доказательство против Лизы, если та попытается смошенничать. Чуть ниже вы увидите, как это работает. Цифровая подпись в заголовке блока создает некоторые проблемы, которые мы исправим в главе 7, заменив цифровые подписи так называемым *доказательством работы*.

Лиза строит блок

Примерно каждые 10 минут Лиза создает новый блок, содержащий неподтвержденные транзакции. Она записывает этот блок в новый файл в общей папке. Право создавать новые файлы в общей папке имеют все, но никто не имеет права удалять или изменять файлы. Когда Лиза записывает блок в файл в общей папке, она *подтверждает* транзакции в этом блоке.

Допустим, Лиза собирается создать новый блок на высоте 20. Она должна:

1. Создать шаблон блока.
2. Подписать его.
3. Опубликовать.

ОБЩАЯ ПАПКА? СЕРЬЕЗНО?

Конечно же, в Биткоине нет никаких общих папок. В данном случае общая папка заменяет одноранговую сеть Биткоин, которую мы рассмотрим в главе 8.

Шаблоны блоков

Сначала Лиза создает *шаблон блока* — блок без подписи (рис. 6.5).

Она собирает несколько транзакций для включения в блок. Затем создает заголовок блока. Хеширует заголовок предыдущего блока, создавая его идентификатор, и включает результат в заголовок нового блока. Корень Меркла создается на основе транзакций, вошедших в шаблон блока, а в качестве времени создания выбирается текущее время.