

Содержание

Над книгой работали	20
Предисловие	22
Глава 1. Блокчейн. Курс молодого бойца	27
Развитие технологии блокчейн	27
Распределенные системы	30
История блокчейна и валюты биткойн	32
Электронные деньги	32
Блокчейн	34
Определение блокчейна	35
Общие элементы блокчейна	38
Как устроен блокчейн	41
Как в блокчейне накапливаются блоки	41
Достоинства и недостатки блокчейна	42
Уровни блокчейновой технологии	43
Возможности блокчейна	45
Типы блокчейна	47
Распределенные реестры	48
Технология распределенных реестров	48
Публичные блокчейны	49
Приватные блокчейны	49
Полуприватные блокчейны	49
Сайдчейны	49
Закрытый распределенный реестр	50
Разделяемый реестр	50
Полностью приватные и проприетарные блокчейны	50
Токенизированные блокчейны	51
Нетокенизированные блокчейны	51
Консенсус	51
Механизм консенсуса	52
Типы механизмов консенсуса	52
Консенсус в блокчейне	53
САР-теорема и блокчейн	55
Заключение	57

Глава 2. Децентрализация	58
Децентрализация с помощью блокчейна	58
Методы децентрализации.....	60
Избавление от посредников	60
Децентрализация на основе состязания.....	61
Пути децентрализации	62
Как происходит децентрализация	63
Пример использования критериев децентрализации.....	63
Блокчейн и полная децентрализация экосистемы	64
Хранилище данных	64
Коммуникация.....	65
Вычислительная мощность и децентрализация	66
Смарт-контракты.....	68
Децентрализованные организации	68
Децентрализованные автономные организации.....	68
Децентрализованные автономные корпорации.....	69
Децентрализованные автономные общества.....	70
Децентрализованные приложения	70
Требования к децентрализованным приложениям.....	70
Операции, проводимые децентрализованными приложениями.....	71
Примеры ДП.....	71
Платформы для децентрализации	71
Ethereum.....	72
MaidSafe.....	72
Lisk.....	72
Заключение	72
Глава 3. Симметричное шифрование	74
Работа с утилитой командной строки OpenSSL	74
Введение.....	75
Математика.....	75
Множество.....	75
Группа.....	76
Поле	76
Конечное поле.....	76
Порядок.....	76
Абелева группа	76
Простые поля	76
Кольцо	76
Циклическая группа	77
Модульная арифметика	77
Криптография.....	77
Конфиденциальность.....	78

Целостность	78
Аутентификация	78
Аутентификация сущности	78
Аутентификация происхождения данных	79
Неотказуемость	79
Подотчетность	80
Базовые элементы криптографии	80
Симметричная криптография	81
Потоковые шифры	81
Блочные шифры	82
Стандарт шифрования данных (DES)	86
Стандарт шифрования AES	86
Как работает AES	86
Заключение	90
Глава 4. Шифрование с открытым ключом	91
Асимметричное шифрование	91
Целочисленная факторизация	93
Дискретное логарифмирование	93
Эллиптические кривые	94
Открытые и закрытые ключи	94
Система RSA	95
Шифрование и дешифрование с помощью RSA	96
Эллиптическая криптография	96
Проблема дискретного логарифмирования в ECC	102
RSA с использованием OpenSSL	104
Пара ключей в RSA: открытый и закрытый ключи	104
Шифрование и дешифрование	106
ECC с использованием OpenSSL	107
Функции хеширования	110
Сжатие данных случайной длины и представление их в форме установленного размера	111
Простота вычислений	111
Вычислительная неразрешимость	111
Вторичная вычислительная неразрешимость	111
Устойчивость к коллизиям	111
Резюме сообщения	113
Алгоритмы безопасного хеширования	113
Деревья Меркла	118
Деревья Patricia	118
Распределенные хеш-таблицы (DHT)	119
Цифровые подписи	119
Алгоритм цифровой подписи RSA	120

Подписать и зашифровать	121
Зашифровать и подписать	121
Алгоритм ECDSA	122
Как создать цифровую подпись в OpenSSL	123
ECDSA при использовании OpenSSL	124
Гомоморфное шифрование	126
Алгоритм Signcryption	127
Доказательства с нулевым разглашением	127
Слепые подписи	127
Схемы кодирования	128
Финансовые рынки и торговля	128
Торговля	128
Обмен	129
Ордера и их свойства	129
Системы электронной доставки и управления ордерами	130
Атрибуты сделки	130
Базовый финансовый инструмент	130
Основные атрибуты	130
Экономические атрибуты	130
Атрибуты продажи	131
Контрагент	131
Жизненный цикл сделки	131
Торговля на опережение	132
Рыночные манипуляции	132
Заключение	132
Глава 5. Знакомство с биткойном	133
Биткойн	135
Определение биткойна	137
Биткойн – взгляд с высоты птичьего полета	138
Отправка платежа другому пользователю	138
Цифровые ключи и адреса	145
Закрытые ключи в Bitcoin	145
Открытые ключи в Bitcoin	147
Адреса в Bitcoin	148
Кодирование Base58Check	149
Косметические адреса	149
Транзакции	151
Цикл жизни транзакции	151
Комиссия транзакций	152
Пулы транзакций	152
Структура данных транзакции	152
Метаданные	154

Вводы.....	154
Выводы.....	154
Верификация.....	155
Скриптовый язык.....	155
Распространенные опкоды.....	156
Типы транзакций.....	156
Транзакции Coinbase.....	158
Контракты.....	159
Верификация транзакций.....	159
Гибкость транзакции.....	160
Блокчейн.....	161
Структура блока.....	161
Структура заголовка блока.....	161
Блок генезиса.....	163
Майнинг.....	165
Задачи майнеров.....	166
Награды майнинга.....	166
Доказательство работы (PoW).....	167
Алгоритм майнинга.....	167
Частота хеширования.....	169
Системы майнинга.....	170
Центральный процессор.....	170
Графический процессор.....	170
FPGA.....	171
ASIC.....	171
Майнинг-пулы.....	173
Заключение.....	175
Глава 6. Сеть и платежи Bitcoin.....	176
Сеть Bitcoin.....	176
Кошельки.....	184
Недетерминированные кошельки.....	185
Детерминированные кошельки.....	185
Иерархические детерминированные кошельки.....	185
Мозговые кошельки.....	186
Бумажные кошельки.....	186
Аппаратные кошельки.....	186
Онлайн-кошельки.....	187
Мобильные кошельки.....	187
Мобильный кошелек Jaxx.....	187
Платежи биткойнами.....	188
Инновации в Bitcoin.....	190
Предложения по улучшению Bitcoin (BIP).....	190

Продвинутые протоколы	190
Серегегированный свидетель (SegWit)	191
Bitcoin Cash	192
Bitcoin Unlimited	192
Bitcoin Gold.....	193
Инвестирование в биткойны и продажа биткойнов.....	193
Заключение	195
Глава 7. Клиенты и API Bitcoin	196
Установка Bitcoin	196
Типы основных клиентов Bitcoin	197
Bitcoind	197
Bitcoin-cli.....	197
Bitcoin-qt	197
Настройка узла Bitcoin	198
Настройка исходного кода	198
Настройка файла bitcoin.conf.....	199
Запуск узла в тестовой сети	199
Запуск узла в режиме regtest	199
Экспериментирование с Bitcoin-cli.....	200
Программирование Bitcoin и интерфейс командной строки.....	201
Заключение	202
Глава 8. Альтернативные криптовалюты	203
Теоретические основы	206
Альтернативы Proof of Work	206
Доказательство хранения	209
Подтверждение доли владения (PoS).....	209
Различные типы долей.....	209
Доказательство возраста монеты.....	209
Доказательство депозита (PoD)	210
Доказательство уничтожения (PoB)	210
Доказательство активности (PoA)	210
Нетрадиционные задачи	210
Настройка сложности и алгоритмы перенацеливания.....	211
Гравитационный колодец Кимото (KGW).....	212
Dark Gravity Wave	212
DigiShield.....	213
MIDAS	213
Ограничения Bitcoin.....	214
Приватность и анонимность.....	214
Протоколы смешивания.....	214
Сторонние протоколы смешивания.....	215

Неотъемлемая анонимность.....	216
Расширенные протоколы над Bitcoin.....	216
Цветные монеты.....	216
Контрагент.....	217
Разработка альтернативных криптовалют.....	218
Алгоритмы консенсуса.....	219
Алгоритмы хеширования.....	219
Алгоритмы настройки сложности.....	219
Время между блоками.....	219
Награды блоков.....	219
Частота разделения награды.....	219
Размер блока и размер транзакции.....	219
Частота процента.....	220
Возраст монеты.....	220
Общее число монет.....	220
Namecoin.....	220
Обмен Namecoin.....	222
Получение Namecoin.....	222
Генерирование записей Namecoin.....	225
Litecoin.....	226
Primescoin.....	229
Обмен Primescoin.....	230
Руководство по майнингу.....	230
Zcash.....	232
Обмен Zcash.....	234
Руководство по майнингу.....	235
Генерирование адресов.....	237
Майнинг на графическом адаптере.....	238
Первичное предложение монет (Initial Coin Offerings – ICO).....	240
Жетоны ERC20.....	241
Заключение.....	241
Глава 9. Смарт-контракты.....	243
История.....	243
Определение.....	244
Рикарданские контракты.....	247
Шаблоны смарт-контрактов.....	250
Оракулы.....	251
Умные оракулы.....	254
Запуск смарт-контрактов в блокчейне.....	254
DAO.....	255
Заключение.....	256

Глава 10. Знакомство с Ethereum	257
Введение.....	257
Желтый документ.....	258
Полезные математические символы.....	258
Блокчейн Ethereum.....	259
Ethereum с высоты птичьего полета.....	260
Сеть Ethereum.....	263
Mainnet.....	264
Testnet.....	264
Частная сеть.....	264
Компоненты экосистемы Ethereum.....	264
Ключи и адреса.....	265
Учетные записи.....	266
Виды учетных записей.....	267
Транзакции и сообщения.....	267
Транзакция с созданием контракта.....	270
Транзакция с вызовом сообщения.....	271
Сообщения.....	271
Вызовы.....	272
Проверка и выполнение транзакций.....	272
Промежуточное состояние транзакции.....	273
Хранение состояния в блокчейне Ethereum.....	273
Глобальное состояние.....	273
Состояние учетной записи.....	273
Квитанции.....	274
Криптовалюта Ether: токены ETC и ETH.....	276
Виртуальная машина Ethereum.....	276
Среда выполнения.....	278
Состояние виртуальной машины.....	279
Функция итератора.....	280
Смарт-контракты.....	280
Стандартные контракты.....	281
Заключение.....	282
Глава 11. Ethereum. Продолжение	283
Языки программирования.....	283
Байт-код среды выполнения.....	284
Команды и их назначение.....	284
Арифметические операции.....	285
Логические операции.....	285
Криптографические операции.....	286
Информация об окружении.....	286
Информация о блоке.....	287

Операции со стеком, памятью, хранилищем и потоком выполнения	287
Операции сохранения	287
Операции дублирования.....	288
Операции замены.....	288
Журнальные операции.....	288
Системные операции	289
Блоки и блокчейн	289
Начальный блок.....	291
Механизм проверки блоков	292
Сложность блока	293
Газ	294
Планирование комиссии.....	295
Ответвления в блокчейне	295
Узлы и майнеры.....	295
Ethash	297
Кошельки и клиентские программы	302
API-интерфейсы, инструменты и децентрализованные приложения	311
Вспомогательные протоколы	312
Whisper	312
Swarm.....	313
Масштабируемость, безопасность и другие вызовы.....	314
Торговля и инвестиции	314
Заключение	315
Глава 12. Среда разработки Ethereum.....	316
Тестовые сети.....	317
Подготовка частной сети	318
Идентификатор сети	318
Файл с начальным блоком	318
Директория с данными	320
Флаги и их назначение.....	320
Статические узлы	320
Запуск частной сети	321
Запуск клиента Mist в частной сети	325
Развертывание контрактов с помощью Mist.....	327
Обозреватель блоков для частных/локальных сетей Ethereum.....	331
Заключение	334
Глава 13. Инструменты разработки и фреймворки	335
Языки программирования.....	336
Компиляторы	337
Компилятор Solidity (solc)	337
Интегрированные среды разработки	339

Инструменты и библиотеки	342
Ganache	343
MetaMask	344
Truffle	346
Разработка и развертывание контрактов	347
Язык программирования Solidity	349
Типы	349
Примитивные типы	350
Литералы	351
Перечисления	352
Функции	352
Ссылочные типы	352
Глобальные переменные	353
Управляющие конструкции	354
Структура исходного файла Solidity	359
Заключение	360
Глава 14. Введение в Web3	361
Web3.....	361
Развертывание контрактов	362
POST-запросы	367
Клиентская сторона на основе HTML и JavaScript	368
Установка web3.js	369
Фреймворки для разработки	375
Truffle	375
Оракулы	397
Развертывание в децентрализованном хранилище с использованием IPFS	399
Распределенные журналы	401
Заключение	402
Глава 15. Hyperledger.....	403
Проекты, входящие в состав Hyperledger.....	403
Fabric	403
Sawtooth Lake	404
Iroha	404
Burrow	405
Indy	405
Explorer	405
Cello	405
Composer	406
Quilt	406
Hyperledger как протокол.....	406

Эталонная архитектура	406
Hyperledger Fabric: требования и архитектурные решения	408
Модульный подход	408
Сохранность личных данных и конфиденциальность	408
Масштабируемость	409
Предсказуемые транзакции	409
Проверка подлинности	409
Проверяемость	409
Интероперабельность	410
Переносимость	410
Гибкие запросы	410
Fabric.....	410
Hyperledger Fabric	411
Сервисы членства	412
Сервисы блокчейна	412
Сервисы консенсуса	412
Распределенный журнал	413
Sawtooth Lake	421
PoET	422
Семейства транзакций	422
Консенсус в Sawtooth	424
Среда разработки для Sawtooth Lake	425
Corda	427
Архитектура	428
Компоненты	430
Среда разработки для Corda	433
Заключение	434
Глава 16. Альтернативные блокчейны.....	435
Блокчейны.....	435
Kadena	436
Ripple	440
Транзакции	443
Interledger	444
Stellar	446
Rootstock	447
Сайдчейн	447
Драйвчейн	447
Quorum	448
Менеджер транзакций	448
Криптоанклав	448
Механизм QuorumChain	448
Менеджер сети	449

Tezos	450
Storj	450
MaidSafe	451
BigchainDB	452
MultiChain	452
Tendermint	452
Ядро Tendermint	453
Протокол сокета Tendermint (TMSP)	453
Платформы и фреймворки	454
Eris	454
Заключение	455
Глава 17. Блокчейн – вне сферы валют	457
Интернет вещей	457
Уровень физических объектов	459
Уровень устройства	459
Сетевой уровень	460
Уровень управления	460
Прикладной уровень	460
Эксперимент блокчейна интернета вещей	464
Настройка первого узла	467
Настройка узла Raspberry Pi	468
Цепь	472
Государственные услуги	478
Пограничный контроль	479
Голосование	481
Идентификация населения (ID-карты)	482
Прочие услуги	483
Здравоохранение	483
Финансы	484
Страхование	484
Расчет после сделок	484
Предотвращение финансовых преступлений	485
Медиа	486
Заключение	487
Глава 18. Масштабируемость и другие вызовы	488
Масштабируемость	489
Плоскость сети	489
Плоскость консенсуса	490
Плоскость хранения	490
Плоскость вида	490
Увеличение размера блока	490

Уменьшение интервала блока	491
Инвертируемые таблицы поиска Bloom	491
Шардинг	492
Каналы состояния	492
Приватный блокчейн	493
Доказательство доли владения	493
Сайдчейны	493
Сабчейны	494
Цепи-деревья	494
Распространение блоков	495
Bitcoin-NG	495
Plasma	496
Приватность	496
Обфускация неразличимости	496
Гомоморфное шифрование	497
Доказательства с нулевым разглашением	497
Каналы состояния	498
Безопасное многостороннее вычисление	498
Применение аппаратного обеспечения для конфиденциальности	498
CoinJoin	499
Конфиденциальные транзакции	499
MimbleWimble	500
Безопасность	500
Безопасность смарт-контрактов	501
Заключение	507
Глава 19. Текущая и дальнейшая перспективы	508
Новые тенденции	508
Блокчейны специфических приложений (ASBC)	508
Корпоративные блокчейны	509
Приватные блокчейны	509
Стартапы	509
Высокий исследовательский интерес	510
Стандартизация	510
Улучшения	511
Реальные реализации	512
Консорциумы	512
Ответы на технические вызовы	512
Сближение	513
Образование в сфере блокчейн-технологий	513
Трудоустройство	513
Криптоэкономика	514
Исследования в криптографии	514

Новые языки программирования	514
Аппаратные исследования и разработка	514
Исследования в формальных методах и безопасности	515
Альтернативы блокчейнам	515
Взаимодействие сетей	516
Блокчейн как сервис	516
Действия по уменьшению расхода электричества	516
Другие вызовы	517
Регулирование	517
Темная сторона	518
Исследования блокчейна	520
Смарт-контракты	520
Проблемы централизации	520
Ограничения в криптографических функциях	520
Алгоритмы консенсуса	520
Масштабируемость	521
Код обфускации	521
Примечательные проекты	521
Zcash на Ethereum	521
CollCo	521
Cello	522
Qtum	522
Bitcoin-NG	522
Solidus	522
Hawk	522
Town-Crier	523
SETLCoin	523
TEEChan	523
Falcon	523
Bletchley	524
Casper	524
Прочие инструменты	524
Расширение Solidity для Microsoft Visual Studio	524
MetaMask	525
Stratis	525
Embark	525
DAPPLE	525
Meteor	525
uPort	526
INFURA	526
Сближение с другими отраслями	526
Будущее	527
Заключение	529
Предметный указатель	530

Над книгой работали

ОБ АВТОРЕ

Имран Башир – магистр информатики, получил научную степень в Королевском колледже Холлоуэй при Лондонском университете. Ранее занимался разработкой ПО, архитектурой решений, управлением инфраструктурой и управлением ИТ-услугами. Также он является членом IEEE (Института инженеров электротехники и электроники) и BCS (Британского общества вычислительной техники).

Имран обладает шестнадцатилетним опытом работы в государственном и финансовом секторе. Он работал на крупномасштабных ИТ-проектах в государственном секторе, а затем перешел в сегмент финансовых услуг. С тех пор он занимал различные технические должности в нескольких крупных финансовых компаниях в Лондоне – финансовой столице Европы. В настоящее время он работает в Лондонском инвестиционном банке в должности вице-президента технологического отдела.

Я хотел бы поблагодарить талантливую команду издательства Packt, в частности Бена Реноу-Кларка, Сюзанну Коутиньо, Алекса Соррентино, Гэри Швартца и Бхагъяшири Рай, которые помогли мне в этом проекте своими своевременными подсказками и ценными замечаниями. Также я исключительно благодарен рецензенту Пранаву Бурнвалу, чьи конструктивные и очень полезные отзывы невероятно помогли мне усовершенствовать материал этой книги.

Благодарю жену и детей, которые позволили мне ночами (и даже в выходные) работать над этой книгой.

Особенно я благодарен родителям, благословения которых позволили мне достичь всего, что только возможно.

О РЕЦЕНЗЕНТЕ

Пранав Бурнвал ранее трудился в сфере НИОКР, а в последние несколько лет занимался ультрасовременными технологиями. Вот их неполный список: блокчейн, большие данные, аналитика (логи и данные), облачные технологии, очереди сообщений, NoSQL, веб-серверы и т. д. Он работал в различных отраслях, среди прочего – в банковском деле, финансах и страховании (БФС), здравоохранении, сфере товаров широкого потребления и в автомобилестроении.

Пранав активно участвует в работе нескольких сообществ. Он является региональным руководителем образовательной сети блокчейна (BEN), это офи-

циально зарегистрированная неправительственная организация, сеть специалистов по блокчейну. Также он организовал множество митапов и индийский «стартап-уикенд».

Пранав активно преподает материалы на тему блокчейна (уже три года), его целевая аудитория варьируется от младших разработчиков до старших вице-президентов. Такая работа также помогает ему осознать, как люди понимают новые и сложные технологии; этот опыт помог ему обработать данную книгу так, чтобы она получилась максимально интересной читателям.

Предисловие

Данная книга написана с единственной целью – познакомить вас с теоретическими и практическими аспектами технологии блокчейн. В книге содержится весь необходимый материал, который позволит вам стать экспертом по блокчейну. Со времени выхода первого издания этой книги технология значительно изменилась, многие аспекты блокчейна усовершенствовались. Именно поэтому возникла необходимость обновить книгу.

Внедрение технологии блокчейн сулит многочисленные выгоды – вот почему к блокчейну пробудился такой неподдельный интерес, охвативший различные сферы, от академической до промышленной. Во всех этих сферах сейчас неустанно исследуют блокчейн. В результате возникло множество консорциумов, рабочих групп, проектов и профессиональных организаций, занятых разработкой и дальнейшим совершенствованием этой технологии. Во втором издании данной книги углубленно рассмотрены следующие темы: что такое децентрализация, умные контракты, что из себя представляют различные блокчейновые платформы, в частности Ethereum, Bitcoin и Hyperledger Fabric. Изучив эту книгу, читатель будет детально понимать внутреннее устройство блокчейна и сможет сам разрабатывать блокчейновые приложения.

В книге рассмотрены все важные темы, касающиеся технологии блокчейн, в том числе криптография, криптовалюты, Bitcoin, Ethereum, а также различные другие платформы и инструменты, связанные с разработкой блокчейна. Ожидается, что читатель обладает базовым пониманием информатики и минимальным опытом программирования – в таком случае он сможет извлечь из этой книги максимальную пользу. Однако и без такого опыта книга читается легко, поскольку важный контекстный материал приводится везде, где это необходимо.

Для кого эта книга

Книга предназначена для всех, кто хочет подробно разобраться в блокчейне. Также она пригодится в качестве справочника тем программистам, которые занимаются разработкой блокчейновых приложений. Кроме того, она может использоваться в качестве учебника на курсе по криптовалютам и блокчейновым технологиям.

Структура книги

Глава 1 «Блокчейн. Курс молодого бойца» знакомит вас с фундаментальными концепциями распределенных вычислений, на которых базируется блокчейновая технология. Здесь также рассмотрены история, определения, характер-

ные черты, типы и достоинства блокчейна, плюс различные механизмы консенсуса, образующие ядро блокчейновой технологии.

Глава 2 «*Децентрализация*» рассматривает концепцию децентрализации и ее связь с блокчейновой технологией. Для децентрализации процесса подойдут различные методы и платформы, и с ними вы также познакомитесь в этой главе.

Глава 3 «*Симметричное шифрование*» знакомит вас с теоретическими основами симметричной криптографии. Этот материал необходим, чтобы разобраться, как реализованы различные службы обеспечения безопасности, гарантирующие, в частности, конфиденциальность и целостность данных.

Глава 4 «*Шифрование с открытым ключом*». Здесь разобраны такие концепции, как открытые и закрытые ключи, цифровые подписи и хеш-функции, приведены практические примеры. Кроме того, дается вводная информация о финансовых рынках, так как технология блокчейна находит множество интересных вариантов применения в финансовом секторе.

Глава 5 «*Знакомство с биткойном*» посвящена валюте биткойн – первой и крупнейшей реализации блокчейна. Здесь подробно описаны технические концепции, связанные с криптовалютой биткойн.

Глава 6 «*Сеть и платежи Bitcoin*» рассматривает сеть Bitcoin, соответствующие протоколы и различные кошельки. Более того, здесь дается вводная информация о сложных протоколах, торговых операциях и платежах с применением биткойна.

Глава 7 «*Клиенты и API Bitcoin*» рассказывает о различных биткойн-клиентах и интерфейсах программирования приложений (API), при помощи которых можно создавать приложения для работы с биткойном.

Глава 8 «*Альтернативные криптовалюты*» рассказывает об альтернативных криптовалютах, появившихся после изобретения биткойна. Также здесь приведены примеры различных альтернативных валют, описаны их свойства, сказано, как их разрабатывали и внедряли.

Глава 9 «*Смарт-контракты*». Здесь подробно обсуждается тема умных контрактов. Затронута их история, дается определение, а также рассмотрены такие темы, как рикардийские контракты, ораклы и теоретические аспекты умных контрактов.

Глава 10 «*Знакомство с Ethereum*». Здесь вы подробно познакомитесь с дизайном и архитектурой блокчейновой валюты Ethereum. В главе рассмотрены различные технические концепции, связанные с блокчейном Ethereum, подробно объясняются базовые принципы, возможности и компоненты этой платформы.

Глава 11 «*Ethereum. Продолжение*». Здесь продолжается рассказ об Ethereum, начатый в предыдущей главе. Рассматриваются темы, связанные с виртуальной машиной Ethereum, майнингом и поддержкой протоколов Ethereum.

Глава 12 «*Среда разработки Ethereum*» охватывает темы, связанные с настройкой частных сетей для разработки и программирования умных контрактов Ethereum.

Глава 13 «*Инструменты разработки и фреймворки*». Это подробное практическое введение в язык программирования Solidity и знакомство с различными важными инструментами и фреймворками, используемыми для разработки Ethereum.

Глава 14 «*Введение в Web3*» описывает разработку децентрализованных приложений и умных контрактов при помощи блокчейна Ethereum. Дается подробное введение в API Web3, а также множество практических примеров и готовый проект.

Глава 15 «*Hyperledger*», где обсуждается проект Hyperledger от Linux Foundation. Hyperledger объединяет различные блокчейновые проекты, предложенные участниками фонда.

Глава 16 «*Альтернативные блокчейны*» знакомит вас с альтернативными блокчейновыми решениями и платформами. В ней описываются технические детали и возможности альтернативных блокчейнов и соответствующих платформ.

Глава 17 «*Блокчейн – вне сферы валют*» практически и подробно рассказывает о возможностях применения блокчейновых технологий вне контекста криптовалют, в частности с интернетом вещей, в государственных программах, СМИ и финансах.

Глава 18 «*Масштабируемость и другие вызовы*» посвящена обсуждению серьезных проблем, с которыми сталкивается блокчейновая технология, и способам их решения.

Глава 19 «*Текущая и дальнейшая перспективы*» рассказывает о сложившемся технологическом ландшафте, проектах и исследовательских разработках, связанных с блокчейновой технологией. Также здесь делаются некоторые прогнозы на основе современного состояния блокчейновых технологий.

КАК ВЫЖАТЬ ИЗ ЭТОЙ КНИГИ МАКСИМУМ

- Все примеры в этой книге разрабатывались на Ubuntu 16.04.1 LTS (Xenial) и macOS версии 10.13.2. Поэтому рекомендуется работать с Ubuntu или другой Unix-подобной системой. Однако вам подойдет и любая другая современная операционная система, например Windows или Linux, но примеры, особенно связанные с установкой, возможно, потребуются соответствующим образом адаптировать.
- Примеры, касающиеся криптографии, разрабатывались при помощи инструмента командной строки OpenSSL 1.0.2g 1 Mar 2016.
- Примеры с Ethereum Solidity разрабатывались в IDE Remix, доступной в интернете по адресу remix.ethereum.org.
- Для разработки примеров, связанных с Ethereum, использовался релиз Ethereum Byzantine. На момент написания книги это была новейшая доступная версия, скачать ее можно по адресу www.ethereum.org.
- Примеры, связанные с интернетом вещей, разрабатывались при помощи комплектации Raspberry Pi от Vilros, однако можно воспользоваться и лю-

бой другой подходящей моделью или комплектацией. В частности, при подготовке аппаратных примеров для интернета вещей использовалась модель Raspberry Pi 3 B V 1.2. Для скачивания соответствующих пакетов и запуска сервера Node.js для примеров с интернетом вещей использовались Node.js V8.9.3 и npm V5.5.1.

- В некоторых примерах развертывания умных контрактов использовался фреймворк Truffle, доступный по адресу truffleframework.com. Также должна подойти любая более новая версия, доступная через npm.

СКАЧИВАНИЕ ФАЙЛОВ С ПРИМЕРАМИ КОДА

Примеры кода к этой книге можно скачать следующим образом.

1. Откройте в браузере страницу по адресу github.com/PacktPublishing/Mastering-Blockchain-Second-Edition.
2. Нажмите кнопку **Clone or Download**.
3. Выберите пункт **Download ZIP**.

Когда файл скачается, разархивируйте его и извлеките папку при помощи последней версии программы:

- WinRAR/7-Zip для Windows;
- Zipeg/iZip/UnRarX для macOS;
- 7-Zip/PeaZip для Linux.

СКАЧИВАНИЕ ЦВЕТНЫХ ИЗОБРАЖЕНИЙ

Также мы предоставляем PDF-файл с цветными вариантами скриншотов и схем из этой книги. Его можно скачать по адресу www.packtpub.com/sites/default/files/downloads/MasteringBlockchainSecondEdition_ColorImages.pdf.

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

В тексте книги используется ряд условных обозначений:

Моноширинным шрифтом обозначается код, встречающийся в тексте, и названия таблиц из баз данных.

Курсивом обозначены имена каталогов и файлов, расширения файлов и имена путей.

Пример: «После выполнения команды `create` создается файл *privatekey.pem*, в котором содержится следующий сгенерированный закрытый ключ».

Листинг с кодом оформляется так:

```
pragma solidity ^0.4.0;
contract TestStruct {
    struct Trade
    {
        uint tradeid;
        uint quantity;
```

Конец ознакомительного фрагмента.

Приобрести книгу можно

в интернет-магазине

«Электронный универс»

e-Univers.ru