

*Эта книга посвящается моему отцу,
со всей моей безмерной любовью и благодарностью.
Это самый ласковый, самоотверженный и трудолюбивый
мужчина, который пожертвовал всем ради меня*



“

*Не стоит переживать, сын мой! Невзгоды приходят
и уходят.*

– Ученый Башир Ахмед Хан

76 → 363 → 1245 → 1003 → 275 → 77 → 60 → 588 → 1 → 12 → 12 → 2215 → ∞

Содержание

От издательства	18
Над книгой работали	19
Предисловие	21
 Глава 1. Блокчейн. Курс молодого бойца	 26
Развитие блокчейна	26
Прогресс на пути к созреванию	27
Рост заинтересованности	28
Распределенные системы	30
CAP-теорема	32
PASELC-теорема	34
История блокчейна	35
Биткойн	36
Электронная наличность	36
Введение в блокчейн	38
Архитектура блокчейна	40
Общие элементы блокчейна	42
Как работает блокчейн	46
Преимущества и возможности блокчейна	48
Ограничения блокчейна	50
Типы блокчейна	52
Распределенные реестры	53
Общедоступный реестр	53
Публичные блокчейны	54
Приватные блокчейны	54
Полуприватные блокчейны	54
Закрытый распределенный реестр	54
Полностью приватные и проприетарные блокчейны	55
Токенизированные блокчейны	55
Нетокенизированные блокчейны	55
Блокчейны первого уровня	56
Блокчейны второго уровня	57
Заключение	57
 Глава 2. Децентрализация	 59
Введение в децентрализацию	59
Методы децентрализации	64

Избавление от посредников	64
Децентрализация на основе состязания	65
Измерение степени децентрализации	65
Преимущества децентрализации	66
Оценка требований	68
Децентрализация всей экосистемы	69
Хранилище данных	70
Коммуникация	71
Вычислительная мощность	72
Децентрализация на практике	74
Смарт-контракты	74
Автономные агенты	74
Децентрализованные организации	74
Децентрализованные автономные организации	75
Децентрализованные автономные корпорации	76
Децентрализованные автономные общества	76
Децентрализованные приложения	77
Требования к децентрализованным приложениям	78
Операции, проводимые децентрализованными приложениями	79
Проектирование ДП	79
Инновационные тенденции	81
Децентрализованная сеть	81
Web 1	82
Web 2	82
Web 3	82
Заключение	83
Глава 3. Симметричное шифрование	84
Введение в криптографию	85
Возможности криптографии	86
Криптографические примитивы	88
Примитивы без ключа	88
Примитивы симметричных ключей	102
Стандарт шифрования AES	110
Стандарт шифрования данных	110
Принцип работы AES	110
Шифрование и дешифрование с помощью AES	112
Заключение	114
Глава 4. Асимметричное шифрование	115
Математические основы	115
Асимметричное шифрование	117
Открытые и закрытые ключи	117
Алгоритмы асимметричной криптографии	119
Интегрированная схема шифрования	120
Введение в RSA	121

Шифрование и дешифрование с помощью RSA	122
Введение в ECC	124
Математический фундамент ECC.....	125
Задача дискретного логарифмирования.....	131
Генерация ключей с помощью ECC.....	133
Цифровые подписи.....	136
Алгоритм цифровой подписи RSA	137
Генерация цифровых подписей RSA.....	138
Алгоритм ECDSA	139
Создание цифровых подписей ECDSA.....	140
Типы цифровых подписей.....	142
Слепые подписи	143
Мультиподписи	144
Пороговые подписи.....	145
Множественная подпись	146
Кольцевые подписи	147
Криптографические конструкции и технология блокчейн	148
Гомоморфное шифрование.....	148
Разделение секрета.....	149
Схемы обязательств.....	149
Доказательства с нулевым разглашением	150
Схемы кодирования	156
Алгоритм VRF	157
Заключение	158
Глава 5. Алгоритмы консенсуса	159
Введение в тему консенсуса	159
Отказоустойчивость	160
FLP-невозможность.....	162
Анализ и проектирование	163
Модель	163
Процессы.....	163
Временные допущения	164
Классификация.....	164
Алгоритмы	165
Алгоритм CFT	166
Алгоритмы BFT	171
Выбор алгоритма.....	199
Окончателность.....	200
Скорость, производительность и масштабируемость.....	200
Заключение	201
Глава 6. Архитектура биткойна.....	202
Знакомство с биткойном	202
Криптографические ключи	204
Закрытые ключи биткойна.....	204

Открытые ключи биткойна	205
Адреса	206
Типичные адреса сети биткойн	207
Расширенные адреса сети биткойн	209
Транзакции	209
Транзакция coinbase	210
Жизненный цикл транзакции	211
Структура данных транзакции	213
Скриптовый язык	216
Ошибки транзакций	222
Блокчейн	223
Структура	223
Блок генезиса	225
Устаревшие и блоки-сироты	225
Вилки	226
Свойства	227
Майнеры	228
Доказательство выполненной работы (PoW)	230
Системы майнинга	232
Майнинг-пулы	234
Сеть	235
Типы сообщений	236
Клиентское программное обеспечение	241
Фильтры Блума	242
Кошельки	244
Заключение	247
Глава 7. Биткойн на практике	248
Биткойн в реальном мире	248
Платежи в сети биткойн	250
Инновации в сети биткойн	252
Предложения по улучшению биткойна	252
Продвинутые протоколы	254
Расширенные протоколы над биткойном	259
Альткойны от биткойна	262
Установка клиента биткойна	263
Типы клиентов и инструментов	263
Настройка биткойн-узла	264
Запуск узла в тестовой сети	265
Запуск узла в режиме regtest	267
Дальнейшие эксперименты с bitcoin-cli	269
Использование инструмента командной строки биткойна	270
Использование интерфейса JSON-RPC	271
Использование интерфейса HTTP REST	273
Программирование биткойна	274
Заключение	274

Глава 8. Смарт-контракты	276
Знакомство со смарт-контрактами	276
Определения	277
Свойства	278
Применение в реальных условиях	280
Рикардианские контракты	281
Шаблоны смарт-контрактов	285
Оракулы	287
Программные и сетевые доказательства	290
Доказательства с помощью аппаратных средств	291
Типы оракулов в блокчейне	294
Сервисы оракулов для блокчейна	298
Развертывание смарт-контрактов	299
The DAO	300
Достижения в области технологии смарт-контрактов	302
Solana Sealevel	302
Digital Asset Modeling Language (DAML)	302
Заключение	304
 Глава 9. Архитектура Ethereum	 306
Введение в Ethereum	306
Криптовалюта	308
Ключи и адреса	309
Учетные записи	313
Транзакции и сообщения	315
Базисное дерево Меркла (MPT)	315
Компоненты транзакций	317
Рекурсивный префикс длины	321
Газ	322
Типы транзакций	324
Сообщения	326
Проверка и выполнение транзакций	327
Состояние и хранение в блокчейне Ethereum	328
Виртуальная машина Ethereum	332
Среда выполнения	335
Состояние виртуальной машины	335
Блоки и блокчейн	336
Блок генезиса	338
Механизм проверки, обработки и завершения работы над блоком	338
Механизм изменения сложности блока	340
Узлы и майнеры	341
Механизм консенсуса	342
Вилки в блокчейне	343
Сеть Ethereum	344
Основная сеть	344
Тестовые сети	344

Частные сети.....	344
Предварительно скомпилированные смарт-контракты.....	349
Языки программирования	351
Solidity	351
Байт-код среды выполнения.....	351
Опкоды	352
Кошельки и клиентские программы.....	352
Кошельки.....	352
Клиент Geth	353
Легкие клиенты.....	353
Вспомогательные протоколы.....	353
Протокол Whisper	354
Протокол Swarm	354
Заключение	355

Глава 10. Ethereum на практике..... 356

Платежи в Ethereum.....	356
Инновации в Ethereum.....	358
Бомба сложности.....	358
EIP-1559.....	359
Обновление Merge и будущие обновления.....	361
Программирование с Geth.....	362
Установка и настройка клиента Geth.....	362
Создание новой учетной записи в Geth	363
Запрос к блокчейну с помощью Geth.....	364
Настройка среды разработки	369
Подключение к тестовым сетям	369
Создание частной сети.....	370
Знакомство с IDE Remix	383
Взаимодействие с блокчейном Ethereum с помощью MetaMask.....	385
Установка MetaMask	386
Создание и пополнение счета в MetaMask	387
Использование MetaMask и IDE Remix для развертывания смарт-контрактов	389
Заключение	403

Глава 11. Инструменты, языки и фреймворки для разработчиков Ethereum..... 404

Языки	405
Компилятор Solidity.....	405
Установка solc.....	406
Эксперименты с solc.....	407
Инструменты, библиотеки и фреймворки	409
Node.js.....	409
Ganache.....	410
Truffle	412

Drizzle	414
Другие инструменты	414
Разработка и развертывание контрактов	415
Написание смарт-контрактов	415
Тестирование смарт-контрактов	416
Развертывание смарт-контрактов	416
Язык Solidity	416
Функции	418
Переменные	422
Типы данных	424
Управляющие структуры	429
События	431
Наследование	431
Библиотеки	432
Обработка ошибок	433
Заключение	434

Глава 12. Реализация Web3 с применением Ethereum..... 435

Взаимодействие с контрактами с применением Web3 и Geth	436
Развертывание контрактов	437
Использование solc для генерации ABI и кода	441
Запрос контрактов с помощью Geth	442
Взаимодействие с Geth с помощью POST-запросов	445
Взаимодействие с контрактами с помощью интерфейсов	447
Установка библиотеки JavaScript web3.js	447
Создание объекта web3	448
Создание JavaScript-файла app.js	449
Создание веб-страницы фронтенда	452
Вызов функций контракта	453
Применение веб-страницы фронтенда	454
Развертывание и работа с контрактами с Truffle	457
Установка и инициализация Truffle	458
Компиляция, тестирование и миграция с помощью Truffle	459
Взаимодействие с контрактом	463
Использование Truffle для тестирования и развертывания смарт-контрактов	465
Развертывание в децентрализованном хранилище с IPFS	470
Заключение	472

Глава 13. Жизнь после The Merge..... 473

Введение	473
Ethereum после The Merge	474
Обновление Beacon Chain	476
Интерфейс P2P (работа с сетью)	490
«Слияние» (The Merge)	491
Шардинг	502

Перспективы развития Ethereum	512
Заключение	514
Глава 14. Hyperledger	515
Проекты в рамках Hyperledger	516
Распределенные реестры	516
Библиотеки	519
Инструменты	520
Специальные приложения	521
Эталонная архитектура Hyperledger	522
Принципы разработки Hyperledger	524
Hyperledger Fabric	527
Ключевые концепции	527
Компоненты	532
Приложения	535
Механизм консенсуса	538
Жизненный цикл транзакции	539
Fabric 2.0	541
Новое управление жизненным циклом чейнкода	541
Новые шаблоны применения чейнкодов	543
Заключение	544
Глава 15. Токенизация	546
Токенизация на блокчейне	547
Преимущества токенизации	547
Недостатки токенизации	549
Типы токенов	551
Взаимозаменяемые токены	551
Невзаимозаменяемые токены	552
Стабильные токены	553
Security-токены	554
Процесс токенизации	554
Предложения токенов	555
Первичные размещения монет	555
Предложения security-токенов	557
Первичное биржевое предложение	557
Предложения токенов акций	557
Децентрализованное автономное первичное размещение монет	558
Другие предложения токенов	558
Стандарты токенов	559
ERC-20	560
ERC-223	560
ERC-777	560
ERC-721	561
ERC-884	561
ERC-1400	561

ERC-1404.....	562
ERC-1155.....	562
ERC-4626.....	563
Создание токена ERC-20.....	564
Создание контракта на Solidity.....	564
Развертывание контракта на виртуальной машине Remix JavaScript	569
Добавление токенов в MetaMask	574
Перспективные концепции.....	576
Токеномика/экономика токенов	576
Инженерная разработка токенов	577
Таксономия токенов	577
Заключение	578
Глава 16. Корпоративный блокчейн.....	579
Корпоративные решения и блокчейн	580
Факторы успеха	581
Ограничивающие факторы	582
Требования.....	584
Приватность	585
Производительность	586
Управление доступом	587
Дополнительные требования.....	587
Корпоративный блокчейн в сравнении с публичным блокчейном	591
Архитектура корпоративного блокчейна.....	592
Проектирование корпоративных решений на блокчейне.....	595
TOGAF.....	595
Метод разработки архитектуры (ADM)	596
Блокчейн в облаке.....	599
Доступные корпоративные блокчейн-платформы	601
Проблемы корпоративных блокчейнов.....	603
Взаимозаменяемость	603
Недостаточная стандартизация	603
Соответствие требованиям	604
Бизнес-задачи	605
Блокчейн VMware	605
Компоненты.....	605
Протокол консенсуса.....	606
Архитектура.....	607
Блокчейн VMware для Ethereum	609
Quorum.....	610
Архитектура.....	610
Криптография	613
Приватность	613
Управление доступом с помощью прав доступа.....	618
Производительность	619
Подключаемый консенсус.....	620

Настройка сети Quorum с помощью IBFT	620
Установка и запуск Quorum Wizard	621
Запуск приватной транзакции	624
Подключение Geth к узлам.....	624
Просмотр транзакции в Cakeshop	627
Дальнейшие исследования с помощью Geth.....	628
Другие проекты Quorum	632
Плагин Remix	632
Подключаемая архитектура	632
Заключение	633
Глава 17. Масштабируемость.....	634
Что такое масштабируемость?	634
Трилемма блокчейна.....	635
Методы улучшения масштабируемости.....	638
Роллапы	652
Заключение	678
Глава 18. Конфиденциальность блокчейна	679
Конфиденциальность	680
Анонимность	680
Конфиденциальность.....	681
Методы достижения конфиденциальности	682
Уровень 0.....	683
Приватность с использованием нулевого знания	694
Пример	713
Заключение	720
Глава 19. Безопасность блокчейна.....	721
Безопасность.....	721
Уровни блокчейна и атаки.....	724
Аппаратный уровень.....	725
Сетевой уровень.....	726
Уровень блокчейна	727
Уровень приложений блокчейна	733
Интерфейсный уровень	738
Атаки на блокчейны уровня 2	741
Криптографический уровень.....	743
Инструменты и механизм анализа безопасности	747
Формальная верификация	749
Безопасность смарт-контрактов	755
Solgraph	758
Моделирование угроз.....	758
Регулирование и соблюдение законов.....	761
Заключение	761

Глава 20. Децентрализованная идентификация	763
Идентичность	763
Цифровая идентичность	764
Централизованная модель идентификации	765
Модель федеративной идентификации	766
Модель децентрализованной идентификации	771
Суверенная идентичность	772
Компоненты SSI	773
Идентичность в Ethereum	789
Идентичность в мире Web3, DeFi и Metaverse	790
Проекты блокчейна с SSI-спецификой	793
Hyperledger Indy, Aries, Ursa и AnonCreds	794
Другие проекты	794
Некоторые другие инициативы	795
Проблемы	795
Заключение	796
Глава 21. Децентрализованные финансы	797
Введение	797
Финансовые рынки	799
Торговля	800
Биржи	801
Применение блокчейна в финансах	805
Страхование	805
Расчеты по сделкам	805
Профилактика финансовых преступлений	806
Платежи	808
Децентрализованные финансы	810
Свойства DeFi	812
Уровни DeFi	812
Примитивы DeFi	814
Сервисы DeFi	815
Преимущества DeFi	831
Uniswap	833
Обмен токена	833
Пул ликвидности Uniswap	834
Заключение	837
Глава 22. Возможности блокчейна и его будущее	838
Сценарии использования	838
IoT	839
Архитектура IoT	840
Уровень физических объектов	841
Уровень устройств	841
Сетевой уровень	842

Уровень управления	842
Уровень приложений	842
Преимущества конвергенции IoT и блокчейна	843
Практическая реализация IoT на основе блокчейна	846
Настройка Raspberry Pi	848
Настройка первого узла	851
Настройка узла Raspberry Pi	851
Установка Node.js	852
Сборка электронной схемы	854
Создание и запуск контракта на Solidity	855
Правительство	860
Пограничный контроль	860
Выборы	863
Идентификация граждан	864
Здравоохранение	865
Медиа	866
Блокчейн и ИИ	867
Некоторые намечающиеся тенденции	869
Некоторые проблемы	872
Заключение	875
Предметный указатель	877

От издательства

Отзывы и пожелания

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв на нашем сайте www.dmkpress.com, зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу dmkpress@gmail.com; при этом укажите название книги в теме письма.

Если вы являетесь экспертом в какой-либо области и заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу http://dmkpress.com/authors/publish_book/ или напишите в издательство по адресу dmkpress@gmail.com.

Список опечаток

Хотя мы приняли все возможные меры для того, чтобы обеспечить высокое качество наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг, мы будем очень благодарны, если вы сообщите о ней главному редактору по адресу dmkpress@gmail.com. Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательство «ДМК Пресс» очень серьезно относится к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконной публикацией какой-либо из наших книг, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

Ссылку на подозрительные материалы можно прислать по адресу электронной почты dmkpress@gmail.com.

Мы высоко ценим любую помощь по защите наших авторов, благодаря которой мы можем предоставлять вам качественные материалы.

Над книгой работали

Об авторе

Имран Башир – магистр информатики, получил научную степень в Королевском колледже Холлоуэй при Лондонском университете. Ранее занимался разработкой ПО, проектированием решений, управлением инфраструктурами, защитой информации и предоставлением ИТ-услуг. На данный момент занимается самыми современными технологиями, такими как блокчейн и квантовые вычисления.

Также является членом IEEE (Института инженеров электротехники и электроники). Имран работал на руководящих должностях технологических подразделений в различных организациях по всему миру.

Я хотел бы поблагодарить Эдварда Докси за его самоотверженность, а издательство Packt – за поддержку и руководство на протяжении всего проекта. Мои слова благодарности адресованы и Джону Корнину, который прочитал предыдущее издание этой книги и предложил некоторые исправления, а также редакторам этого издания.

Благодарю жену и детей за их поддержку в процессе написания книги. Особенно в те моменты, которые я должен был провести рядом с ними.

Наконец, я хочу поблагодарить своего отца, который всегда был и будет рядом со мной. И мою маму, ведь благодаря ее поддержке я легко преодолеваю все трудности. Молитвы моих родителей и их безусловная любовь дают мне силы добиться всего, чего я хочу.

Дисклеймер: Информация и точка зрения, изложенные в этой книге, принадлежат автору и не обязательно работодателям автора или их аффилированным лицам.

О рецензентах

Брайан Ву – старший архитектор и консультант по блокчейну. У него более 20 лет практического опыта работы с различными технологиями, включая блокчейн, большие данные, облачные вычисления, искусственный интеллект, системы обработки информации и инфраструктуру. За свою карьеру он работал более чем над 50 проектами.

Брайан написал девять книг, опубликованных издательствами O'Reilly, Packt и Apress. Все его работы относятся к сфере блокчейна, включая *Learn*

Ethereum, First Edition; Learn Ethereum, Second Edition; Blockchain for Teens; Hands-On Smart Contract Development with Hyperledger Fabric V2; Hyperledger Cookbook; Blockchain Quick Start Guide; Security Tokens and Stablecoins Quick Start Guide; Blockchain By Example; and Seven NoSQL Databases in a Week.

Шайлеш Б. Наир – компьютерный инженер и разработчик ПО в течение 21 года. Примерно 8 лет он занимается разработкой блокчейн-решений, используя различные специализированные фреймворки, такие как Ethereum (L1, L2, L3), Substrate, Polkadot, Solana, Cosmos (IBC), CasperLabs, Tezos и т. д., с применением таких языков программирования, как C++, Rust, Golang, Ocaml и Haskell.

С 2014 года он сотрудничал со многими криптовалютными стартапами, а в качестве консультанта по блокчейну работал при создании Mina Protocol, FTX и других решений.

Я хотел бы поблагодарить моих друзей, работавших со мной над блокчейн-проектами.

Конец ознакомительного фрагмента.

Приобрести книгу можно

в интернет-магазине

«Электронный универс»

e-Univers.ru