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;
```