

Оглавление

Предисловие к русскому изданию.....	11
Об авторе.....	13
О рецензентах.....	15
Издательство «Ракт».....	17
Предисловие	19
О чем эта книга?	19
Что понадобится в дополнение к этой книге?.....	20
Для кого эта книга?	20
Обозначения.....	20
Обратная связь.....	21
Поддержка читателей.....	22
Скачивание исходных кодов программ	22
Цветные иллюстрации.....	22
Электронный архив файлов для русского издания.....	23
Исправления.....	23
Пиратство	23
Вопросы.....	23
Глава I. Децентрализованные приложения.....	25
Что такое ДП?	25
Достоинства децентрализованных приложений.....	27
Недостатки децентрализованных приложений.....	27
Децентрализованная автономная организация	27
Личность пользователя в ДП.....	28
Учетные записи пользователей	30
Доступ к централизованным приложениям	30
Внутренняя валюта приложений.....	31
Недостатки внутренней валюты.....	32

Приложения с контролируемым доступом	32
Популярные приложения	32
Bitcoin	32
Что такое регистр?	33
Что такое блокчейн?	33
Легален ли биткойн?	33
Почему мы используем биткойн?	34
Ethereum	34
Hyperledger	35
IPFS	35
Как работает IPFS?	36
Filecoin	36
Namecoin	37
Домены в зоне <i>.bit</i>	37
Dash	38
Децентрализованное управление и бюджетирование	39
Децентрализованные услуги	39
BigChainDB	40
OpenBazaar	40
Ripple	40
Заключение	43
Глава 2. Принципы работы Ethereum	44
Знакомство с Ethereum	44
Учетная запись Ethereum	45
Транзакции	45
Консенсус	46
Метка времени	48
Число поппе	48
Время блока	49
Ветвление	51
Генезис	52
Депоминация эфира	52
Виртуальная машина Ethereum	53
Газ	53
Обнаружение узлов	54
Протоколы Whisper и Swarm	55
Geth	55
Установка Geth	56
OS X	56
Ubuntu	56
Windows	56
JSON-RPC и консоль JavaScript	57
Подкоманды и опции	57
Подключение к сети <i>mainnet</i>	57
Создание частной сети	57
Создание аккаунта	58
Майнинг	58
Быстрая синхронизация	59

Ethereum Wallet	59
Mist	61
Уязвимости Ethereum	62
Атака Сибиллы	62
Атака 51%	62
Обновление Serenity	62
Платежные каналы и каналы состояния	63
Протокол консенсуса Casper	63
Разделение данных	64
Заключение	64
Глава 3. Разработка смарт-контрактов	65
Файлы исходного кода Solidity	65
Структура смарт-контракта	66
Расположение данных	67
Что такое типы данных?	68
Массивы	69
Строки	70
Структуры	71
Перечисление	72
Сопоставление	72
Оператор <i>delete</i>	73
Преобразование элементарных типов	74
Ключевое слово <i>var</i>	74
Управляющие структуры	75
Оператор <i>new</i> и создание контракта	76
Исключения	77
Вызов внешних функций	77
Свойства контракта	79
Видимость	79
Модификаторы	81
Резервная функция	83
Наследование	83
Ключевое слово <i>super</i>	85
Абстрактные контракты	86
Библиотеки	86
Конструкция <i>using ... for</i>	88
Возврат нескольких значений	89
Импорт файлов исходных кодов Solidity	89
Глобальные переменные	90
Свойства блока и транзакции	90
Свойства, связанные с адресом	91
Переменные, связанные с контрактом	91
Единицы эфира	91
Доказательство наличия, целостности и принадлежности файла	91
Компиляция и развертывание контракта	93
Заключение	96

Глава 4. Учимся работать с web3.js	97
Введение в web3.js	97
Импортирование web3.js	98
Подключение к узлу	98
Структура API	99
Библиотека BigNumber.js	100
Конвертация денежных единиц	101
Запрос цены газа, баланса и деталей транзакции	101
Отправка эфира	103
Работа с контрактами	104
Отслеживание событий контракта	106
Разработка клиентского приложения для контракта	109
Структура проекта	110
Разработка серверной части	110
Разработка клиентской части	112
Тестирование клиентской части	116
Заключение	119
Глава 5. Разработка сервиса кошелька	120
Различие между онлайн- и оффлайн-кошельками	120
Библиотеки hooked-web3-provider и ethereumjs-tx	121
Что такое HD-кошелек?	124
Введение в функции формирования ключа	125
Знакомство с LightWallet	126
Путь вывода HD-кошелька	127
Разработка сервиса кошелька	127
Предварительная подготовка	127
Структура проекта	128
Разработка серверной части	128
Разработка клиентской части	129
Тестирование	136
Заключение	142
Глава 6. Разработка платформы для смарт-контрактов	143
Вычисление <i>nonce</i> для транзакции	144
Знакомство с solcjs	145
Установка solcjs	145
API solcjs	146
Использование различных версий компилятора	147
Связывание библиотек	148
Обновление ABI	149
Разработка платформы для развертывания контрактов	149
Структура проекта	150
Разработка серверной части	150
Разработка клиентской части	156
Тестирование	160
Заключение	161

Глава 7. Приложение для ставок на результат матча.....	162
Знакомство с Oraclize.....	163
Как работает Oraclize?.....	163
Источники данных.....	163
Доказательство подлинности.....	164
Стоимость услуг Oraclize.....	166
Основы работы с API Oraclize.....	167
Настройка типа и места хранения доказательства.....	167
Отправка запросов.....	167
Отложенные запросы.....	168
Расходование газа.....	168
Функции обратного вызова.....	169
Синтаксический разбор результатов.....	170
Получение цены запроса.....	171
Шифрование запросов.....	171
Расшифровка источника данных.....	171
IDE Oraclize.....	172
Работа со строками.....	172
Разработка контракта для ставок на спорт.....	174
Разработка приложения для ставок.....	177
Разработка структуры приложения.....	178
Разработка серверной части.....	178
Разработка клиентской части.....	181
Тестирование приложения.....	189
Заключение.....	193
Глава 8. Разработка смарт-контрактов уровня предприятия.....	194
Знакомство с <i>ethereumjs-testrpc</i>	195
Установка и использование <i>ethereumjs-testrpc</i>	195
Приложение командной строки <i>testrpc</i>	195
Использование <i>ethereumjs-testrpc</i> в качестве провайдера <i>web3</i> или HTTP-сервера.....	197
Доступные методы RPC.....	198
Что такое заголовки событий?.....	199
Знакомство с пакетом <i>truffle-contract</i>	201
Установка и импорт <i>truffle-contract</i>	202
Настройка тестового окружения.....	203
API <i>truffle-contract</i>	203
API абстракции контракта.....	204
Создание экземпляра контракта.....	209
API экземпляра контракта.....	211
Введение в Truffle.....	212
Установка Truffle.....	212
Инициализация Truffle.....	212
Компиляция контрактов.....	214
Файлы конфигурации.....	214
Развертывание контрактов.....	215
Файлы переноса.....	216
Написание кода переноса.....	216

Юнит-тесты контрактов	218
Написание тестов на JavaScript	219
Написание тестов на Solidity	221
Как перевести валюту на тестовый контракт?	224
Запуск тестов	224
Управление пакетами	225
Управление пакетами через NPM	225
Управление пакетами через EthPM	225
Использование контрактов из пакета	227
Использование артефактов пакета в коде JavaScript	227
Доступ к адресам развернутых контрактов пакета в Solidity	227
Работа с консолью Truffle	228
Запуск внешних скриптов в контексте Truffle	229
Создание клиента в Truffle	229
Запуск внешних команд	230
Запуск пользовательских функций	230
Конструктор Truffle по умолчанию	231
Создание клиента	233
Сервер Truffle	236
Заключение	238
Глава 9. Разработка блокчейна для консорциума	239
Что такое блокчейн консорциума?	240
Что такое консенсус с доказательством полномочий?	240
Введение в Parity	241
Принципы работы Aura	241
Начинаем работу с Parity	243
Установка Rust	243
Скачивание, установка и запуск Parity	244
Создание частной сети	244
Создание аккаунтов	244
Создание файла спецификации	244
Запуск узлов	248
Подключение узлов	249
Полномочия и приватность	249
Заключение	250
Приложение. Описание электронного файлового архива	251
Предметный указатель	253