

# Основы блокчейна



Даниэль Дрешер

Даниэль Дрешер

# ОСНОВЫ БЛОКЧЕЙНА

Вводный курс для начинающих  
в 25 небольших главах

Daniel Drescher

# BLOCKCHAIN BASICS

**A Non-Technical Introduction  
in 25 Steps**

**Apress®**

Даниэль Дрешер

# ОСНОВЫ БЛОКЧЕЙНА

Вводный курс для начинающих  
в 25 небольших главах



Москва, 2018

**УДК 004.62:004.738.5**

**ББК 32.972.134**

**Д73**

Дрешер Д.  
Д73 Основы блокчейна: вводный курс для начинающих в 25 небольших главах / пер. с англ. А. В. Снастина. – М.: ДМК Пресс, 2018. – 312 с.: ил.

**ISBN 978-5-97060-591-2**

Книга подробно рассматривает технические концепции технологии блокчейн, такие как пиринговые и распределенные системы, структуры данных, транзакции, криптография и хэш-значения, целостность систем и достижение консенсуса в распределенной среде. Книга написана в диалоговом стиле, без использования компьютерного и математического жаргона. Материал излагается в пошаговой, логически связанной манере, что позволяет последовательно, уровень за уровнем, наращивать знания о технологии блокчейна. Многочисленные примеры, аналогии и метафоры помогают лучше понять, как работают блокчейн-системы даже тем, кто до этого ничего не знал об этом.

Издание предназначено для широкого круга читателей с различным уровнем технических знаний, желающих разобраться, что же такое блокчейн.

**УДК 004.62:004.738.5**

**ББК 32.972.134**

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 978-1-4842-2603-2 (анг.)

ISBN 978-5-97060-591-2 (рус.)

Copyright © 2017 by Daniel Drescher

© Оформление, издание, перевод,  
ДМК Пресс, 2018



# СОДЕРЖАНИЕ

<b>Об авторе</b> .....	18
<b>О техническом рецензенте</b> .....	19
<b>Предисловие</b> .....	20
<b>Часть I. ТЕРМИНОЛОГИЯ И ОСНОВЫ ТЕХНОЛОГИИ</b> .....	26
<b>Глава 1. Понимание уровней и аспектов</b> .....	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
<b>Глава 2. Более подробная картина</b> .....	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**

<b>собственностью .....</b>	<b>66</b>
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..... 76**

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



<b>Часть III. КАК РАБОТАЕТ БЛОКЧЕЙН</b>	<b>83</b>
<b>Глава 8. Проектирование блокчейна</b>	<b>84</b>
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
<b>Глава 9. Документирование права владения</b>	<b>91</b>
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
<b>Глава 10. Хэширование данных</b>	<b>99</b>
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
<b>Глава 11. Хэширование на практике .....</b>	<b>110</b>
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**

<b>пользователей .....</b>	<b>125</b>
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 .....**

<b>.....</b>	<b>136</b>
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
<b>Глава 14. Хранение данных транзакций .....</b>	<b>145</b>
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
<b>Глава 15. Использование хранилища данных.....</b>	<b>159</b>
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

<b>Глава 18. Методы проверки и добавления транзакций</b>	<b>190</b>
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
<b>Глава 19. Выбор хронологии транзакций</b>	<b>204</b>
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.....245**

### **Глава 22. Обзор ограничений.....246**

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 .....255**

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 двигаемся 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
<b>Список литературы .....</b>	<b>296</b>
<b>Предметный указатель .....</b>	<b>300</b>



# ОБ АВТОРЕ

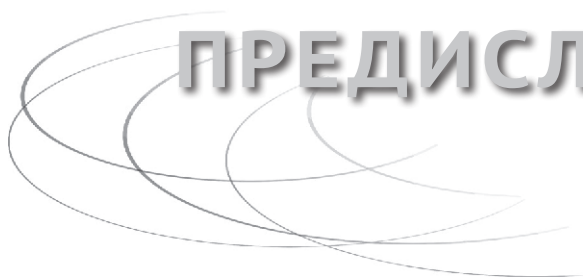
**Даниэль Дрешер** (Daniel Drescher) – опытный профессионал в банковской сфере, работавший в области электронной торговли ценными бумагами в нескольких банках. В последнее время его деятельность сосредоточена на задачах автоматизации, машинного обучения и обработки больших данных в сфере торговли ценными 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-



логий. Наконец, метафоры формируют простые практические правила для запоминания новых концепций без затруднений.

## Как организована эта книга

Книга состоит из 25 глав-этапов, сгруппированных по пяти основным темам (частям), которые в совокупности формируют процесс обучения с постепенным наращиванием знаний о технологии блокчейна. В главах рассматриваются основы программной инженерии, объясняется необходимая терминология, обосновывается необходимость применения технологии блокчейна, описываются отдельные концепции, заложенные в основу этой технологии, а также взаимодействие между ее компонентами, рассматриваются приложения блокчейна и направления разработок и активных исследований в этой области.

### *Часть I: Терминология и основы технологии*

В главах 1–3 рассматриваются основные концепции программной инженерии и группа терминов, необходимых для понимания последующих глав. К концу главы 3 вы получите общее представление об основных концепциях и общую картину области использования технологии блокчейна.

### *Часть II: Зачем нужна технология блокчейна*

В главах 4–7 объясняется, зачем нужна технология блокчейна, какие задачи она решает, почему решение этих задач важно, а также описываются потенциальные возможности блокчейна. К концу главы 7 вы будете хорошо понимать проблемную область технологии блокчейна, среды, в которой применение блокчейна наиболее эффективно, и почему в этих областях применение блокчейна рассматривается в первую очередь.

### *Часть III: Как работает блокчейн*

Третья часть является главной частью книги, поскольку подробно описывает внутреннее устройство и функционирование блокчейна. В главах 8–21 последовательно представлены 15 различных технических концепций, в совокупности составляющих основу

технологии блокчейна. К концу главы 21 вы будете полностью понимать все основные концепции блокчейна, их функционирование по отдельности, а также их взаимодействие для создания крупного комплексного механизма, называемого блокчейн.

### ***Часть VI: Ограничения и способы их преодоления***

В главах 22 и 23 главное внимание уделено основным ограничениям технологии блокчейна, описываются их причины и кратко намечаются способы их преодоления. К концу главы 23 вы будете понимать, почему основополагающая идея технологии блокчейна, подробно описанная в предыдущих главах, может оказаться не подходящей для крупных коммерческих приложений с потенциальной возможностью масштабирования, какие изменения были внесены для преодоления этих ограничений и как эти изменения повлияли на свойства блокчейна.

### ***Часть V: Использование технологии блокчейна, общие выводы и перспективы***

В главах 24 и 25 рассматриваются возможные варианты практического применения технологии блокчейна в реальном мире, а также вопросы, на которые необходимо найти ответы при выборе блокчейн-приложения. В этой части также определяются области разработок и активных исследований технологии блокчейна. К концу главы 25 вы будете полностью понимать технологию блокчейна и обладать вполне достаточной подготовкой для чтения более сложных технических материалов и участия в постоянно продолжающихся обсуждениях технологии блокчейна.

## **Дополнительные материалы**

Веб-сайт [www.blockchain-basics.com](http://www.blockchain-basics.com) предоставляет дополнительные материалы по темам некоторых глав данной книги.



# ЧАСТЬ I

## **ТЕРМИНОЛОГИЯ И ОСНОВЫ ТЕХНОЛОГИИ**

В этой части описываются основные концепции программной инженерии, а также устанавливаются правила организации и стандартизации при обсуждении основ технологии. Этот этап обучения также представляет концепции программной архитектуры и целостности программного обеспечения, а еще их связь с технологией блокчейна. К концу этого этапа вы будете хорошо понимать цели и задачи технологии блокчейна и ее потенциальные возможности.



# ГЛАВА 1

## ПОНИМАНИЕ УРОВНЕЙ И АСПЕКТОВ

**Анализ систем  
посредством разделения их  
на уровни и аспекты**

Эта глава закладывает основу для дальнейшего процесса изучения технологии блокчейна, четко определяя правила и способы организации и стандартизации при обсуждении основ технологии. В главе рассматриваются возможные методики анализа программных систем, объясняется, почему важно рассматривать программную систему как совокупность уровней. Далее наглядно демонстрируется, какие преимущества можно извлечь при анализе различных уровней системы и как такой подход помогает понять технологию блокчейна. В конце главы приводится краткое вводное описание концепции целостности программного обеспечения и подчеркивается ее важность.

### Метафора

У вас есть мобильный телефон? Я почти уверен, что есть, так как у подавляющего большинства людей имеется, по крайней мере, один мобильный телефон. Что вы знаете о разнообразных протоколах беспроводного обмена информацией, используемых для отправки и приема данных? Что вы знаете об электромагнитных волнах, являющихся основой мобильной связи? Большинству из нас не слишком много известно об этих технических подробностях, потому что такие знания не являются необходимыми для

практического использования мобильного телефона. К тому же почти все мы настолько заняты, что у нас вряд ли найдется время на изучение этих тонкостей. Мысленно разделяя мобильный телефон на общеизвестные составные части, мы учитываем, что обязательное присутствие этих частей невозможно игнорировать или считать само собой разумеющимся.

Такой подход к технологии не ограничивается только мобильными телефонами. Мы используем его во всех случаях, когда приходится осваивать новый телевизор, компьютер, стиральную машину и т. п. Но такие «мысленные» составные части в высшей степени индивидуальны, так как каждый по-своему решает, что считать важным, а что не зависит от наших индивидуальных предпочтений, от конкретной технологии, от наших целей и практических знаний. В результате ваше мысленное разделение мобильного телефона на составные части может отличаться от моего разделения того же самого мобильного телефона. Обычно это приводит к проблемам при обмене информацией, особенно если я пытаюсь объяснить вам, что необходимо знать об устройстве конкретной модели мобильного телефона. Таким образом, единый универсальный подход к разделению системы на составляющие компоненты является ключевым моментом при изучении и обсуждении любой технологии. В этой главе описывается, как следует разделять систему на составные части или уровни и соответствующим образом формулировать основные положения при обсуждении технологии блокчейна.

## Уровни программной системы

На протяжении всей книги при разделении любой системы на составные части используются следующие две методики:

- сопоставление приложения и его реализации;
- разделение на функциональные и нефункциональные аспекты.

### *Сопоставление приложения и его реализации*

Мысленное отделение потребностей пользователя от технических подробностей внутреннего устройства системы приводит к разделению уровня приложения и уровня реализации. Все, принад-

лежащее к уровню приложения, рассматривается как потребности пользователя (например, прослушивание музыки, фотографирование, заказ номера в отеле и т. д.). Все, принадлежащее к уровню реализации, рассматривается с точки зрения обеспечения выполнения вышеперечисленных действий (например, преобразование цифровой информации в акустические сигналы, определение цвета пиксела в цифровой видеокамере или передача сообщения по сети Интернет в систему бронирования номеров отеля). Элементы уровня реализации являются техническими по своей сущности и рассматриваются как средства достижения той или иной цели.

### ***Разделение на функциональные и нефункциональные аспекты***

Различие между тем, что система делает и как она это делает, приводит к разделению функциональных и нефункциональных аспектов. Примерами функциональных аспектов являются: передача данных по сети, воспроизведение музыки, фотографирование и редактирование отдельных пикселей в изображении. Примеры нефункциональных аспектов: удобный графический пользовательский интерфейс, быстрое программное обеспечение, возможность безопасного хранения пользовательских данных и защита их приватности. Другими важными нефункциональными аспектами системы являются безопасность и целостность. Целостность (integrity) означает, что система ведет себя именно так, как от нее ожидают, в то же время понятие целостности включает в себя и многие другие аспекты, такие как, например, безопасность (защищенность) и корректность [8]. Эффективным способом запоминания различий между функциональными и нефункциональными аспектами системы является аналогия с грамматикой русского или английского языка: глаголы описывают действия (что делается), а наречия – как выполняются эти действия. Например, человек может идти быстро или медленно. В обоих случаях действие «идти» одинаково, но способы выполнения этого действия различны. Поэтому в качестве практического правила можно предложить аналогию: функциональные аспекты соответствуют глаголам, нефункциональные аспекты соответствуют наречиям.

## Одновременное изучение двух уровней

Определение функциональных и нефункциональных аспектов и разделение на уровень приложения и уровень реализации можно выполнять одновременно, получая в результате двумерную таблицу. В табл. 1.1 показан результат мысленного разделения на уровни системы «мобильный телефон» с одновременным определением функциональных и нефункциональных аспектов.

**Таблица 1.1** Пример мысленного разделения на уровни мобильного телефона

Уровень	Функциональные аспекты	Нефункциональные аспекты
Приложения	Фотографирование Телефонные вызовы Отправка сообщений электронной почты Навигация по Интернету Отправка сообщений в чаты	Графический пользовательский интерфейс выглядит привлекательно Удобство пользования Сообщения отправляются очень быстро
Реализации	Внутренний механизм сохранения пользовательских данных Установка соединения с ближайшим узлом мобильной связи Возможность доступа к отдельным пикселям в цифровой фото(видео) камере	Эффективное хранение данных Экономия энергии Обеспечение целостности Защита приватности пользователя

Таблица 1.1 может описывать видимость (или невидимость) конкретных элементов системы для ее пользователей. Функциональные аспекты уровня приложения в большинстве своем являются видимыми элементами системы, поскольку предназначены для удовлетворения очевидных потребностей пользователей. Эти элементы обычно хорошо знакомы пользователям. С другой стороны, нефункциональные аспекты уровня реализации редко проявляют себя как основные элементы системы. Их наличие считается само собой разумеющимся.

## Целостность

Целостность (integrity) – это важный нефункциональный аспект любой программной системы. Понятие целостности включает три главных компонента [5]:

- целостность данных (data integrity): данные, используемые и сопровождаемые системой, должны быть полными, корректными и непротиворечивыми;
- целостность поведения (behavioral integrity): система ведет себя, как предполагается, и не допускает логических ошибок;
- безопасность (защита) (security): система способна ограничить доступ к своим данным и функциональным возможностям, разрешая его только авторизованным пользователям.

Возможно, большинство людей считает целостность программных систем фактом, не требующим подтверждения, потому что большую часть времени имеет дело с системами, сохраняющими свою целостность. Это становится возможным благодаря тому, что программисты и инженеры затратили огромное количество времени и усилий на разработку систем, обеспечивающих собственную целостность. Иногда возможна не совсем верная оценка труда инженеров по созданию систем, обеспечивающих высокий уровень целостности. Но наше мнение может измениться, как только мы встретимся с системой, не обладающей этим свойством. Это могут быть случаи потери данных, необъяснимого поведения программного обеспечения или обнаружения факта доступа посторонних лиц к вашим личным закрытым данным. Это ситуации, когда ваш мобильный телефон, компьютер, программа электронной почты, текстовый процессор или электронная таблица заставляет вас разозлиться и забыть о хороших манерах. Во всех подобных случаях мы действительно начинаем понимать, насколько важным аспектом является целостность программного обеспечения. Поэтому не должно вызывать удивления то обстоятельство, что профессиональные разработчики программного обеспечения затрачивают огромное количество времени на кажущийся незначительным аспект уровня реализации.

## Перспектива

В этой главе представлена вводная информация о некоторых общих принципах программной инженерии. Здесь рассматривались концепции целостности, функциональные и нефункциональные аспекты, уровни приложения и реализации программной системы. Понимание этих концепций поможет вам более широко взглянуть на среду, в которой существует технология блокчейна. В следую-