



СОДЕРЖАНИЕ

Об авторе	18
О техническом рецензенте	19
Предисловие	20
Часть I. ТЕРМИНОЛОГИЯ И ОСНОВЫ ТЕХНОЛОГИИ	26
Глава 1. Понимание уровней и аспектов	27
Метафора.....	27
Уровни программной системы.....	28
Сопоставление приложения и его реализации.....	28
Разделение на функциональные и нефункциональные аспекты.....	29
Одновременное изучение двух уровней.....	30
Целостность.....	30
Перспектива.....	31
Резюме.....	32
Глава 2. Более подробная картина	33
Метафора.....	33
Платежная система.....	34
Два типа архитектуры программного обеспечения.....	35
Преимущества распределенных систем	36
Более высокая вычислительная мощность.....	36
Снижение стоимости (накладных расходов, издержек).....	36
Более высокая надежность.....	37
Возможность естественного роста.....	37
Недостатки распределенных систем.....	38
Издержки на координацию работы.....	38
Издержки на организацию обмена информацией.....	38
Зависимость от сетевой среды.....	38
Более высокая сложность программного обеспечения.....	39

Проблемы безопасности	39
Распределенные пиринговые системы.....	39
Объединение централизованных и распределенных систем.....	40
Идентификация распределенных систем.....	41
Цель технологии блокчейна	42
Перспектива	43
Резюме	43
Глава 3. Определение потенциальных возможностей.....	45
Метафора.....	45
Как пиринговая система изменила целую отрасль промышленности	46
Потенциальные возможности пиринговых систем.....	47
Терминология и связь с технологией блокчейна.....	49
Определение пиринговой системы.....	50
Архитектура пиринговых систем	50
Связь между пиринговыми системами и технологией блокчейна.....	51
Потенциальные возможности технологии блокчейна	51
Перспектива	52
Резюме	52
Часть II. ЗАЧЕМ НУЖНА ТЕХНОЛОГИЯ БЛОКЧЕЙНА	54
Глава 4. Исследование основной задачи	55
Метафора.....	55
Обеспечение доверительности и целостности в пиринговых системах	56
Угрозы целостности в пиринговых системах.....	57
Технические отказы (сбои)	57
Злоумышленники-партнеры в системе	58
Главная задача, решаемая технологией блокчейна.....	58
Перспектива	59
Резюме	59
Глава 5. Однозначное определение термина.....	60
Определение термина.....	60
Структура данных	61
Алгоритм.....	61
Набор (стек) технологий	61
Гипероним (обобщающее понятие) для полностью распределенных пиринговых систем с общей прикладной областью.....	62
Использование термина блокчейн в данной книге.....	62

Предварительное определение термина.....	62
Роль управления правом владения.....	63
Область применения блокчейна, рассматриваемая в данной книге	64
Перспектива	64
Резюме	64

Глава 6. Понимание сущности права владения

собственностью	66
Метафора.....	66
Право владения и доказательства.....	67
Основания права владения	68
Небольшое отступление, касающееся безопасности	70
Идентификация.....	70
Аутентификация.....	71
Авторизация.....	71
Цели и свойства регистра	72
Право владения и блокчейн	73
Перспектива	74
Резюме	75

Глава 7. Двойное расходование.....

Метафора.....	76
Проблема двойного расходования	77
Уточнение термина.....	78
Двойное расходование как проблема копирования цифровой продукции.....	78
Двойное расходование как проблема распределенной пиринговой системы реестров	79
Двойное расходование как пример нарушения целостности в полностью распределенных пиринговых системах.....	79
Как решить проблему двойного расходования.....	79
Решение проблемы двойного расходования как проблемы копирования цифровой продукции.....	80
Решение проблемы двойного расходования как проблемы в распределенных пиринговых системах реестров	80
Решение проблемы двойного расходования как примера нарушения целостности распределенных пиринговых систем	80
Использование термина двойное расходование в этой книге	81
Перспектива	81
Резюме	81

Часть III. КАК РАБОТАЕТ БЛОКЧЕЙН	83
Глава 8. Проектирование блокчейна	84
Цель	84
Исходный пункт	85
План проектирования и разработки	85
Задача 1: описание права владения	86
Задача 2: защита права владения	86
Задача 3: хранение данных транзакций	86
Задача 4: подготовка реестров к распространению в ненадежной среде	87
Задача 5: распространение реестров	88
Задача 6: добавление новых транзакций в реестры	88
Задача 7: определение, в каких реестрах представлены правильные данные	88
Перспектива	89
Резюме	90
Глава 9. Документирование права владения	91
Метафора	91
Цель	92
Главная задача	92
Основная идея	92
Краткое отступление по поводу инвентаризационной ведомости и данных транзакции	93
Как это работает	93
Описание передачи права владения	93
Обслуживание хронологии актов передачи прав	94
Почему это работает	95
Важность упорядоченности	95
Целостность хронологии транзакций	96
Формальная корректность	96
Семантическая (смысловая) корректность	96
Авторизация	97
Перспектива	97
Резюме	98
Глава 10. Хэширование данных	99
Метафора	99
Цель	99
Как это работает	100

Быстрая генерация хэш-значений для любого типа данных.....	100
Детерминированность	101
Обеспечение псевдослучайности хэш-значений.....	101
Односторонние функции	101
Устойчивость к коллизиям	101
Проверка на практике	102
Шаблоны хэширования данных	104
Независимое хэширование.....	104
Повторяющееся хэширование	105
Комбинированное хэширование	106
Последовательное хэширование	107
Иерархическое хэширование	108
Перспектива	108
Резюме	109
Глава 11. Хэширование на практике	110
Сравнение данных.....	110
Цель	110
Основная идея	111
Как это работает	111
Почему это работает	111
Обнаружение изменений в данных.....	111
Цель	111
Основная идея	111
Как это работает	112
Почему это работает	112
Обращение к данным, которые не должны изменяться.....	112
Цель	113
Основная идея	113
Как это работает	113
Схематическое описание	114
Почему это работает	115
Хранение данных, которые не должны изменяться.....	115
Цель	116
Основная идея	116
Как это работает	116
Цепочка.....	116
Дерево.....	117
Почему это работает	118
Выполнение долговременных вычислений.....	119
Цель	119

Основная идея	119
Как это работает	120
Практический пример.....	121
Уровень сложности.....	122
Почему это работает	122
Использование хэширования в блокчейне	123
Перспектива	123
Резюме	123

Глава 12. Идентификация и защита учетных записей пользователей

пользователей	125
Метафора.....	125
Цель.....	126
Главная задача.....	126
Основная идея.....	127
Краткий обзор криптографии.....	127
Основная задача криптографии.....	127
Терминология	127
Симметричная криптография	128
Асимметричная криптография	129
Асимметричная криптография на практике	131
Создание и распространение ключей.....	131
Использование ключей.....	131
От открытого ключа к закрытому ключу.....	132
От закрытого ключа к открытому ключу.....	132
Асимметричная криптография в технологии блокчейна.....	133
Идентификация учетных записей.....	133
Авторизация транзакций	133
Перспектива	134
Резюме	134

Глава 13. Авторизация транзакций

Метафора.....	136
Цель.....	137
Главная задача.....	137
Идея	137
Краткий обзор цифровых подписей.....	138
Создание цифровой подписи.....	138
Проверка данных с использованием цифровой подписи.....	139
Выявление факта мошенничества с использованием цифровой подписи	140

Как это работает.....	141
Цифровая подпись транзакции	141
Проверка (верификация) транзакции.....	142
Почему это работает.....	142
Перспектива	143
Резюме	143
Глава 14. Хранение данных транзакций	145
Метафора.....	145
Цель.....	146
Главная задача.....	146
Идея	146
Преобразование обычной книги в структуру данных блокчейна	147
Исходная позиция: обычная книга	147
Преобразование 1: создание явной зависимости между страницами.....	147
Преобразование 2: отделение содержимого	149
Преобразование 3: замена номеров страниц	150
Преобразование 4: создание числовых ссылок.....	151
Преобразование 5: отказ от переплета книги.....	151
Цель достигнута: оценка результата.....	152
Структура данных блокчейна.....	153
Воображаемый элемент, состоящий из страницы упорядоченного каталога и соответствующей ему страницы содержимого	154
Упорядоченный каталог.....	154
Страницы содержимого.....	155
Числовые ссылки на страницы каталога.....	155
Числовые ссылки на содержимое.....	155
Хранение транзакций в структуре данных блокчейна.....	156
Перспектива	157
Резюме	158
Глава 15. Использование хранилища данных.....	159
Метафора.....	159
Добавление новых транзакций.....	160
Обнаружение изменений	162
Изменение содержимого данных транзакции	163
Изменение ссылки на дерево Меркле.....	163
Замена транзакции	164
Изменение корня дерева Меркле.....	165
Изменение ссылки на заголовок блока.....	166
Корректное изменение данных.....	167

Преднамеренные и непреднамеренные изменения.....	168
Перспектива	168
Резюме.....	169
Глава 16. Защита хранимых данных.....	170
Метафора.....	170
Цель.....	172
Главная задача.....	172
Идея.....	172
Краткий обзор свойства неизменяемости.....	172
Как это работает: общая схема	173
Обнаружение любых изменений.....	173
Принудительная перезапись всей хронологии при внутренних изменениях.....	174
Добавление данных чрезвычайно многозатратно с точки зрения вычислительных мощностей.....	174
Как это работает: подробности.....	175
Обязательность данных.....	175
Процесс создания нового блока.....	175
Правила проверки.....	176
Почему это работает.....	177
Накладные расходы при изменении структуры данных блокчейна.....	177
Хранилище неизменяемых данных в реальном мире	178
Перспектива	179
Резюме.....	179
Глава 17. Распространение хранилища данных в пиринговой системе.....	181
Метафора.....	181
Цель.....	182
Главная задача.....	182
Идея.....	183
Как это работает: общий обзор.....	183
Как это работает: подробности.....	185
Сохранение существующих соединений в работоспособном состоянии.....	185
Установление новых соединений	186
Распространение новой информации	186
Почему это работает.....	187
Перспектива	187
Резюме.....	188

Глава 18. Методы проверки и добавления транзакций	190
Метафора.....	190
Последствия.....	191
Цель.....	192
Главная задача.....	192
Идея.....	193
Как это работает: структурные элементы системы.....	193
Правила проверки.....	193
Правила проверки для данных транзакций.....	193
Правила проверки для заголовков блоков.....	194
Поощрение.....	194
Наказание.....	195
Конкуренция.....	195
Конкуренция по скорости.....	196
Конкуренция по качеству.....	196
Управление партнерами.....	197
Как это работает: общая схема.....	197
Как это работает: подробности.....	198
Почему это работает.....	199
Реакция на нечестное поведение.....	201
Перспектива.....	202
Резюме.....	202
Глава 19. Выбор хронологии транзакций	204
Метафора.....	204
Цель.....	205
Главная задача.....	205
Идея.....	206
Как это работает.....	208
Критерий самой длинной цепочки.....	208
Критерий самой затратной цепочки.....	212
Следствия выбора единственной цепочки.....	213
Блоки-«сироты».....	214
Отмена поощрений.....	214
Уточнение права владения.....	214
Повторная обработка транзакций.....	215
Увеличение размера общего ствола.....	215
Сохранение общей целостности.....	216
Устойчивость против сторонних манипуляций.....	217
Опасности для схемы голосования.....	218
Важная роль хэш-головоломок.....	219

Почему это работает.....	219
Перспектива	220
Резюме	220
Глава 20. Плата за сохранение целостности.....	223
Метафора.....	223
Роль вознаграждений в блокчейн-системе	224
Воздействие на целостность системы.....	225
Воздействие на открытость системы.....	225
Воздействие на распределенную сущность системы	226
Воздействие на философию системы.....	226
Краткое отступление: появление криптографических валют.....	227
Перспектива	228
Резюме	228
Глава 21. Соединяем все элементы	230
Обзор концепций и технологий	230
Что такое блокчейн	232
Предназначение блокчейн-системы: функциональные аспекты уровня приложения	233
Уточнение и подтверждение права владения собственностью	233
Передача права владения собственностью.....	233
Свойства блокчейн-системы: нефункциональные аспекты.....	234
Высокая доступность.....	234
Защита от цензуры	234
Надежность	234
Открытость.....	234
Псевдоанонимность.....	235
Безопасность	235
Гибкость.....	235
Общая согласованность.....	235
Сохранение целостности.....	235
Внутренняя функциональность: функциональные аспекты уровня реализации	236
Логика прав владения собственностью.....	236
Защита транзакций.....	237
Логика обработки транзакций.....	238
Логика хранения.....	239
Пиринговая архитектура	240
Логика согласования.....	241
Повышаем уровень абстракции.....	241

Перспектива	242
Резюме	243

Часть IV. ОГРАНИЧЕНИЯ И СПОСОБЫ ИХ ПРЕОДОЛЕНИЯ

Глава 22. Обзор ограничений

Главная задача	246
Технические ограничения блокчейна	247
Недостаточная секретность	247
Модель защиты	247
Ограниченная масштабируемость	248
Высокий уровень накладных расходов	249
Скрытая централизация	249
Недостаточная гибкость	250
Критический размер	251
Нетехнические ограничения блокчейна	251
Недоверие с юридической точки зрения	251
Недоверие со стороны пользователей	252
Преодоление ограничений	252
Технические ограничения	253
Нетехнические ограничения	253
Перспектива	253
Резюме	254

Глава 23. Новая жизнь блокчейна

Метафора	255
Конфликтующие цели блокчейн-системы	256
Конфликт прозрачности (открытости) и секретности	256
Безопасность и скорость	256
Главные причины конфликтов	257
Разрешение конфликтов	257
Разрешение конфликта открытости и секретности	258
Разрешение конфликта безопасности и скорости	258
Четыре версии блокчейн-системы	259
Последствия	260
Пиринговая архитектура	260
Распределенная сущность	260
Главная цель	261
Немного пересмотрим определение главной задачи блокчейна	262
Использование термина блокчейн в оставшейся части книги	262

Перспектива	263
Резюме	263

Часть V. ПРАКТИЧЕСКОЕ ИСПОЛЬЗОВАНИЕ БЛОКЧЕЙНА, ОБЗОР И ПЕРСПЕКТИВЫ 265

Глава 24. Практическое применение технологии блокчейна 266

Метафора.....	266
Характеристики блокчейн-системы	267
Обобщенные шаблоны приложений	267
Подтверждение существования	268
Подтверждение несуществования	268
Подтверждение времени наступления какого-либо события.....	268
Подтверждение порядка следования.....	268
Подтверждение подлинности личности	269
Подтверждение авторства.....	269
Подтверждение права владения собственностью	270
Особые варианты использования.....	270
Анализ блокчейн-приложений	271
Выполнены ли требования к использованию блокчейн-системы?.....	272
Какой тип блокчейн-системы используется?.....	273
Каков размер добавленной стоимости при использовании полностью распределенной пиринговой системы?.....	274
Какова основная идея (замысел) данного приложения?	274
Какой бизнес-вариант используется?	275
Как реализована компенсация для партнеров за предоставление ресурсов рассматриваемой системе?	276
Перспектива	277
Резюме	277

Глава 25. Подводим итоги и движемся дальше 279

Метафора.....	279
Будущие направления разработок и альтернативные варианты	280
Минимальные технические усовершенствования и вариации.....	281
Улучшение масштабируемости	281
Концептуальное развитие.....	282
Права доступа	282
Секретность.....	282
Распределенный консенсус.....	283
Транзакции	284

Данные реестра	285
Структура данных.....	285
Основные перспективы технологии блокчейна	286
Устранение посредников.....	287
Автоматизация	287
Стандартизация.....	287
Ускорение процессов.....	287
Увеличение скорости обработки данных.....	288
Снижение стоимости	288
Смещение доверительных отношений в область технических протоколов и технологии	288
Формирование доверительного отношения к предметам потребления (товарам).....	289
Более полная информированность о технологии.....	289
Вероятные недостатки	290
Недостаточная закрытость (секретность)	290
Отсутствие личной ответственности.....	291
Потеря рабочих мест.....	291
Возобновление посредничества	292
Перспективы на будущее	292
Небольшие проекты энтузиастов	292
Крупномасштабное коммерческое применение	293
Государственные (и муниципальные) проекты.....	293
Подводим итоги.....	294
Резюме	294
Список литературы.....	296
Предметный указатель	300



ОБ АВТОРЕ

Даниэль Дрешер (Daniel Drescher) – опытный профессионал в банковской сфере, работавший в области электронной торговли ценными бумагами в нескольких банках. В последнее время его деятельность сосредоточена на задачах автоматизации, машинного обучения и обработки больших данных в сфере торговли ценными бумагами. Кроме того, Даниэль имеет докторскую степень по эконометрике (математической экономике) в Берлинском Техническом университете и степень магистра инженерии программного обеспечения, присвоенную Оксфордским университетом.

О ТЕХНИЧЕСКОМ РЕЦЕНЗЕНТЕ



Лоренс Керк (Laurence Kirk) после успешной карьеры автора оперативного финансового прикладного программного обеспечения для делового центра Сити в Лондоне заинтересовался потенциальными возможностями технологии создания распределенного программного обеспечения для финансового учета. Он поступил в Оксфордский университет для получения степени магистра и основал компанию Extropy.io, консультирующую стартапы по разработке прикладных программ для платформы Ethereum.

Увлеченный возможностями технологии распределенного программного обеспечения, сейчас он является разработчиком, экспертом-консультантом и инструктором по вопросам использования платформы Ethereum.



ПРЕДИСЛОВИЕ

Данное предисловие отвечает на самый важный вопрос, на который обязан ответить любой автор: зачем читать эту книгу? Или на более конкретный вопрос: зачем читать еще одну книгу по технологии Blockchain? Продолжайте читать, и вы поймете, зачем написана эта книга, чего ждать от нее и чего в ней не следует искать. Вы также узнаете, для какой аудитории написана эта книга и как она организована.

Зачем нужна еще одна книга о технологии блокчейна?

Технология блокчейна (Blockchain, или цепочка блоков транзакций) сразу после своего появления привлекла большое внимание при крупномасштабных обсуждениях и в специализированных средствах массовой информации. Некоторые энтузиасты даже объявили блокчейн самым великим изобретением с момента появления Интернета. Поэтому за несколько последующих лет о блокчейне было написано большое количество книг и статей. Но если вы хотите узнать больше о том, как устроен и как работает блокчейн, то вскоре можете просто потеряться в бездне книг, в которых технические подробности описываются весьма поверхностно, или базовые технические концепции излагаются на чрезмерно формализованном уровне. Первый вариант не удовлетворяет любознательного читателя, поскольку не дает описания технических деталей, необходимых для понимания и оценки по достоинству технологии блокчейна, во втором случае при изучении требуется владение именно теми знаниями, которые вы хотите получить.

Эта книга предназначена для заполнения разрыва между абсолютно технической литературой по блокчейну, с одной стороны,

и книгами, в которых почти все внимание сосредоточено на специализированных приложениях, или на описаниях предполагаемого экономического эффекта от применения этих приложений, или даже на рассуждениях о будущем блокчейна, с другой стороны.

Эта книга написана, потому что концептуальное понимание технических основ блокчейна необходимо, чтобы понять функциональность специализированных блокчейн-приложений, исследовать бизнес-варианты деятельности блокчейн-стартапов или полноправно участвовать в обсуждении ожидаемых экономических эффектов. Без хорошего понимания базовых теоретических концепций невозможно дать числовую оценку реального эффекта или потенциального воздействия блокчейна вообще или числовую оценку полезности, добавляемой специализированными блокчейн-приложениями. Главное внимание в этой книге уделено основополагающим теоретическим концепциям блокчейна, так как недостаточное понимание новой технологии может привести к чрезмерному увлечению внешними ее сторонами и последующему разочарованию, когда не оправдываются иллюзорные, ничем не обоснованные ожидания.

В этой книге излагаются теоретические концепции, на основе которых сформирована технология блокчейна, в лаконичном и понятном стиле, рассчитанном на неподготовленных (с технической точки зрения) читателей. Книга отвечает на три главных вопроса, возникающих при знакомстве с любой новой технологией: что это такое? зачем это нужно мне? как это работает?

Чего не следует ждать от этой книги

В этой книге преднамеренно не рассматриваются приложения, использующие блокчейн. Несмотря на то что криптовалюты в целом и Bitcoin в частности являются основными приложениями на основе блокчейна, в книге блокчейн описывается как «технология вообще». Такой подход выбран для того, чтобы ярче выделить общие ключевые концепции и технические шаблоны блокчейна, а не ограничиваться более узкими специализированными частными случаями конкретных приложений. Таким образом:

- эта книга не о Bitcoin или какой-либо другой криптовалюте;
- эта книга не рассматривает какого-то одного специализированного блокчейн-приложения;

- в этой книге нет математических доказательств основных концепций блокчейна;
- эта книга не о программировании с использованием технологии блокчейна;
- в этой книге не обсуждаются последствия применения технологии блокчейна с точки зрения законодательства;
- в этой книге не рассматриваются социальное, экономическое и этическое воздействия технологии блокчейна на наше общество или на человечество в целом.

Тем не менее некоторые из этих тем в некоторой степени обсуждаются в соответствующих подразделах данной книги.

Чего следует ожидать от этой книги

Книга подробно описывает технические концепции технологии блокчейна, такие как транзакции, хэш-значения, криптография, структуры данных, пиринговые системы, распределенные системы, целостность систем и консенсус в распределенной среде в стиле, понятном для читателей с недостаточно высоким уровнем технической подготовки. Дидактический подход к изложению материала основан на четырех элементах:

- диалоговый («разговорный») стиль;
- отсутствие математических выкладок и формул;
- постепенное продвижение по проблемной области;
- использование метафор и аналогий.

Диалоговый («разговорный») стиль

Эта книга преднамеренно написана в диалоговом, или «разговорном», стиле. Здесь абсолютно не применяется математический и компьютерный жаргон, чтобы устранить все препятствия для читателей, не вполне подготовленных с технической точки зрения. Но здесь представлена и объяснена вся терминология, необходимая для участия в обсуждениях и для понимания других публикаций по теме блокчейна.

Отсутствие математических выкладок и формул

Главные элементы технологии блокчейна, такие как криптография и алгоритмы, основаны на сложных математических концепциях, которые, в свою очередь, предъявляют свои особые требования к их пониманию, а также приводят к необходимости изучения математических выкладок и формул, устрашающих на вид. И все же в книге намеренно не используются ни математические выкладки, ни формулы, чтобы избежать ненужной сложности и не создавать дополнительных затруднений для читателей с недостаточной технической подготовкой.

Постепенное продвижение по проблемной области

Главы в этой книге соответствуют своего рода шагам, или этапам, по вполне обоснованной причине. Такие шаги, или этапы, формируют процесс обучения, в котором последовательно, уровень за уровнем наращиваются знания о технологии блокчейна. Порядок этапов обучения был выбран с особой тщательностью. Они охватывают основы программной инженерии, подробно описывают терминологию, дают обоснование необходимости использования блокчейна и подробно рассматривают отдельные концепции, заложенные в основу технологии блокчейна, и взаимодействие ее составляющих. Строгая последовательность глав-этапов подчеркивает их взаимозависимость и дидактические цели. Тем самым обеспечивается логически связное изложение материала, а не набор отдельных глав, которые можно читать в любом порядке.

Использование метафор и аналогий

Каждая глава-этап, представляющая новую концепцию, начинается с образного описания ситуации из реальной жизни. Такие метафоры служат четырем основным целям. Во-первых, они готовят читателя к правильному восприятию новой технической концепции. Во-вторых, объединяя техническую концепцию с простой жизненной ситуацией, метафора устраняет психологический барьер при «исследовании новой территории». В-третьих, метафоры позволяют изучать новые концепции с помощью подобия и ана-

Конец ознакомительного фрагмента.
Приобрести книгу можно
в интернет-магазине
«Электронный универс»
e-Univers.ru