

Оглавление

Предисловие	18
Целевая аудитория	18
Условные обозначения в книге.....	18
Примеры исходного кода.....	19
Использование примеров исходного кода	20
Ссылки на компании и продукты.....	20
Адреса и транзакции в этой книге	20
Как с нами связаться	20
Связь с Андреасом.....	20
Связь с Рене.....	21
Связь с Олаолувой Осунтокун.....	21
Признательности от Андреаса.....	21
Признательности от Рене.....	21
Признательности от Олаолувы Осунтокун	22
Участники проекта	22
Источники	23
Об авторах	24
Об иллюстрации на обложке (Колофон)	25
ЧАСТЬ I. ПОНИМАНИЕ СЕТИ LIGHTNING	27
Глава 1. Введение	28
Базовые понятия сети Lightning.....	28
Доверие в децентрализованных сетях.....	30
Справедливость без центральной власти	31
Доверительные протоколы без посредников	32
Протокол справедливости в действии	33
Примитивы безопасности как строительные блоки.....	34
Пример протокола справедливости	35
Мотивация для сети Lightning	36
Масштабирование блочных цепей.....	36
Определяющие признаки сети Lightning.....	38
Примеры использования сети Lightning, пользователи и их истории.....	39
Вывод.....	40

Глава 2. Приступаем к работе	41
Первый кошелек Lightning Алисы	41
Узлы Lightning.....	42
Проводники Lightning	42
Кошельки Lightning	43
Тестовая сеть Bitcoin.....	46
Уравновешивание сложности и контроля	47
Скачивание и инсталляция кошелька Lightning	48
Создание нового кошелька	49
Ответственность за хранение ключей	49
Мнемонические слова.....	49
Безопасное хранение мнемоники.....	50
Загрузка биткойна в кошелек	51
Приобретение биткойна	51
Получение биткойна	52
Из системы Bitcoin в сеть Lightning.....	56
Каналы сети Lightning.....	56
Открытие канала Lightning.....	58
Покупка чашки кофе с помощью сети Lightning.....	61
Кофейня Боба.....	61
Счет Lightning	62
Вывод.....	64
Глава 3. Как работает сеть Lightning	65
Что такое платежный канал?	66
Основы платежного канала	66
Маршрутизирование платежей по каналам	67
Платежные каналы	68
Мультиподписной адрес	69
Финансовая транзакция.....	69
Пример плохой процедуры открытия канала	70
Фиксационная транзакция	70
Обман с предыдущим состоянием.....	72
Объявление канала.....	75
Закрытие канала	75
Взаимное закрытие (хороший путь)	76
Принудительное закрытие (плохой путь)	77
Нарушение протокола (уродливый путь)	78
Счета.....	79
Платежный хеш и прообраз.....	80
Дополнительные метаданные	81
Доставка платежа.....	82
Эпидемический протокол обмена сообщениями между одноранговыми узлами.....	82
Отыскание пути и маршрутизация	83
Отыскание пути на основе источника	84
Луковичная маршрутизация	85
Алгоритм пересылки платежей	87

Шифрование однорангового обмена сообщениями	88
Мысли о доверии	89
Сравнение с системой Bitcoin.....	89
Адреса против счетов, транзакции против платежей.....	89
Выбор выходов против отыскания пути.....	90
Выходы со сдачей в Bitcoin против отсутствия сдачи в Lightning	91
Майнинговые комиссионные против маршрутизационных комиссионных	91
Комиссионные, варьирующиеся в зависимости от трафика, против объявленных комиссионных	91
Публичные Bitcoin-транзакции против частных платежей Lightning ...	92
Ожидание подтверждений против денежного расчета Lightning.....	93
Отправка произвольных сумм против ограничений по емкости.....	93
Стимулы для крупных платежей против малых платежей.....	94
Использование блочной цепи в качестве реестра против судебной системы.....	94
Офлайн против онлайн, асинхронность против синхронности	94
Сатоши против миллисатоши	95
Общие черты сетей Bitcoin и Lightning.....	95
Денежная единица.....	95
Необратимость и окончательность платежей	96
Доверие и риск контрагента.....	96
Безразрешительная работа.....	96
Открытый исходный код и открытая система	96
Вывод.....	96

Глава 4. Программное обеспечение узла Lightning..... 97

Среда разработки Lightning	98
Использование командной строки	98
Скачивание репозитория книги.....	99
Docker-контейнеры	100
Bitcoin Core и regtest.....	102
Сборка контейнера Bitcoin Core	102
Взаимодействие с контейнером bitcoin core	103
Проект c-lightning узла Lightning	105
Сборка c-lightning в качестве Docker-контейнера	105
Настройка сети Docker	106
Оперирование контейнерами bitcoind и c-lightning	107
Инсталлирование c-lightning из исходного кода	108
Инсталлирование необходимых библиотек и пакетов.....	108
Копирование исходного кода c-lightning.....	109
Компилирование исходного кода c-lightning.....	109
Проект демона узла сети Lightning	111
Docker-контейнер LND	111
Оперирование контейнерами bitcoind и LND	112
Инсталлирование LND из исходного кода.....	114
Копирование исходного кода LND	115
Компилирование исходного кода LND.....	115

Проект узла Lightning Eclair	116
Docker-контейнер Eclair	116
Оперирование контейнерами bitcoind и Eclair	117
Инсталлирование Eclair из исходного кода	118
Копирование исходного кода Eclair	119
Компилирование исходного кода Eclair.....	119
Сборка полной сети из разнообразных узлов Lightning.....	120
Использование docker-compose для оркестрирования Docker- контейнеров	120
Конфигурация docker-compose	121
Запуск образца сети Lightning.....	121
Открытие каналов и маршрутизирование платежа	122
Вывод.....	124

Глава 5. Оперирование узлом сети Lightning..... 125

Выбор своей платформы.....	126
Почему для оперирования узлом Lightning важна надежность?	126
Типы аппаратных узлов Lightning	127
Оперирование в «облаке»	127
Оперирование узлом дома	128
Какое оборудование требуется для работы узла Lightning?	129
Переключение серверной конфигурации в облаке.....	130
Постоянное хранилище данных (накопитель)	131
Использование инсталлятора или помощника	131
RaspiBlitz	131
myNode	133
Umbrel.....	133
BTCPay Server	134
Узел Bitcoin или облегченный узел Lightning.....	135
Выбор операционной системы.....	136
Выбор имплементации узла Lightning.....	136
Инсталлирование узла Bitcoin или Lightning	137
Фоновые службы.....	138
Изоляция процесса.....	138
Запуск узла.....	139
Конфигурирование узла.....	140
Конфигурирование сети.....	141
Это просто работает!.....	142
Автоматическая переадресация портов с использованием UPnP	143
Использование Tor для входящих соединений	144
Ручная переадресация портов.....	145
Безопасность вашего узла.....	146
Безопасность операционной системы.....	146
Доступ к узлу.....	147
Резервное копирование узла и каналов.....	148
Риск со стороны горячего кошелька	150

Зачистка средств.....	150
Внутрицепная зачистка	151
Внецепная зачистка	151
Зачистка на основе подводного свопа	151
Подводные свопы с помощью петли.....	152
Время безотказной работы и доступность узла Lightning.....	153
Допускайте неисправности и автоматизируйте	154
Мониторинг доступности узла	154
Сторожевые вышки	155
Управление каналами	156
Открытие исходящих каналов.....	157
Автопилот	157
Получение входящей ликвидности	160
Заккрытие каналов.....	161
Перебалансировка каналов.....	161
Комиссионные за маршрутизацию.....	162
Управление узлом.....	164
Ride The Lightning	164
Indmon	164
ThunderHub	165
Вывод.....	165

ЧАСТЬ II. СЕТЬ LIGHTNING В ДЕТАЛЯХ 167

Глава 6. Архитектура сети Lightning 168

Комплект протоколов сети Lightning.....	168
Lightning в деталях.....	169

Глава 7. Платежные каналы..... 171

Другой способ использования системы Bitcoin	172
Владение биткойном и контроль над ним.....	173
Разнообразие форм (независимого) владения и мультиподпись.....	174
Совместное владение без независимого контроля.....	174
Предотвращение «привязанности» и нерасходуемости биткойна	174
Строительство платежного канала.....	175
Приватный и публичный ключи узла	175
Сетевой адрес узла	175
Идентификаторы узлов.....	176
Соединение узлов в качестве прямых одноранговых участников сети.....	176
Строительство канала	177
Одноранговый протокол для управления каналами	177
Поток сообщений об установлении канала	177
Сообщение open_channel	179
Сообщение accept_channel	180
Финансовая транзакция.....	181
Генерирование мультиподписного адреса	181
Сборка финансовой транзакции	181

Удерживание подписанных транзакций без широковещательной передачи	182
Возврат средств до финансирования	182
Сборка предварительно подписанной возвратной транзакции	183
Выстраивание транзакций в цепь без широковещательной передачи	183
Решение проблемы деформируемости (сегрегированный свидетель)	184
Сообщение <code>funding_created</code>	185
Сообщение <code>funding_signed</code>	186
Широковещательная передача финансовой транзакции	186
Сообщение <code>funding_locked</code>	187
Отправка платежей по каналу	187
Разделение остатка	187
Конкурирующие фиксации	188
Обман со старыми фиксационными транзакциями	189
Отзыв старых фиксационных транзакций	189
Асимметричные фиксационные транзакции	190
Задержанное (привязанное ко времени) расходование выхода <code>to_self</code>	191
Отзывные ключи	192
Фиксационная транзакция	193
Продвижение состояния канала вперед	195
Сообщение <code>commitment_signed</code>	196
Сообщение об отзыве и возврате	196
Отзыв и рефиксация	197
Обман и наказание на практике	197
Резерв канала: обеспечение личной заинтересованности	200
Заккрытие канала (кооперативное закрытие)	200
Сообщение <code>shutdown</code>	201
Сообщение <code>closing_signed</code>	202
Транзакция кооперативного закрытия	202
Вывод	203

Глава 8. Маршрутизация в сети платежных каналов..... 205

Маршрутизирование платежа	205
Маршрутизация против отыскания пути	207
Создание сети платежных каналов	207
Физический пример «маршрутизирования»	208
Протокол справедливости	214
Имплементирование атомарных бездоверительных многопереходных платежей	214
Возвращаясь к примеру с донатами	215
Внутрицепное и внецепное улаживание HTLC-контрактов	216
Контракты с привязкой к хешу и времени	216
HTLC-контракты на Bitcoin Script	217
Платежный прообраз и верификация хеша	218
Распространение HTLC-контрактов от Алисы к Дины	219
Обратное распространение секрета	220
Привязка подписи: предотвращение кражи HTLC-контрактов	222

Оптимизация хеша.....	223
Кооперативный отказ и отказ тайм-аута по HTLC-контракту.....	225
Декрементирование привязок ко времени.....	226
Вывод.....	227
Глава 9. Работа канала и пересылка платежей.....	228
Локальный (один) канал против маршрутизируемых (многочисленных) каналов.....	229
Пересылка платежей и обновление фиксаций с помощью HTLC-контрактов.....	229
HTLC-контракт и поток фиксационных сообщений.....	230
Пересылка платежей с помощью HTLC-контрактов.....	230
Добавление HTLC-контракта.....	231
Сообщение update_add_HTLC.....	231
HTLC-контракт в фиксационных транзакциях.....	232
Новая фиксация с выходом из HTLC-контракта.....	233
Алиса фиксирует.....	234
Боб признает новую фиксацию и отзывает старую.....	235
Боб фиксирует.....	238
Несколько HTLC-контрактов.....	239
Исполнение HTLC-контракта.....	240
Распространение HTLC-контракта.....	240
Дина исполняет HTLC-контракт с Чаном.....	240
Боб улаживает HTLC-контракт с Алисой.....	241
Удаление HTLC-контракта из-за ошибки или истечения срока.....	244
Осуществление локального платежа.....	245
Вывод.....	245
Глава 10. Луковичная маршрутизация.....	246
Физический пример, иллюстрирующий луковичную маршрутизацию.....	247
Выбор пути.....	247
Сборка слоев.....	248
Отслаивание слоев.....	250
Введение в луковичную маршрутизацию на основе HTLC-контрактов.....	251
Алиса выбирает путь.....	251
Алиса конструирует полезные грузы.....	253
Полезный груз для Дины в заключительном узле.....	253
Переходный полезный груз для Чана.....	254
Переходный полезный груз для Боба.....	255
Окончательные полезные грузы переходов.....	256
Генерация ключей.....	256
Сеансовый ключ Алисы.....	257
Детали генерации ключей.....	258
Генерация совместных секретов.....	258
Обертывание луковичных слоев.....	260
Луковицы фиксированной длины.....	260
Обертывание луковицы (в общих чертах).....	261

Обертывание переходного полезного груза Дины	262
Луковично-маршрутизация защита от повторного воспроизведения и его обнаружение	265
Обертывание переходного полезного груза Чана	266
Обертывание переходного полезного груза Боба	267
Заключительный луковичный пакет	268
Отправка луковицы	269
Сообщение <code>update_add_htlc</code>	269
Алиса отправляет луковицу Бобу	269
Боб проверяет луковицу	270
Боб генерирует заполнитель	270
Боб распутывает свой переходный полезный груз	271
Боб извлекает внешний НМАС для следующего перехода	272
Боб удаляет свой полезный груз и сдвигает луковицу влево	272
Боб конструирует новый луковичный пакет	273
Боб верифицирует детали HTLC-контракта	273
Боб отправляет <code>update_add_htlc</code> Чану	274
Чан пересылает луковицу	274
Дина получает заключительный полезный груз	275
Возвращение ошибок	275
Сообщения о сбоях	276
Застрявшие платежи	278
Спонтанные платежи <code>keysend</code>	279
Конкретно-прикладные луковичные TLV-записи	279
Отправка и получение платежей <code>keysend</code>	280
Платеж <code>keysend</code> и конкретно-прикладные записи в приложениях Lightning	280
Вывод	280
Глава 11. Сплетни и каналный граф	281
Обнаружение одноранговых узлов	283
Самозагрузка P2P-узлов	284
Самозагрузка адресов DNS-серверов	284
Рабочий поток самозагрузки нового однорангового узла	285
Опции SRV-запроса	288
Канальный граф	289
Ориентированный граф	289
Сообщения эпидемического протокола	290
Сообщение <code>node_announcement</code>	291
Структура сообщения <code>node_announcement</code>	291
Валидация объявлений узла	292
Сообщение <code>channel_announcement</code>	292
Необъявленные (приватные) каналы	293
Локализация канала в блочной цепи Bitcoin	293
Короткий ID канала	294
Структура сообщения <code>channel_announcement</code>	294
Валидация объявления канала	296
Сообщение <code>channel_update</code>	296

Текущее сопровождение канального графа	297
Вывод.....	298
Глава 12. Отыскание пути и доставка платежа.....	299
Отыскание пути в рамках комплекта протоколов Lightning.....	299
Где же BOLT?	300
Отыскание пути: какую задачу мы решаем?.....	300
Выбор наилучшего пути.....	301
Отыскание путей в математике и информатике	302
Емкость, остаток, ликвидность.....	302
Неопределенность остатков	303
Сложность отыскания пути.....	304
Без лишних сложностей	304
Отыскание пути и процесс доставки платежа.....	305
Построение канального графа.....	305
Неопределенность в канальном графе	308
Неопределенность ликвидности и вероятность.....	309
Комиссионные и другие метрики канала	310
Отыскание кандидатных путей.....	312
Доставка платежа (цикл проб и ошибок)	312
Первая попытка (путь №1)	313
Учеба на ошибках	313
Вторая попытка (путь № 4).....	313
Учеба на успехах	314
Застоявшиеся знания?	314
Многокомпонентные платежи	314
Использование MPP	315
Разбивка платежей	315
Метод проб и ошибок в течение нескольких «раундов».....	316
Вывод.....	318
Глава 13. Проводной протокол: фреймирование	
и расширяемость.....	319
Слой обмена сообщениями в рамках комплекта протоколов Lightning	319
Проводное фреймирование	320
Высокоуровневое фреймирование.....	320
Кодировка типа.....	321
Расширения «Тип–длина–значение для сообщений»	322
Протокол буферизует формат сообщения	322
Прямая и обратная совместимости.....	323
Формат «Тип–длина–значение»	323
Целочисленная кодировка BigSize	324
Ограничения TLV-кодирования	325
Каноническое TLV-кодирование	325
Биты функциональностей и расширяемость протокола	325
Биты функциональностей как механизм обеспечения	
обнаруживаемости модернизаций	326

TLV для прямой и обратной совместимостей.....	327
Таксономия механизмов модернизации.....	328
Модернизации внутренней сети.....	328
Сквозные модернизации.....	328
Модернизации уровня строительства канала.....	329
Вывод.....	329
Глава 14. Шифрованный транспорт сообщений Lightning	330
Шифрованный транспорт в рамках комплекта протоколов Lightning.....	330
Введение.....	330
Канальный граф как децентрализованная инфраструктура публичных ключей.....	331
Почему не TLS?.....	332
Каркас криптосвязи на основе протокола Noise.....	333
Шифрованный транспорт Lightning в деталях.....	333
Noise_XK: рукопожатие Noise в сети Lightning.....	333
Нотация рукопожатия и поток протокола.....	334
Высокоуровневый обзор.....	334
Рукопожатие в трех действиях.....	335
Инициализация состояния сеанса рукопожатия.....	337
Акты рукопожатия.....	337
Акт первый.....	338
Акт второй.....	339
Акт третий.....	340
Шифрование транспортных сообщений.....	342
Ротация ключей сообщений Lightning.....	343
Вывод.....	343
Глава 15. Платежные запросы Lightning.....	345
Счета в комплекте протоколов Lightning.....	345
Введение.....	345
Платежные запросы Lightning против Bitcoin-адресов.....	346
BOLT #11: сериализация и интерпретация платежных запросов Lightning.....	347
Кодирование платежного запроса на практике.....	347
Человекочитаемый префикс.....	347
bech32 и сегмент данных.....	348
Тегированные поля счета.....	349
Вывод.....	350
Глава 16. Безопасность и конфиденциальность сети Lightning	351
Почему важна конфиденциальность?.....	351
Определения конфиденциальности.....	351
Процесс оценивания конфиденциальности.....	352
Анонимностное множество.....	353

Различия между сетями Lightning и Bitcoin с точки зрения конфиденциальности	354
Атаки на Lightning	356
Наблюдение за суммами платежей	356
Связывание отправителей и получателей	356
Раскрытие остатков каналов (прощупывание)	358
Отказ в обслуживании	360
DoS в Bitcoin	360
DoS в Lightning	361
Известные DoS-атаки	361
Закливание фиксаций	362
Запирание ликвидности канала	362
Межслоевая деанонимизация	362
Внутрицепная кластеризация Bitcoin-сущностей	363
Контрмеры	364
Внецепная кластеризация узлов Lightning	364
Контрмеры	364
Межслоевое связывание: узлы Lightning и Bitcoin-сущности	365
Граф Lightning	365
Как выглядит граф Lightning в реальности?	365
Граф Lightning сегодня	366
Атаки на основе топологии	366
Темпоральность сети Lightning	367
Централизация в сети Lightning	368
Экономические стимулы и графовая структура	368
Практические советы пользователям по защите их конфиденциальности	369
Необъявленные каналы	369
Соображения по маршрутизации	370
Принятие каналов	371
Вывод	372
Справочные материалы и дальнейшее чтение	372
Конфиденциальность и атакиощупыванием	372
Атаки переполнением	372
Соображения по маршрутизации	372
Глава 17. Заключение	373
Децентрализованные и асинхронные инновации	373
Инновации в Bitcoin-протоколе и в Bitcoin Script	374
Инновация в протоколе Lightning	374
Расширяемость TLV	375
Строительство платежного канала	375
Сквозные функциональности в порядке выбора	375
Lightning-приложения (LApps)	376
На старт, внимание, марш!	377

Приложение А. Обзор основных принципов системы Bitcoin	378
Ключи и цифровые подписи.....	378
Приватные и публичные ключи	379
Хеши	380
Цифровые подписи	382
Типы подписей	383
Транзакции Bitcoin	383
Входы и выходы.....	383
Транзакционные цепочки	385
TxID: идентификаторы транзакций.....	386
Выходные точки: выходные идентификаторы	387
Bitcoin Script.....	388
Работа языка Bitcoin Script.....	388
Привязывающие и отвязывающие скрипты	390
Привязывание к публичному ключу (подписи)	390
Привязывание к хешу (секрету)	391
Мультиподписные скрипты.....	392
Скрипты привязки ко времени	393
Скрипты с несколькими условиями.....	394
Использование управления потоком в скриптах.....	395
Приложение В. Базовая инсталляция и использование Docker	397
Инсталляция Docker	397
Базовые команды Docker	398
Сборка контейнера.....	398
Оперирование контейнером	398
Исполнение команды в контейнере	398
Остановка и запуск контейнера	398
Удаление контейнера по имени	399
Выведение списка оперируемых контейнеров	399
Выведение списка Docker-образов	399
Вывод.....	399
Приложение С. Сообщения проводного протокола.....	400
Типы сообщений.....	400
Структура сообщения.....	402
Сообщения об установлении соединения	402
Сообщение init.....	402
Сообщения об ошибке.....	403
Сообщение error	403
Оживленность соединения	404
Сообщение ping	404
Сообщение pong	404

Финансирование канала	405
Сообщение open_channel	405
Сообщение accept_channel	406
Сообщение funding_created	406
Сообщение funding_signed	407
Сообщение funding_locked	407
Заккрытие канала	407
Сообщение shutdown.....	408
Сообщение closing_signed	408
Операция канала	408
Сообщение update_add_htlc	408
Сообщение update_fulfill_htlc.....	409
Сообщение update_fail_htlc	409
Сообщение commitment_signed.....	409
Сообщение revoke_and_ack.....	410
Сообщение update_fee	410
Сообщение update_fail_malformed_htlc	410
Объявление канала.....	411
Сообщение channel_announcement	411
Сообщение node_announcement	411
Сообщение channel_update	412
Сообщение announce_signatures.....	412
Синхронизация канального графа.....	413
Сообщение query_short_chan_ids	413
Сообщение reply_short_chan_ids_end.....	413
Сообщение query_channel_range.....	413
Сообщение reply_channel_range.....	414
Сообщение gossip_timestamp_range	414
Приложение D. Источники и уведомления о лицензиях.....	415
Источники	415
Сервер BTCPay Server	416
Lamassu Industries AG	416
Глоссарий.....	417
Предметный указатель	436

Предисловие

Сеть Lightning (Lightning Network, аббр. LN, или сеть-молния) – это второслойная одноранговая сеть, которая позволяет совершать платежи Bitcoin «вне цепи», то есть без фиксации их в качестве транзакций в блочной цепи (блокчейне) системы Bitcoin.

Сеть Lightning предоставляет безопасные, дешевые, быстрые и гораздо более приватные платежи Bitcoin, даже для очень малых платежей.

Основываясь на идее платежных каналов, впервые предложенной изобретателем системы Bitcoin Сатоши Накамото, сеть Lightning представляет собой маршрутизируемую сеть платежных каналов, в которой платежи делают «прыжки» вдоль пути платежных каналов от отправителя к получателю.

Первоначальная идея сети Lightning была предложена в 2015 году в новаторской статье Джозефа Пуна (Joseph Poon) и Тадеуша Дриджа (Thaddeus Dryja) «Сеть Lightning в рамках системы Bitcoin: масштабируемые мгновенные платежи вне цепи» (The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments). К 2017 году в интернете была запущена «тестовая» сеть Lightning, по мере того разные группы строили совместимые имплементации и координировали работу, чтобы установить какие-нибудь стандарты совместимости. В 2018 году сеть Lightning заработала, и потекли платежи.

В 2019 году Андреас М. Антонопулос, Олаолува Осунтокун и Рене Пикхардт согласились сотрудничать в написании этой книги. И похоже, мы добились успеха!

ЦЕЛЕВАЯ АУДИТОРИЯ

Эта книга в основном предназначена для технически подкованных читателей, имеющих представление об основах системы Bitcoin и других открытых блочных цепей.

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ В КНИГЕ

В книге используются следующие типографические условные обозначения:

курсивный шрифт

обозначает новые термины, URL-адреса, адреса электронной почты, имена файлов и расширения файлов;

моноширинный шрифт

используется для листингов программ, а также внутри абзацев для ссылки на элементы программ, такие как переменные или имена функций, базы данных, типы данных, переменные среды, инструкции и ключевые слова;

жирный моноширинный шрифт

показывает команды либо другой текст, который должен быть набран пользователем;

моноширинный шрифт курсивом

показывает текст, который должен быть заменен значениями, передаваемыми пользователем, либо значениями, определяемыми по контексту.



Данный элемент обозначает подсказку или совет.



Данный элемент обозначает общее замечание.



Данный элемент обозначает предупреждение или предостережение.

ПРИМЕРЫ ИСХОДНОГО КОДА

Примеры проиллюстрированы на языках Go, C++, Python и с использованием командной строки Unix-подобной операционной системы. Все фрагменты исходного кода доступны в репозитории на GitHub в подкаталоге *code*. Сделайте ответвление исходного кода книги, попробуйте примеры кода или отправьте исправления через GitHub¹.

Все фрагменты исходного кода могут быть воспроизведены в большинстве операционных систем с минимальной инсталляцией компиляторов, интерпретаторов и библиотек для соответствующих языков.

Там, где это необходимо, мы предоставляем базовые инструкции по инсталляции и пошаговые примеры результата работы этих инструкций.

Некоторые фрагменты исходного кода и результаты его работы были переформатированы для печати. Во всех таких случаях строки были разделены символом обратной косой черты (`\`), за которым следует символ новой строки. При транскрибировании примеров удалите эти два символа и снова соедините строки, и вы должны увидеть результаты, идентичные тем, которые показаны в примере.

Во всех фрагментах исходного кода, там, где это возможно, используются реально существующие значения и вычисления, так что вы можете переходить

¹ См. <https://github.com/lnbook/lnbook>.

от примера к примеру и видеть одни и те же результаты в любом программном коде, который вы пишете для вычисления одних и тех же значений. Например, все приватные ключи и соответствующие им публичные ключи и адреса реально существуют.

ИСПОЛЬЗОВАНИЕ ПРИМЕРОВ ИСХОДНОГО КОДА

Если у вас возникли технические вопросы или проблемы с использованием примеров исходного кода, то, пожалуйста, отправьте электронное письмо по адресу bookquestions@oreilly.com.

СЫЛКИ НА КОМПАНИИ И ПРОДУКТЫ

Все ссылки на компании и продукты предназначены для образовательных, демонстрационных и справочных целей. Авторы не поддерживают ни одну из упомянутых компаний или продуктов. Мы не тестировали работу или безопасность ни одного из продуктов, проектов или сегментов исходного кода, показанных в этой книге. Используйте их на свой страх и риск!

АДРЕСА И ТРАНЗАКЦИИ В ЭТОЙ КНИГЕ

Адреса, транзакции, ключи, QR-коды и данные блочной цепи Bitcoin, используемые в этой книге, по большей части реальны. Это означает, что вы можете просматривать блочную цепь, просматривать предлагаемые в качестве примеров транзакции, извлекать их с помощью ваших собственных скриптов или программ и т. д.

Однако обратите внимание, что приватные ключи, использованные для создания адресов, напечатанных в этой книге, были «сожжены». Это означает, что если вы отправите деньги на любой из этих адресов, то деньги будут либо потеряны навсегда, либо (что более вероятно) присвоены, поскольку любой, кто читает книгу, может забрать их, используя напечатанные здесь приватные ключи.



НЕ ОТПРАВЛЯЙТЕ ДЕНЬГИ НИ НА ОДИН ИЗ АДРЕСОВ, УКАЗАННЫХ В ЭТОЙ КНИГЕ. Ваши деньги будут взяты другим читателем или потеряны навсегда.

КАК С НАМИ СВЯЗАТЬСЯ

Информация о книге «Освоение сети Lightning», а также открытое издание и переводы доступны по адресу <https://lnbook.info>.

Связь с Андреасом

С Андреасом М. Антонопулосом можно связаться на его личном веб-сайте: <https://aantonop.com>.

Подпишитесь на канал Андреаса на YouTube:

<https://www.youtube.com/aantonop>.

Оставьте свой лайк на странице Андреаса в Facebook:

<https://www.facebook.com/AndreasMAntonopoulos>.

Читайте твиты Андреаса в Твиттере: <https://twitter.com/aantonop>.

Свяжитесь с Андреасом в LinkedIn: <https://linkedin.com/company/aantonop>.

Андреас также хотел бы поблагодарить патронов, которые поддерживают его работу ежемесячными пожертвованиями. Вы можете поддержать Андреаса на Patreon по адресу <https://patreon.com/aantonop>.

Связь с Рене

С Рене Пикхардтом можно связаться на его личном веб-сайте:

<https://ln.rene-pickhardt.de>.

Подпишитесь на канал Рене на YouTube:

<https://www.youtube.com/user/RenePickhardt>.

Читайте твиты Рене в Твиттере: <https://twitter.com/renepickhardt>.

Свяжитесь с Рене в LinkedIn:

<https://www.linkedin.com/in/rene-pickhardt-80313744>.

Рене также хотел бы поблагодарить всех патронов, которые поддерживают его работу ежемесячными пожертвованиями. Вы можете поддержать Рене на Patreon по адресу <https://patreon.com/renepickhardt>.

Или же вы можете поддержать его работу напрямую посредством системы Bitcoin (также через сеть Lightning) по адресу <https://donate.ln.rene-pickhardt.de>, за что Рене так же благодарит, как и своих патронов.

Связь с Олаолувой Осунтокун

С Олаолувой Осунтокуном можно связаться по его профессиональному электронному адресу: laolu@lightning.engineering.

Читайте твиты Олаолувы в Twitter: <https://twitter.com/roasbeef>.

ПРИЗНАТЕЛЬНОСТИ ОТ АНДРЕАСА

Своей любовью к словам и книгам я обязан своей матери Терезе, которая вырастила меня в доме, где книги стояли вдоль каждой стены. Моя мать также купила мне мой первый компьютер в 1982 году, несмотря на то что я называл себя технофобом. Мой отец Менелаос, инженер-строитель, опубликовавший свою первую книгу в 80 лет, был именно тем, кто научил меня логическому и аналитическому мышлению, а также любви к науке и технике.

Спасибо вам всем за то, что поддерживали меня на протяжении всего этого путешествия.

ПРИЗНАТЕЛЬНОСТИ ОТ РЕНЕ

Я хочу поблагодарить немецкую систему образования, благодаря которой я приобрел знания, на которых строится моя работа. Это один из величайших

даров, которые мне были даны. Точно так же я хочу поблагодарить немецкую общественную систему здравоохранения и каждого человека, посвящающего свое время работе в этой отрасли. Ваши усилия и выносливость делают вас моими личными героями, и я никогда не забуду помощь, терпение и поддержку, которые я получал, когда нуждался. Выражаю благодарность всем студентам, которым мне разрешили преподавать и которые участвовали в интересных дискуссиях и задавали вопросы. У вас я научился большому. Я очень благодарен сообществу системы Bitcoin и сети Lightning, которое тепло приветствовало меня, а также энтузиастам и частным лицам, которые финансово поддерживали и продолжают поддерживать мою работу. В частности, я благодарен всем разработчикам открытого исходного кода (не только сети Bitcoin и сети Lightning) и людям, которые их финансируют, чтобы сделать эту технологию возможной. Особая благодарность моим соавторам за то, что они прошли со мной через шторм. И последнее, но не менее важное: я благодарен своим близким.

ПРИЗНАТЕЛЬНОСТИ ОТ ОЛАЛУВЫ ОСУНТОКУН

Хотел бы поблагодарить удивительную команду компании Lightning Labs, так как без вас всех не было бы LND. Я также хотел бы поблагодарить авторов оригинальной спецификации BOLT: Расти Рассела, Фабриса Друина, Коннера Фромнкета, Пьера Мари Падиу, Лайзу Нейгут и Кристиана Декера. И последнее, но не менее важное: хотел бы поблагодарить Джозефа Пуна и Тадж Дриджа, авторов оригинальной статьи о сети Lightning, поскольку без них не было бы сети Lightning, о которой можно было бы написать книгу.

УЧАСТНИКИ ПРОЕКТА

Многие авторы предлагали комментарии, исправления и дополнения к книге, по мере того как она писалась совместно на GitHub.

Ниже приведен отсортированный в английском алфавитном порядке список всех участников GitHub, включая их идентификаторы GitHub в круглых скобках:

- 8go (@8go);
- Акиль Азиз (@batmanscode);
- Александр Гнип (@quantumctulhu);
- Альфа К. Смит (@alpha_github_id);
- Бен Ски (@benskee);
- Брайан Л. Макмайкл (@brianmcmichael);
- CandleHater (@CandleHater);
- Дэниел Гокель (@dancodery);
- Дапенг Ли (@luislee818);
- Дариус Э. Парвин (@DariusParvin);
- Дору Мунтян (@критон);
- Эдуардо Лима III (@elima-iii);
- Эмилио Норрманн (@enormann);
- Франсиско Кальдерон (@grunch);
- Франсиско Рекена (@FrankyFFV);

- Франсуа Дегрос (@fdegros);
- Джованни Зотта (@GiovanniZotta);
- Густаво Сильва (@GustavoRSSilva);
- Гай Таякорн (@saguywalker);
- Хаоюй Линь (@HAOYUatHZ);
- Хатим Буфничель (@boufni95);
- Имран Лоргат (@ImranLorgat);
- Джеффри Макларти (@jnmclarty);
- Джон Дэвис (@tigeryant);
- Жюльен Вендлинг (@trigger67);
- Юсси Тиира (@juhi24);
- Кори Ньютон (@korynewton);
- Лоуренс Уэббер (@lwebbz);
- Луиджи (@джин);
- Максимилиан Караш (@mknoszlig);
- Omega X. Last (@omega_github_id);
- Оуэн Ганден (@ogunden);
- Патрик Лемке (@PatrickLemke);
- Пол Вакероу (@wackerow);
- Рэнди Макмиллан (@RandyMcMillan);
- Рене Кенке (@rene78);
- Рикардо Маркес (@RicardoM17);
- Себастьян Фальбесонер (@Thestack);
- Сергей Тихомиров (@s-tikhomirov);
- Северин Александр Бюлер (@SeverinAlexB);
- Симона Бови (@SimoneBovi);
- Шриджан Бхушан (@srijanb);
- Тейлор Мастерсон (@tjmasterson);
- Умар Болатов (@bolatovumar);
- Уоррен Ван (@wlwanpan);
- Ибинь Чжан (@z4y1b2);
- Закари Хадденхэм (@senf42).

Без предложенной всеми перечисленными выше людьми помощи эта книга была бы невозможна. Ваш вклад демонстрирует силу открытого исходного кода и открытой культуры, и мы бесконечно благодарны вам за помощь.

Спасибо.

Источники

Некоторые материалы в этой книге взяты из различных общедоступных источников, источников с открытой лицензией или с разрешения автора. Подробности об источнике, лицензии и атрибуции см. в приложении D.

Об авторах

Андреас М. Антонопулос – автор бестселлеров, оратор, преподаватель и очень востребованный эксперт по системе Bitcoin и открытым технологиям на основе блочных цепей. Он известен тем, что облегчает понимание сложных тем и подчеркивает как положительное, так и отрицательное воздействие, которое эти технологии могут оказывать на наши глобальные общества.

Андреас написал еще два технических бестселлера для программистов с O'Reilly Media, «Освоение системы Bitcoin» (Mastering Bitcoin) и «Освоение системы Ethereum» (Mastering Ethereum). Он также опубликовал серию книг «Интернет денег», в которых основное внимание уделяется социальному, политическому и экономическому значению и последствиям этих технологий. Андреас еженедельно выпускает бесплатный образовательный контент на своем канале YouTube и проводит виртуальные семинары на своем веб-сайте. Узнайте больше по адресу aantonop.com.

Олаолува Осунтокун является соучредителем и техническим директором компании Lightning Labs, а также ведущим разработчиком Ind, одной из главных имплементаций сети Lightning. Он получил степень бакалавра и магистра в области информатики в UCSB и в 2019 году был членом класса Forbes 30 для молодых специалистов до 30 лет. Во время учебы в аспирантуре он сосредоточился на прикладной криптографии, в частности на шифрованном поиске. Более пяти лет он активно участвовал в разработке системы Bitcoin и является автором нескольких предложений по совершенствованию системы Bitcoin (BIP-157 и 158). В наши дни его основное внимание сосредоточено на строительстве, конструировании и разработке частных масштабируемых автономных протоколов блочной цепи, таких как Lightning.

Рене Пикхардт – опытный математик и консультант по науке о данных, который использует свои статистические знания для проведения исследований с NTNU по отысканию путей, конфиденциальности, надежности платежей и соглашениям об уровне обслуживания в сети Lightning. Рене ведет технический и ориентированный на разработчиков канал YouTube² о сети Lightning и уже ответил примерно на половину вопросов о работе сети Lightning на бирже Bitcoin, что делает его одним из лучших консультантов для всех новых разработчиков, которые хотят присоединиться к этому пространству. Рене провел множество публичных и частных семинаров о сети Lightning, в том числе обучал студентов резидентуры Chaincode Labs 2019 года вместе с другими ключевыми разработчиками сети Lightning.

² См. <https://www.youtube.com/renepickhardt>.

Конец ознакомительного фрагмента.

Приобрести книгу можно

в интернет-магазине

«Электронный универс»

e-Univers.ru