

---

# Оглавление

Предисловие научного редактора .....	15
Предисловие .....	16
Как читать эту книгу .....	17
Целевая аудитория .....	17
Условные обозначения .....	17
Примеры кода .....	18
Использование примеров кода .....	19
Ссылки на компании и продукты .....	19
Адреса и транзакции на Ethereum, указанные в книге .....	20
Как связаться с Андреасом .....	20
Как связаться с Гэвином .....	20
Благодарности от Андреаса .....	21
Благодарности от Гэвина .....	21
Люди, внесшие свой вклад .....	21
Источники .....	25
Краткий глоссарий .....	26
Глава 1. Что такое Ethereum? .....	38
Сравнение с Bitcoin .....	38
Компоненты блокчейна .....	39
Рождение Ethereum .....	41
Четыре стадии разработки Ethereum .....	43
Ethereum: блокчейн общего пользования .....	44
Компоненты Ethereum .....	45
Дополнительный материал .....	46
Ethereum и полнота по Тьюрингу .....	46
Полнота по Тьюрингу как отдельная «возможность» .....	47
Последствия полноты по Тьюрингу .....	48
От блокчейна общего пользования до децентрализованных приложений (DApps) .....	49
Интернет третьего поколения .....	50
Культура разработки в Ethereum .....	50
Зачем изучать Ethereum? .....	52
Чему эта книга вас научит .....	52

Глава 2. Основы Ethereum .....	53
Единица валюты эфир .....	53
Выбор кошелька Ethereum .....	54
Контроль и ответственность .....	56
Начало работы с MetaMask .....	58
Создание кошелька .....	58
Переключение между сетями .....	61
Получение эфира для тестирования .....	62
Отправка эфира из MetaMask .....	64
Исследование истории транзакций для определенного адреса .....	66
Знакомство с глобальным компьютером .....	67
Учетные записи и контракты с внешними владельцами .....	68
Простой контракт: тестовый контракт faucet с эфиром .....	69
Компиляция контракта Faucet .....	72
Создание контрактов на блокчейне .....	74
Взаимодействие с контрактом .....	76
Просмотр адреса контракта в обозревателе (explorer) .....	76
Пополнение контракта .....	77
Списание средств с контракта .....	78
Выводы .....	82
Глава 3. Клиенты Ethereum .....	83
Сети Ethereum .....	84
Стоит ли запускать полноценную ноду? .....	84
Преимущества и недостатки полноценной ноды .....	86
Преимущества и недостатки публичной тестовой сети .....	86
Преимущества и недостатки локальной симуляции блокчейна .....	87
Запуск клиента Ethereum .....	88
Аппаратные требования для запуска полноценной ноды .....	88
Требования к программному обеспечению для сборки и запуска клиента (ноды) .....	90
Parity .....	91
Go-Ethereum (Geth) .....	93
Первая синхронизация с блокчейнами на основе Ethereum .....	96
Запуск Geth или Parity .....	97
Интерфейс JSON-RPC .....	97
Удаленные клиенты Ethereum .....	100
Мобильные кошельки (для смартфонов) .....	100
Кошельки в браузере .....	101
Выводы .....	103

Глава 4. Криптография .....	104
Ключи и адреса .....	105
Криптография с публичным ключом и криптовалюта .....	106
Приватные (закрытые) ключи .....	108
Генерация приватного ключа из случайного числа .....	109
Публичные ключи .....	111
Подробнее об эллиптической криптографии .....	112
Арифметические операции с эллиптической кривой .....	115
Генерация публичного ключа .....	116
Библиотеки эллиптической криптографии .....	118
Криптографические функции хеширования .....	118
Криптографическая функция хеширования в Ethereum: Keccak-256 .....	120
Какую функцию хеширования вы используете? .....	121
Адреса Ethereum .....	122
Форматы адресов Ethereum .....	123
Протокол обмена клиентскими адресами .....	123
Шестнадцатеричная кодировка (EIP-55) .....	125
Выводы .....	128
Глава 5. Кошельки .....	129
Обзор технологий кошельков .....	129
Недетерминистические (случайные) кошельки .....	131
Детерминистические кошельки .....	133
Иерархические детерминистические кошельки (BIP-32/BIP-44) .....	133
Значения seed и мнемонические коды (BIP-39) .....	134
Лучшие практики работы с кошельками .....	135
Мнемоническая кодовая фраза (BIP-39) .....	136
Создание HD-кошелька с помощью seed .....	144
HD-кошельки (BIP-32) и пути (BIP-43/44) .....	145
Выводы .....	150
Глава 6. Транзакции .....	151
Структура транзакции .....	151
Одноразовый код транзакции .....	153
Отслеживание одноразовых кодов .....	154
Разрывы между одноразовыми кодами, дубликация и подтверждение .....	157
Параллелизм, происхождение транзакции и одноразовые коды .....	158
Газ для транзакций .....	159
Получатель транзакции .....	161
Значение и данные транзакции .....	162

Передача значения учетным записям ЕОА и контрактам .....	164
Передача полезных данных учетным записям ЕОА и контрактам .....	165
Специальные транзакции: создание контрактов .....	167
Цифровые подписи .....	170
Алгоритм цифровых подписей на основе эллиптической кривой .....	170
Принцип работы цифровых подписей .....	171
Проверка подписи .....	172
Математические вычисления алгоритма ECDSA .....	172
Подписание транзакции на практике .....	174
Создание «сырых транзакций» и подписание .....	175
Создание «сырой транзакции» с помощью EIP-155 .....	176
Префиксное значение подписи (v) и восстановление	
публичного ключа .....	177
Разделение операции подписания и передачи (офлайн-подписание) .....	178
Распространение транзакций .....	180
Запись в блокчейн .....	181
Транзакции с несколькими подписями .....	182
Выводы .....	183
Глава 7. Смарт-контракты и язык Solidity .....	184
Что такое смарт-контракт? .....	184
Жизненный цикл смарт-контракта .....	185
Введение в языки высокого уровня, доступные в Ethereum .....	187
Написание смарт-контракта на языке Solidity .....	189
Выбор версии Solidity .....	190
Загрузка и установка .....	190
Среда разработки .....	191
Написание простой программы на языке Solidity .....	191
Компиляция с помощью компилятора Solidity (solc) .....	192
ABI-интерфейс контрактов в Ethereum .....	192
Выбор версии компилятора и языка Solidity .....	194
Программирование на языке Solidity .....	195
Типы данных .....	195
Встроенные глобальные переменные и функции .....	197
Определение контракта .....	199
Функции .....	200
Конструктор контракта и его самоуничтожение .....	202
Добавление конструктора и деструктора в пример контракта faucet ..	203
Модификаторы функций .....	205
Наследование контрактов .....	206

Обработка ошибок (assert, require, revert) .....	208
События .....	210
Вызов других контрактов (send, call, callcode, delegatecall) .....	214
Соображения относительно газа .....	221
Избегайте динамических массивов .....	222
Избегайте вызовов других контрактов .....	222
Оценка расходования газа .....	222
Выводы .....	224
Глава 8. Смарт-контракты и Vyper .....	225
Уязвимости и Vyper .....	225
Сравнение с Solidity .....	226
Модификаторы .....	226
Наследование классов .....	228
Ассемблерные вставки .....	228
Перегрузка функций .....	229
Приведение типов переменных .....	229
Предусловия и постусловия .....	231
Декораторы .....	232
Порядок добавления функций и переменных .....	232
Компиляция .....	234
Защита от ошибок переполнения буфера на этапе компиляции .....	235
Чтение и запись данных .....	236
Выводы .....	237
Глава 9. Безопасность смарт-контрактов .....	238
Лучшие практики безопасности .....	238
Риски обеспечения безопасности и антишаблоны .....	240
Реентерабельность .....	240
Уязвимость .....	240
Превентивные меры .....	244
Реальный пример: DAO .....	245
Арифметическое переполнение и антипереполнение .....	246
Уязвимость .....	246
Превентивные меры .....	249
Реальные примеры: PoWNC и переполнение пакетной передачи (CVE-2018-10299) .....	251
«Неожиданный» эфир .....	252
Уязвимость .....	252
Превентивные меры .....	256
Другие примеры .....	257

DELEGATECALL .....	257
Уязвимость .....	258
Превентивные меры .....	263
Реальный пример: кошелек Parity с «мультисиг» подписями (второй взлом) .....	263
Видимость по умолчанию .....	266
Уязвимость .....	266
Превентивные меры .....	267
Реальный пример: кошелек Parity с «мультисиг» подписями (первый взлом) .....	267
Иллюзия энтропии .....	269
Уязвимость .....	269
Превентивные меры .....	270
Реальный пример: контракты, использующие генератор псевдослучайных чисел .....	270
Ссылки на внешние контракты .....	270
Уязвимость .....	271
Превентивные меры .....	275
Реальный пример: ловушка реентерабельности .....	276
Атака короткого адреса/параметра .....	278
Уязвимость .....	279
Превентивные меры .....	280
Непроверяемые значение, возвращенные из вызова CALL .....	280
Уязвимость .....	281
Превентивные меры .....	282
Реальный пример: Etherpot и King of the Ether .....	282
Состояние гонки и фронт-раннинг .....	284
Уязвимость .....	284
Превентивные меры .....	286
Реальные примеры: ERC20 и Bancor .....	287
Атака на отказ в обслуживании (DoS) .....	288
Уязвимость .....	288
Превентивные меры .....	291
Реальный пример: GovernMental .....	291
Манипуляции с временной меткой блока .....	292
Уязвимость .....	292
Превентивные меры .....	293
Реальный пример: GovernMental .....	294
Неточности в названиях конструкторов .....	294

Уязвимость .....	295
Превентивные меры .....	296
Реальный пример: Rubixi .....	296
Хранение неинициализированных указателей .....	296
Уязвимость .....	297
Превентивные меры .....	299
Реальные примеры: ловушки OpenAddressLottery и CryptoRoulette ...	299
Плавающая запятая и точность .....	300
Уязвимость .....	300
Превентивные меры .....	301
Реальный пример: Ethstick .....	302
Аутентификация с помощью Tx. Origin .....	303
Уязвимость .....	303
Превентивные меры .....	305
Библиотеки для контрактов .....	305
Выводы .....	306
Глава 10. Токены .....	307
Способы применения токенов .....	308
Токены и взаимозаменяемость .....	310
Риск контрагента .....	310
Токены и их свойства (назначение) .....	311
Назначение токенов: утилитарные токены и токены-акции .....	312
Это утка! .....	313
Утилитарные токены: кому они нужны? .....	313
Токены в Ethereum .....	315
Стандарт токенов ERC20 .....	316
Запуск собственного токена ERC20 .....	321
Проблемы с токенами ERC20 .....	335
ERC223: предложенный стандарт интерфейса для контракта токена .....	337
ERC777: предложенный стандарт интерфейса для контракта токена .....	338
ERC721: стандарт (актов) невзаимозаменяемых токенов .....	341
Использование стандартов токенов .....	344
Что такое стандарты токенов? Каково их назначение? .....	344
Стоит ли использовать эти стандарты? .....	344
Безопасность, основанная на зрелости .....	345
Расширение стандартов интерфейса токенов .....	346
Токены и процедура выпуска токенов (ICO) .....	347

Выводы .....	348
Глава 11. Оракулы .....	349
Зачем нужны оракулы? .....	349
Примеры оракулов и их использование .....	350
Шаблоны проектирования оракулов .....	352
Подлинность данных .....	356
Вычислительные оракулы .....	358
Децентрализованные оракулы .....	360
Клиентские интерфейсы оракулов в Solidity .....	362
Выводы .....	367
Глава 12. Децентрализованные приложения (DApps) .....	368
Что такое DApp-приложение? .....	369
Серверная часть (смарт-контракт) .....	370
Клиентская часть (пользовательский веб-интерфейс) .....	371
Хранилище данных .....	372
Децентрализованные протоколы взаимодействия на основе сообщений .....	373
Пример простого децентрализованного приложения: аукцион .....	373
Децентрализованный аукцион: смарт-контракты на стороне сервера ....	375
Децентрализованный аукцион: клиентский пользовательский интерфейс .....	379
Дальнейшая децентрализация приложения-аукциона .....	381
Хранение децентрализованного аукциона в Swarm .....	382
Подготовка Swarm .....	382
Загрузка файлов в Swarm .....	384
Сервис имен Ethereum (ENS) .....	386
История появления сервиса имен Ethereum .....	386
Спецификация ENS .....	387
Нижний слой: имена владельцев и сопоставителей .....	387
Средний слой: ноды (узла) .eth .....	390
Верхний слой: deed-контракты (акты) .....	392
Регистрация имени .....	393
Управление ENS именем .....	396
ENS-сопоставители .....	398
Сопоставление имени с Swarm хешем (его содержимым. — <i>Ред.</i> ) .....	399
От «обычного» приложения к DApp .....	401
Выводы .....	402
Глава 13. Виртуальная машина Ethereum .....	403
Что такое EVM? .....	403



Сравнение с существующими технологиями .....	405
Набор инструкций EVM (операции на основе байт-кода) .....	406
Состояние Ethereum .....	410
Компиляция кода Solidity в байт-код EVM .....	412
Код развертывания контракта .....	416
Дизассемблирование байт-кода .....	417
Полнота по Тьюрингу и газ .....	423
Газ .....	424
Учет газа во время выполнения .....	425
Как ведется учет газа .....	425
Расход и цена газа .....	426
Лимит газа для блока .....	427
Выводы .....	428
Глава 14. Консенсус .....	429
Консенсус на основе доказательства работы .....	430
Консенсус на основе доказательства доли владения .....	431
Ethash: алгоритм PoW в Ethereum .....	432
Casper: алгоритм доказательства доли владения в Ethereum .....	433
Принципы консенсуса .....	434
Разногласия и конкуренция .....	435
Выводы .....	435
Дополнение А. История ответвлений Ethereum .....	437
Ethereum Classic (ETC) .....	437
Децентрализованная автономная организация .....	438
Ошибка реентерабельности .....	438
Технические подробности .....	439
Порядок выполнения атаки .....	439
Жесткое ответвление DAO .....	439
Хронология жесткого ответвления DAO .....	441
Ethereum и Ethereum Classic .....	443
EVM .....	443
Разработка основного кода сети .....	444
Другие хардфорки Ethereum, заслуживающие внимания .....	444
Дополнение Б. Стандарты Ethereum .....	447
Предложения по улучшению Ethereum .....	447
Таблица наиболее важных документов EIP и ERC .....	448
Дополнение В. Опкоды EVM и потребление газа в Ethereum .....	457
Дополнение Г. Инструменты разработки, фреймворки и библиотеки .....	467
Фреймворки .....	467

Truffle .....	467
Embark .....	477
OpenZeppelin .....	478
ZeppelinOS .....	483
Утилиты .....	484
EthereumJS helpeth: утилита командной строки .....	484
dapp.tools .....	485
SputnikVM .....	485
Библиотеки .....	486
web3.js .....	486
web3.py .....	486
EthereumJS .....	486
web3j .....	486
EtherJar .....	487
Nethereum .....	487
ethers.js .....	487
Платформа Emerald .....	487
Тестирование смарт-контрактов .....	488
Тестирование в рамках блокчейна .....	489
Ganache: локальный блокчейн для тестирования .....	490
Дополнение Д. Руководство по работе с web3.js .....	492
Описание .....	492
Простое взаимодействие с контрактами в асинхронном стиле с помощью web3.js .....	492
Выполнение скрипта Node.js .....	493
Обзор демонстрационного скрипта .....	493
Взаимодействие с контрактом .....	494
Асинхронные операции с помощью await .....	497
Дополнение Е. Список сокращенных ссылок .....	498
Безопасность смарт-контрактов .....	498
Токены .....	500
Об авторах .....	501
В завершение .....	503
Алфавитный указатель .....	504