

УДК 004.738.5:336.74  
ББК 32.971.35+65.262.6с  
Б33

**Башир И.**

Б33 Блокчейн: архитектура, криптовалюта, инструменты разработки, смарт-контракты / пер. с англ. М. А. Райтмана. – М.: ДМК Пресс, 2019. – 538 с.: ил.

**ISBN 978-5-97060-624-7**

Книга познакомит вас с теоретическими и практическими аспектами технологии блокчейн. Углубленно рассмотрены архитектура блокчейна, децентрализация, симметричное шифрование и шифрование с открытым ключом. Описаны смарт-контракты и различные блокчейн-платформы, в частности Bitcoin, Ethereum, Hyperledger Fabric. Также уделено внимание инструментам разработки и фреймворкам для работы с децентрализованными приложениями.

Издание будет полезно в первую очередь разработчикам, желающим использовать мощь распределенных систем в своей работе.

УДК 004.738.5:336.74  
ББК 32.971.35+65.262.6с

Authorized Russian translation of the English edition of Mastering Blockchain, Second Edition  
ISBN 9781788839044 © 2018 Packt Publishing.

This translation is published and sold by permission of Packt Publishing, 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 978-1-78883-904-4 (англ.)  
ISBN 978-5-97060-624-7 (рус.)

Copyright © 2018 Packt Publishing  
© Оформление, издание, перевод, ДМК Пресс, 2019

# Содержание

<b>Над книгой работали .....</b>	<b>20</b>
<b>Предисловие .....</b>	<b>22</b>
<b>Глава 1. Блокчейн. Курс молодого бойца .....</b>	<b>27</b>
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

<b>Глава 2. Децентрализация</b> .....	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
<b>Глава 3. Симметричное шифрование</b> .....	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
Заклучение .....	132
<b>Глава 5. Знакомство с биткойном .....</b>	<b>133</b>
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
<b>Глава 6. Сеть и платежи Bitcoin.....</b>	<b>176</b>
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
Серегрированный свидетель (SegWit) .....	191
Bitcoin Cash .....	192
Bitcoin Unlimited .....	192
Bitcoin Gold.....	193
Инвестирование в биткойны и продажа биткойнов.....	193
Заключение .....	195
<b>Глава 7. Клиенты и API Bitcoin .....</b>	<b>196</b>
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
<b>Глава 8. Альтернативные криптовалюты .....</b>	<b>203</b>
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
<b>Глава 9. Смарт-контракты .....</b>	<b>243</b>
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



<b>Глава 10. Знакомство с Ethereum.....</b>	<b>257</b>
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
Закключение .....	282
 <b>Глава 11. Ethereum. Продолжение .....</b>	 <b>283</b>
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
<b>Глава 12. Среда разработки Ethereum.....</b>	<b>316</b>
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
<b>Глава 13. Инструменты разработки и фреймворки .....</b>	<b>335</b>
Языки программирования.....	336
Компиляторы .....	337
Компилятор Solidity (solc) .....	337
Интегрированные среды разработки .....	339

## 14 ❖ Содержание

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
<b>Глава 14. Введение в Web3 .....</b>	<b>361</b>
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
<b>Глава 15. Hyperledger.....</b>	<b>403</b>
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
<b>Глава 16. Альтернативные блокчейны .....</b>	<b>435</b>
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 .....**

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 .....**

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
<b>Глава 19. Текущая и дальнейшая перспективы .....</b>	<b>508</b>
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
<b>Предметный указатель .....</b>	<b>530</b>