Beginning Blockchain

A Beginner's Guide to Building Blockchain Solutions

Bikramaditya Singhal
Gautam Dhameja
Priyansu Sekhar Panda

Apress®

Блокчейн

Руководство для начинающих разработчиков

Бикрамадитья Сингхал
Гаутам Дамеджа
Приянсу Сехар Панда

Санкт-Петербург
«БХВ-Петербург»
2019

УДК 004.75+519.83+336.7
ББК 32.973.26-018
С38

Сингхал, Б.

С38 Блокчейн. Руководство для начинающих разработчиков: Пер. с англ. / Б. Сингхал, Г. Дамеджа, П. С. Панда. — СПб.: БХВ-Петербург, 2019. — 288 с.: ил.

ISBN 978-5-9775-4052-0

Книга предназначена для изучения фундаментальных основ блокчейна и решения прикладных задач. С нуля изложены основы криптографии, устройство блокчейна и его основные компоненты: математика, криптография, теория игр. Изложены технические основы самых известных блокчейнов в мире — Bitcoin и Ethereum. Продемонстрировано, как можно запрограммировать блокчейн для разных вариантов использования, не ограничиваясь только криптовалютой. Рассмотрен процесс разработки кода для управления транзакциями на языках JavaScript и Solidity, показано, как самостоятельно создавать и размещать умные контракты. Продемонстрирован полный цикл разработки децентрализованного приложения (DApps).

Для программистов, преподавателей и студентов,
а также специалистов отделов развития компаний и банков

УДК 004.75+519.83+336.7
ББК 32.973.26-018

Группа подготовки издания:

Руководитель проекта	*Евгений Рыбаков*
Зав. редакцией	*Екатерина Сависте*
Перевод с английского	*Валерия Яценкова*
Компьютерная верстка	*Ольги Сергиенко*
Оформление обложки	*Карины Соловьевой*

"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20.

ISBN 978-1-4842-3443-3 (англ.)
ISBN 978-5-9775-4052-0 (рус.)

Оглавление

Об авторах **11**

О техническом рецензенте **13**

Благодарности **15**

Предисловие **17**

ГЛАВА 1. Знакомство с блокчейном **19**
1.1. Происхождение блокчейна 19
1.2. Что такое блокчейн? 21
Шаг 1 25
Шаг 2 25
Шаг 3 25
1.3. Централизованные и децентрализованные системы 26
1.3.1. Централизованные системы 28
1.3.2. Децентрализованные системы 29
1.4. Уровни блокчейна 31
1.4.1. Прикладной уровень (application layer) 32
1.4.2. Уровень выполнения (execution layer) 33
1.4.3. Семантический уровень (semantic layer) 33
1.4.4. Уровень распространения (propagation layer) 34
1.4.5. Уровень консенсуса (consensus layer) 35
1.5. Почему блокчейн так важен? 35
1.5.1. Ограничения централизованных систем 35
1.5.2. Долго ли ждать блокчейн? 36
1.6. Практическое применение блокчейна 37
1.7. Заключение 39
1.8. Рекомендуемые источники 39

ГЛАВА 2. Как работает блокчейн? **41**
2.1. Фундаментальные основы блокчейна 41
2.2. Криптография 43
2.2.1. Криптография с симметричным ключом 45
Принцип Керкгоффса и функция XOR 46

Потоковое и блочное шифрование....47
Одноразовый блокнот....49
Стандарт шифрования данных DES....50
Расширенный стандарт шифрования AES....54
Расширение ключа AES....57
Проблемы криптографии с симметричным ключом....59
2.2.2. Криптографические хэш-функции....59
Обзор различных хэш-функций....63
SHA-2....64
SHA-256 и SHA-512....66
RIPEMD....67
SHA-3....67
Применение хэш-функций....71
Примеры кода хэш-функций....72
2.2.3. MAC и HMAC....73
2.2.4. Криптография с асимметричным ключом....74
RSA....77
Алгоритм цифровой подписи DSA....81
Криптография на эллиптических кривых....82
Алгоритм ECDSA....85
Примеры кода для криптографии с открытым ключом....87
2.2.5. Обмен ключами по Диффи — Хеллману....89
2.2.6. Открытый или закрытый ключ?....92
2.3. Теория игр....93
2.3.1. Равновесие по Нэшу....95
2.3.2. Дилемма заключенного....96
2.3.3. Проблема византийских генералов....98
2.3.4. Игры с нулевой суммой....99
2.3.5. Зачем изучать теорию игр?....100
2.4. Информатика....100
2.4.1. Хэш-указатель....101
2.4.2. Дерево Меркла....103
2.4.3. Сниппеты кода для дерева Меркла....105
2.5. Обобщаем знания....107
2.5.1. Свойства блокчейн-решений....108
Неизменность....108
Стойкость к подделке....108
Демократичность....109
Устойчивость к двойным расходам....109
Согласованное состояние реестра....110
Жизнестойкость....110
Проверяемость....110
2.5.2. Транзакции и блокчейн....110
2.5.3. Механизмы распределенного консенсуса....112
Доказательство работы (PoW)....113
Доказательство владения долей (PoS)....114
Алгоритм PBFT....115
2.6. Применение блокчейна....116

2.7. Масштабирование блокчейна 119
2.7.1. Вычисления вне блокчейна 120
2.7.2. Шардинг 122
2.8. Заключение 123
2.9. Рекомендуемые источники 124

ГЛАВА 3. Как работает Bitcoin? 127
3.1. История денег 127
3.2. Появление биткойна 130
3.2.1. Что такое биткойн? 131
3.2.2. Работа с биткойнами 133
3.3. Блокчейн Bitcoin 134
3.3.1. Структура блока 136
Дерево Меркла 137
Уровень сложности 139
3.3.2. Блок генезиса 141
3.4. Сеть Bitcoin 143
3.4.1. Регистрация нового узла в сети 145
3.4.2. Bitcoin-транзакции 149
3.4.3. Консенсус и майнинг блоков 153
3.4.4. Распространение блока 159
3.5. Промежуточные итоги главы 160
3.6. Скрипты Bitcoin 161
3.6.1. Еще раз про транзакции в сети Bitcoin 161
3.6.2. Скрипты 167
3.7. Полные узлы или SPV? 170
3.7.1. Полные узлы 170
3.7.2. Упрощенная проверка транзакций 171
3.8. Биткойн-кошельки 172
3.9. Заключение 175
3.10. Рекомендуемые источники 175

ГЛАВА 4. Как работает Ethereum? 177
4.1. От Bitcoin до Ethereum 177
4.1.1. Ethereum как блокчейн нового поколения 179
4.1.2. Философия блокчейна Ethereum 180
4.2. Введение в блокчейн Ethereum 180
4.2.1. Структура данных блокчейна Ethereum 181
4.2.2. Счета Ethereum 183
Преимущества концепции UTXO 185
Преимущества концепции счетов 186
Состояние счета 186
4.2.3. Применение префиксного trie-дерева 188
4.2.4. Дерево Меркла — Патриции 189
4.2.5. RLP-кодирование 190
4.2.6. Транзакция Ethereum и структура сообщения 191
4.2.7. Функция перехода состояния Ethereum 194
4.2.8. Газ и стоимость транзакции 196

4.3. Умные контракты Ethereum 200
4.3.1. Создание контракта 202
4.4. Виртуальная машина Ethereum и выполнение кода 202
4.5. Экосистема Ethereum 206
4.5.1. Swarm 207
4.5.2. Whisper 207
4.5.3. Децентрализованное приложение (DApp) 207
4.5.4. Компоненты разработки 207
4.6. Заключение 208
4.7. Рекомендуемые источники 208

ГЛАВА 5. Разработка блокчейн-приложений 209
5.1. Децентрализованные приложения 209
5.2. Создание блокчейн-приложений 210
5.2.1. Программирование приложений Bitcoin и Ethereum 211
5.2.2. Библиотеки и инструменты 212
5.3. Взаимодействие с блокчейном Bitcoin 212
5.3.1. Установка и инициализация библиотеки BitcoinJS в приложении node.js 213
5.3.2. Создание пары ключей для отправителя и получателя 214
5.3.3. Получение тестовых биткойнов 215
5.3.4. Получение неизрасходованных остатков 216
5.3.5. Подготовка биткойн-транзакции 217
5.3.6. Подписание входных данных транзакции 219
5.3.7. Создание HEX-кода транзакции 219
5.3.8. Трансляция транзакции в сеть 219
5.4. Программное взаимодействие с Ethereum — отправка транзакций 220
5.4.1. Настройка библиотеки и подключения 222
5.4.2. Настройка счетов Ethereum 222
5.4.3. Получение тестового эфира на счет отправителя 223
5.4.4. Подготовка транзакции Ethereum 224
5.4.5. Подписание транзакции 224
5.4.6. Отправка транзакции в сеть Ethereum 225
5.5. Создание умного контракта Ethereum 226
5.5.1. Подготовка 227
5.5.2. Программируем умный контракт 227
5.5.3. Получение сведений о контракте 230
5.5.4. Развертывание контракта в сети Ethereum 232
5.6. Вызов функций умного контракта 235
5.6.1. Получение ссылки на смарт-контракт 235
5.6.2. Вызываем функцию умного контракта 236
5.7. Блокчейн с новой точки зрения 238
5.8. Публичные и частные блокчейны 239
5.9. Архитектура децентрализованных приложений 239
5.9.1. Публичные и локальные узлы 239
5.9.2. Децентрализованные приложения и серверы 241
5.10. Заключение 241
5.11. Рекомендуемые источники 241

ГЛАВА 6. Разработка приложений Ethereum 243
6.1. Децентрализованное приложение 243
6.2. Настройка частной сети Ethereum 244
6.2.1. Установка клиента GoEthereum 245
6.2.2. Создание каталога данных geth 245
6.2.3. Создание учетной записи geth 245
6.2.4. Создание файла конфигурации genesis.json 246
6.2.5. Запуск первого узла частной сети 247
6.2.6. Запуск второго узла частной сети 250
6.3. Создание умного контракта 253
6.4. Развертывание умного контракта 259
6.4.1. Настройка библиотеки web3 и подключения 259
6.4.2. Развертывание контракта в частной сети 260
6.5. Клиентское веб-приложение 268
6.6. Заключение 278
6.7. Рекомендуемые источники 278

Приложение. Описание электронного архива 279

Предметный указатель 281

Об авторах

Бикрамадитья Сингхал (Bikramaditya Singhal) — эксперт по блокчейну и специалист по искусственному интеллекту с опытом работы в различных отраслях. Он обладает обширными знаниями в области криптографии, кибербезопасности и науки о данных, владеет навыками работы с блокчейнами Bitcoin, Ethereum и Hyperledger. Бикрамадитья Сингхал работал с такими компаниями, как WISeKey, Tech Mahindra, Microsoft India, Broadridge и Chelsio Communications, а также основал компанию под названием Mund Consulting, которая специализируется на анализе больших данных и искусственном интеллекте. Имеет большой опыт обучения и консультирования по технологии блокчейна, разработал множество блокчейн-решений. Активный докладчик на различных конференциях, встречах и семинарах. Является также автором книги под названием «Spark for Data Science».

Гаутам Дамеджа (Gautam Dhameja) — консультант по блокчейн-приложениям из Берлина, Германия. В течение последнего десятилетия он занимался разработкой и поставкой корпоративного программного обеспечения, включая веб-приложения и мобильные приложения, облачные гипермасштабируемые решения Интернета вещей и, в последнее время, децентрализованные приложения на основе блокчейна (DApps). Он обладает глубоким пониманием децентрализованного стека, архитектуры облачных решений и объектно-ориентированного проектирования. Гаутам Дамеджа специализируется на блокчейне, облачных корпоративных решениях, Интернете вещей, распределенных системах, а также специальных и гибридных мобильных приложениях. Является активным блоггером и регулярно выступает на технических конференциях и мероприятиях.

Прияну Сехар Панда (Priyansu Sekhar Panda) — инженер-исследователь компании Underwriters Laboratories, Бангалор, Индия. Он сотрудничал с другими ИТ-компаниями, такими как Broadridge, Infosys Limited и Tech Mahindra. Обладает навыками применения блокчейнов Bitcoin, Ethereum, Hyperledger, а также знаниями в области теории игр, Интернета вещей и искусственного интеллекта. Текущие исследования автора направлены на создание приложений нового поколения, использующих блокчейн, Интернет вещей и искусственный интеллект. Прияну Сехар Панда трудится над созданием децентрализованных автономных организаций (DAO), а также изучает безопасность, масштабируемость и механизмы консенсуса блокчейнов.

О техническом рецензенте

Навин Манасви (Navin K Manaswi) уже много лет разрабатывает решения и приложения с использованием передовых технологий на основе искусственного интеллекта. Работая в консалтинговых компаниях в Малайзии, Сингапуре и в проекте Dubai Smart City, он приобрел редкий навык разработки комплексных проектов в области искусственного интеллекта. Навин Манасви создал решения для видеосвязи, документооборота и корпоративных чат-роботов. В настоящее время решает проблемы делового взаимодействия в сфере здравоохранения, бизнеса, промышленного Интернета вещей и розничной торговли в инкубаторе Symphony AI, где работает архитектором систем глубокого машинного обучения. С помощью этой книги он хочет как можно шире популяризовать децентрализованные вычисления и сервисы, особенно среди разработчиков программного обеспечения, специалистов по обработке данных, инженеров баз данных, бизнес-аналитиков и руководителей компаний.

Благодарности

Авторы хотели бы поблагодарить Никхила (Nikhil) и Дивью (Divya) за их сотрудничество и поддержку на всем протяжении работы над книгой. Большое спасибо Навину Манасви за его тщательный технический анализ этой книги. Мы также благодарим всех, кто прямо или косвенно внес в эту книгу свой вклад.

Предисловие

«Блокчейн с нуля» — это книга для тех, кто хочет изучить технические основы блокчейна и вопросы разработки и применения прикладных приложений для работы с блокчейном. Краткое, но тщательно продуманное изложение истории платежных систем и основ криптографии поможет погрузиться в изучение технологии блокчейна, а примеры прикладного кода помогут читателю быстро приступить к разработке приложений.

Глава 1 знакомит вас с историей платежных систем и происхождением технологии блокчейна. В *главе 2* детально рассмотрены основные компоненты блокчейна: математика, криптография, теория игр. *Глава 3* посвящена техническим основам самого известного блокчейна в мире — Bitcoin (Биткойн) и содержит примеры использования этой криптовалюты. *Глава 4* посвящена блокчейн-платформе Ethereum (Эфириум) и демонстрирует, как можно запрограммировать блокчейн для разных вариантов использования, не ограничиваясь только криптовалютой. В *главе 5* вы познакомитесь с разработкой кода для управления транзакциями на языках JavaScript и Solidity и научитесь создавать и размещать умные контракты. *Глава 6* завершает книгу и демонстрирует полный цикл разработки децентрализованного приложения (Decentralized Applications, DApps). К концу этой главы вы овладеете достаточным количеством инструментов и методов для решения различных прикладных задач с помощью технологии блокчейна. Сделайте первый шаг на пути к безграничным возможностям!

ГЛАВА 1

Знакомство с блокчейном

Блокчейн — это очередная волна перемен, которая уже начала менять структуру деловых, социальных и политических связей, а также способы перемещения средств. С другой стороны, блокчейн — это не просто перемены, а некая сущность, которая никогда не стоит на месте. На момент подготовки этой книги более 40 ведущих финансовых учреждений и множество фирм в различных отраслях начали осваивать блокчейн — чтобы снизить транзакционные издержки, ускорить прохождение транзакций, снизить риск мошенничества и устранить посредников. Некоторые фирмы пытаются с его помощью перестроить устаревшие системы и сервисы, чтобы вывести их на следующий уровень, а также предложить новые виды услуг.

Мы будем детально исследовать блокчейн на протяжении всей книги. Если вы новичок, то можете последовательно изучать главу за главой или выбрать только те главы, которые вам нужнее. Эта глава расскажет о том, что такое блокчейн, как он развивался, где применяется и почему так важен в современном мире. Вы получите из нее общее представление о блокчейне, которое поможет вам глубже погрузиться в его изучение.

1.1. Происхождение блокчейна

Одним из первых переломных моментов цифровой истории стало появление в 1970-х годах протокола TCP/IP[1], на котором основан современный Интернет. До появления TCP/IP мы жили в эпоху коммутируемых каналов, которые нуждались в прямом физическом соединении между двумя устройствами.

[1] Transmission Control Protocol/Internet Protocol — протокол управления передачей/протокол сети Интернет (*англ.*). — *Здесь и далее примечания от редакции русского перевода.*

Когда в начале 1990-х годов Интернет явился общественности в виде «сетевой паутины» World Wide Web (WWW), ему пришлось обеспечивать связь всех со всеми. Это связано с тем, что Интернет построен поверх открытого и децентрализованного протокола TCP/IP. Когда какие-либо новые технологии, особенно революционные, попадают на рынок, они либо умирают сами по себе, либо приобретают такое влияние, что становятся общепринятой нормой. Общество приспособилось к сетевой революции и по-своему воспользовалось возможностями, которые она предлагала. В результате сеть сформировалась, пожалуй, не совсем в том виде, как это было задумано. Она могла бы стать более открытой, доступной и равноправной. Однако многие новые технологии начали накладываться на существующие структуры, и к сегодняшнему дню Интернет стал таким, каков он есть, — более централизованным. Люди склонны привыкать к ограничениям технологии. Нынче они вполне довольны, если международный перевод средств занимает несколько дней[2], или обходится слишком дорого, или недостаточно надежен.

Давайте подробнее рассмотрим банковскую систему и ее эволюцию. Начиная с первобытной меновой системы и вплоть до фиатных валют[3], между сделкой и ее подтверждением не было никакой реальной разницы, поскольку они не были двумя отдельными действиями. Например, если Алисе нужно заплатить 10 долларов Бобу, она просто передает Бобу банкноту номиналом 10 долларов. На этом сделка полностью завершена. Банку не нужно было списывать 10 долларов со счета Алисы и записывать на счет Боба или служить поручителем, чтобы Алиса не обманула Боба. Однако прямое взаимодействие с каждым человеком весьма затруднительно. Поэтому в банковской сфере появилось множество услуг, включая денежные переводы из любого уголка мира. Появление Интернета сломало последние преграды, и банковское дело стало проще, чем когда-либо. Но не только банковское дело — Интернет облегчил и другие способы перемещения ценности через сетевую паутину.

Традиционная технология позволяет кому-либо из Индии совершить денежную сделку с кем-либо в Соединенном Королевстве, но с некоторыми издержками. Для урегулирования таких транзакций требуются дни, и вдобавок они дорого обходятся. Банку всегда необходимо гарантировать доверие и обеспечить безопасность для таких сделок между двумя или более сторонами. А что, если найдется технология, которая может обеспечить доверие и безопасность без этих посредников и централизованных систем? По какой-то причине эта часть технологии — обеспечение доверия — отстала в развитии, и в результате расплодились централизованные системы, такие как банки, службы условного депонирования, клиринговые палаты, регистраторы и многие другие подобные учреждения. Блокчейн стал той недостающей частью интернет-революции, которая превращает уязвимую систему обмена ценностями в криптографически защищенную крепость.

---

[2] Даже если адресат получил средства через несколько секунд, в традиционной банковской системе взаимные расчеты банков закрываются через клиринговую палату в срок от нескольких дней до месяца.

[3] Фиатная валюта — валюта, которую правительство позиционирует как единственное законное платежное средство.

Тот, кто ныне скрывается под всемирно известным псевдонимом Сатоши Накамото, прекрасно понимал, что банковская система образца 1980-х годов отстала от технологической революции. Банки создали централизованные организации, которые хранят транзакционные записи, контролируют взаимодействие, обеспечивают доверие и безопасность и регулируют всю систему. Вся коммерция опирается на эти финансовые учреждения, которые служат доверенными посредниками при обработке платежей. Посредничество финансовых учреждений увеличивает затраты и время на прохождение транзакции, а также ограничивает размеры транзакций. Посредники необходимы для разрешения споров, но по сути это означает, что совершенно необратимая транзакция невозможна — ведь посредник может ее отменить. Это следует из ситуации, когда для совершения сделки с контрагентом требуется доверенный посредник. Разумеется, эта бюрократическая система рано или поздно должна измениться, чтобы идти в ногу с наступающей цифровой трансформацией экономики. Итак, Сатоши изобрел криптовалюту под названием биткойн, в основу которой заложен блокчейн. Биткойн — это всего лишь частный случай использования блокчейна, который учитывает внутреннюю уязвимость моделей, основанных на доверии. В этой книге мы рассмотрим фундаментальные основы как биткойна, так и блокчейна.

1.2. Что такое блокчейн?

Интернет радикально изменил многие аспекты жизни, общества и бизнеса. Однако в предыдущем разделе мы отмечали, что способы проведения транзакций между людьми и организациями за последние несколько десятилетий не сильно изменились. Блокчейн, как мы уже говорили, ставит все на свои места и делает систему транзакций более открытой, доступной и надежной.

Чтобы понять сущность блокчейна, вы должны посмотреть на него как с точки зрения бизнеса, так и с технической точки зрения. Давайте сначала рассмотрим блокчейн в контексте бизнес-транзакций, чтобы понять *что* он дает, а в следующих главах углубимся в техническую составляющую, чтобы понять *как* он это делает.

Итак, блокчейн — это система записей о переносе любой ценности (а не только денег!) по принципу «от равного к равному» (peer-to-peer). Это означает, что нет необходимости в посредниках, таких как банки, брокеры или другие службы депонирования, которые служат доверенной третьей стороной. Например, если Алиса заплатит Бобу 10 долларов, почему они обязательно должны проходить через банк? Взгляните на рис. 1.1.

Давайте рассмотрим другой пример. Типичная операция с акциями происходит за доли секунды, но сведение балансов через клиринговую палату длится недели. Приемлемо ли это в цифровую эпоху? Конечно же, нет! На рис. 1.2 показана текущая ситуация.

Но если кто-то хочет купить акции у компании или у человека, они могут, используя блокчейн, купить их напрямую и с немедленной регистрацией сделки, без

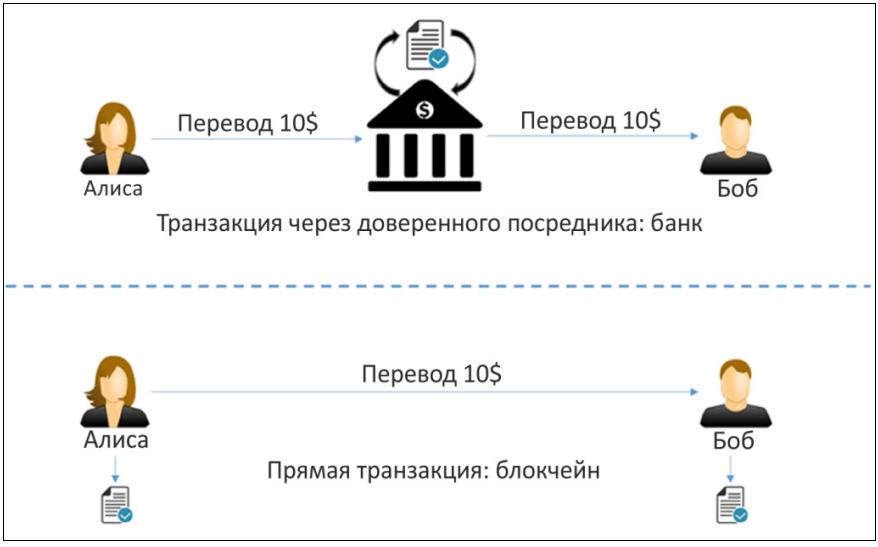

Рис. 1.1. Транзакция через посредника и прямая транзакция

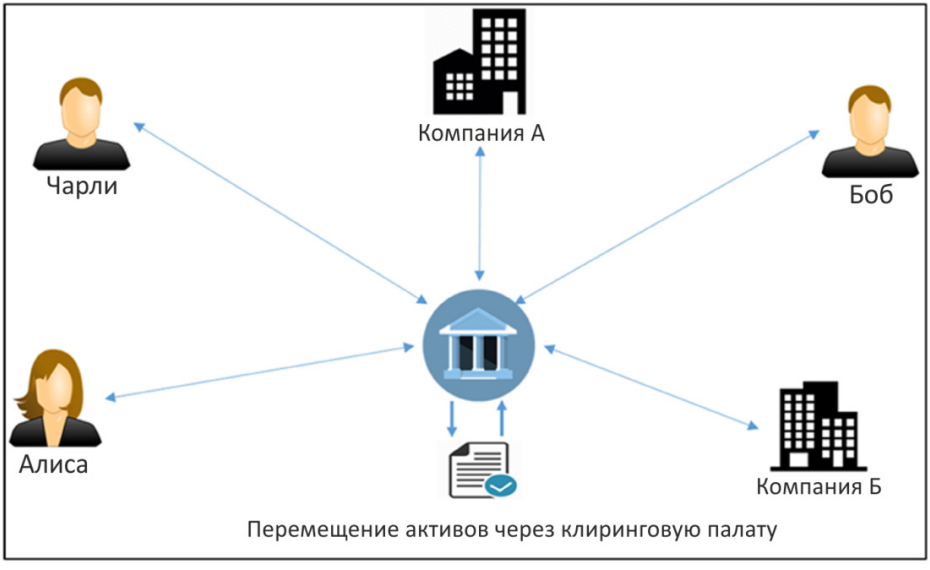

Рис. 1.2. Биржевая торговля через клиринговую палату

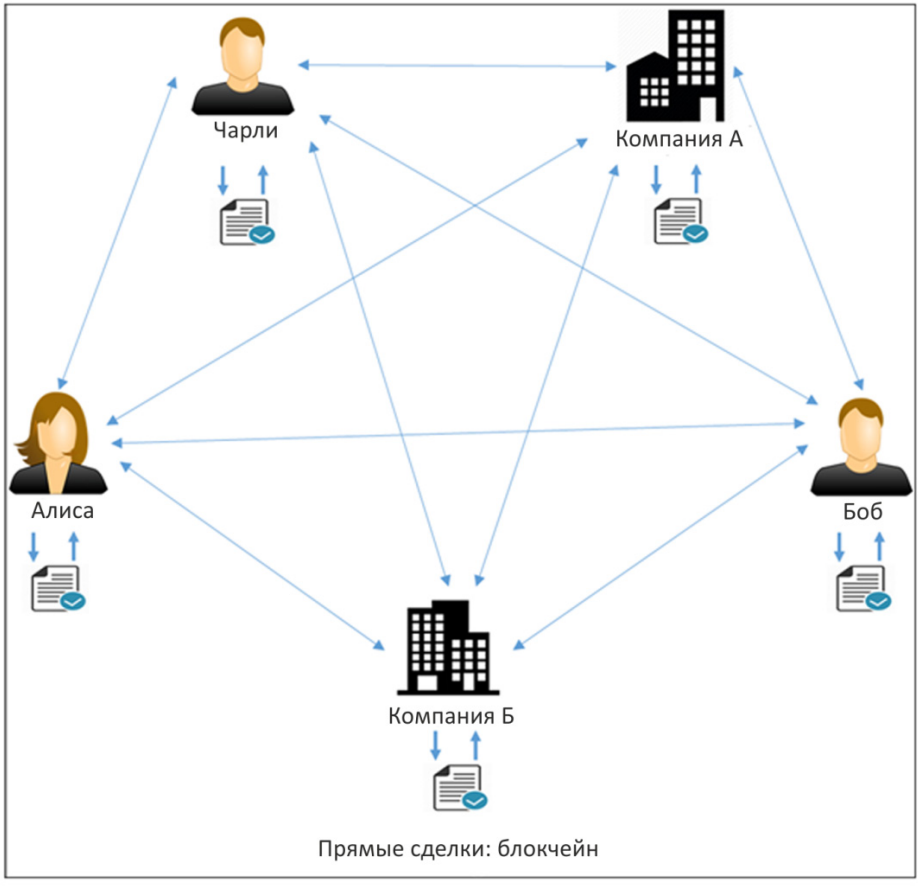

Рис. 1.3. Сделки в одноранговой сети

необходимости участия брокеров, клиринговых палат или других финансовых учреждений. Децентрализованное и одноранговое решение такой задачи может выглядеть, как показано на рис. 1.3.

Обратите внимание, что транзакция и подтверждение сделки не являются двумя разными сущностями в среде блокчейна! Транзакции здесь аналогичны денежным сделкам, где, к примеру, кто-то платит банкнотой номиналом 10 долларов и больше не владеет ею, а банкнота физически передается новому владельцу.

Теперь, когда вы поняли функциональную суть блокчейна на верхнем уровне, давайте взглянем на его устройство с технической точки зрения, и нам станет понятно, почему блокчейн называют именно этим словом. Сейчас мы увидим, *что* это такое, а изучение того, *как* это работает, оставим для *главы 2*.

- Блокчейн — это одноранговая система передачи ценности без участия доверенной третьей стороны.
- Это общий, децентрализованный и открытый реестр транзакций. База данных реестра реплицируется (копируется) на большое количество узлов.

- База данных реестра работает только в режиме добавления записей и не может быть изменена или исправлена. Это означает, что каждая запись является постоянной и неизменной. Любая новая запись появляется во всех копиях базы данных, размещенных на разных узлах.
- Нет необходимости, чтобы доверенные третьи стороны выступали в качестве посредников для проверки, обеспечения безопасности и подтверждения транзакций.
- Блокчейн — это еще один функциональный слой поверх Интернета, и он может сосуществовать с другими интернет-технологиями.
- Точно так же, как протокол TCP/IP был разработан для создания открытой системы обмена данными, технология блокчейна была разработана для подлинной децентрализации обмена ценностями. Руководствуясь этой идеей, создатели биткойна открыли исходный код, чтобы на него могли опираться разработчики других децентрализованных приложений.

Типичный блокчейн в общем виде выглядит так, как показано на рис. 1.4.

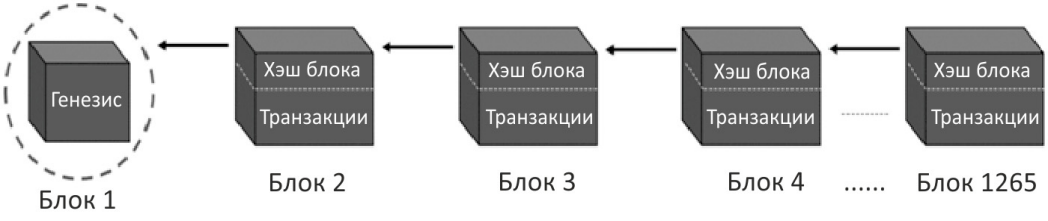

Рис. 1.4. Структура данных блокчейна

Каждый узел в сети имеет идентичную копию блокчейна, условно показанную на рис. 1.4, где каждый блок представляет собой совокупность транзакций и связь с предыдущим блоком — отсюда и происходит название[4] технологии. Как вы можете видеть, каждый блок состоит из двух частей: *заголовка* и *тела* блока. Заголовок ссылается на предыдущий блок в цепочке. Каждый заголовок блока содержит хэш предыдущего блока, поэтому никто не может незаметно изменить транзакцию в предыдущем блоке (подробности этой концепции мы рассмотрим в следующих главах). Тело блока содержит список проверенных транзакций, их суммы, адреса сторон и некоторые другие подробности. Таким образом, имея последний блок, можно получить последовательный доступ ко всем предыдущим блокам в цепочке блоков.

Чтобы понять, как работает эта система, рассмотрим практический пример и проследим, как происходят транзакции и обновляется реестр.

Предположим, что есть три участника: Алиса, Боб и Чарли, которые проводят некоторые денежные транзакции между собой в сети блокчейна. Давайте проследуем по пути транзакций шаг за шагом, чтобы понять, как работают открытые и децентрализованные функции блокчейна.

[4] Block — блок, chain — цепь (*англ.*).

Шаг 1

Допустим, что у Алисы в кошельке было 50 долларов, что является *генезисом* (начальной точкой) всех транзакций, и каждый узел сети знает об этом (рис. 1.5).

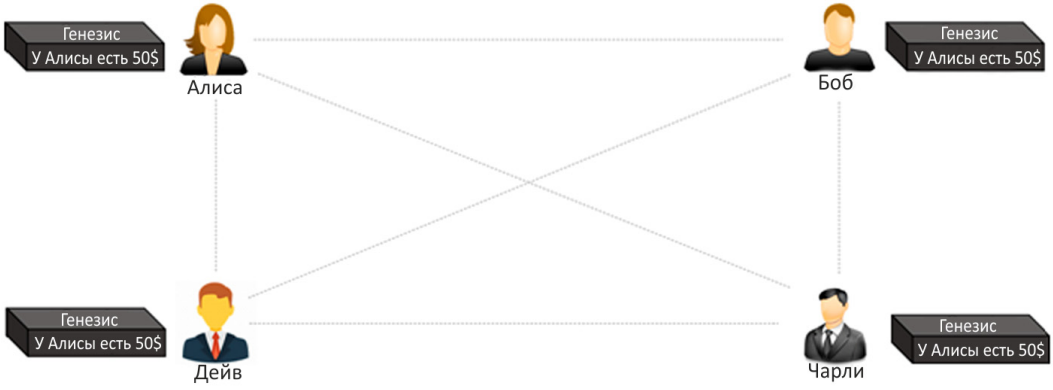

Рис. 1.5. Генезис — начальный блок в цепочке транзакций

Шаг 2

Алиса совершает сделку, заплатив 20 долларов Бобу. Обратите внимание, что блокчейн обновился на каждом узле (рис. 1.6).

Рис. 1.6. Первая транзакция

Шаг 3

Боб совершает другую сделку, заплатив 10 долларов Чарли, и блокчейн снова обновляется (рис. 1.7).

Рис. 1.7. Вторая транзакция

Обратите внимание, что данные транзакций в блоках неизменяемы. Все транзакции полностью необратимы. Любое изменение породит новую транзакцию, которая будет подтверждена всеми участниками. У каждого узла есть своя копия блокчейна.

Если сейчас у вас появились разные вопросы, например: «Что, если Алиса одновременно выплатит Дейву такую же сумму, как и Бобу (двойное списание), или что, если она запустит транзакцию, не имея достаточного количества средств на своем счете?», «Как обеспечивается безопасность?» — это замечательно! Мы рассмотрим эти вопросы в следующих главах.

1.3. Централизованные и децентрализованные системы

Причина, по которой мы обсуждаем централизацию и децентрализацию, состоит лишь в том, что блокчейн создан для децентрализации и отвергает централизованный подход. Тем не менее, термины «децентрализованный» и «централизованный» не всегда понятны. Зачастую они очень плохо определены и вводят в заблуждение. Дело в том, что почти не существует систем, которые являются чисто централизованными или децентрализованными. Большинство идей и примеров в этом разделе основано на заметках Виталика Бутерина, основателя блокчейна Ethereum.

Что такое *распределенная система*? Чтобы не примешивать это понятие к текущему обсуждению, давайте сначала разберемся с ним и отложим в сторону. Дело в том, что независимо от того, централизована или децентрализована система, ее все равно можно распределить. *Централизованная распределенная система* — это такая система, в которой есть главный узел, ответственный за дробление задач или данных и распределение нагрузки между узлами. Напротив, *децентрализованная распределенная система* — это такая система, где нет главного узла как такового, но все же вычисления могут быть распределены. Блокчейн — один из таких примеров, и позже мы рассмотрим различные графические представления блокчейна.

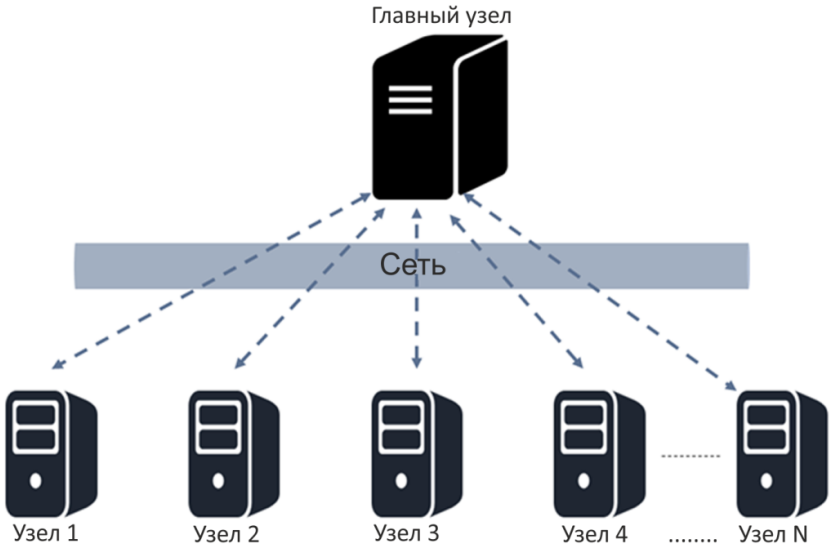

Рис. 1.8. Пример распределенной системы с централизованным управлением

Пример того, как может выглядеть централизованная распределенная система, показан на рис. 1.8.

Например, это представление соответствует тому, как реализована сеть распределенных вычислений Hadoop. Хотя вычисление в таких проектах происходит быстрее благодаря распределению, оно также страдает от ограничений из-за централизации.

Вернемся к обсуждению вопросов централизации и децентрализации. Крайне важно отметить, что централизация или децентрализация системы определяется не только технической архитектурой. Мы хотим подчеркнуть, что система может быть централизованной или децентрализованной с *технической* точки зрения, но *логически* или *политически* может быть устроена совершенно иначе. Давайте рассмотрим эти аспекты архитектур, чтобы иметь возможность правильно спроектировать систему, исходя из потребностей пользователей.

- **Технический аспект.** Система может быть централизованной или децентрализованной с точки зрения технической архитектуры. Здесь мы анализируем, сколько физических компьютеров (или узлов) используется для создания системы, количество отказов узлов, которые она может выдержать до того, как вся система рухнет, и т. д.
- **Политический аспект.** Здесь мы анализируем контроль, который человек, группа людей или организация имеют над системой в целом. Если все компьютеры системы контролируются узким кругом лиц, то система совершенно очевидно централизована. Однако если ни один конкретный индивид или группа не контролируют систему, и у всех пользователей есть равные на нее права, то в политическом смысле это децентрализованная система.