Содержание

Над книгой работали

Об авторе

Имран Башир – магистр информатики, получил научную степень в Королевском колледже Холлоуэй при Лондонском университете. Ранее занимался разработкой ПО, архитектурой решений, управлением инфраструктурой и управлением IT-услугами. Также он является членом IEEE (Института инженеров электротехники и электроники) и BCS (Британского общества вычислительной техники).

Имран обладает шестнадцатилетним опытом работы в государственном и финансовом секторе. Он работал на крупномасштабных IT-проектах в государственном секторе, а затем перешел в сегмент финансовых услуг. С тех пор он занимал различные технические должности в нескольких крупных финансовых компаниях в Лондоне – финансовой столице Европы. В настоящее время он работает в Лондонском инвестиционном банке в должности вице-президента технологического отдела.

Я хотел бы поблагодарить талантливую команду издательства Packt, в частности Бена Реноу-Кларка, Сюзанну Коутиньо, Алекса Соррентино, Гэри Швартца и Бхагъяшри Рай, которые помогли мне в этом проекте своими своевременными подсказками и ценными замечаниями. Также я исключительно благодарен рецензенту Пранаву Бурнвалу, чьи конструктивные и очень полезные отзывы невероятно помогли мне усовершенствовать материал этой книги.

Благодарю жену и детей, которые позволили мне ночами (и даже в выходные) работать над этой книгой.

Особенно я благодарен родителям, благословения которых позволили мне достичь всего, что только возможно.

О рецензенте

Пранав Бурнвал ранее трудился в сфере НИОКР, а в последние несколько лет занимался ультрасовременными технологиями. Вот их неполный список: блокчейн, большие данные, аналитика (логи и данные), облачные технологии, очереди сообщений, NoSQL, веб-серверы и т. д. Он работал в различных отраслях, среди прочего – в банковском деле, финансах и страховании (БФС), здравоохранении, сфере товаров широкого потребления и в автомобилестроении.

Пранав активно участвует в работе нескольких сообществ. Он является региональным руководителем образовательной сети блокчейна (BEN), это офи-

циально зарегистрированная неправительственная организация, сеть специалистов по блокчейну. Также он организовал множество митапов и индийский «стартап-уикенд».

Пранав активно преподает материалы на тему блокчейна (уже три года), его целевая аудитория варьируется от младших разработчиков до старших вице-президентов. Такая работа также помогает ему осознать, как люди понимают новые и сложные технологии; этот опыт помог ему обработать данную книгу так, чтобы она получилась максимально интересной читателям.

Предисловие

Данная книга написана с единственной целью – познакомить вас с теоретическими и практическими аспектами технологии блокчейн. В книге содержится весь необходимый материал, который позволит вам стать экспертом по блокчейну. Со времени выхода первого издания этой книги технология значительно изменилась, многие аспекты блокчейна усовершенствовались. Именно поэтому возникла необходимость обновить книгу.

Внедрение технологии блокчейн сулит многочисленные выгоды – вот почему к блокчейну пробудился такой неподдельный интерес, охвативший различные сферы, от академической до промышленной. Во всех этих сферах сейчас неустанно исследуют блокчейн. В результате возникло множество консорциумов, рабочих групп, проектов и профессиональных организаций, занятых разработкой и дальнейшим совершенствованием этой технологии. Во втором издании данной книги углубленно рассмотрены следующие темы: что такое децентрализация, умные контракты, что из себя представляют различные блокчейновые платформы, в частности Ethereum, Bitcoin и Hyperledger Fabric. Изучив эту книгу, читатель будет детально понимать внутреннее устройство блокчейна и сможет сам разрабатывать блокчейновые приложения.

В книге рассмотрены все важные темы, касающиеся технологии блокчейн, в том числе криптография, криптовалюты, Bitcoin, Ethereum, а также различные другие платформы и инструменты, связанные с разработкой блокчейна. Ожидается, что читатель обладает базовым пониманием информатики и минимальным опытом программирования – в таком случае он сможет извлечь из этой книги максимальную пользу. Однако и без такого опыта книга читается легко, поскольку важный контекстный материал приводится везде, где это необходимо.

Для кого эта книга

Книга предназначена для всех, кто хочет подробно разобраться в блокчейне. Также она пригодится в качестве справочника тем программистам, которые занимаются разработкой блокчейновых приложений. Кроме того, она может использоваться в качестве учебника на курсе по криптовалютам и блокчейновым технологиям.

Структура книги

Глава 1 «*Блокчейн. Курс молодого бойца*» знакомит вас с фундаментальными концепциями распределенных вычислений, на которых базируется блокчейновая технология. Здесь также рассмотрены история, определения, характер-

ные черты, типы и достоинства блокчейна, плюс различные механизмы консенсуса, образующие ядро блокчейновой технологии.

Глава 2 «*Децентрализация*» рассматривает концепцию децентрализации и ее связь с блокчейновой технологией. Для децентрализации процесса подойдут различные методы и платформы, и с ними вы также познакомитесь в этой главе.

Глава 3 «*Симметричное шифрование*» знакомит вас с теоретическими основами симметричной криптографии. Этот материал необходим, чтобы разобраться, как реализованы различные службы обеспечения безопасности, гарантирующие, в частности, конфиденциальность и целостность данных.

Глава 4 «*Шифрование с открытым ключом*». Здесь разобраны такие концепции, как открытые и закрытые ключи, цифровые подписи и хеш-функции, приведены практические примеры. Кроме того, дается вводная информация о финансовых рынках, так как технология блокчейна находит множество интересных вариантов применения в финансовом секторе.

Глава 5 «*Знакомство с биткойном*» посвящена валюте биткойн – первой и крупнейшей реализации блокчейна. Здесь подробно описаны технические концепции, связанные с криптовалютой биткойн.

Глава 6 «*Сеть и платежи Bitcoin*» рассматривает сеть Bitcoin, соответствующие протоколы и различные кошельки. Более того, здесь дается вводная информация о сложных протоколах, торговых операциях и платежах с применением биткойна.

Глава 7 «*Клиенты и API Bitcoin*» рассказывает о различных биткойн-клиентах и интерфейсах программирования приложений (API), при помощи которых можно создавать приложения для работы с биткойном.

Глава 8 «*Альтернативные криптовалюты*» рассказывает об альтернативных криптовалютах, появившихся после изобретения биткойна. Также здесь приведены примеры различных альтернативных валют, описаны их свойства, рассказано, как их разрабатывали и внедряли.

Глава 9 «*Смарт-контракты*». Здесь подробно обсуждается тема умных контрактов. Затронута их история, дается определение, а также рассмотрены такие темы, как рикардийские контракты, ораклы и теоретические аспекты умных контрактов.

Глава 10 «*Знакомство с Ethereum*». Здесь вы подробно познакомитесь с дизайном и архитектурой блокчейновой валюты Ethereum. В главе рассмотрены различные технические концепции, связанные с блокчейном Ethereum, подробно объясняются базовые принципы, возможности и компоненты этой платформы.

Глава 11 «*Ethereum. Продолжение*». Здесь продолжается рассказ об Ethereum, начатый в предыдущей главе. Рассматриваются темы, связанные с виртуальной машиной Ethereum, майнингом и поддержкой протоколов Ethereum.

Глава 12 «*Среда разработки Ethereum*» охватывает темы, связанные с настройкой частных сетей для разработки и программирования умных контрактов Ethereum.

Глава 13 «*Инструменты разработки и фреймворки*». Это подробное практическое введение в язык программирования Solidity и знакомство с различными важными инструментами и фреймворками, используемыми для разработки Ethereum.

Глава 14 «*Введение в Web3*» описывает разработку децентрализованных приложений и умных контрактов при помощи блокчейна Ethereum. Дается подробное введение в API Web3, а также множество практичных примеров и готовый проект.

Глава 15 «*Hyperledger*», где обсуждается проект Hyperledger от Linux Foundation. Hyperledger объединяет различные блокчейновые проекты, предложенные участниками фонда.

Глава 16 «*Альтернативные блокчейны*» знакомит вас с альтернативными блокчейновыми решениями и платформами. В ней описываются технические детали и возможности альтернативных блокчейнов и соответствующих платформ.

Глава 17 «*Блокчейн – вне сферы валют*» практично и подробно рассказывает о возможностях применения блокчейновых технологий вне контекста криптовалют, в частности с интернетом вещей, в государственных программах, СМИ и финансах.

Глава 18 «*Масштабируемость и другие вызовы*» посвящена обсуждению серьезных проблем, с которыми сталкивается блокчейновая технология, и способам их решения.

Глава 19 «*Текущая и дальнейшая перспективы*» рассказывает о сложившемся технологическом ландшафте, проектах и исследовательских разработках, связанных с блокчейновой технологией. Также здесь делаются некоторые прогнозы на основе современного состояния блокчейновых технологий.

Как выжать из этой книги максимум

- Все примеры в этой книге разрабатывались на Ubuntu 16.04.1 LTS (Xenial) и macOS версии 10.13.2. Поэтому рекомендуется работать с Ubuntu или другой Unix-подобной системой. Однако вам подойдет и любая другая современная операционная система, например Windows или Linux, но примеры, особенно связанные с установкой, возможно, потребуется соответствующим образом адаптировать.
- Примеры, касающиеся криптографии, разрабатывались при помощи инструмента командной строки OpenSSL 1.0.2g 1 Mar 2016.
- Примеры с Ethereum Solidity разрабатывались в IDE Remix, доступной в интернете по адресу remix.ethereum.org.
- Для разработки примеров, связанных с Ethereum, использовался релиз Ethereum Byzantine. На момент написания книги это была новейшая доступная версия, скачать ее можно по адресу www.ethereum.org.
- Примеры, связанные с интернетом вещей, разрабатывались при помощи комплектации Raspberry Pi от Vilros, однако можно воспользоваться и лю-

бой другой подходящей моделью или комплектацией. В частности, при подготовке аппаратных примеров для интернета вещей использовалась модель Raspberry Pi 3 B V 1.2. Для скачивания соответствующих пакетов и запуска сервера Node.js для примеров с интернетом вещей использовались Node.js V8.9.3 и npm V5.5.1.

- В некоторых примерах развертывания умных контрактов использовался фреймворк Truffle, доступный по адресу truffleframework.com. Также должна подойти любая более новая версия, доступная через npm.

Скачивание файлов с примерами кода

Примеры кода к этой книге можно скачать следующим образом.

1. Откройте в браузере страницу по адресу github.com/PacktPublishing/Mastering-Blockchain-Second-Edition.
2. Нажмите кнопку **Clone or Download**.
3. Выберите пункт **Download ZIP**.

Когда файл скачается, разархивируйте его и извлеките папку при помощи последней версии программы:

- WinRAR/7-Zip для Windows;
- Zipeg/iZip/UnRarX для macOS;
- 7-Zip/PeaZip для Linux.

Скачивание цветных изображений

Также мы предоставляем PDF-файл с цветными вариантами скриншотов и схем из этой книги. Его можно скачать по адресу www.packtpub.com/sites/default/files/downloads/MasteringBlockchainSecondEdition_ColorImages.pdf.

Условные обозначения

В тексте книги используется ряд условных обозначений:

`Моноширинным` шрифтом обозначается код, встречающийся в тексте, и названия таблиц из баз данных.

Курсивом обозначены имена каталогов и файлов, расширения файлов и имена путей.

Пример: «После выполнения команды `create` создается файл *privatekey.pem*, в котором содержится следующий сгенерированный закрытый ключ».

Листинг с кодом оформляется так:

```
pragma solidity ^0.4.0;
contract TestStruct {
  struct Trade
  {
    uint tradeid;
    uint quantity;
```

```
    uint price;
    string trader;
  }
// Эту структуру можно инициализировать и использовать, как показано ниже
  Trade tStruct = Trade({tradeid:123, quantity:1, price:1, trader:"equinox"});
}
```

Когда мы хотим обратить ваше внимание на конкретную часть листинга, эта часть выделяется **полужирным** шрифтом:

```
pragma solidity ^0.4.0;
contract TestStruct {
  struct Trade
  {
    uint tradeid;
    uint quantity;
    uint price;
    string trader;
  }
// Эту структуру можно инициализировать и использовать, как показано ниже
  Trade tStruct = Trade({tradeid:123, quantity:1, price:1, trader:"equinox"});
}
```

Любой ввод или вывод в оболочке командной строки записывается вот так:

```
$ sudo apt-get install solc
```

Полужирный шрифт: новые термины, важные слова или слова, которые вы видите на экране, URL-адреса, пользовательский ввод и имена пользователей в Twitter. Например, таким шрифтом записываются слова, встречающиеся в меню или диалоговых окнах. Пример: «Введите пароль и нажмите кнопку **Send Transaction** (**Отправить транзакцию**), чтобы развернуть контракт».

Так обозначаются предупреждения или важные замечания.

Так обозначаются советы и подсказки.

Отзывы и пожелания

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв прямо на нашем сайте www.dmkpress.com, зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу dmkpress@gmail.com, при этом напишите название книги в теме письма.

Если есть тема, в которой вы квалифицированы, и вы заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу http://dmkpress.com/authors/publish_book/ или напишите в издательство по адресу dmkpress@gmail.com.

Список опечаток

Хотя мы приняли все возможные меры, для того чтобы удостовериться в качестве наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг — возможно, ошибку в тексте или в коде, — мы будем очень благодарны, если вы сообщите нам о ней. Сделав это, вы избавите других читателей от расстройств и поможете нам улучшить последующие версии данной книги.

Если вы найдете какие-либо ошибки в коде, пожалуйста, сообщите о них главному редактору по адресу dmkpress@gmail.com, и мы исправим это в следующих тиражах.

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательства «ДМК Пресс» и Packt очень серьезно относятся к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконно выполненной копией любой нашей книги, пожалуйста, сообщите нам адрес копии или веб-сайта, чтобы мы могли принять меры.

Пожалуйста, свяжитесь с нами по адресу электронной почты dmkpress@gmail.com со ссылкой на подозрительные материалы.

Мы высоко ценим любую помощь по защите наших авторов, помогающую нам предоставлять вам качественные материалы.

Глава 1

Блокчейн. Курс молодого бойца

Если вы читаете эту книгу, то весьма вероятно, что вы уже слышали о блокчейне и имеете общее представление о его колоссальном потенциале. Если нет – позвольте сообщить вам, что эта технология, как ожидается, должна положительно повлиять практически на все промышленные отрасли, в частности (но не ограничиваясь): IT, финансы, госпрограммы, СМИ, медицина и право.

Эта глава – введение в технологию блокчейн, рассказ о ее технических основах, теории и различных техниках, которые были интегрированы в единое целое и породили то, что сегодня именуется блокчейном.

В этой главе будут описаны теоретические основы распределенных систем. Далее мы поговорим о предтечах биткойна, вместе с которыми возникла сама идея блокчейна. Наконец, вы познакомитесь с технологией блокчейн. Именно в таком порядке наиболее логично объяснять технологию блокчейн, поскольку корнями она уходит в распределенные системы. Здесь мы вкратце рассмотрим большой объем базовой информации, но не волнуйтесь – далее в книге мы вернемся к большинству этих тем и обсудим их гораздо подробнее.

Развитие технологии блокчейн

После того как в 2008 году был изобретен биткойн, в мире возник новый феномен, который сегодня, вероятно, может совершить революцию во всем обществе. Считается, что он должен повлиять на все промышленные отрасли, в частности финансовый сектор, госслужбу, СМИ, право и искусство. Некоторые сравнивают блокчейн с революцией, но есть и другая трактовка, в которой блокчейну обещают эволюционное развитие и полагают, что первую практическую пользу блокчейн принесет еще через много лет. Вторая точка зрения в некоторой мере верна, но я думаю, что блокчейновая революция уже началась.

Многие авторитетные организации во всем мире создают рабочие модели (proof of concept) с использованием блокчейна, поскольку преобразующий потенциал этой технологии уже оценен по достоинству. Пока многие организа-

ции остаются на этапе предварительных исследований, хотя, по мере дозревания технологии, их исследования должны ускориться. Речь о технологии, также влияющей на другие современные технологии и способной изменить их до основания.

Если обратить внимание на то, что происходило в последние годы, то можно заметить, что стали возникать идеи о возможности применения блокчейна не только с криптовалютами, но и в других сферах. На тот момент блокчейн использовался прежде всего именно с криптовалютами, тогда возникло множество новых «монет». На рис. 1.1 в общем виде показано (в проекции на годы), как развивалась и усваивалась технология блокчейн. Годы, откладываемые по оси *x*, позволяют судить, на какой период приходится конкретный этап развития блокчейна. У каждого этапа есть название (характеризующее этап), откладываемое по оси *x*, начиная от «**ИДЕИ И МЫСЛИ**» и заканчивая «**ЗРЕЛОСТЬ И ДАЛЬНЕЙШАЯ СТАНДАРТИЗАЦИЯ**». По оси *y* откладывается уровень действия, вовлеченности и активность принятия блокчейновой технологии. Согласно графику, примерно **в 2025 году** блокчейновая технология вполне созреет и приобретет многочисленных пользователей.

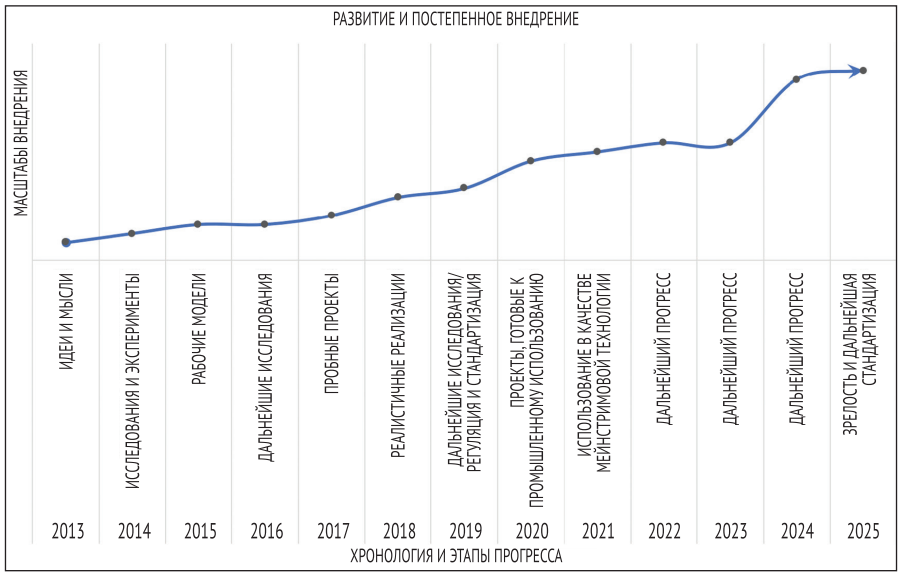

Рис. 1.1 ❖ Хронология созревания и внедрения блокчейновых технологий

Как показано на этом графике, в 2013 году возникли **ИДЕИ И МЫСЛИ** относительно применения блокчейновых технологий за пределами криптовалют. Затем в 2014 году начались первые **ИССЛЕДОВАНИЯ И ЭКСПЕРИМЕНТЫ**, в результате которых появились **РАБОЧИЕ МОДЕЛИ**, пошли **ДАЛЬНЕЙШИЕ ИССЛЕДОВАНИЯ**, и в период с 2015 по 2017 год были запущены полномас-

штабные **ПРОБНЫЕ ПРОЕКТЫ**. В 2018 году мы видим **РЕАЛИСТИЧНЫЕ РЕАЛИЗАЦИИ**. Уже разрабатывается множество проектов, призванных заменить существующие системы. Например, **Австралийская биржа ценных бумаг (ASX)** вскоре станет первой организацией, которая заменит унаследованную систему клиринга и систему взаиморасчетов блокчейновыми технологиями.

Подробнее об этом см. по адресу www.asx.com.au/services/chess-replacement.htm.

Ожидается, что в 2019 году исследования блокчейна продолжатся, а также возникнет интерес к регуляции и стандартизации этой технологии. После этого с 2020 года появятся реалистичные проекты и готовые продукты, в которых используются блокчейновые технологии, а к 2021 году ожидается, что эти технологии станут мейнстримом. Прогресс блокчейновых технологий вполне сравним с *бумом доткомов* конца 1990-х. Предполагается, что наряду с дальнейшим дозреванием и внедрением блокчейновых технологий продолжится их исследование. Наконец, предположительно к 2025 году технология станет вполне состоявшейся, чтобы использоваться в повседневной практике. Отмечу, что хронология, показанная на графике, не очень строга и в будущем может варьироваться, так как очень сложно спрогнозировать, когда именно блокчейн дозреет как технология. График экстраполирован на основе информации об исследованиях, выполненных в последние годы, а также на сложившейся конъюнктуре, связанной с работами, интересом и энтузиазмом, сопутствующими этой технологии. Исходя из таких данных, можно полагать, что к 2025 году технология блокчейн станет достаточно зрелой.

За последние годы интерес к блокчейновым технологиям очень заметно вырос. Ранее от них отмахивались как от каких-то гиковских денег (в контексте криптовалют) либо как от причуды, которая просто не стоит внимания. Сегодня исследованиями блокчейна занимаются крупнейшие организации во всем мире. Миллионы долларов затрачиваются на разработку экспериментов с применением этой технологии. Взять хотя бы недавние меры Европейского союза, объявившего о намерении к 2020 году потратить на исследования блокчейна почти 340 млн евро.

Подробнее об этом можно почитать здесь: www.irishtimes.com/business/technology/boost-for-blockchain-research-as-eu-increases-funding-four-fold-1.3383340.

Согласно другому отчету, глобальные инвестиции в исследования блокчейна могут достичь 9,2 млрд долларов к 2021 году.

Подробнее см. bitcoinmagazine.com/articles/report-suggests-global-spending-blockchain-tech-could-reach-92-billion-2021/.

Существуют различные консорциумы, например **Enterprise Ethereum Alliance** (**EEA**), **Hyperledger** и **R3**, созданные для исследования и разработки блокчейновых технологий. Более того, уже существует множество стартапов, пред-

лагающих решения на основе блокчейна. Простой запрос в приложении Google Тренды демонстрирует колоссальный интерес к блокчейновым технологиям за последние несколько лет. Популярность поискового запроса «blockchain» особенно возросла с начала 2017 года, что видно на рис. 1.2.

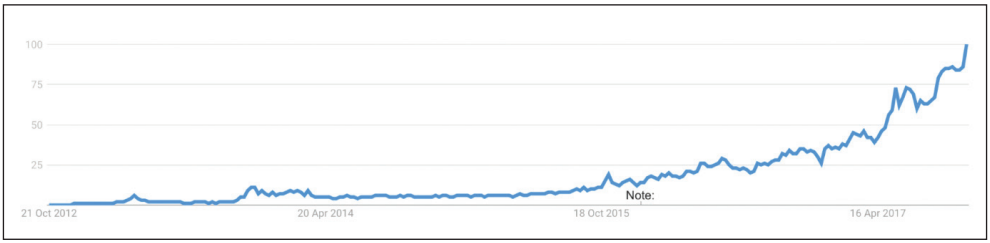

Рис. 1.2 ❖ Интерес к блокчейну по данным Google Тренды

Предполагается, что эта технология принесет различные блага, в частности децентрализованное доверие, сбережения, прозрачность и эффективность. Однако в сфере, где ведутся активные исследования блокчейна, по-прежнему сохраняется множество вызовов, связанных, в частности, с масштабированием и приватностью.

В этой книге будет рассказано, как блокчейновая технология помогает воплотить вышеупомянутые блага. Вы узнаете, что именно представляют собой блокчейновые технологии, как они помогают переформатировать бизнес, различные промышленные отрасли и даже повседневную жизнь благодаря таким многочисленным достоинствам, как эффективность, возможность сбережений, прозрачность и безопасность. Мы исследуем, что такое технология распределенных реестров, децентрализация и умные контракты, какие технологические решения можно разработать и внедрить при помощи ведущих блокчейновых платформ, таких как Ethereum и Hyperledger. Также мы обсудим, с какими вызовами предстоит справиться, прежде чем блокчейн сможет превратиться в мейнстримовую технологию.

В главе 18 рассказывается о границах возможностей блокчейна и вызовах, которые с ним связаны.

Распределенные системы

Чтобы понять технологию блокчейна, совершенно необходимо разбираться в сути распределенных систем, поскольку блокчейн – это, по существу, распределенная система. Это распределенный реестр, который можно централизовать и децентрализовать. Исходно блокчейн предполагалось использовать как децентрализованную платформу. Можно считать его системой, сочетающей признаки децентрализованных и распределенных парадигм. Это распределенно-децентрализованная система.

Распределенные системы соответствуют такой вычислительной парадигме, где два или более узлов скоординированно взаимодействуют друг с другом для достижения совместного результата. Система моделируется таким образом, что пользователи воспринимают ее как единую логическую платформу. Например, поисковик Google работает на основе большой распределенной системы, но для пользователя она выглядит единой согласованной платформой.

Узел можно охарактеризовать как отдельного игрока в распределенной системе. Все узлы могут отправлять и принимать сообщения, обмениваясь ими друг с другом. Узлы могут быть исправными, неисправными или вредоносными, каждый из них обладает памятью и процессором. Узел, действующий алогично, также именуется **византийским**, по так называемой «задаче византийских генералов».

Задача византийских генералов

В 1982 году Лэмпорт и др. предложили одноименный мысленный эксперимент в своей исследовательской статье «Задача византийских генералов», доступной по адресу www.microsoft.com/en-us/research/publication/byzantine-generals-problem/. Согласно эксперименту, каждый из нескольких генералов ведет свой легион византийской армии и планирует, защищать ли город либо отступить из него. Генералы могут общаться только через ординарцев. Чтобы победить, генералы должны договориться об одновременной атаке. Проблема в том, что среди генералов может оказаться один или несколько предателей, которые могут отправить обманное сообщение. Следовательно, в данном случае требуется надежный механизм связи между генералами, который бы позволил войскам, верным присяге, все равно атаковать одновременно, даже если среди генералов есть предатели. В случае распределенных систем на месте верных генералов могут быть обычные узлы, на месте предателей – вредоносные узлы, а на месте ординарца – канал связи между генералами.

В 1999 году эту задачу решили Кастро и Лисков, предложившие алгоритм **«практический подход к византийской отказоустойчивости»** (**PBFT**), где консенсус достигается после обмена некоторым количеством сообщений, содержащих одну и ту же подписанную информацию.

Подобные несогласованные действия византийских узлов могут происходить по вине злоумышленника, пагубно влияя на всю сеть. Любое незапланированное поведение узла в сети, в том числе вредоносное, может считаться византийским.

Миниатюрная модель распределенной системы показана на рис. 1.3. В ней шесть узлов, один из которых (**N4**) является византийским и может вызывать несогласованность данных. **L2** – это поврежденный или просто медленный канал, из-за которого сеть может фрагментироваться.

Основная проблема при проектировании распределенных систем заключается в координации между узлами и отказоустойчивости. Даже если некоторые из узлов отказывают либо нарушается работа сетевых каналов, распределенная система должна с этим справляться и продолжать работать для достижения нужного результата. Много лет этот аспект проектирования распределенных систем активно исследуется, для преодоления таких проблем предложено несколько алгоритмов и механизмов.

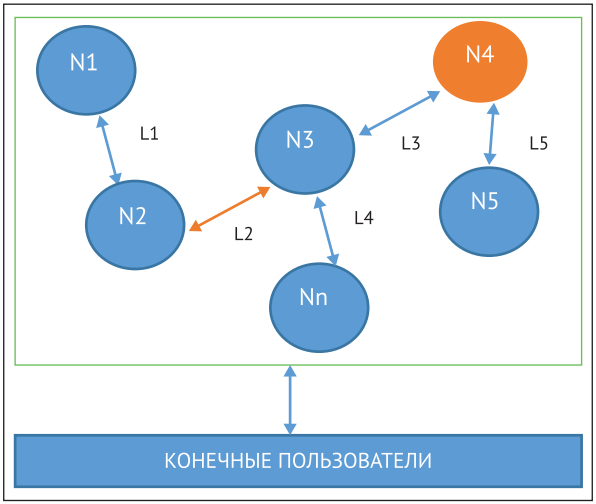

Рис. 1.3 ❖ Схема распределенной системы:
N4 – это византийский узел, L2 – поврежденный или медленный канал в сети

Проектировать распределенные системы настолько сложно, что была доказана гипотеза под названием «**теорема CAP**», согласно которой ни одна распределенная система не может одновременно обладать тремя важнейшими свойствами, а именно: согласованностью данных, доступностью и устойчивостью к разделению. Мы подробно обсудим теорему CAP ниже в этой главе.

История блокчейна и валюты биткойн

Блокчейн возник с изобретением биткойна в 2008 году. Его первая практическая реализация появилась в 2009 году. В рамках этой главы достаточно очень кратко рассмотреть биткойн, так как мы гораздо подробнее поговорим о нем в главе 5. Однако ссылаться на биткойн необходимо, поскольку без него история блокчейна получилась бы неполной.

Электронные деньги

Концепция электронных денег, или цифровой валюты, не нова. С 1980-х существовали протоколы электронных денег, основанные на модели, предложенной Дэвидом Чаумом (David Chaum).

Для понимания технологии блокчейна важно разобраться не только в сути распределенных систем, но и в идее электронных денег; ведь именно в этом сегменте возник биткойн, первая ошеломительно успешная реализация блокчейна, а вслед за биткойном появились и другие криптовалюты.

При работе с электронными деньгами необходимо решить две фундаментальные проблемы: обеспечить анонимность и учет средств.

Учет средств (accountability) нужен для того, чтобы гарантировать, что любая сумма может быть потрачена только один раз (проблема двойного расходования) и только владельцем этих средств. Проблема двойного расходования возникает, когда одни и те же деньги могут быть потрачены дважды. Поскольку копировать цифровые данные очень легко, это крупная проблема, касающаяся цифровых валют (можно накопировать себе сколько угодно цифровых денег).

Анонимность нужна для защиты приватности клиента. Как и в случае с обычной валютой, практически невозможно отследить, кто именно потратил цифровые деньги.

Дэвид Чаум исследовал эти проблемы в 1980-е и смог обеспечить как учет средств, так и анонимность, воспользовавшись двумя криптографическими операциями, а именно **слепой подписью** и **разделением секрета**. Эти термины и смежные концепции будут подробно рассмотрены в главах 3 и 4. Пока достаточно сказать, что слепая подпись позволяет завизировать документ, не видя его, а разделение секрета – это феномен, позволяющий отследить двойное расходование, то есть повторное использование уже зафиксированного токена электронной валюты.

В 2009 году появилась первая практическая реализация системы электронных денег (e-cash) под названием биткойн. Термин «криптовалюта» появился позже. Эта система впервые позволила решить проблему распределенного консенсуса в недоверенной сети.

В ней использовались **криптография с открытым ключом** и механизм доказательства выполнимости (PoW), обеспечивавшие безопасный, контролируемый и децентрализованный метод чеканки цифровой валюты. Ключевая инновация заключалась в идее упорядоченного списка блоков, состоящих из транзакций и криптографически защищенных при помощи PoW-механизма. Эта концепция будет подробно разобрана в главе 5.

Среди других технологий, которые используются в биткойне, но существовали до него, – деревья Меркла, хеш-функции и хеш-цепочки. Все эти концепции достаточно подробно объяснены в главе 4.

Рассматривая все вышеупомянутые технологии и их историю, легко заметить, как разные концепции – от схем электронных денег до распределенных систем – были скомбинированы для создания биткойна и феномена, ныне известного под названием «блокчейн». Всю структуру можно представить в виде схемы на рис. 1.4.

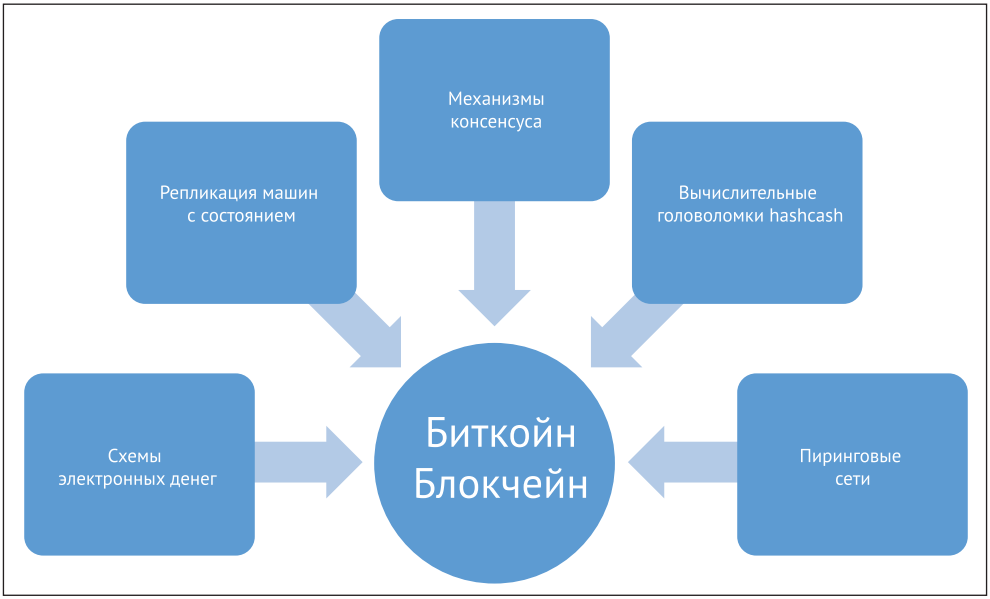

Рис. 1.4 ❖ Различные идеи, на основе которых возникли биткойн и блокчейн

Блокчейн

В 2008 году вышла эпохальная статья под названием «*Биткойн. Децентрализованная электронная денежная система*» на тему пиринговой электронной валюты, написанная под псевдонимом Сатоши Накамото (Satoshi Nakamoto). Именно в ней появился термин «цепочка блоков». Никому не известно, кто именно скрывается под именем Сатоши Накамото. После появления биткойна он оставался активным разработчиком этой системы до 2011 года. Затем он передал развитие биткойна основной команде разработчиков и попросту исчез. С тех пор от него не было никаких вестей, его личность и сам факт его существования покрыты завесой тайны. Термин «*цепочка блоков*» с годами изменился, и теперь этот феномен называется «*блокчейн*».

Как говорилось выше, у технологии блокчейн масса прикладных вариантов, которые могут быть реализованы в различных сегментах экономики. Так, считается, что достигнутое в финансовом секторе значительное усовершенствование транзакций и расчетов позволило как следует ускорить эти процессы и сократить издержки на них.

Эти аспекты блокчейна будут дополнительно объяснены в главе 17, где мы подробно рассматриваем практические возможности использования блокчейна в различных отраслях. Пока достаточно сказать, что в отдельных сегментах практически всех промышленных отраслей уже оценены (или вскоре будут оценены) потенциал и многообещающие перспективы блокчейна, после чего придет время зарабатывать на этой технологии.

Определение блокчейна

Упрощенное: блокчейн – это непрерывно растущая, безопасная, разделяемая система учета записей, где у каждого пользователя данных есть такая копия этих данных, обновить которую можно лишь при условии, что на это согласятся все стороны, участвующие в транзакции.
Техническое: блокчейн – это пиринговый криптографически защищенный распределенный, (практически) неизменяемый реестр, поддерживающий только добавление блоков, обновляемый лишь в результате соглашения (договоренности) между всеми участниками.

Теперь давайте подробнее разберем вышеизложенные определения. По очереди рассмотрим все упомянутые в них ключевые слова.

Пиринговый
Первый термин в техническом описании – «пиринговый». Он означает, что в сети нет центрального контрольного органа и все участники напрямую коммуницируют друг с другом. Благодаря такому свойству денежные транзакции могут происходить между участниками сети без вмешательства каких-либо посредников, например банка.

Распределенный реестр
Далее в техническом определении выясняем, что блокчейн – это *распределенный реестр*, то есть реестр, рассредоточенный по сети между всеми ее участниками, причем у каждого участника есть исчерпывающая копия всего реестра.

Криптографически безопасный
Далее отмечаем, что реестр является *криптографически безопасным* – то есть безопасность в реестре обеспечивается при помощи криптографии, и благодаря криптографии реестр защищен от подделки и злоупотреблений. К сервисам безопасности относятся неотказуемость, целостность данных и аутентификация источника данных. О реализации этих механизмов рассказано в главе 3, где вы познакомитесь с увлекательным миром криптографии.

Только добавление
Еще одно характерное свойство блокчейна заключается в том, что блоки в цепочку можно *только добавлять* в *хронологически последовательном порядке*. Это свойство подразумевает, что как только данные добавлены к блокчейну, эти данные почти невозможно скорректировать, поэтому они могут считаться практически неизменяемыми. Тем не менее изменить данные можно в ситуациях, когда в блокчейновой сети удается устроить коллизию и завладеть более чем 51% ее мощностей. Могут существовать вполне обоснованные причины, по которым потребуется изменить данные, попавшие в блокчейновую сеть, – например, *право на забвение* или *право на стирание* (также прописанное в Общем регламенте по защите данных (GDPR) https://gdpr-info.eu/art-17-gdpr/).

Однако это частные случаи, которые должны рассматриваться отдельно и которые требуют изящного технического решения. В обычной практике блокчейн действительно неизменяем.

Обновляемый по соглашению

Наконец, наиболее принципиальным атрибутом блокчейна является *возможность обновления* цепочки лишь по общему согласию. В этом и заключается мощь децентрализации. В таком сценарии отсутствует какой-либо центральный орган, который отвечал бы за обновление реестра. Напротив, любое обновление блокчейна проверяется на соответствие строгим критериям, определенным в блокчейновом протоколе, и осуществляется только по достижении общего консенсуса между всеми релевантными участниками/узлами в сети. Достижение консенсуса упрощается благодаря множеству различных алгоритмов, специально предназначенных для этой цели, гарантирующих, что всех причастных устраивает итоговое состояние данных в блокчейновой сети и все участники сети решительно соглашаются с тем, что это обновление является верным. Алгоритмы консенсуса рассматриваются ниже в этой главе и далее по книге там, где изложен касающийся их материал.

Блокчейн можно представить в виде распределенной пиринговой сети, наложенной и действующей поверх интернета, как показано на рис. 1.5. Блокчейн аналогичен протоколам SMTP, HTTP или FTP, работающим поверх TCP/IP.

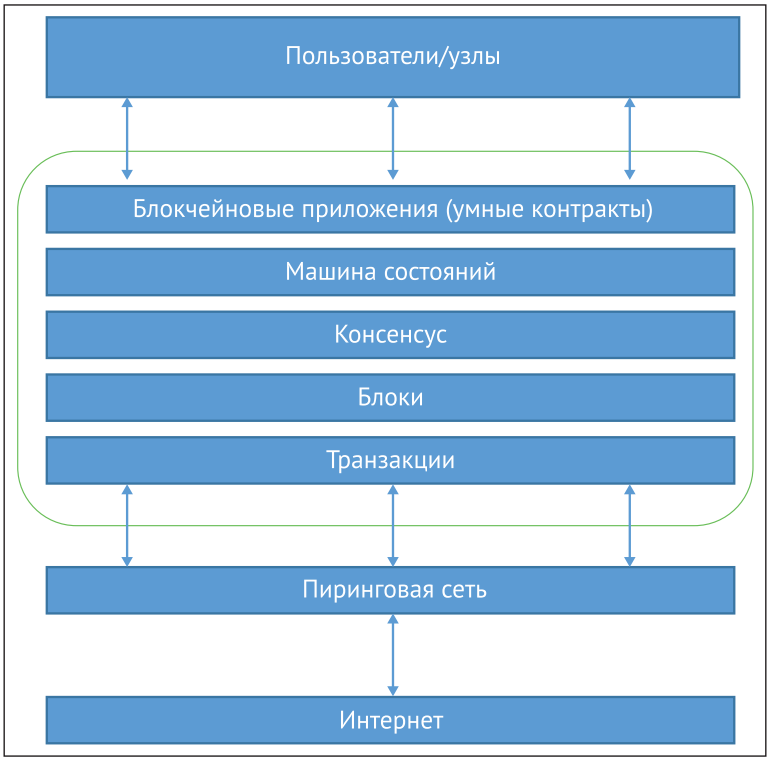

Рис. 1.5 ❖ Блокчейн с сетевой точки зрения

В основании вышеприведенной схемы расположен интернет, служащий базовым уровнем коммуникации в любой сети. В данном случае пиринговая сеть работает поверх интернета, и уже поверх нее располагается еще один уровень – блокчейн. На этом уровне находятся транзакции, блоки, механизмы консенсуса, машины состояний и умные контракты блокчейна. Все эти компоненты показаны как единая логическая сущность в одной рамке, где блокчейн находится поверх пиринговой сети. Наконец, на самом верхнем уровне у нас пользователи или узлы, подключающиеся к блокчейну и выполняющие различные операции, как то: достижение консенсуса, проверка операций и обработка. Эти концепции будут подробно рассмотрены ниже в данной книге.

С точки зрения бизнеса блокчейн можно описать как платформу, участники которой могут обмениваться активами/электронными деньгами при помощи транзакций, не прибегая при этом к участию центрального арбитра. Например, при переводах наличности банк действует в качестве доверенного посредника. В финансовом трейдинге центральная клиринговая организация действует в качестве арбитра между двумя трейдерами. Это амбициозная концепция, и стоит только ее усвоить – и вы поймете весь колоссальный потенциал блокчейновой технологии. Такая дезинтермедиация позволяет блокчейну действовать в качестве децентрализованного механизма, обеспечивающего консенсус, причем здесь нет никакого центрального органа, который бы контролировал базу данных. Здесь сразу видно важное преимущество децентрализации: ведь если можно обойтись без банков и централизованных клиринговых палат, то сразу экономятся издержки, все транзакции ускоряются, и устанавливается доверие.

Блок – это просто подборка логически организованных транзакций, объединенных в пакет. **Транзакция** – это регистрация события, например события пересылки денег со счета отправителя на счет бенефициара. Блок состоит из транзакций, а размер его может варьироваться в зависимости от типа и структуры используемого блокчейна.

Также в блоке содержится ссылка на предыдущий блок, если только речь не о первичном блоке. **Первичный блок** (genesis block) идет первым в блокчейновой цепочке, он жестко запрограммирован в момент создания данной блокчейновой цепочки. Структура блока также зависит от типа и устройства конкретного блокчейна. Однако, как правило, есть всего несколько критичных атрибутов, необходимых для функционирования блока: это заголовок блока, состоящий из указателя на предыдущий блок, временной метки, одноразового номера (нонса), корня дерева Меркла и тела блока (в теле содержатся транзакции). В блоке присутствуют и другие атрибуты, но, как правило, вышеупомянутые компоненты есть в блоке всегда.

Нонс – это случайное число, которое генерируется и используется лишь однажды. Нонсы широко применяются в различных криптографических операциях и обеспечивают защиту от повторного воспроизведения, аутентификацию и шифрование. В блокчейне нонс используется в PoW-алгоритмах консенсуса, а также применяется для защиты транзакций от повторного воспроизведения.

Корень дерева Меркла – это хеш всех узлов, содержащихся в дереве Меркла. Деревья Меркла широко используются для безопасной и эффективной валидации больших структур данных. В мире блокчейна деревья Меркла часто используются для эффективной верификации транзакций. Корень дерева Меркла в блокчейне присутствует в заголовке блока и представляет собой хеш всех транзакций, содержащихся в блоке. Таким образом, достаточно проверить только корень дерева Меркла – и так будут верифицированы все транзакции, содержащиеся в дереве Меркла; проверять каждую транзакцию в отдельности не требуется. Мы подробнее обсудим все эти концепции в главе 4.

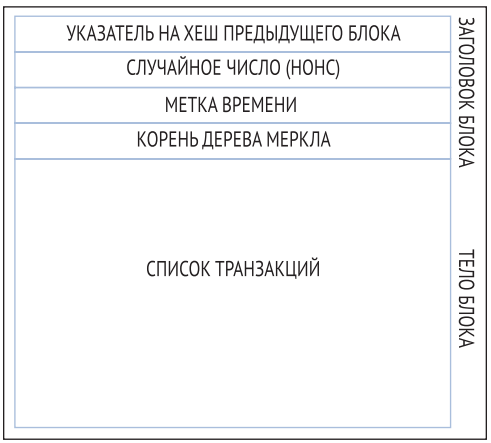

Рис. 1.6 ❖ Структура блока в обобщенном виде

На рис. 1.6 представлена простая схема, изображающая блок. Конкретные структуры блоков, применяемые в тех или иных блокчейновых технологиях, будут рассмотрены в книге далее, со всеми техническими подробностями.

Общие элементы блокчейна

Теперь давайте рассмотрим наиболее общие элементы блокчейна. Этот раздел может послужить вам хорошей шпаргалкой, если когда-нибудь понадобится припомнить, из каких частей состоит блокчейн. Более детально конкретные элементы будут рассмотрены в следующих главах книги, посвященных специфичным блокчейнам, например Ethereum. В обобщенном виде структуру блокчейна можно изобразить так, как показано на рис. 1.7.

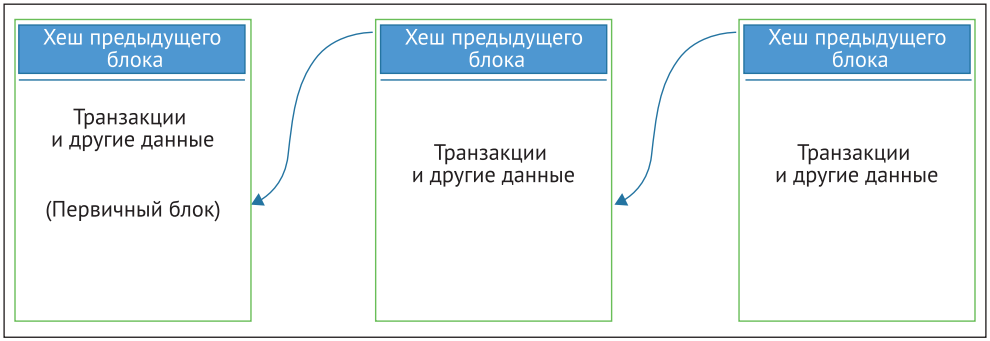

Рис. 1.7 ❖ Структура блокчейна в обобщенном виде

Далее по порядку описаны элементы типичного блокчейна. Вам обязательно придется иметь с ними дело, работая с блокчейном.

- **Адрес**: адреса – это уникальные идентификаторы, применяемые при блокчейновой транзакции для обозначения отправителя и получателя. Как правило, адрес – это открытый ключ, либо он выводится из открытого ключа. Адреса пригодны для многократного использования одним и тем же пользователем, но сами по себе уникальны. Однако на практике один и тот же пользователь может не пользоваться одинаковым адресом помногу раз и генерировать новый для каждой транзакции. Такой новоиспеченный адрес будет уникальным. Фактически биткойн – это псевдонимная система. Обычно не удается напрямую идентифицировать конечных пользователей, но ряд исследований по устранению анонимности пользователей биткойна показал, что их вполне можно обнаружить. Пользователю рекомендуется генерировать новый адрес для каждой транзакции, чтобы разные транзакции не указывали на одного владельца и обнаружить его было нельзя.
- **Транзакция**: транзакция – это фундаментальный элемент блокчейна. Транзакция – это передача актива с одного адреса на другой.
- **Блок**: блок состоит из множества транзакций и других элементов, таких как хеш предыдущего блока (указатель хеша), метка времени и случайное число.
- **Пиринговая сеть**: как понятно из названия, речь идет о такой сетевой топологии, где все участники сети могут общаться друг с другом, отправлять и получать сообщения.
- **Скриптовый язык или язык программирования**: скрипты или программы совершают с транзакцией различные операции для обеспечения тех или иных функций. Например, скрипты биткойн-транзакций пишутся на языке **Script**, состоящем из наборов команд, позволяющих узлам передавать токены с адреса на адрес. Однако возможности языка Script ограничены в том смысле, что на нем можно выразить лишь ключевые

операции, необходимые для совершения транзакций, но он не поддерживает стандартных заранее запрограммированных арифметических операций. В этом смысле скриптовый язык валюты биткойн нельзя назвать *тьюринг-полным*. Проще говоря, тьюринг-полным называется такой язык, на котором можно запрограммировать любое вычисление. Термин напоминает об Алане Тьюринге (Alan Turing), разработавшем идею машины Тьюринга, способной выполнить сколь угодно сложный алгоритм. В тьюринг-полных языках требуются циклы и возможности ветвления, чтобы выполнять сложные вычисления. Таким образом, скриптовый язык биткойна не является тьюринг-полным, а язык Solidity для валюты Ethereum – является.

Чтобы обеспечить разработку любых программ для блокчейна, нужен тьюринг-полный язык программирования, и сегодня такое свойство блокчейнов считается очень желательным. Все равно, что говорить о компьютере, для которого можно написать любую программу на языке программирования. Тем не менее остаются острые вопросы по поводу безопасности таких языков, и в данной сфере ведутся активные исследования. Эти темы будут подробнее рассмотрены в главах 5, 9 и 13.

- **Виртуальная машина**. Это расширение транзакционного скрипта, рассмотренного выше. *Виртуальная машина* позволяет выполнять тьюринг-полный код в блокчейне (в виде умных контрактов), тогда как практические возможности транзакционного скрипта ограничены. Однако не во всех блокчейнах есть свои виртуальные машины. Среди виртуальных машин для запуска таких программ следует упомянуть **Ethereum Virtual Machine** (**EVM**) и **Chain Virtual Machine** (**CVM**). EVM применяется с блокчейном Ethereum, а CVM – это виртуальная машина, разработанная для блокчейна **Chain Core**, используемого на больших предприятиях.
- **Машина состояний**: блокчейн можно считать механизмом изменения состояний, где состояние переходит из одной формы в другую и так до конечной, распространяясь по узлам блокчейновой сети в результате выполнения, проверки и завершения транзакций.
- **Узел**: узел в блокчейновой сети выполняет различные функции в зависимости от принимаемой роли. Узел может предлагать и проверять транзакции, выполнять майнинг для обеспечения консенсуса и защищать блокчейн. Эта цель достигается путем следования **протоколу консенсуса** (чаще всего PoW). Также узлы могут выполнять и другие функции, например простую проверку платежа (легковесные узлы), валидацию и множество других функций в зависимости от типа используемого блокчейна и роли, присвоенной узлу. Еще узлы выполняют подписывание транзакций. Сначала транзакция создается на узле, а затем снабжается цифровой подписью, в которой используются закрытые ключи – как доказательство, что отправитель действительно владеет тем активом, который хочет передать какому-то другому участнику блокчейновой

сети. Таким активом обычно является токен или виртуальная валюта, например биткойн, однако это может быть и совершенно реальный актив, конвертированный в токены в блокчейновой сети.

- **Умный контракт**: это программа, работающая на основе блокчейна и инкапсулирующая бизнес-логику, которая должна выполняться в случае соблюдения тех или иных условий. Эти программы могут выполняться принудительно и автоматически. Работа с умными контрактами доступна не на всех блокчейновых платформах, однако в настоящее время такая возможность становится все более желательной благодаря той силе и гибкости, которую придают блокчейновым приложениям умные контракты. Практика использования умных контрактов очень широка, в частности: управление идентификацией, рынки капиталов, финансовые сделки, делопроизводство, страхование и электронное управление. Умные контракты будут подробнее рассмотрены в главе 9.

Как устроен блокчейн

Итак, мы определили и описали блокчейн. Теперь давайте разберемся, как он работает. Узлы действуют либо в качестве *майнеров*, создающих новые блоки и чеканящих валюту (монеты), либо в качестве *представителей*, проверяющих транзакции и снабжающих их цифровой подписью. Важнейшее решение, которое требуется принимать в любой блокчейновой сети, – определить, какой узел, как правило, будет добавлять следующий блок к цепочке. Это решение принимается в соответствии с *механизмом консенсуса*. Механизм консенсуса подробнее описан ниже в этой главе.

Теперь давайте рассмотрим, как блокчейн валидирует транзакции, создает блоки и добавляет их в цепочку, наращивая ее таким образом.

Как в блокчейне накапливаются блоки

Рассмотрим в общем виде создание блоков. Эта схема описана здесь, чтобы вы могли составить общее впечатление о том, как генерируются блоки и как они соотносятся с транзакциями.

1. Узел начинает транзакцию, создав ее, а затем скрепив цифровой подписью, для которой использует свой закрытый ключ. Транзакция в блокчейне может означать различные действия. Как правило, это структура данных, представляющая передачу активов между пользователями блокчейновой сети. Транзакционная структура данных обычно содержит некоторую логику передачи актива, действующие правила, адрес отправителя и адрес получателя, а также другую проверочную информацию. Эти темы будут подробнее рассмотрены в книге далее, в конкретных главах, посвященных блокчейну и Ethereum.
2. Транзакция распространяется между участниками сети при помощи протокола затопления, именуемого Gossip, и участники проверяют транзакцию на основе предустановленных критериев. Как правило, для проверки транзакции требуется более одного узла.

3. После проверки транзакция включается в блок, который затем распространяется по сети. На данном этапе транзакция считается подтвержденной.
4. Новоиспеченный блок становится частью реестра, и новый блок криптографически подцепляется к этому блоку. Такая связь называется указателем хеша. На данном этапе транзакция получает второе подтверждение, а блок – первое.
5. Затем транзакции перепроверяются всякий раз при создании нового блока. Как правило, в сети биткойн требуется шесть подтверждений, чтобы транзакция считалась завершенной.

Необходимо отметить, что шаги 4 и 5 считаются необязательными, поскольку фактически транзакция завершается после 3-го этапа; однако подтверждение блока и дальнейшие переподтверждения транзакций являются необходимыми и выполняются на этапах 4 и 5.

На этом мы заканчиваем базовое знакомство с блокчейном. В следующем разделе будет рассказано о достоинствах и недостатках этой технологии.

Достоинства и недостатки блокчейна

Во многих отраслях обсуждаются многочисленные преимущества блокчейновой технологии, новые предложения поступают от ведущих интеллектуалов со всего мира, работающих в сфере блокчейн. Наиболее заметные преимущества этой технологии таковы:

- **децентрализация.** Это ключевая концепция и основное достоинство блокчейна. Она не требует участия доверенного третьего лица или посредника, который бы проверял транзакции; вместо этого используется механизм консенсуса, по которому согласовывается правомерность транзакций;
- **прозрачность и доверие**. Поскольку блокчейны являются разделяемыми, и каждому видно, что находится в блокчейне, так обеспечивается прозрачность системы. В результате устанавливается доверие. Этот фактор более важен в таких сценариях, как выплата средств или бенефиций, где необходимо ограничивать личное усмотрение при выборе бенефициаров;
- **неизменяемость**. После того как данные были записаны в блокчейн, отменить такую операцию исключительно сложно. Блокчейновые данные не являются неизменяемыми по природе своей, но подправить их настолько тяжело (почти невозможно), что данное свойство неизменяемого реестра транзакций считается одним из его достоинств;
- **высокая доступность**. Поскольку система основана на тысячах узлов, объединенных в пиринговую сеть, а данные реплицируются и проверяются на каждом узле, система получается высокодоступной. Даже если некоторые узлы выпадут из сети или окажутся недоступными, система сохранит работоспособность и высокую доступность. Все это достигается благодаря избыточности;

- **высокая безопасность**. Все транзакции в блокчейне криптографически защищены, что обеспечивает целостность данных в сети;
- **упрощение существующих парадигм**. Современная блокчейновая модель, применяемая во многих отраслях, например в финансах и здравоохранении, несколько дезорганизована. В такой модели множество организаций ведут собственные базы данных, и обмен данными может очень осложняться по причине разрозненности этих систем. Однако, поскольку блокчейн может служить единым распределенным реестром для множества заинтересованных сторон, данная модель может упроститься, если правильно управлять отдельными системами, которые поддерживает каждая организация;
- **ускорение сделок**. В финансовой индустрии, особенно при обеспечении расчетов после сделки, блокчейн может оказаться жизненно важен как механизм ускорения этих операций. Блокчейн обходится без длительного процесса подтверждения, согласования и клиринга, поскольку сразу доступна конечная версия данных, которая всех устраивает, и эта информация хранится в распределенном реестре, доступном финансовым организациям;
- **экономия**. Поскольку в блокчейновой модели не требуется ни доверенного посредника, ни клиринговой палаты, такая модель позволяет радикально сократить издержки, избавившись от комиссий, обычно выплачиваемых таким посредникам.

Как и с любой технологией, сначала требуется справиться с некоторыми вызовами, чтобы система стала более надежной, полезной и доступной. Блокчейн – не исключение. На самом деле для устранения вызовов блокчейновой технологии ведется огромная работа как на академическом, так и на промышленном поприще. Наиболее острые проблемы блокчейна таковы:

- масштабируемость;
- адаптируемость;
- регуляция;
- относительная незрелость;
- конфиденциальность.

Все эти проблемы и возможные варианты их решения будут подробно рассмотрены в главе 18.

Уровни блокчейновой технологии

В этом разделе описаны различные уровни блокчейновой технологии. Считается, что из-за стремительного развития и прогресса, достигаемого в блокчейне, будет разработано множество его прикладных вариантов. Некоторые из этих прорывов уже воплощены, другие ожидаются в ближайшем будущем, учитывая, какими темпами блокчейн развивается сейчас.

Три уровня, о которых здесь пойдет речь, изначально были описаны в книге Мелани Суон (Melanie Swan) «*Blockchain: Blueprint for a New Economy*», вышедшей в издательстве O'Reilly Media в 2015 году, где разные решения рассортирова-

ны по этим уровням. Именно так развивается блокчейн, и такое версионирование демонстрирует различные уровни эволюции и использования блокчейновых технологий. Фактически все блокчейновые платформы, за немногими исключениями, поддерживают такой функционал и возможности применения. Данное версионирование – просто логическое разграничение различных категорий блокчейна в зависимости от их использования в настоящий момент, их эволюции и ожидаемой эволюции.

Также отметим, что данное версионирование приводится здесь для полноты картины и по историческим причинам, поскольку все эти определения сегодня немного размыты, и, не считая биткойна (блокчейн 1.0), все более новые блокчейновые платформы поддерживают разработку умных контрактов и программирование функций и приложений, относящихся ко всем уровням блокчейна: 1.0, 2.0, 3.0 и выше.

Вдобавок к уровням 1, 2, 3 и X (будущее) я излагаю здесь мои собственные представления о том, к чему может привести развитие блокчейновых технологий.

- **Блокчейн 1.0**: этот уровень возник после изобретения биткойна и используется преимущественно для работы с криптовалютами. Кроме того, поскольку биткойн был первой реализацией криптовалют, целесообразно отнести к первому поколению блокчейна лишь криптографические криптовалюты. Сюда относится биткойн, а также все альтернативные криптовалюты. Основные приложения этой технологии – например, платежи. Первый этап начался в 2009 году с изобретением биткойна, и закончился в начале 2010 года.
- **Блокчейн 2.0**: второе поколение блокчейна нашло применение в сфере финансовых услуг и умных контрактов. На этом уровне находятся различные финансовые активы, в частности деривативы, опционы, свопы и облигации. Здесь находятся приложения, не ограничивающиеся валютами, финансами и рынками. Ethereum, Hyperledger и другие сравнительно новые блокчейновые платформы причислятся к уровню блокчейн 2.0. История этого поколения началась с идей о переориентации блокчейна для других целей, такие идеи зародились в 2010 году.
- **Блокчейн 3.0**. Третье поколение блокчейна связано с реализацией приложений, не относящихся к финансовой индустрии и используемых в государственном управлении, здравоохранении, СМИ, искусстве и юриспруденции. Опять же, как и в случае с блокчейн 2.0, к этому уровню причисляются Ethereum, Hyperledger и более новые блокчейны, для которых можно программировать умные контракты. Это поколение блокчейна возникло около 2012 года, когда активно исследовались многочисленные варианты применения блокчейна в разных индустриях.

Machina Economicus – это феномен из сферы **искусственного интеллекта** (**ИИ**) и вычислительной экономики. Его можно определить как машину, принимающую логичные и идеальные решения. Прежде чем такая мечта сможет воплотиться, придется справиться с разнообразными техническими вызовами.