LEARNING MADE EASY

3rd Edition

Blockchain

for dummies®
A Wiley Brand

Peek under the hood of tech changing finance

Learn how Blockchain powers cryptocurrency

Launch your own blockchain apps on stable platforms

Tiana Laurence

Blockchain pioneer and investor

Blockchain

for dummies®
A Wiley Brand

Blockchain

3rd Edition

by Tiana Laurence

for dummies®
A Wiley Brand

Blockchain For Dummies®, 3rd Edition

Published by: **John Wiley & Sons, Inc.,** 111 River Street, Hoboken, NJ 07030-5774, www.wiley.com

Published simultaneously in Canada

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: WHILE THE PUBLISHER AND AUTHORS HAVE USED THEIR BEST EFFORTS IN PREPARING THIS WORK, THEY MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES, WRITTEN SALES MATERIALS OR PROMOTIONAL STATEMENTS FOR THIS WORK. THE FACT THAT AN ORGANIZATION, WEBSITE, OR PRODUCT IS REFERRED TO IN THIS WORK AS A CITATION AND/OR POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE PUBLISHER AND AUTHORS ENDORSE THE INFORMATION OR SERVICES THE ORGANIZATION, WEBSITE, OR PRODUCT MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING PROFESSIONAL SERVICES. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR YOUR SITUATION. YOU SHOULD CONSULT WITH A SPECIALIST WHERE APPROPRIATE. FURTHER, READERS SHOULD BE AWARE THAT WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ. NEITHER THE PUBLISHER NOR AUTHORS SHALL BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

For general information on our other products and services, please contact our Customer Care Department within the U.S. at 877-762-2974, outside the U.S. at 317-572-3993, or fax 317-572-4002. For technical support, please visit https://hub.wiley.com/community/support/dummies.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at http://booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2023931209

ISBN 978-1-394-15966-6 (pbk); ISBN 978-1-394-15967-3 (ebk); ISBN 978-1-394-15968-0 (ebk)

Contents at a Glance

Table of Contents

Introduction

Welcome to *Blockchain For Dummies!* If you want to find out what blockchains are and the basics of how to use them, this is the book for you. Many people think blockchains are difficult to understand. They may also think that blockchains are just about cryptocurrencies like Bitcoin, but they're so much more. Anyone can master the basics of blockchains.

In this book, you find helpful advice for navigating the blockchain world and cryptocurrencies that run them. You also find practical step-by-step tutorials that will build your understanding of how blockchains work and where they add value. You don't need a background in programming, economics, or world affairs to understand this book, but I do touch on all these subjects because blockchain technology intersects all of them.

About This Book

This book explains the basics of blockchains, smart contracts, and cryptocurrencies. You probably picked up this book because you've heard about blockchains and know they're important, but you have no idea what they are, how they work, or why you should care. This book answers all these questions in easy-to-understand terms.

This book is a bit different from just about any other blockchain book on the market. It provides a survey of all the key blockchains in the public market, how they work, what they do, and something useful you can try with them today.

This book also covers the landscape of blockchain technology and points out some of the key things to be aware of for your own blockchain projects. Here, you find out how to install an Ethereum wallet, create and execute a smart contract, make entries into Bitcoin, and earn cryptocurrencies.

You don't have to read the book cover to cover. Just flip to the subject that you're interested in.

Finally, within this book, you may note that some web addresses break across two lines of text. If you're reading this book in print and want to visit one of these web pages, simply key in the web address exactly as it's noted in the text, pretending as though the line break doesn't exist. If you're reading this as an e-book, you've got it easy — just click the web address to be taken directly to the web page.

Foolish Assumptions

I don't make many assumptions about you and your experience with cryptocurrency, programming, and legal matters but I do assume the following:

- You have a computer, a smartphone, and access to the Internet.
- You know the basics of how to use your computer and the Internet.
- You know how to navigate through menus within programs.
- You're new to blockchain and you aren't a skilled programmer. Of course, if you are a skilled programmer, you can still get a lot out of this book — you just may be able to breeze past some of the step-by-step guidelines.

Icons Used in This Book

Throughout this book, I use icons in the margin to draw your attention to certain kinds of information. Here's what the icons mean:

TIP

The Tip icon marks tips and shortcuts that you can use to make blockchains easier to use.

REMEMBER

The Remember icon marks the information that's especially important to know — the stuff you'll want to commit to memory. To siphon off the most important information in each chapter, just skim through these icons.

TECHNICAL STUFF

The Technical Stuff icon marks information of a highly technical nature that you can skip over without missing the main point of the subject at hand.

WARNING

The Warning icon tells you to watch out! It marks important information that may save you headaches — or tokens.

Beyond the Book

In addition to the material in the print or e-book you're reading right now, this product also comes with some access-anywhere goodies on the web. Check out the free Cheat Sheet for more on blockchains. To get this Cheat Sheet, simply go to `www.dummies.com` and type **Blockchain For Dummies Cheat Sheet** in the Search box.

Where to Go from Here

You can apply blockchain technology to virtually every business domain. Right now there is explosive growth in financial, health care, government, insurance industries, and this is just the beginning. The whole world is changing and the possibilities are endless.

1 Getting Started with Blockchain

IN THIS PART . . .

Discover what blockchains are all about and how they can benefit your organization.

Identify the right type of technology and the steps to developing and executing an effective blockchain project.

Make your own smart contracts on Bitcoin, and determine where this technology can fit within your organization.

IN THIS CHAPTER

- Discovering the new world of blockchains
- Understanding why they matter
- Identifying the three types of blockchains
- Deepening your knowledge of how blockchains work

Chapter 1
Introducing Blockchain

Originally, *blockchain* was just the computer science term for how to structure and share data. Today blockchains are hailed the "fifth evolution" of computing. Or more commonly now the backbone of the Web3 movement.

Blockchains are a novel approach to the distributed database. The innovation comes from incorporating old technology in new ways. You can think of blockchains as distributed databases that a group of individuals controls and that store and share information.

There are many different types of blockchains and blockchain applications. Blockchain is an all-encompassing technology that is integrating across platforms and hardware all over the world.

Beginning at the Beginning: What Blockchains Are

A blockchain is a data structure that makes it possible to create a digital ledger of data and share it among a network of independent parties. There are many different types of blockchains.

- **Public blockchains:** Public blockchains, such as Bitcoin, are large distributed networks that are run through a native cryptocurrency. A *cryptocurrency* is a unique bit of data that can be traded between two parties. Public blockchains are open for anyone to participate at any level and usually have open-source code that their community maintains.
- **Permissioned blockchains:** Permissioned blockchains, such as Ripple, control roles that individuals can play within the network. They're still large and distributed systems that use a native token. Their core code may or may not be open source.
- **Private blockchains:** Private blockchains also known as distributed ledger technology (DLT) tend to be smaller and do not utilize a token or cryptocurrency. Their membership is closely controlled. These types of blockchains are favored by consortiums that have trusted members and trade confidential information.

All three types of blockchains use cryptography to allow each participant on any given network to manage the ledger in a secure way without the need for a central authority to enforce the rules. The removal of central authority from the database structure is one of the most important and powerful aspects of blockchains.

All types of blockchains are contributing to what is known as Web3 also referred to as Web 3.0. It is as much a social movement as a new evolution of the World Wide Web. The general idea behind this trend is that individuals are taking ownership of their own data by using tools that decentralization, blockchain technologies, and token-based economics give them. In contrast with Web 2.0, where data and content are controlled by a small group of mega companies such as Apple, Google, and Facebook.

REMEMBER

Blockchains create permanent records and histories of transactions, but nothing is really permanent. The permanence of the record is based on the dependability and health of the network. In the context of blockchains, this means that if a large portion of the blockchain community wanted to change information written to their blockchain, they could. Cryptocurrency is used as a reward to incentivize lots of users to facilitate the healthy function of the network through competition. If the records are changed inappropriately, this is known as a 51 percent attack.

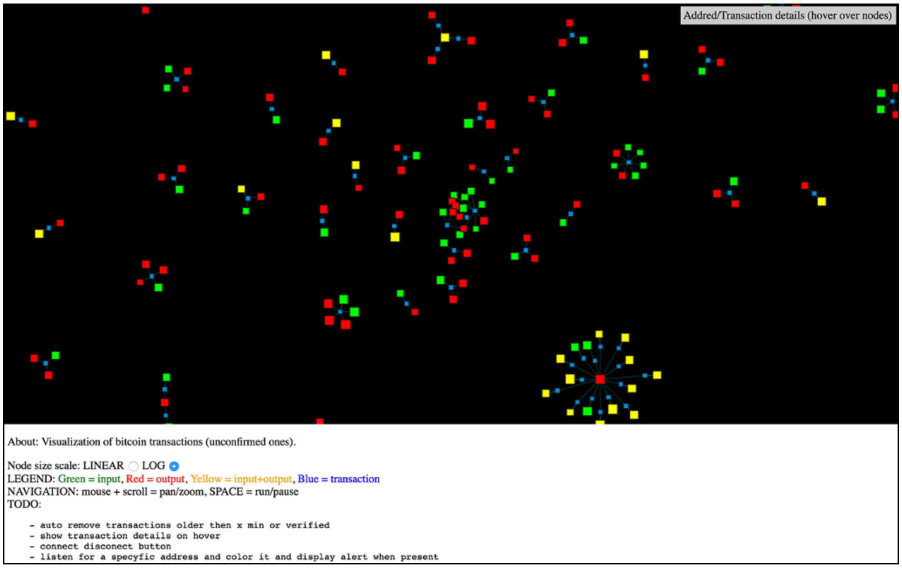
Small networks with few independent minors are vulnerable because it doesn't take much effort to change their information, and powerful miners could do so and gain extra cryptocurrency. Ethereum experienced just this type of attack.

When data is recorded in a blockchain, it's extremely difficult to change or remove it. When someone wants to add a record to a blockchain, also called a *transaction* or an *entry*, users in the network who have validation control verify the proposed transaction. This is where things get tricky because every blockchain has a slightly different spin on how this works and who can validate transactions.

What blockchains do

A blockchain is a peer-to-peer system with no central authority managing data flow. One of the key ways to removing central control while maintaining data integrity is to have a large distributed network of independent users. This means that the computers that make up the network are in more than one location. These computers are often referred to as *full nodes.*

Figure 1-1 shows a visualization of the structure of the Bitcoin blockchain network. You can see it in action at `http://dailyblockchain.github.io`.



About: Visualization of bitcoin transactions (unconfirmed ones).

Node size scale: LINEAR ○ LOG ●
LEGEND: Green = input, Red = output, Yellow = input+output, Blue = transaction
NAVIGATION: mouse + scroll = pan/zoom, SPACE = run/pause
TODO:

```
    - auto remove transactions older then x min or verified
    - show transaction details on hover
    - connect disconect button
    - listen for a specyfic address and color it and display alert when present
```

FIGURE 1-1: The structure of the Bitcoin blockchain network.

To prevent the network from being corrupted, not only are blockchains decentralized but they often also utilize a cryptocurrency. Blockchain networks produce cryptocurrencies as an incentive to maintain the integrity of the network. Many cryptocurrencies are traded on exchanges like stocks.

Cryptocurrencies work a little differently on each blockchain. Basically, the software pays the hardware to operate. The software is the blockchain protocol. Well-known blockchain protocols include Bitcoin, Ethereum, Ripple, Cardano, Solana, and Polkadot. The hardware consists of the full nodes that are securing the data in the network.

Why blockchains matter

Blockchains are recognized as the "fifth evolution" of computing because they're a new trust layer for the Internet. The blockchain space has matured significantly since its inception around 2009. Now individual users have access to higher levels of security and autonomy.

Before blockchains, trust was established by central authorities that would issue certificates. One certificate you may be familiar with is Secure Sockets Layer (SSL). An SSL certificate is the "lock" that you see next to an address in your web browser. It lets you know you're on a secure website. SSL certificates have proven to not be foolproof, however. Certificates have been stolen from the domains of the Central Intelligence Agency (CIA), the U.K.'s Secret Intelligence Service (commonly known as MI6), Microsoft, Yahoo!, Skype, Facebook, and Twitter. Relying on a third party allows for a single point of failure, and hackers have frequently taken advantage of this vulnerability.

Blockchains, on the other hand, establish trust in novel ways. Proof-of-work (POW) blockchains require miners to have a full and accurate history of their transactions to participate on the network. Proof-of-stake (PoS) blockchains create trust by requiring nodes that are processing transactions to "stake" some cryptocurrency that may be forfeited if they're caught defrauding the network. Private blockchains build confidence by distributing data across a network of connected but independent participants that are known by each other and can be held accountable. Each type of blockchain uses a different incentive system to establish trust that each participant in the network will cooperate in keeping a full and unaltered history of each transaction or entry that is made within the database they share.

So, in short, blockchains don't have a single point of attack; they distribute the same replicated date across their network of nodes. Each node adds to the difficulty in tampering with that network's data, at least in theory.

It's very important to note that blockchains are not all equal in their distribution of data control and security. The fifth evolution of the Internet has become progressively more mainstream. More specifically, blockchain-enabled games and nonfungible tokens (NFTs) have generated billions of dollars in sales. They've also impowered a new generation of makers and creatives globally.

The blockchain industry has also renamed itself to Web 3.0. This moniker refers to how people interact online and who controls digital assets and data. For reference, Web 1.0 was a more static Internet experience, where individuals browsed content and built static websites. Web 2.0 is the interactive Internet accessed through commercial portals like Google, Facebook, and Twitter. In the Web 2.0 Internet, data is controlled by commercial entities and privacy is rare for average individual users.

Web 3.0 is a global social movement that pushes back against the egregious privacy violations and fraud that have become ubiquitous online. It also appeals to the entrepreneurial and creative spirit of artists and makers. Web 3.0 software allows users to interact with each other via a sovereign digital identity that each user controls. The user's digital credentials are authenticated via their digital wallet (such as MetaMask), a browser extension, the user's private keys (see Chapter 3).

A user-controlled identity allows average individual users to control their data and privacy. Users also can own digital assets, create new digital assets, and sell them directly. The Internet has enabled digital commerce for a very long time. What makes Web 3.0 special is how elegantly it allows anyone anywhere in the world who has access to a smart device and the Internet to create and transact with any other individual directly.

Global governments have responded strongly to Web 3.0 and have acted quickly to control the inflow and outflow of fiat currency into the blockchain space — for example, requiring Anti–Money Laundering (AML) and Know Your Customer (KYC) verification on individuals moving more than $1,000 of value from one wallet to another.

When data is permanent and reliable in a digital format, you can transact business online in ways that, in the past, were only possible offline. Everything that has stayed analog, including property rights and identity, can now be created and maintained online. Slow business and banking processes, such as money wires and fund settlements, can now be done nearly instantaneously. The implications for secure digital records are enormous for the global economy.

Blockchains are important because they allow for new efficiency and reliability in the exchange of valuable and private information that once required a third party to facilitate, such as the movement of money and the authenticity of identity. This is a big deal because much of our society and economy has been structured around establishing trust, enforcing trust when it's broken, and third parties that facilitate trust. You can imagine how this simple software can be utilized to fix areas that have proven to not be foolproof, such as voting, supply chain management, money movement, and the exchange of property.

The Structure of Blockchains

Each blockchain is structured slightly differently. However, Bitcoin is a great blockchain to study because it was used as a template for most subsequent blockchains. The data on Bitcoin is structured so that each full *node* (the computers running the network) contains all the data in the network. This model is compelling from a data persistence point of view. It ensures that the data will stay intact even if a few of the nodes become compromised. However, because every node has a full copy of the history of transactions, since the very beginning, and every transaction in the future, it requires that the entries be as small as possible from a storage capacity point of view.

Comparatively, other distributed networks you may have heard of like Napster and Pirate Bay are an online index of data. Individual files are shared from specific nodes in the network. This allows sharing of large files. However, because the data you may be interested in is not available on all the participants in the network, obtaining the data you're interested in is problematic. It's also difficult to know if the data that you're pulling down is intact and has not been corrupted or contains information you don't want, such as a virus.

The way that Bitcoin coordinates the organization and input of new data comprises three core elements:

- **Block:** A list of transactions recorded into a ledger over a given period. The size, period, and triggering event for blocks is different for every blockchain.

  Not all blockchains are recording and securing a record of the movement of their cryptocurrency as their primary objective. But all blockchains do record the movement of their cryptocurrency or token. Think of the *transaction* as simply being the recording of data. Assigning a value to it (such as happens in a financial transaction) is used to interpret what that data means.

- **Chain:** A hash that links one block to another, mathematically "chaining" them together. This is one of the most difficult concepts in blockchain to comprehend. It's also the magic that glues blockchains together and allows them to create mathematical trust.

  The hash in blockchain is created from the data that was in the previous block. The hash is a fingerprint of this data and locks blocks in order and time.

  TECHNICAL STUFF

  Although blockchains are a relatively new innovation, hashing is not. Hashing was invented over 70 years ago. This old innovation is being used because it creates a one-way function that cannot be decrypted. A hashing function creates a mathematical algorithm that maps data of any size to a bit string of a fixed size. A bit string is usually 32 characters long, which then represents the data that was hashed. The Secure Hash Algorithm (SHA) is one of some cryptographic hash functions used in blockchains. SHA-256 is a common algorithm that generates an almost-unique, fixed-size 256-bit (32-byte) hash. For practical purposes, think of a hash as a digital fingerprint of data that is used to lock it in place within the blockchain.

- **Network:** The network is composed of "full nodes." Think of them as the computer running an algorithm that is securing the network. Each node contains a complete record of all the transactions that were ever recorded in that blockchain.

  The nodes are located all over the world and can be operated by anyone. It's difficult, expensive, and time-consuming to operate a full node, so people don't do it for free. They're incentivized to operate a node because they want to earn cryptocurrency. The underlying blockchain algorithm rewards them for their service. The reward is usually a token or cryptocurrency, like Bitcoin.

TIP

The terms *Bitcoin* and *blockchain* are often used interchangeably, but they're not the same. Bitcoin has a blockchain. The Bitcoin blockchain is the underlying protocol that enables the secure transfer of Bitcoin. The term *Bitcoin* is the name of the cryptocurrency that powers the Bitcoin network. The blockchain is a class of software, and Bitcoin is a specific cryptocurrency.

Blockchain Applications

Blockchain applications are built around the idea that their blockchain network and the established rules it was created on will be the arbiter of all transactions and keeper of all information. This type of system is an unforgiving and blind environment. Computer code becomes law, and rules are executed as they were written and interpreted by the network. Computers don't have the same social biases and behaviors as humans do.

The network can't interpret intent (at least not yet). Insurance contracts arbitrated on a blockchain have been heavily investigated as a use case built around this idea.

Another interesting thing that blockchains enable is impeccable record keeping. They can be used to create a clear timeline of who did what and when. Many industries and regulatory bodies spend countless hours trying to assess this problem. Blockchain-enabled record keeping will relieve some of the burdens that are created when we try to interpret the past.

The Blockchain Life Cycle

Blockchains originated with the creation of Bitcoin. It demonstrated that a group of individuals who had never met could operate online within a system that was desensitized to cheat others that were cooperating on the network.

The original Bitcoin network was built to secure the Bitcoin cryptocurrency. At the time of writing, it has around 13,000 full nodes that are globally distributed. It's primarily used to trade Bitcoin and exchange value, but the community saw the potential of doing a lot more with the network. Because of its size and time-tested security, it's also being used to secure other smaller blockchains and blockchain applications.

The Ethereum network is a second evolution of the blockchain concept. It takes the traditional blockchain structure and adds several new programming languages that are built inside of it. Like Bitcoin, it has over 10,000 full nodes and is globally distributed. Ethereum is primarily used to trade Ether and create smart contracts. The most popular Ethereum smart contract is the ERC 20. It allows for the generation of interchangeable tokens. These tokens can be used for fundraising purposes. You can discover more about smart contracts in Chapter 5.

There is a third evolution in blockchain technology that is under active development addressing speed and data size constraints. Fixing these issues will enable blockchain technology to be used more realistically with mainstream applications. It will take several years before it is clear what structure will win out.

Popular new developments include *sharding*, a type of database partitioning that separates large databases into smaller parts called *data shards.* An Ethereum development effort called *fork choice rule* splits the Ethereum blockchain into several parallel networks. It may allow Ethereum to scale more efficiently and reduce the congestion on the network, increasing transaction speeds and lowering transaction costs.

Another popular scaling theory is called PoS. I cover this subject in more detail in Chapter 8. Broadly, PoS is the concept of putting up tokens or cryptocurrency as a bond for processing transactions. If the node is corrupted and does not process the transactions accurately, the node may forfeit their tokens or cryptocurrency.

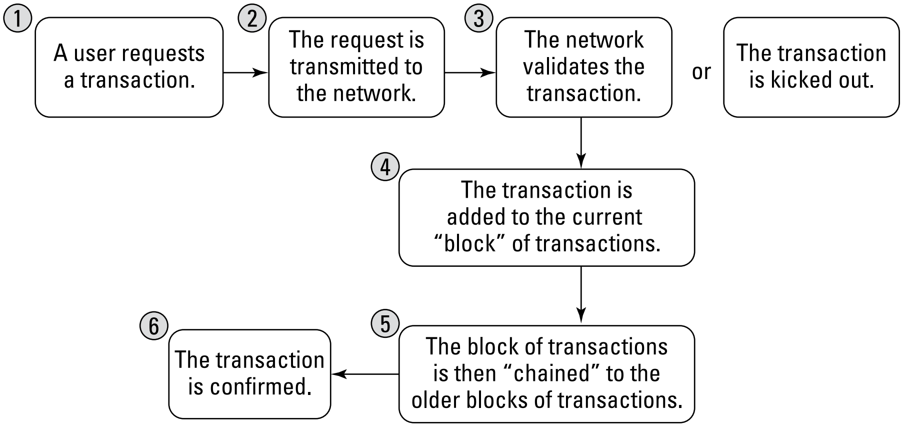
A third effort to scale blockchain technology utilizes trusted nodes. For example, Accumulate, the hard fork of the Factom network, operates with federated nodes and an unlimited number of auditing nodes. These nodes are trusted with ensuring the system. Accumulate's elected network is small, just over 60 nodes. To hedge for security risks, Accumulate anchors itself into other distributed networks to piggyback on the security of more extensive systems. Accumulate also partitions its network into smaller, faster, more easily managed parts called *chains.* Accumulate has faster transaction speeds and lower transaction costs than POW blockchains, and it doesn't have the sunk costs of PoS blockchains.

Consensus: The Driving Force of Blockchains

Blockchains are powerful tools because they create honest systems that self-correct without the need of a third party to enforce the rules. They accomplish the enforcement of rules through their consensus algorithm.

In the blockchain world, *consensus* is the process of developing an agreement among a group of commonly mistrusting shareholders. These are the full nodes on the network. The full nodes are validating transactions that are entered into the network to be recorded as part of the ledger.

Figure 1-2 shows the concept of how blockchains come to agreement.



1
A user requests a transaction.
2
The request is transmitted to the network.
3
The network validates the transaction.
or
The transaction is kicked out.
4
The transaction is added to the current "block" of transactions.
5
The block of transactions is then "chained" to the older blocks of transactions.
6
The transaction is confirmed.

FIGURE 1-2: How blockchains work.

Each blockchain has its own algorithms for creating agreement within its network on the entries being added. There are many different models for creating consensus because each blockchain is creating different kinds of entries. Some blockchains are trading value, others are storing data, and others are securing systems and contracts.

Bitcoin, for example, is trading the value of its token between members on its network. The tokens have a market value, so the requirements related to performance, scalability, consistency, threat model, and failure model will be higher. Bitcoin operates under the assumption that a malicious attacker may want to corrupt the history of trades in order to steal tokens. Bitcoin prevents this from happening by using a consensus model called "proof of work" that solves the Byzantine general's problem: "How do you know that the information you are looking at has not been changed internally or externally?" Because changing or manipulating data is almost always possible, the reliability of data is a big problem for computer science.

Most blockchains operate under the premise that they will be attacked by outside forces or by users of the system. The expected threat and the degree of trust that the network has in the nodes that operate the blockchain will determine the type of consensus algorithm that they use to settle their ledger. For example, Bitcoin has a high degree of threat and uses a strong consensus algorithm called *proof of work.* There is no trust in the network.

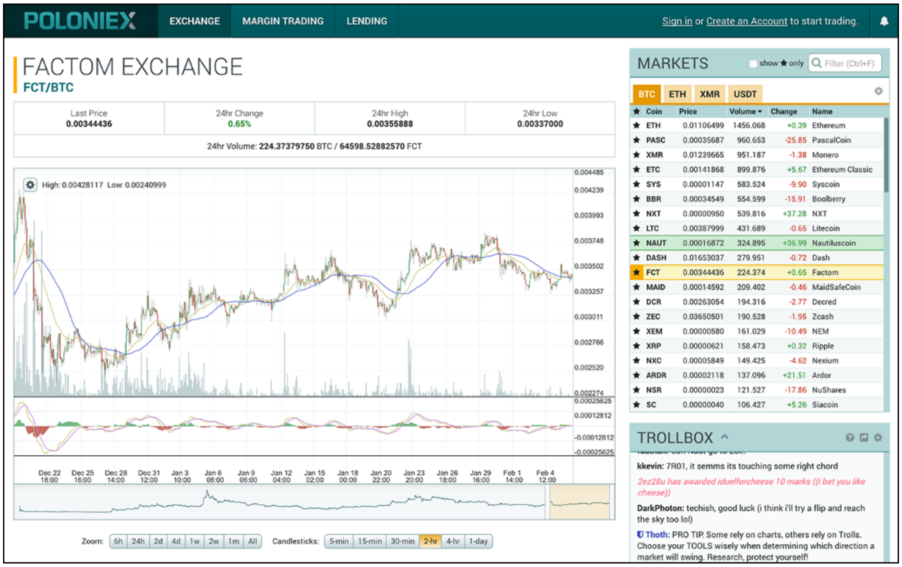
On the other end of the spectrum, blockchains that are used to record financial transactions between known parties can use a lighter and faster consensus. Their need for high-speed transactions is more important. Proof of work is too slow and costly for them to operate because of the comparatively few participants within the network and immediate finality need for each transaction. They also do not need a token or cryptocurrency to incentivize transaction processing. So, they eliminate these things from their system and run faster and cheaper than POW systems.

Blockchains in Use

There are currently thousands of blockchains and blockchain-based applications in use around the world. These systems allow for the creation of nonfungible tokens (NFTs), the use of cryptocurrency in gaming, faster movement of money through distributed networks, and the development of secure and trustworthy applications and hardware. The global interest in these technologies continues to grow as people discover the numerous benefits and possibilities they offer.

You can see many of these public blockchains by going to a cryptocurrency exchange.

Figure 1-3 shows the altcoin exchange for Poloniex (`https://poloniex.com`), a cryptocurrency trading platform.



Sign in or Create an Account to start trading.

FACTOM EXCHANGE
FCT/BTC

Last Price	24hr Change	24hr High	24hr Low
0.00344436	0.65%	0.00355888	0.00337000

24hr Volume: **224.37379750** BTC / **64598.52882570** FCT

★	Coin	Price	Volume	Change	Name
★	ETH	0.01106499	1456.068	+0.39	Ethereum
★	PASC	0.00035687	960.653	-25.85	PascalCoin
★	XMR	0.01239665	951.187	-1.38	Monero
★	ETC	0.00141868	899.876	+5.67	Ethereum Classic
★	SYS	0.00001147	583.524	-9.90	Syscoin
★	BBR	0.00034549	554.599	-15.91	Boolberry
★	NXT	0.00000950	539.816	+37.28	NXT
★	LTC	0.00387999	431.689	-0.65	Litecoin
★	NAUT	0.00016872	324.895	+36.99	Nautiluscoin
★	DASH	0.01653037	279.951	-0.72	Dash
★	FCT	0.00344436	224.374	+0.65	Factom
★	MAID	0.00014592	209.402	-0.46	MaidSafeCoin
★	DCR	0.00263054	194.316	-2.77	Decred
★	ZEC	0.03650501	190.528	-1.95	Zcash
★	XEM	0.00000580	161.029	-10.49	NEM
★	XRP	0.00000621	158.473	+0.32	Ripple
★	NXC	0.00005849	149.425	-4.62	Nexium
★	ARDR	0.00002118	137.096	+21.51	Ardor
★	NSR	0.00000023	121.527	-17.86	NuShares
★	SC	0.00000040	106.427	+5.26	Siacoin

kkevin: 7R01, it semms its touching some right chord

2ez28u has awarded iduelforcheese 10 marks ((i bet you like cheese))

DarkPhoton: techish, good luck (i think i'll try a flip and reach the sky too lol)

Thoth: PRO TIP. Some rely on charts, others rely on Trolls. Choose your TOOLS wisely when determining which direction a market will swing. Research, protect yourself!

FIGURE 1-3: The altcoin exchange platform.

Blockchains are moving beyond the trading value market and are being incorporated into all sorts of industries. Blockchains add a new trust layer that now makes working online secure in a way that was not possible beforehand.

Current blockchain uses

The first blockchain applications revolve around moving money or other forms of value quickly and cheaply. This includes trading public company stock, paying employees in other countries, and exchanging one currency for another. Blockchains are also now being used as part of a software security stack. The U.S. Department of Homeland Security has been investigating blockchain software that secures Internet of Things (IoT) devices and supply chain integrity. The IoT world has some of the most to gain from this innovation, because it's especially vulnerable to spoofing and other forms of hacking. IoT devices have also become more pervasive, and security has become more reliant on them. Hospital systems, self-driving cars, and safety systems are prime examples.

Initial Coin Offerings (ICOs) are another exciting blockchain innovation. They're a type of smart contract that allows the issuer to offer a token in exchange for investment funds. Often used as a non-dilutive fundraising option, entrepreneurs globally have raised billions of dollars. Governments and regulators have been quick to crack down on ICOs. The tokens may be unlicensed securities, and the offering may be defrauding investors. The technology is impressive even if compliance issues are still being addressed.

One of the fantastic innovations inherent in ICO tokens is that they're a self-clearing and self-settling instrument. In our current system for trading securities, there are two types of clearing agencies: clearing corporations and depositories. Clearing corporations audit transactions and act as intermediaries in making settlements. Depositories hold securities certificates and maintain ownership records of the securities. Blockchains perform both these functions for tokens without needing third parties to audit and retain possession of the assets. You can learn more about ICO tokens in Chapter 15.

NFTs and crypto play-to-earn games have also pumped billions of dollars into the industry and empowered average users with the ability to create and sell their own digital assets. Social media, web browsing, and secure communication enabled by blockchains are also becoming more popular every year. Also, governments (including the Central African Republic and El Salvador) are adopting Bitcoin as their legal tender.

Future blockchain applications

The blockchain revolution has spread across the Internet and is quickly transforming formerly Web 2.0 digital experiences to ones more closely controlled by the end user. Humanity is experiencing late-stage globalization. This is a world were digital-based labor is becoming commoditized and equalized in price. An accountant in New York will one day cost the same as an equivalent accountant who lives in New Kingston or New Delhi.

Blockchain applications will become seamless within the lives of billions of people because it will function as identity and money and enable trusted data across all applications.

The possibilities of a blockchain-infused future have excited the imaginations of business people, governments, political groups, and humanitarians across the world. Countries such as the UK, Singapore, and the United Arab Emirates see it as a way to cut cost, create new financial instruments, and keep clean records. They have active investments and initiatives exploring blockchain.

Blockchains have laid a foundation where the need for trust has been taken out of the equation. Where before asking for "trust" was a big deal, with blockchains it's small. Also, the infrastructure that enforces the rule if that trust is broken can be lighter. Much of society is built on trust and enforcement of rules. The social and economic implications of blockchain applications can be emotionally and politically polarizing because blockchain will change how we structure value-based and socially based transactions.

IN THIS CHAPTER

- Discovering the right blockchain for your needs
- Making a plan for your project
- Uncovering obstacles to your project
- Building a project road map

Chapter 2
Picking a Blockchain

The blockchain industry is complex and growing in size and capabilities every day. When you understand the three core types of blockchains and their limitations, you'll know what's possible with this new technology.

This chapter is all about assessing blockchain technology and developing a project plan. It puts the following chapters about individual blockchain platforms and applications into context.

Here, you see how to assess the three different types of blockchain platforms, what's being built on each type, and why. I give you a few tools that help you outline your project, predict obstacles, and overcome challenges.

Where Blockchains Add Substance

There's a lot of buzz surrounding blockchains and the cryptocurrencies that run them. Some of this buzz just stems from the fluctuation in the value of cryptocurrencies and the fear that blockchain technology will disrupt many industry and government functions. A lot of money has poured into research and development because stakeholders don't want to be made obsolete and entrepreneurs want to explore new business models.

When it comes to finding an opportunity for blockchain technology to add value to an organization, often the question arises, "Where do blockchains add value and how are they different from existing technologies?"

Blockchains are a special type of database. A database is a collection of data that is organized in a specific way and stored electronically. Databases are designed to store, retrieve, and manage large amounts of data quickly and efficiently. They are commonly used to store *structured data* (data that follows a specific format and is organized in a specific way) and are widely used in a variety of applications, including financial systems, customer relationship management systems, and online shopping websites.

A blockchain is like a database in that it's a digital record-keeping system that stores data in a structured manner. One key difference is that a blockchain is a *distributed database* — it isn't stored in a single location, but is spread across a network of computers or nodes. Most blockchains require full nodes in the network and have a copy of the entire blockchain, and when a new piece of data is added to the blockchain, it's added to all copies of the blockchain in the network. This decentralized structure makes it difficult for any single entity to alter the data in the blockchain, because any changes would have to be made simultaneously on all copies of the blockchain.

After data has been added to the blockchain, generally speaking, it can't be altered or deleted. This makes the blockchain a secure and reliable record-keeping system, because it ensures the integrity and authenticity of the data stored on it. Some blockchains have implemented systems to delete data unless you pay to keep it posted, but this is not the norm.

In contrast, traditional databases are often centralized and can be more easily altered or manipulated by a single entity with access to the database. They're also less secure, because they can be vulnerable to hacking and data breaches. As you consider the uses of blockchains, it's important to note that you can utilize a blockchain anywhere you would use a normal database — but it may not make sense to go through the trouble and expense of using a blockchain when a normal database can do the job. A blockchain is an intentionally inefficient database that is distributed across the web.

You really see value in using some form of a blockchain when you want to share information with parties you don't fully trust, your data needs to be audited, or your data is at risk of being compromised internally or externally. The majority of blockchains publish a public record of themselves. Even if the data has been encrypted, it may not be private in the future when quantum computing becomes cheaper and more readily available. None of these questions is simple, and the correct solutions can be difficult to ascertain.

This section helps narrow down your options.

Determining your needs

Blockchains come in a lot of flavors. You'll find one that matches your needs — the trick is finding it! Mapping your needs to the best blockchain can be overwhelming. Whenever I have lots of options and often conflicting needs, I like to utilize a weighted decision matrix.

A weighted decision matrix is an excellent tool for evaluating the needs of a project and then mapping those needs to possible solutions. The key advantage of the matrix is to help you quantify and prioritize individual needs for your project and simplify decision making. Weighted decision matrixes also prevent you from becoming overwhelmed by individual criteria. If done properly, this tool allows you to converge on a single idea that is compatible with all your goals.

To create a weighted decision matrix, follow these steps:

1. **Brainstorm the key criteria or goals that your team needs to meet.**

   TIP

   If you aren't sure of the criteria you need to consider when evaluating your blockchain project, here are a few things to keep in mind:

   - Scale and volume
   - Speed and latency
   - Security and immutability
   - Storage capacity and structural needs

   Your team will have its own list of objects and priorities. These are just a few to consider while evaluating the correct platform to use to meet your needs.

2. **Reduce the list of criteria to no more than ten items.**

   TIP

   If you're having a hard time refining your list of needs, consider using a comparison matrix tool.

3. **Create a table in Microsoft Excel or a similar program.**
4. **Enter the design criteria in the first column.**

5. **Assign a relative weight to each criterion based on how important that objective is to the success of the project.**

   Limit the number of points to 10 and distribute them between all your criteria — for example, 1 = low, 2 = medium, and 3 = high priority.

   TIP

   If you're working in a team, have each member weight the criteria separately.

6. **Add up the numbers for each objective and divide by the number of team members for a composite team weight.**

7. **Make any needed adjustment to weights to make sure each criteria are weighted correctly.**

Congratulations! You now have a ranked list of criteria you need to meet to be successful with your blockchain project.

Defining your goal

You can easily get lost building a blockchain project that doesn't have a clear goal or purpose. Take the time to understand where you and your team would like to go and what the final objective is. For example, a goal might be to trade an asset with a partner company with no intermediary. This is a big goal with many stakeholders.

Build back to a small project that is a minimal viable use case for the technology that clearly articulates added value or savings for your company. Along the same lines as the earlier example, a smaller goal would be to build a private network that can exchange value between trusted parties.

Then build on that value. The next win might be building an instrument that is tradable on your new platform. Each step should demonstrate a small win and value created.

Choosing a Solution

There are three core types of blockchains: public networks like Bitcoin, permissioned networks such as Ripple, and private ones like R3.

Blockchains do a few straightforward things:

- They move value and trade value quickly and at a very low cost.
- They create nearly permanent data histories.

Blockchain technology also allows for a few less-straightforward solutions such as the ability to prove that you have a "thing" without revealing it to the other party. It is also possible to "prove the negative," or prove what is missing within a dataset or system. This feature is particularly useful for auditing and proving compliance.

Table 2-1 lists common uses cases that are suited for each type of blockchain.

TABLE 2-1 Public versus Private Blockchain Uses

Primary Purpose	Type of Blockchain
Move value between untrusted parties	Public
Move value between trusted parties	Private
Trade value between unlike things	Permissioned
Trade value of the same thing	Public
Create decentralized organization	Public or permissioned
Create decentralized contract	Public or permissioned
Trade securitized assets	Public or permissioned
Build identity for people or things	Public
Publish for public recordkeeping	Public
Publish for private recordkeeping	Public or permissioned
Preform auditing of records or systems	Public or permissioned
Publish land title data	Public
Trade digital money or assets	Public or permissioned
Create systems for Internet of Things (IoT) security	Public
Build systems security	Public

There may be exceptions depending on your project, and it is possible to use a different type of blockchain to reach your goal. But in general, here is how to break down different types of networks and understand their strengths and weaknesses:

- **Public networks** are large and decentralized, anyone can participate within them at any level — this includes things like running a full node, mining cryptocurrency, trading tokens, or publishing entries. They tend to be more secure and immutable then private or permissioned networks. They're often slower and more expensive to use. They're secured with a cryptocurrency and have limited storage capacity.

- **Permissioned networks** are viewable to the public, but participation is controlled. Many of them utilize a cryptocurrency, but they can have a lower cost for applications that are built on top of them. This feature makes it easier to scale project and increase transaction volume. Permissioned networks can be very fast with low latency and have higher storage capacity over public networks.
- **Private networks** are shared between trusted parties and may not be viewable to the public. They're very fast and may have no latency. They also have a low cost to run and can be built in an industrious weekend. Most private networks do not utilize a cryptocurrency and do not have the same immutability and security of decentralized networks. Storage capacity may be unlimited.

There are also hybrids between these three core types of blockchains that seek to find the right balance of security, auditability, scalability, and data storage for applications built on top of them.

Drawing a blockchain decision tree

Some of the decisions you face while working on a blockchain project within your organization can be difficult and challenging. It pays to take time making decisions that involve

- **Uncertainty:** Many of the facts around blockchain technology may be unknown and untested.
- **Complexity:** Blockchains have many interrelated factors to consider.
- **High-risk consequences:** The impact of the decision may be significant to your organization.
- **Alternatives:** There may be alternative technologies and types of blockchains, each with its own set of uncertainties and consequences.
- **Interpersonal issues:** You need to understand how blockchain technology could affect different people within your organization.

A decision tree is a useful support tool that will help you uncover consequences, event outcomes, resource costs, and utility of developing a blockchain project.

You can draw decision trees on paper or use a computer application. Here are the steps to create one for uncovering other challenges around your project:

1. **Get a large sheet of paper.**

   TIP

   The more choices there are, and the more complicated the decision, the bigger the sheet of paper you'll need.

2. **Draw a square on the left side of the paper.**
3. **Write a description of the core goal and criteria for your project in that square.**
4. **Draw lines to the right of the square for each issue.**
5. **Write a description of each issue along each line.**

   TIP

   Assign a probability value to encounter each issue.

6. **Brainstorm solutions for each issue.**
7. **Write a description of each solution along each line.**
8. **Continue this process until you've explored each issue and discovered a possible solution for each.**

Have teammates challenge and review all your issues and solutions before finalizing it.

Making a plan

At this point, you should have a clear understanding of your goals, obstacles, and what blockchain options you have available.

Here's a simple road map for building your project:

1. **Explain the project to key stakeholders and discuss its key components and foreseen outcomes.**
2. **Write up a project plan.**

   This is a living set of documents that will change over the life of your project.

3. **Develop the performance measurements, scope statement, schedule, and cost baselines.**
4. **Consider creating a risk management plan and a staffing plan.**
5. **Get buy-in and define roles and responsibilities.**

6. **Hold a kickoff meeting to begin the project.**

   The meeting should cover the following:

   - Vision for the project
   - Project strategy
   - Project timeline
   - Roles and responsibilities
   - Team-building activities
   - Team commitments
   - How your team will make decisions
   - Key metrics the project will be measured against

REMEMBER

After you complete your project, you aren't done! Go back and analyze your successes and failures. Here are some questions to ask yourself:

- Are my key stakeholders happy?
- Did the project stay on schedule?
- If not, what caused it to be delayed?
- What did I learn from this project?
- What do I wish I had done differently?
- Did I actually create new value for my company or save money?

TIP

You may want to return to this chapter when you have a deeper knowledge of blockchain technology and you're developing a plan to build a project.

IN THIS CHAPTER

- » Creating and using a Bitcoin and Ethereum wallet
- » Exchanging Bitcoin for Ether
- » Creating a blockchain asset
- » Leasing a blockchain asset

Chapter 3

Getting Your Hands on Blockchain

Blockchains are very powerful tools and are changing how the world moves money, secures systems, and builds digital identities. If you aren't a core developer, you probably won't be doing any in-depth blockchain development in the near future. That said, you still need to understand how blockchains work and what their core limitations are because they'll be integrated into many everyday online interactions in the near future — from how businesses pay people to how governments know that their systems and data are intact and secure.

In this chapter, you dive right into blockchain technology. You purchase your first cryptocurrency and learn how to exchange it for other currencies. You set up special applications that will give you access to a whole ecosystem of decentralized applications (known as dApps). You also set up a secure environment to use your cryptocurrency. In this chapter, you also create and lease out digital blockchain assets through a blockchain game.

After working through this chapter, you'll understand many of the basic functionalities that blockchain technology offers. You'll also have a basic understanding of some of the additional security you need to have while working with cryptocurrency. This chapter also helps you establish the basic crypto accounts that you need in later chapters.

Diving into Blockchain Technology

The Ethereum blockchain is one of the largest and most powerful blockchains in the world. It was designed to build dApps, which are applications that are built within a trustless decentralized network. Within the Ethereum network, developers utilize smart contracts to build these applications. Ethereum also utilizes a cryptocurrency called Ether to reward users for providing computing power and creating the trustless system that these smart contracts need to execute.

Smart contracts are not really like a contract you may have seen for a business. Instead, smart contracts are code deployed across a decentralized network. Like a business contract, they have predefined terms. A key difference is that smart contracts are enforced by their blockchain network. They're an important computing innovation because they allow individuals who don't know or trust one another to collaborate without fear that the other party won't perform as outlined by the terms that the two parties have agreed on.

TIP

Blockchains that utilize a cryptocurrency can sometimes be called "trustless" systems because the code is enforced by the network (as opposed to a business contract, which is enforced by a court system).

In the following sections, you set up accounts to purchase your first Bitcoin. You also exchange some of the Bitcoin you buy for Ether so you can utilize Ethereum dApps in the following sections.

Creating a secure environment

The first thing you need to do is create a secure environment to work online. There are a growing number of reasons for you to think about using a secure browser and a virtual private network (VPN). They prevent your data from being collected without your consent and help to avoid hackers. The average user can be targeted by hackers when using cryptocurrency and an unsecured Internet connection.

In this section, you download the Brave web browser, ProtonVPN, and a MetaMask browser extension. You can use all three of these services without paying. However, they also offer improved service for a fee.

TIP

Get a piece of paper and pen ready to write down important information. Never take a screenshot or photo of things like passwords or seed phrases.

Downloading and installing the Brave browser

Brave is a new Google Chromium–based secure web browser that is fast, open source, and privacy focused. It blocks advertisements, trackers, and has a feature that lets you reward publishers you like with tokens. Internet pioneer Brendan Eich created Brave; he invented JavaScript and co-founded Mozilla, too.

To download the Brave web browser, follow these steps:

1. **Go to `https://brave.com`.**
2. **Click Download Brave.**
3. **Go to your downloads folder.**
4. **Double click the Brave browser file.**
5. **Drag and drop the new Brave browser icon to your applications folder.**

Now that you have a more secure web browser, you can add the blockchain extension to it that allows you to explore decentralized applications.

The Brave browser is a great browser on its own, but if you want to kick your security up a notch, you can use the Brave Tor browser. Tor (short for The Onion Router) is free and open-source software for anonymous communication and web browsing. It directs Internet traffic through a worldwide volunteer overlay network that helps you conceal your location and usage from anyone performing network surveillance or traffic analysis. This may seem like overkill, but crypto users are targeted by rogue nations and terrorist groups that want to steal their assets.

With Tor connectivity, you get two additional benefits: Your IP address is hidden from the sites you visit, and the sites you visit are hidden from passive network observers. Note that Tor may slow down browsing or break some websites.

TIP

To use the Brave Tor browser, choose File ⇨ New Private Window with Tor from within your Brave browser.

A private window with Tor makes it more difficult, but not impossible, for your Internet service provider (ISP) to see what sites you visit. A private window with Tor won't, however, fully defend against tracking, and you may consider reviewing *Cybersecurity For Dummies*, 2nd Edition, by Joseph Steinberg (Wiley) to learn more about staying safe online.

Downloading and installing ProtonVPN

ProtonVPN is a VPN run by a Swiss company. When you use ProtonVPN to browse the web, your Internet connection is encrypted so any would-be attackers can't eavesdrop on your activity. It also allows you to access websites that may be blocked.

To download ProtonVPN, follow these steps:

1. **Go to `https://protonvpn.com`.**
2. **Click Get ProtonVPN Now.**
3. **Click Get Free.**
4. **Enter your email address when prompted.**

To install ProtonVPN, follow these steps:

1. **Go to your download folder on Mac or PC.**
2. **Double-click the ProtonVPN file.**
3. **Drag and drop the new ProtonVPN icon to your applications folder.**

A VPN is a good second layer of security to help make sure that your connection is secure. To learn more about how you can protect yourself and your devices check out *Cybersecurity For Dummies* by Joseph Steinberg (Wiley).

Downloading, installing, and securing MetaMask

MetaMask is a browser extension that allows you to run Ethereum dApps right in your browser without running a full Ethereum node. (Ethereum is one of the largest blockchains in the world; see Chapter 5 for more information). MetaMask includes a secure identity vault. It allows you to log into websites, manage your identities on the web, and sign blockchain transactions. You can also keep some Ether cryptocurrency in your MetaMask wallet to make payments online.

To download and install MetaMask, follow these steps:

1. **Open the Brave web browser.**

   See "Downloading and installing the Brave browser," earlier in this chapter if you haven't installed it already.
2. **Go to `https://metamask.io`.**
3. **Click Download for Brave.**
4. **Click Add to Brave.**

5. **Click Add Extension inside the new window.**

   You should now see a small fox icon in the upper-right corner of your Brave browser.

Because MetaMask is a wallet, you'll also need to secure and back up your wallet with a strong password and secure your backup seed. A backup seed allows you to recover your wallet if you lose your password.

Grab a pen and notebook or a piece of paper that you can keep private. Then follow these steps:

1. **At the top of your piece of paper, write "MetaMask," "Brave browser," the date, and the device you've downloaded it on.**
2. **Open the Brave web browser.**
3. **Click the fox icon in the upper-right corner.**
4. **Click Continue.**
5. **Create a strong and unique password.**
6. **Write down your username and password.**
7. **Click Create.**

Get another notebook or a separate piece of paper for this next series of steps. Don't use the same notebook or piece of paper on which you've just written down your username and password. Be sure to secure these documents in a place where they can't be destroyed or found. Many individuals open bank vaults or use a safe to keep their backup phrases and passwords because access to one or the other is access to your crypto.

1. **At the top of your piece of paper, write "MetaMask," "Brave browser," the date, the device you downloaded Brave on, and "Seed phrase."**
2. **Open the Brave web browser.**
3. **Click the fox icon on the upper-right corner.**
4. **Click Accept.**
5. **Click the lock icon.**
6. **Write down and number the 12-word phrase.**
7. **Click Next.**
8. **Reorder the seed phrase using what you wrote down.**
9. **Click Done.**

TIP

Consider laminating the pieces of paper with your username and password and your backup seed. And remember not to store these two pieces of paper in the same location.

Buying your first Bitcoin

There are several places where you can purchase your first Bitcoin. If you're within the United States, you'll experience some friction in setting up an account and linking it to your credit card or bank account. It may take a day or two for you to be authenticated and allowed to purchase your first cryptocurrency. All virtual asset service providers (VASPs) must perform Anti-Money Laundering (AML) and Know Your Customer (KYC) verification on customers who transact more than $1,000 due to the new global travel rule (see the nearby sidebar).

I recommend using one of the following websites if you're within the United States and would like to purchase some cryptocurrency for the first time:

- **Cash App:** `https://cash.app`
- **Coinbase:** `www.coinbase.com`
- **Gemini:** `https://gemini.com/`
- **Robinhood:** `https://robinhood.com`

Go to one of these sites or another of your choosing and set up an account. You'll want to purchase $10 to $20 worth of cryptocurrency. I suggest purchasing Bitcoin. It's universally accepted and traded for all other cryptocurrencies. You may also have the option to purchase Ether, the Ethereum cryptocurrency used for running dApps. If so, go ahead and purchase $5 to $10 worth because you'll be using it in the next section. If you're only able to buy Bitcoin, that's okay. You'll be able to trade it for Ether within your wallet using ShapeShift, a low-friction cryptocurrency exchange.

An important note to remember is that cryptocurrency has been in the regulatory gray zone. At the writing of this book, it's possible to purchase and withdraw funds from these sources. Buying and withdrawing cryptocurrency may not be available in the future or within your country or region. If that's the case, you may want to move on to Chapter 5. There, you'll be able to mine on the test net and receive test Ether.

THE NEW GLOBAL TRAVEL RULE

The global travel rule is a set of guidelines that requires VASPs, such as Coinbase and Gemini, to collect and transmit certain information when facilitating the transfer of virtual assets between VASPs or between a VASP and a non-VASP. The purpose of the global travel rule is to help combat money laundering and terrorism financing by providing a way for law enforcement agencies to track the movement of virtual assets and identify the parties involved in transactions.

The global travel rule was developed by the Financial Action Task Force (FATF), an intergovernmental organization that sets standards and best practices for combating money laundering and terrorism financing. The global travel rule applies to a wide range of virtual assets, including cryptocurrencies, and requires VASPs to collect and transmit the following information when facilitating a transaction:

- The originator's name and address
- The originator's account number or virtual asset address
- The beneficiary's name and address
- The beneficiary's account number or virtual asset address
- The amount of the transaction
- The date and time of the transaction

VASPs are required to transmit this information to the recipient VASP or non-VASP, as well as retain it for a certain period of time for potential investigation by law enforcement agencies.

Securing and Exchanging Your Cryptocurrency

If you were able to buy Ether when you set up your account, feel free to skip this section. Here, you'll be setting up a Jaxx wallet to exchange the Bitcoin you bought for Ether using the built-in ShapeShift exchange. The Jaxx wallet was developed by Anthony Di Iorio. He is an early blockchain pioneer and a co-founder of Ethereum.

The device you download the wallet onto can be a computer or phone. For this exercise, you're going to download the Chrome extension. If you choose to download the other wallet types, don't forget that your devices can be compromised. Common cryptocurrency hacking is done through social engineering, like a SIM card hack. You can also lose your assets because you have an insecure Internet connection. Jaxx is considered a hot wallet because it's connected to the Internet, so it has some vulnerabilities.

TIP

There are a few things you can do to help mitigate your risks:

- Use your VPN.
- Use Google Authenticator.
- Use a Google Voice number.
- Keep a separate email you use only for cryptocurrency accounts.
- Have a device you use only on a secure connection for your cryptocurrency activities.
- Never keep any digital records of your passwords and recovery seeds.

Downloading Jaxx

In this section, you will download and set up a cryptocurrency wallet. There are many on the market that help you secure the Bitcoin and other assets that you use. The Jaxx Liberty is a user-friendly wallet that supports more than 80 different cryptocurrencies. It also works great for iOS, Android, desktop, and has a Google Chrome version, too. Feel free to look at other options, too. For example, Exodus.io (`www.exodus.io`) is also another great and easy-to-use wallet.

1. **In your Brave browser, go to `https://jaxx.io`.**
2. **Click Downloads.**
3. **Select Add the Jaxx Liberty Google Chrome Extension to Your Browser.**
4. **Click Add to Chrome.**
5. **Click Add Extension in the popup window.**

Securing your Jaxx wallet

Now you're ready to secure your Jaxx wallet. You'll need at least two clean sheets of paper to write down your seed phrase and password.

REMEMBER

Do not keep your password with your seed phrase.

Follow these steps:

1. **At the top of one sheet of paper, write "Jaxx," "Brave browser," the date, and the device you've downloaded Jaxx on.**
2. **Open the Brave web browser.**
3. **Click the heart icon in the upper-right corner.**
4. **Click Create New Wallet.**
5. **Click I Agree.**
6. **Click Continue.**
7. **Click Back Up Now.**
8. **Select Yes when you see the warning.**
9. **Click Start Backup.**
10. **Write down and number your seed phrase.**
11. **Retype your words in order.**
12. **Click Confirm.**
13. **Click Jaxx Liberty Home.**

TIP

In the next section, you'll secure a password for your Jaxx wallet for your Brave browser. Don't skip this step — you'll need the password later to access your assets. If you have difficulty getting Jaxx to open, try navigating to a dApp website such as `www.cryptokitties.co` and try the preceding steps again.

Follow these steps:

1. **At the top of the second piece of paper, write "Jaxx," "Brave browser," the date, and the device you have downloaded Jaxx on.**
2. **Open the Brave web browser.**
3. **Click the heart icon in the upper-right corner.**
4. **Click the menu icon in your Jaxx wallet.**
5. **Click Security Password.**
6. **Select Yes when you see the warning.**
7. **Click Set Password.**
8. **Write down a strong unique password on your sheet of paper.**
9. **Enter your password twice and click Continue.**

REMEMBER

Store these two pieces of paper in separate locations. You may want to laminate them just to be safe.

Transferring Bitcoin to Jaxx

In this section, you will add some Bitcoin cryptocurrency to your Jaxx wallet for your Brave browser. As of this writing, it was possible to buy Bitcoin from within the Jaxx Brave browser wallet, so you may consider doing that instead of transferring assets from an exchange such as Coinbase. That said don't skip buying some crypto — you'll need it later to buy Ether for the CryptoKitties exercise.

Follow these steps:

1. **Open the Brave web browser.**
2. **Click the heart icon in the upper-right corner.**
3. **Click Wallets.**
4. **Click Bitcoin.**
5. **Click Receive.**
6. **Click Copy Address.**

Trading Bitcoin for Ether

Now you need to open the account in which you keep your Bitcoin. You'll look for a transfer or send button and paste the address into the field when it's presented. After you've received your Bitcoin into your Jaxx wallet, you can use the exchange function. Follow these steps:

1. **Open the Brave web browser.**
2. **Click the heart icon in the upper-right corner.**
3. **Click Wallets.**
4. **Click Bitcoin.**
5. **Click Exchange.**
6. **Select Ethereum ETH.**
7. **Input the amount you would like to exchange.**

   For the next section, you'll need $5 to $10 of Ether.
8. **Click Continue.**
9. **Click Exchange.**

Loading up your MetaMask account

After your exchange has gone through, you can follow the same directions given earlier to send your Ether to your MetaMask account:

1. **Go to the account where you have Ether.**
2. **Click Account.**
3. **Click Send.**
4. **Click the fox icon in the upper-right corner of your browser.**
5. **Click the menu icon.**
6. **Click the Ether address.**
7. **Copy the address.**
8. **Paste your MetaMask Ether address into the Recipient window.**
9. **Enter the amount you want to send.**
10. **Click Continue.**
11. **Click Confirm.**

Setting up a CryptoKitties account

In this section, you have a bit of fun using the Ethereum blockchain. Here you learn how to buy a unique blockchain asset, create your very own unique blockchain assets, and then sell your asset on a global market.

This incredibly complex exercise of creating and selling blockchain-based assets is disguised as adorable cat images. Called CryptoKitties, it allows you to collect and create a new digital cat. Each image has unique characteristics that it has inherited from its parent images. When you have "bred" a new CryptoKitty, you can then lease your cat to be bred to create new assets or sell it for Ether.

Follow these steps:

1. **In your, Brave web browser, go to `www.cryptokitties.co`.**
2. **Click Start.**
3. **Click Connect.**
4. **Click Sign In.**
5. **Click Sing in the popup window.**

Purchasing CryptoKitties

In this section, you find two kitties to purchase. This will allow you to "breed" a new kitty and lease out your cats to others to breed.

Follow these steps:

1. **In your, Brave web browser, go to `www.cryptokitties.co`.**
2. **Click Sign In.**
3. **Click Sing in the popup window.**
4. **Under Great-Value Kitties, click Browse All.**
5. **Select a cute cat.**

   TIP

   You have a lot of options, but because this exercise is mostly just for fun, be cheap. Also, look for a kitty that is "Swift" and "low-gen." They're faster at breeding and have shorter cooldown times between breeding.
6. **Click Buy Now.**
7. **Click OK, Buy This Kitty.**
8. **Click Confirm.**
9. **Select your second cat and follow the buy instructions.**

Breeding your CryptoKitties

In this section, you'll take the two cats that you purchased in the preceding section and breed them to create a new kitty. This is a very interesting activity in that you're creating a new digital asset that is unique, has verifiable provenance, and can be traded on an open global market without an intermediary to facilitate the authentication or transfer.

Depending on the speed of the Ethereum network at the time you purchased your cats, it may take a few minutes to see them under Kitties. Be patient — they will show up. You can always check your transaction log to look at the status.

Follow these steps:

1. **In your, Brave web browser, go to `www.cryptokitties.co`.**
2. **Click Sign In.**
3. **Click My Profile.**
4. **Select one of your cats.**

5. **Click Breed.**

   Breeding is represented by an eggplant icon.

6. **Click Sire with My Kitties.**
7. **Click OK, Let's Get Started.**
8. **Click the box that says Select Your Kitty.**
9. **Select the other cat.**
10. **Click OK, Give Them Some Privacy.**
11. **Click Confirm in the popup window.**

Leasing your CryptoKitties

In this section, we'll be putting out one of your cats to breed in the market. By doing this, you're leasing your asset on an open market with no intermediaries. If one of your cats is still pregnant, select the other cat to be leased.

Follow these steps:

1. **In your Brave web browser, go to `www.cryptokitties.co`.**
2. **Click Sign In.**
3. **Click My Profile.**
4. **Select one of your cats.**
5. **Click Breed.**
6. **Click Sire to the Public.**
7. **Adjust the prices and time as desired or leave the default settings.**
8. **Click Done.**
9. **Click Confirm in the popup window.**

Congratulations! You've bought your first Bitcoin and traded it for Ether. You then purchased blockchain assets and created your own. Finally, you leased out your assets in an open global marketplace to earn more Ether. Except for your first purchase, all these actions were enabled on an open public blockchain and did not need a bank or intermediary to facilitate. If you enjoyed CryptoKitties, and you'd like to learn how to create your own blockchain-based game, you can go through a simple online tutorial that teaches you how to do everything. You can find this tutorial at `https://cryptozombies.io`.

2

Developing Your Knowledge

IN THIS PART . . .

Discover the beginning of blockchain technology with the Bitcoin blockchain.

Clarify your knowledge of the Ethereum network, and expand your understanding of decentralized autonomous organizations and smart contracts.

Identify the core concept of Cardano and how it’s building a new platform for creating blockchain applications that scale.

Look at the new ecosystem of Polkadot and how it utilizes proof of stake and substrates.

Get to know the new super blockchain Solana and its high-performance platform for decentralized applications that scale.

IN THIS CHAPTER

- » Understanding where the Bitcoin blockchain came from
- » Diving into Bitcoin Cash
- » Straightening out some myths about Bitcoin
- » Staying safe when using Bitcoin
- » Mining for Bitcoins
- » Making a paper wallet to hold your Bitcoins

Chapter 4 Beholding the Bitcoin Blockchain

Warning! After reading this chapter, you may become hooked on this cool emerging technology. Read at your own peril.

Bitcoin demonstrates the purest aspects of blockchain technology. It's the baseline that all other blockchains are compared to and the framework that nearly all have drawn upon. Knowing the basics of how the Bitcoin blockchain operates will allow you to better understand all the other technology you encounter in this ecosystem.

In this chapter, I fill you in on the fundamentals of how the Bitcoin blockchain operates. I offer safety tips that will make your Bitcoin experience smoother and more successful. I also show you practical things you can start doing now with Bitcoin. In these pages, you find out how to mine the Bitcoin token, giving you a new way to get your hands on Bitcoins without buying them. Finally, you discover how to transfer your tokens to paper wallets, and other practical ways to keep your tokens safe online.

Getting a Brief History of the Bitcoin Blockchain

Bitcoin and the concept of its blockchain were first introduced in the fall of 2008 as a whitepaper and later released as open-source software in 2009. (You can read the Bitcoin whitepaper at `www.bitcoin.org/bitcoin.pdf`.)

The author who first introduced Bitcoin in that 2008 whitepaper is an anonymous programmer or cohort working under the name of Satoshi Nakamoto. Nakamoto collaborated with many other open-source developers on Bitcoin until 2010. This individual or group has since stopped its involvement in the project and transferred control to prominent Bitcoin core developers. There have been many claims and theories concerning the identity of Nakamoto, but none of them have been confirmed as of this writing.

Regardless, what Nakamoto created is an extraordinary peer-to-peer payment system that enables users to send Bitcoin, the value transfer token, directly and without an intermediary to hold the two parties accountable. The network itself acts as the intermediary by verifying the transactions and assuring that no one tries to cheat the system by spending Bitcoins twice.

Nakamoto's goal was to close the large hole in digital trust, and the concept of the blockchain was his answer. It solves the Byzantine general's problem, which is the ultimate human problem, especially online: How do you trust the information you are given and the people who are giving you that information, when self-interest, malicious third parties, and the like can deceive you? Many Bitcoin enthusiasts feel that blockchain technology is the missing piece that will allow societies to operate entirely online because it reframes trust by recording relevant information in a public space that cannot be removed and can always be referenced making deception more difficult.

Blockchains mix many old technologies that society has been using for thousands of years in new ways. For example, cryptography and payment are merged to create cryptocurrency. *Cryptography* is the art of secure communication under the eye of third parties. Payment through a token that represents values is also something humans have been doing for a very long time, but when merged, it creates cryptocurrencies and becomes something entirely new. Cryptocurrency lets you take the concept of money and move it online with the ability to trade value securely through a token.

Blockchains also incorporate *hashing* (transforming data of any size into short, fixed-length values). Hashing also incorporates another old technology called Merkle trees, which take many hashes and squeeze them down to one hash, while still being able to prove each piece of data that was individually hashed (see Figure 4-1).

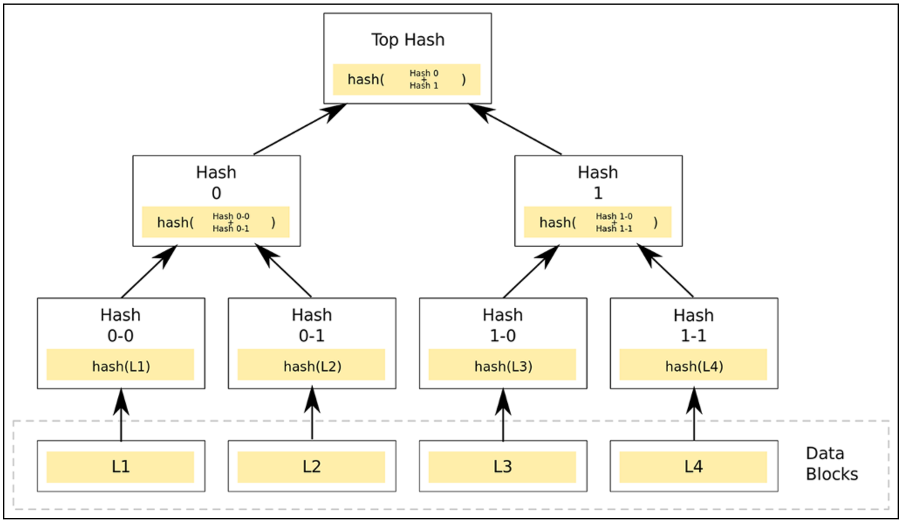


FIGURE 4-1: A Merkle tree.

Ultimately, blockchains are ledgers, which society has been using for thousands of years to keep financial accounts. When all these old models are merged and facilitated online in a distributed database, they become revolutionary.

Bitcoin was designed primarily to send the Bitcoin cryptocurrency. But very quickly, the creators realized that it had a much larger potential. With that in mind, they architected the blockchain of Bitcoin to be able to record more than the data concerning the movement of the token. The Bitcoin blockchain is the oldest, and one of the largest, blockchains in the world. It's composed of thousands of nodes that are running the Bitcoin protocol. The protocol is creating and securing the blockchain.

REMEMBER

In very simple terms, the *blockchain* is a public ledger of all transactions in the Bitcoin network, and the *nodes* are computers that are recording entries into that ledger. The *Bitcoin protocol* is the rules that govern this system.

Nodes safeguard the network by mining for the cryptocurrency Bitcoin. New Bitcoins are created as a reward for processing transactions and recording them inside the blockchain. Nodes also earn a small fee for confirming transactions.

Anyone can run the Bitcoin protocol and mine the token. It's an open-source project that thrives as more individuals participate in the network. The fewer people who participate, the more centralized it becomes — and centralization weakens the system. The primary thing that makes Bitcoin a secure system is the large number of independent nodes that are globally distributed.

The most successful miners have robust systems that can outperform slower miners. Early in its history, you could run the Bitcoin protocol and earn Bitcoins on a desktop computer. Now, in order to have any hope of ever receiving Bitcoins, you need to purchase expensive specialized equipment or use a cloud service.

In order to create a message in the Bitcoin blockchain, you have to send some Bitcoin from one account to another. When you send a transaction in Bitcoin, the message is broadcast across the whole network. After the message is sent, it's impossible to alter it because the message is recorded inside the Bitcoin blockchain. This feature makes it imperative that you always choose your message wisely and never broadcast sensitive information.

Broadcasting the same message to thousands of nodes and then saving it forever in the token's ledger can add up in a hurry. So, Bitcoin requires that you keep your communications very short. There are a few ways to write a message on the Bitcoin blockchain, such as the OP_Return field. Currently, you can write up to 83 characters.

The New Bitcoin: Bitcoin Cash

There is significant conflict around the core development of Bitcoin. Dubbed the "Bitcoin Civil War" or the "block size limit debate," the general conflict is between keeping Bitcoin core as it is and enlarging the functionality of the software. This conflict appears simple, but the repercussions are enormous. Bitcoin's permanent nature and the billions of dollars' worth of assets that Bitcoin software secures mean that every code change is rigorously reviewed and debated.

Bitcoin hard-forked and split into two separate blockchains in 2017. The community of developers and Bitcoin miners couldn't agree on how to address growth. Bitcoin had become increasingly unreliable and expensive to use. It had once been a nearly instant and almost free system; now transactions were costing more than $50 and taking hours to days to clear. The high cost and slow speed drove away users.

A primary issue was that Bitcoin's transaction speeds were too slow, at seven transactions per second, to meet the demand on the network. Transaction fees climbed as users competed to have their transactions processed faster. One of the limiting factors was that Bitcoin's block size limit was 1MB in 2017.

Bitcoin Cash used the same codebase as Bitcoin but adjusted the block size limit. They increased the block size to 32MB. At the time of the fork, anyone holding Bitcoin was also given the same number of Bitcoin Cash. The increase was controversial because it disenfranchised smaller miners who had slower equipment.

Many miners feared that they couldn't be competitive mining larger blocks. There was also concern that the larger block size would lead to centralization of the Bitcoin blockchain network.

Bitcoin is a living and ever-changing system. The Bitcoin core development community is actively seeking ways to improve the system by making it stronger and faster. Anyone can contribute to the Bitcoin protocol by engaging on its GitHub page (`www.github.com/bitcoin`). However, there is a small community of dominant core developers of Bitcoin. The most prolific contributors are Wladimir Van Der Laan, Pieter Wuille, and Gavin Andresen.

THE LIMITATIONS OF BITCOIN

Blocks that make up the Bitcoin blockchain are limited to 1MB in size. This limits the number of transactions that the Bitcoin blockchain can handle to seven transactions per second. New blocks occur on average about every ten minutes, but they aren't guaranteed.

These limitations are hard-coded into the Bitcoin protocol and help ensure that the network stays decentralized. And decentralization is key to Bitcoin's robustness. Larger blocks would impose hardships on the miners and might push out small operations.

Bitcoin has built-in limitations that prevent it from handling the global volume of monetary transactions. It is also being used to secure other types of data and systems. The demand to use the secure Bitcoin ledger is high. This difficulty is referred to as *Bitcoin bloat,* and it has slowed down the network and increased the cost of transactions.

At this point, most blockchain developers are only experimenting with expanding the utility of the Bitcoin blockchain. Most are not at a point where they need to scale up their prototypes and concepts so that the Bitcoin blockchain can handle their request. Other new blockchain technologies have also helped bring down the pressure on Bitcoin and given developers cheaper options to secure data.

AS THE WORLD TURNS: THE DRAMA OF BITCOIN

Bitcoin is under intense scrutiny from the outside. The decentralized nature of Bitcoin that may displace central authorities made it a target for regulators. Bitcoin is also favored by people who want to purchase illicit items anonymously or move money from a controlled economy to a noncontrolled economy, bypassing governmental controls. All these factors have given Bitcoin a bad rap and drawn the judgment of society. Entrepreneurs that wanted to capitalize on the technology of Bitcoin rebranded it. The change in terminology was used to differentiate the software structure of Bitcoin and other cryptocurrencies. Software that used the structure of cryptocurrencies began being called *blockchain.* The shift to deemphasize the controversial tokens and highlight the structure of cryptocurrencies changed both government and commercial views of Bitcoin from fear to excitement.

Debunking Some Common Bitcoin Misconceptions

People are often suspicious of anything new, especially new things that aren't easy to understand. So, it's only natural that Bitcoin — a totally new currency unlike anything the world had ever seen before — would confound people, and a few misconceptions would result.

Here are some of the misconceptions you might have heard about Bitcoin:

- **Bitcoin was hacked.** There was one known instance in 2011 where someone double spent their Bitcoin, but it was resolved within an hour. Since this issue, there have been no known successful attacks on the Bitcoin blockchain that resulted in stolen Bitcoins. However, many central systems that use Bitcoin have been hacked. And wallets and Bitcoin exchanges are often hacked due to inadequate security. The Bitcoin community has fought back by developing elegant solutions to keep their coins safe, including wallet encryption, multiple signatures, offline wallets, paper wallets, and hardware wallets, just to name a few.
- **Bitcoin is used to extort people.** Because of the semi-anonymous nature of Bitcoin, it's used in ransomware attacks. Hackers breach networks and hold them hostage until payment is made to them. Hospitals and schools have been victims of these types of attacks. However, unlike cash, which was favored by thieves in the past, Bitcoin always leaves a trail in the blockchain that investigators can follow.

- **Bitcoin is a pyramid scheme.** Bitcoin is the opposite of a pyramid scheme from the point of view of Bitcoin miners. The Bitcoin protocol is designed like a cannibalistic arms race. Every additional miner prompts the protocol to increase the difficulty of mining. From a social point of view, Bitcoin is a pure market. The price of Bitcoins fluctuates based on market supply, demand, and perceived value. Bitcoin is not a pyramid scheme, but there are many scams surrounding Bitcoin so be careful.
- **Bitcoin will collapse after 21 million coins are mined.** Bitcoin has a limit to the number of tokens it will release. That number is hard-coded at 21 million. The estimated date of Bitcoin issuing its last coin is believed to be in the year 2140. No one can predict what will happen at that point, but miners will always earn some profit from transaction fees. Plus, users of the blockchain and the Bitcoins themselves will be incentivized to protect the network, because if mining stops, Bitcoins become vulnerable and so does the data that has been locked into the blockchain.
- **Enough computing power could take over the Bitcoin network.** This is true, but it would be extremely difficult, with little to no reward. The more nodes that enter the Bitcoin network, the harder this type of attack becomes. In order to pull this off, an attacker would need the equivalent of all the energy production of Ireland. The payoff of this sort of attack is also extremely limited. It would only allow the attacker to roll back his own transaction. He couldn't take anybody else's Bitcoins or fake transactions or coins.
- **Bitcoin is a good investment.** Bitcoin is a new and interesting evolution in how people trade value. It isn't backed by any single government or organization, and it's only worth something because people are willing to trade it for goods and services. People's willingness and ability to utilize Bitcoin fluctuates a lot. It's an unstable investment that should be approached cautiously.

Bitcoin: The New Wild West

The Bitcoin world is much like the early days of the Wild West. It's best to approach cautiously until you figure out who the good guys and bad guys are and which saloon serves the coldest beer. If you fall victim to a scam, you'll have little to no protection.

WARNING

Bitcoins and other decentralized cryptocurrencies are considered currency in many countries, but there is little to no oversight or protection in place for consumers.

In this section, I list three of the common scams that are prevalent in the cryptocurrency world. They all revolve around stealing your coins and look a lot like traditional cons you might already be familiar with. This list isn't exhaustive, and crooks are nothing if not creative, so be very cautious when using Bitcoins. You never know what's around the next corner.

Fake sites

Websites that look like exchanges or web wallets but are fakes have plagued some of the top Bitcoin websites. This type of scam is common in the Bitcoin world and on the web in general. Scammers hope to make money by stealing login information from users or misleading them into sending Bitcoins.

TIP

Always double-check the URL and only use secure websites (those that start with `https://`) to avoid this problem. If a website or claim seems doubtful, check to see if it's listed on `https://db.aa419.org`. This is not an exhaustive list, but has many of the bad players listed.

No, you first!

"Send me your Bitcoins, and then I'll ship you the goods." Smells fishy, right? Scams like this are similar to money wire fraud. In this type of fraud, an individual pretends to sell you something but never delivers.

The semi-anonymous nature of Bitcoins — combined with the inability to do a charge back — make it tough to get your money back. Plus, governments do not currently offer protection for Bitcoin transactions, so you're up that proverbial creek without a paddle.

Fraudsters will try to win your trust by sending fake IDs or even impersonating other people you may know. Always double-check the information they send you.

TIP

The best way to dodge this sort of scam is to listen to your instinct and never put more Bitcoins at risk than you're willing to lose. If there is a way to verify the identity of the person offline, do so.

Get-rich-quick schemes

Crazy get-rich-quick schemes have proliferated the cryptocurrency world. The good news is: It's easy to recognize them if you know what to look for.

Often, you'll be promised massive returns, and there is some kind of recruitment and indoctrination process. This process could include things like sales training, asking you to recruit your friends and family, and promising that this is a risk-free investment and that you'll never lose your money. This includes never give anyone access to your private keys.

The bottom line: If a scheme looks too good to be true, it probably is. No matter what, take a hard look at how the investment is generating value outside of what you'll receive from your investment. If there is no clear and rational reason that a significant amount of value is generation rate, it's a scam.

TIP

Run all investments by a lawyer and a CPA. They can help you understand your risks and tax implications.

Mining for Bitcoins

You can get started earning Bitcoins in a variety of ways. Mining for Bitcoin is how to earn Bitcoins by participating in the network. It's usually handled by special mining hardware that is expensive and specialized. The equipment also needs Bitcoin mining software to connect to the blockchain and your *mining pool* (a collaboration of many miners jointly work together and then splitting the rewards of their efforts).

Here are three standard ways to explore mining Bitcoin:

- **Bitcoin-QT:** The Bitcoin-QT client is the original software written by Satoshi Nakamoto. You can download it at `https://bitcoin.org/en/download`.
- **CGminer:** CGminer is one of the most popular mining software. It is open source and available for Windows, Linux, and OS at `www.github.com/ckolivas/cgminer`.
- **Multiminerapp:** The Multiminerapp is an easy Bitcoin client to run. You can download it at `www.multiminerapp.com`.

REMEMBER

Bitcoin is a very competitive environment, and unless you buy specialized mining equipment, you may never earn any Bitcoins. I don't endorse or recommend any particular mining equipment in this book because the industry is constantly changing and quickly out of date. Expect to pay between $500 and $5,000 per machine on average. Amazon.com is a good place to look. They have a large offering and many customer reviews to help guide you.

Cloud mining allows you to start earning Bitcoins in an industrious afternoon, without the need to download software or buy equipment. Always read the reviews on cloud-mining service providers — the industry has been dodgy in the past. One platform you may want to consider is ECOS. ECOS helps you start cloud mining Bitcoin fairly easily. It also sells equipment with high hash power, a crypto wallet, an exchanger, and cryptocurrency portfolios. Just follow these steps:

1. **Navigate to** `https://ecos.am`**.**
2. **Click on Sign Up.**
3. **Enter your email address and click Next.**

   A verification code is sent to your email address.

   TIP

   Check your spam folder if you don't see a verification code right away.
4. **Enter the verification code you received.**
5. **Create a new password.**

   Use a strong password and store it in a place offline like a notebook. This is important for keeping your account secure.
6. **Enter your cellphone number.**

   A verification code is texted to your phone number.
7. **Enter the verification code you received.**

   Congratulations! You've set up your cloud-mining dashboard. From here, you can navigate to Buy Hashrate, which will let you buy time on a cloud device to start mining your Bitcoin.

WARNING

The return on investment for cloud mining can be negative. Review your options carefully to make sure it's a positive investment.

Making Your First Paper Wallet

A *paper wallet* is a paper copy of your public and private key for your Bitcoins. Because they're completely offline, paper wallets are one of the most secure ways to hold Bitcoins when done correctly. The advantage is that your private key is not stored digitally, so it isn't subject to hacking. That said, paper wallets have some inherent risks that need to be considered:

- You have to store paper wallets securely, because they can be easily stolen if they fall into the wrong hands.

- Regular pieces of paper can be easily damaged by water, fire, or other elements, rendering them unreadable. To prevent this, it may be necessary to store paper wallets in a fireproof, waterproof, or damage-proof container, and to print them on high-quality paper with quality ink. Some people even laminate their paper wallets for added protection.
- The websites used to generate paper wallets can be hacked, so you need to choose a reputable service.

To further increase the security of paper wallets, there are tools available such as Cryptotag, which allow you to store your wallet seed on a nearly indestructible titanium plate. Some popular paper wallet generators include BitAddress, WalletGenerator, and Mycellium Entropy, which is a hardware device specifically designed for generating highly secure paper wallets. You may consider a hardware device for securing large sums.

Making a paper wallet is fairly easy on BitAddress. Just follow these steps:

1. **Go to `www.bitaddress.org`.**
2. **Move your mouse around the screen until the amount of randomness shows 100%.**
3. **Click the Paper Wallet button.**

   This gives the option to create a paper wallet that you can print.
4. **In the Addresses to Generate field, enter 1.**

   You can make several wallets at once, if you need to, but you might as well just start with one to get the hang of it.
5. **Click the Generate button.**

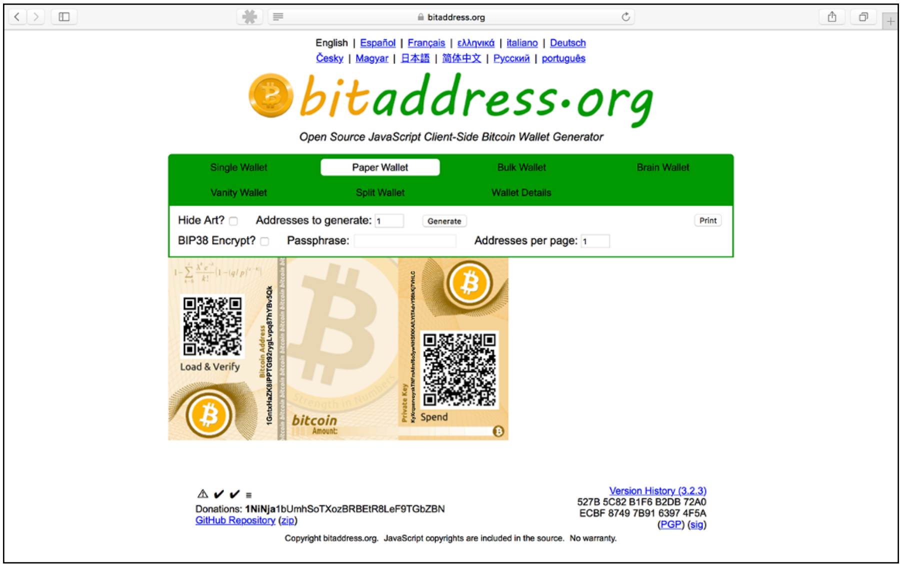
   Figure 4-2 shows a paper wallet I created.
6. **Click the Print button.**

WARNING

Do not let anyone watch you create your paper wallet. This isn't something you want to do at a public computer. Make sure to use a printer that is private and not connected to the Internet so you're not at risk of your private keys being hacked.

TIP

Laminate your paper wallet to make it a little more durable.



Open Source JavaScript Client-Side Bitcoin Wallet Generator

Hide Art? □ Addresses to generate: 1

BIP38 Encrypt? □ Passphrase: Addresses per page: 1

Donations: **1NiNja**1bUmhSoTXozBRBEtR8LeF9TGbZBN
GitHub Repository (zip)

Version History (3.2.3)
527B 5C82 B1F6 B2DB 72A0
ECBF 8749 7B91 6397 4F5A
(PGP) (sig)

Copyright bitaddress.org. JavaScript copyrights are included in the source. No warranty.

FIGURE 4-2: A paper wallet.

IN THIS CHAPTER

» Seeing how and why Ethereum started

» Discovering the Ethereum blockchain

» Uncovering blockchain hacks

» Getting started with Ethereum

» Creating a decentralized autonomous organization

» Creating your own token

» Building smart contracts and decentralized corporations

Chapter 5
Encountering the Ethereum Blockchain

The Ethereum project is one of the most developed and accessible blockchains in the ecosystem. It is also an industry leader in blockchain innovation and use cases. Understanding this technology is essential because it's leading the charge in smart contracts, decentralized organizations, and token offerings.

In this chapter, I cover the makeup of Ethereum and explain the new way to build organizations and companies on the Ethereum blockchain. I also go into depth on safety and practical business applications of the Ethereum blockchain. I fill you in on how the project started and where it plans to go.

This chapter sets you up to create your own decentralized organization. I explain how to mine the cryptocurrency on the test net to fuel your projects. After reading this chapter, you'll be able to set up your own Ethereum wallet and trade the token. You'll also be able to generate your own custom token that can be traded globally.

Exploring the Brief History of Ethereum

Ethereum was first described in 2013 in a whitepaper written by Vitalik Buterin, who was very active in the Bitcoin community as a writer and programmer. Buterin saw that there was significantly more potential in Bitcoin than the ability to move value without a central authority. He had been contributing to the colored coin effort within Bitcoin to expand the utility of Bitcoin beyond the trade of its native token. Buterin believed that other business and government use cases that require a central authority to control them could also be built with blockchain structures.

At that time, there was a fierce debate about the Bitcoin network being "bloated" by lots of low-value transactions from applications securing themselves against Bitcoin. The main concerns were that additional applications, built on the Bitcoin protocol, would have problems scaling in volume. Also, at that time there was not the ability to do scripting to allow for things like smart contracts. Bitcoin was not built to handle the number of transactions needed by the applications. Vitalik and many others saw that in order for people to build decentralized applications in the Bitcoin blockchain, either the blockchain would need a massive code overhaul or they would need to build a new blockchain altogether.

Bitcoin had already been well established at that point. It was clear that the kinds of upgrades to core code that were needed were well beyond what was realistically possible. The politics of Bitcoin would stall any changes to the network. Vitalik and his team established the Ethereum foundation in early 2014 to raise funds to build a blockchain network with a programming language built within it. Vitalik hoped to create a network that would allow him to build blockchain-secured applications.

The initial development was funded by an online public crowd sale during July and August of 2014. The foundation initially raised a record $18 million through the sale of its cryptocurrency token called *ether.* People have passionately debated whether this sort of crowd sale is illegal because it may constitute an unlicensed security offering.

The regulatory gray zone has not hindered the project. If anything, the cutting-edge nature of the project has attracted more attention and talent to the foundation. Discontented and disenfranchised developers and entrepreneurs from around the world have flocked to the project. Decentralization is seen as the perfect solution to corrupt and oppressive central authorities.

The $18 million raised in the token sale gave the foundation the funds it needed to hire a large development team to build Ethereum. Ethereum Frontier, the first release of the Ethereum network, went live to the public in July 2015. It was a bare-bones software release that only the more technically savvy could use to build their applications.

Ethereum Improvement Proposals (EIPs) are suggestions for improving the Ethereum network. They can be about changing the way the network works or adding new features. In 2022, EIP-3675 upgraded the Ethereum Mainnet to use a new way of reaching an agreement (consensus) about the state of the network called proof-of-stake (PoS). This changed Ethereum from the original proof-of-work (PoW) consensus mechanism for changes to the block structure, block processing, fork choice rule, and network interface.

PoS is different from PoW because it involves holding onto a certain amount of the Ethereum cryptocurrency to help make decisions about the network instead of using computer power to solve complex math problems. This EIP explains how the upgrade to PoS would work and what changes would need to be made to the network. It was written by Mikhail Kalinin, Danny Ryan, and Vitalik Buterin and has been finalized.

Ethereum: The Open-Source World Wide Computer

Ethereum may be one of the most complex blockchains ever built. It has several of its own *Turing-complete programming languages* (full-functioning programing languages that allow developers to create any application). These new programming languages closely resemble popular programming languages such as JavaScript and Python. The Ethereum protocol can do just about anything that your regular programming languages can do. The exception is that the code is written to the Ethereum blockchain and has the added benefits and security that comes with that. If you can imagine a software project, it can be built on Ethereum.

The Ethereum ecosystem is currently the best place to build decentralized applications. It has lovely documentation and user-friendly interfaces that get you up and running quickly. Rapid development time, security for small applications, and the ability for applications to easily interact with one another are key characteristics of this system.

The Turing-complete programming languages are the main feature that makes the Ethereum blockchain vastly more potent than the Bitcoin blockchain for building new programs. Ethereum's scripting language makes things like Twitter applications possible in few lines of code, and extremely secure.

Smart contracts, like the one you create in Chapter 3, can also be built on Ethereum. The Ethereum protocol has opened up a whole new genre of applications. You can take just about any business, government, or organization's processes and build a digital representation of it inside of Ethereum. Currently, Ethereum's platform is being used to manage *digital assets* (a new class of asset that lives online and may represent a whole digital asset such as a Bitcoin token or a digital representation of a real-world asset such as corn commodities), financial instruments (like mortgage-backed securities), recording ownership of assets such as land, and decentralized autonomous organizations (DAOs). Ethereum has also sparked a major fundraising effort by startups globally that used the ERC token standard to raise capital to build their innovations. Ethereum has opened a new way of organizing business, nonprofit, and government. It has made it possible to hold, share, and trade value without ever meeting the other party or using a third party to facilitate. The code does the work.

Decentralized applications: Welcome to the future

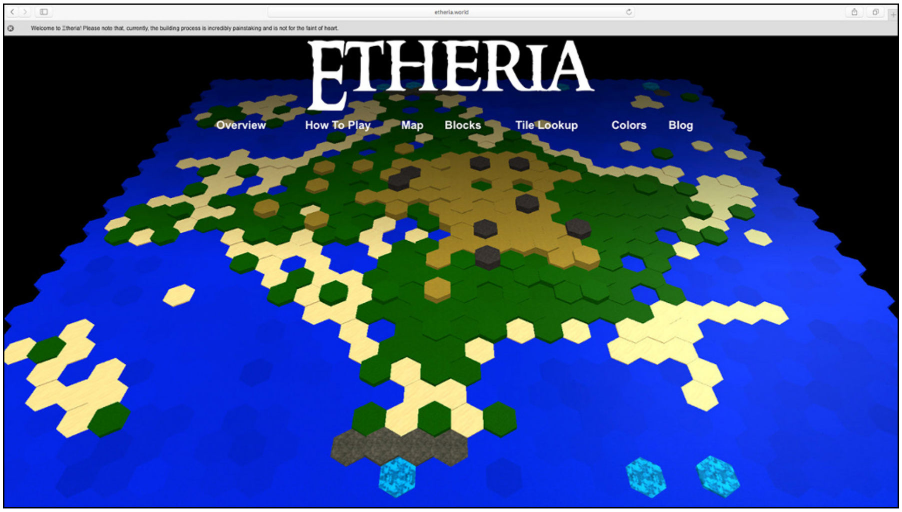
The most revolutionary and controversial manifestation of Ethereum is the self-governing and decentralized application (dApp). dApps can manage things like digital assets and DAOs.

dApps were created to replace centralized management of assets and organizations. This structure has a lot of appeal because many people believe that absolute power corrupts absolutely. For those who are fearful of losing control, this type of structure has massive implications.

New dApps are popping up every day. You can explore and discover new ones built on Ethereum by going to `https://dappradar.com`. DappRadar updates a list of all the latest Ethereum dApps and gives you a preview of what they do. One of the first ever created was Etheria (see Figure 5-1).

The power of decentralized autonomous organizations

DAOs are a type of Ethereum application that represents a virtual entity within Ethereum. When you create a DAO, you can invite others to participate in the governance of the organization. The participants can remain anonymous and never meet, which could trigger Know Your Customer (KYC) rules (the process a business must go through to verifying the identity of its clients) and Anti-Money Laundering (AML; the laws and regulations designed to stop the practice of generating income through illegal means) compliance issues.

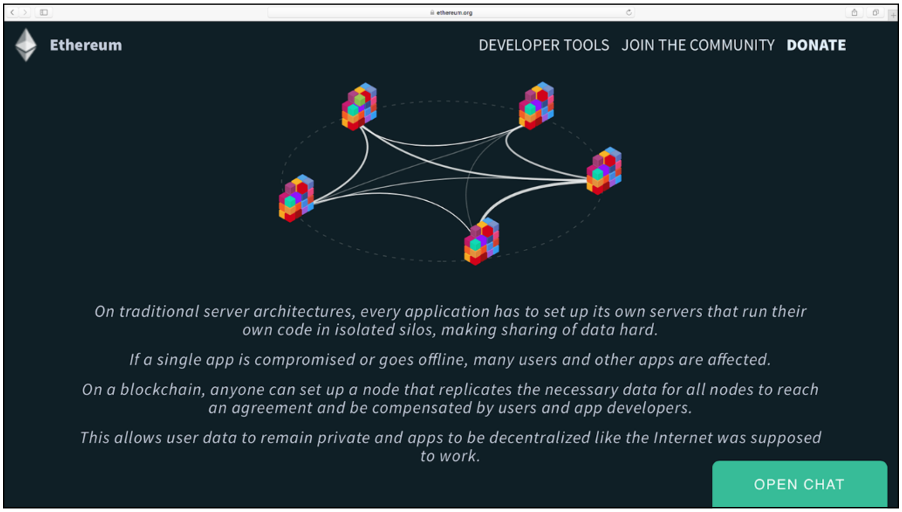


Welcome to Ξtheria! Please note that, currently, the building process is incredibly painstaking and is not for the faint of heart.

FIGURE 5-1: The world's first immortal digital game, Etheria.

DAOs have been created for raising funds for investing, but they could also be designed for civic or nonprofit purposes. Ethereum gives you a basic framework for governance. It's up to the organizers to determine what's being governed. Ethereum has created templates for you to help in the creation of DAOs.

Figure 5-2 shows a depiction of the organization of an Ethereum application.



On traditional server architectures, every application has to set up its own servers that run their own code in isolated silos, making sharing of data hard.

If a single app is compromised or goes offline, many users and other apps are affected.

On a blockchain, anyone can set up a node that replicates the necessary data for all nodes to reach an agreement and be compensated by users and app developers.

This allows user data to remain private and apps to be decentralized like the Internet was supposed to work.

FIGURE 5-2: Ethereum.org blockchain application depiction.

Here's how DAOs basically work:

1. A group of people writes a smart contract to govern the organization.
2. People add funds to the DAO and are given tokens that represent ownership.

   This structure works kind of like stock in a company, but the members have control of the funds from day one.
3. When the funds have been raised, the DAO begins to operate by having members propose how to spend the money. Voting may be affected by how much Ether the member risks or stakes in the DAO.
4. The members vote on these proposals.
5. When the predetermined time has passed and the predetermined number of votes has accrued, the proposal passes or fails.
6. Individuals act as contractors to service the DAO.

Unlike most traditional investment vehicles, where a central party makes decisions about investments, the members of a DAO control 100 percent of the assets. They vote on new investments and other decisions. This type of structure threatens to displace traditional financial managers.

DAOs are built with code that can't be changed on the fly. The appeal of this is that malicious hackers can't monkey with the funds in a traditional sense. Hackers can still find ways to execute the code in unexpected ways and withdraw funds. The immutable nature of a DAO's code makes it nearly impossible to fix any bugs once the DAO is live in Ethereum.

WITH GREAT POWER COMES . . . GREAT POWER

The first Ethereum DAO ever built is called, confusingly enough, "The DAO." It's an example of some of the dangers that come with decentralized and autonomous entities.
It is the largest crowdfunded project in the world — its founders raised approximately $162 million in 26 days with more than 11,000 members. What people had thought was the greatest strength of The DAO became its greatest weakness. The immutable code within The DAO locked into place how the organization would be governed and how funds would be distributed. This allowed the members to feel secure in their investment. Although the code was well reviewed, not all the bugs had been worked out.

The first significant threat to Ethereum came from the hack of The DAO. An unexpected code path in The DAO's contract allowed any sophisticated user to withdraw funds. An unknown user managed to remove about $50 million before he could be stopped.

The Ethereum community debated bitterly about whether it could or should reclaim the ether. The DAO hacker had not technically done anything wrong or even hacked the system. Fundamentalists within the Ethereum community felt that code was law and, therefore, nothing should be done to recover the funds.

The very thing that made Ethereum strong was also its greatest weakness. Decentralization, immutability, and autonomy meant no central authority could decide what to do quickly. There was also no one to punish for the misuse of the system. It really did not have any consumer protection measures. It was a new frontier, like the software name suggested.

After spending several weeks discussing the problem, the Ethereum community decided to shut down The DAO and create a new Ethereum. This process is called *hard forking*. When the Ethereum community hard-forked the network, it reversed the transaction the hacker had committed. It also created two Ethereums: Ethereum and Ethereum Classic.

Not everyone was in agreement with this decision. The community continues to use Ethereum Classic. The tokens for Ethereum Classic are still traded but have lost significant market value. The new Ethereum token still hasn't regained its old high from before the hack.

The decision to fork rocked the blockchain world. It was the first time a majority blockchain project had hard-forked to make whole an investor. It called into question many of the principles that make blockchain technology so attractive in the first place.

Hacking a Blockchain

Ethereum has never been hacked. The hard fork in 2016 due to the DAO hack mentioned in the "With great power comes . . . great power" sidebar was not an actual hack of the system, but confusingly is often referred to as a hack. Ethereum worked perfectly. The problem was it was too perfect. It became necessary to restart the system when a large amount of money and a majority of its users were threatened.

The only way to correct an action on a blockchain like Ethereum is to do a *hard fork*, which allows for a fundamental change to the protocol. A hard fork makes previously valid blocks and transactions invalid. Ethereum did this to protect the funds that were being pulled out of the first DAO by a user. The DAO hack was conceptually, one of the largest bug bounties ever.

That said, many scams and hacking attempts occur in the cryptocurrency space. Most of these attacks target centralized exchanges and applications. Many hackers want to steal cryptocurrency. It has real value and isn't protected in the same ways that regular money is protected by governments. The anonymous nature of cryptocurrency also makes it appealing to crooks. Catching and prosecuting these individuals is difficult. The cryptocurrency community is fighting back, however, and creating new measures to protect themselves.

REMEMBER

Hacking one place is significantly easier and cheaper than trying to overcome a decentralized network. When you read about hacking in the blockchain world, it's likely just a website or a cryptocurrency wallet that has been hacked, not the whole network.

Unearthing Ethereum DAOs

Ethereum was built for DAOs. Ethereum is, in effect, its own DAO. It uses consensus from its distributed nodes to govern its function. Ethereum developed smart contract code that can't be modified after it's published; this allows the DAO to function by the rules the participants have agreed on at inception. Finally, smart contracts are the trusted third party for when you need to send or receive funds.

In the following sections, I cover the importance of setting up your DAO for the future. I also dive into the concept of delegation in DAOs, which allows token holders to delegate their votes to nominated individuals who will represent them and steward the Ethereum protocol. Many DAOs use delegation as a management tool for day-to-day operations.

DAO governance

You'll need to consider many things when creating or joining a DAO. Given that it's nearly impossible to change the rules or reverse a transaction after a DAO smart contract has been published, make sure to consider how voting and proposals work.

DAO DELEGATION

Delegation works a lot like how people elect officials to represent them in government. The DAO version of representative democracy requires token holders to delegate their votes to users who have been nominated. The nominated individuals then commit to stewarding the Ethereum protocol and stay actively involved.

An example is ENS, the most widely integrated naming standard for blockchain. At the time of writing this book, more 500,000 users had registered more than 2.6 million names. ENS token holders can delegate their votes to engaged community members to represent them within the ENS DAO.

CLAIMING YOUR NAME ON ENS

In this section, you dive into Ethereum Name Service (ENS) to claim a name on ENS. You do this by going to the ENS website, logging in with your MetaMask wallet, and searching for and registering your desired name. This process is to purchase a domain name. Just follow these steps:

1. **Navigate to `https://claim.ens.domains`.**
2. **Click your MetaMask wallet in your web browser.**

   This will log you into the ENS website. If you haven't yet set up your MetaMask wallet, head back to Chapter 3 and follow the instructions.
3. **Click Go to App.**
4. **Enter the name you would like to reserve.**

   Think of this name as you would a website domain.
5. **Click Search.**
6. **Click Register.**

If the name you wanted is available, you'll have the option to buy it as you would a domain. Repeat this process with a new name if your desired name is not available.

Congratulations! You've now secured your first Web 3.0 domain!

AUTOMATIC TRANSACTION GOVERNANCE ON DAOs

In many DAOs, transactions will be automatically executed if a quorum of members votes affirmative. A *quorum* is the number of members that the smart contract specifies are required to pass a new transaction. A prominent example of this is Nouns DAO (`https://nouns.wtf`). The Nouns DAO enables a transaction to be automatically executed if a quorum of votes is met for the transaction.

THE MULTISIG GOVERNANCE OF DAOs

Although DAOs may have thousands of voting members, the actual governance of funds is controlled by a wallet shared by 5 to 20 active community members. These members are trusted, and their public identities are usually known to the community. Normally when a proposal is made to the DAO, the members will vote for approval. Each voting member does this via a transaction on Ethereum using multisig.

A multisig (short for multisignature) address is a type of address that requires multiple signatures to authorize a transaction. This can also be used to add an extra layer of security to a cryptocurrency wallet or account.

For example, let's say you have a multisig address that requires two signatures to authorize a transaction. You could set it up so that one signature is required from your personal device, and another is required from a device belonging to a trusted friend. This means that in order to send funds from the multisig address, both you and your trusted friend would need to sign the transaction using your respective devices. By adding this feature, it adds an extra layer of security to their transactions and requires the consent of multiple parties.

Multisig addresses can also require more than two signatures, depending on the specific implementation. A DAO could potentially require thousands or more signatures. Imagine if a government used a DAO as the infrastructure to authorize the passing of new laws or voting for the election of public officials. The multisig feature is useful for organizations that want to organize in a world that is trustless.

Overall, multisig addresses can be a useful tool for adding an extra layer of security to cryptocurrency transactions, DAO, token offerings, and especially in cases where multiple parties need to be involved in the authorization process.

DAO membership

You can become a member of a DAO via a few different models. Your membership typically revolves around voting rights that you're granted through the smart contract. There are several common DAO structures:

THE LEGALITY OF DAO

In 2021, Wyoming became the first state to establish laws recognizing DAOs as a legal business entity. As of the writing of this book, Wyoming, Vermont, and the Virgin Islands have DAO laws in some form.

A notable example of a recognized DAO is the CityDAO, which used Wyoming's DAO law to buy 40 acres of land near Yellowstone National Park to build an on-chain, community-governed, crypto city.

- **Token-based membership:** Token-based membership means you're a member by default just by holding the DAO token. These types of DAO are ordinarily open to anyone with the ways and means to join — often called *fully permissionless.* Your governance tokens can be traded permissionless on a decentralized exchange and may even have some monetary value. It's also possible to have a nontransferable token; these types of tokens are called *soul bound.* Other types of DAOs require you to gain tokens by performing services, such as providing liquidity or doing proof-of-work to secure transactions.

  An interesting example of this type of DAO is the MakerDAO. Its token, MKR, is used on decentralized exchanges, and you can buy it and gain voting power on the Maker protocol. The Maker protocol allows you to create a price-stable currency that you control called, Dai. Dai powers a growing ecosystem of more than 400 apps, including wallets, decentralized finance (DeFi) platforms, and games.

- **Share-based membership:** Share-based DAOs are more permissioned groups that require you to submit a proposal to join the DAO. They also often require you to pay for membership through tokens or work you perform for the group. Your tokens represent your voting power and ownership. Usually, you can leave the DAO at any time with your proportionate share of the DAO's treasury.

  These types of DAO are created for human-centric organizations like charities, worker collectives, and investment clubs. The MolochDAO is a fantastic example of this type of DAO. The members of MolochDAO contribute capital to fund the development of Ethereum. It acts as a nonprofit focused on infrastructure as an essential digital public good. MolochDAO requires a membership proposal so the group can assess whether you have the necessary expertise and capital to make informed judgments about potential grantees. You can't buy access to the DAO.

- **Reputation-based membership:** Another interesting DAO structure is reputation-based membership, which is a proof-of-participation structure that grants you voting power within the DAO. Reputation-based DAOs don't transfer ownership to contributors — this is a soul-bound structure. Reputation can't be bought, assigned, or delegated to someone else. You earn your reputation through your participation. Voting is permissionless when you have your soul-bound token. Prospective members can submit proposals to join the DAO. New requests receive reputation and tokens as a reward for their contributions. This type of DAO is great for decentralized development and governance of protocols and dApps.

The DXdao uses this type of structure. Members of the DAO develop, govern, and grow DeFi products. Spawned in May 2019, DXdao is a collective of some 400 individuals focused on the DeFi ecosystem. It's a fascinating example of a global sovereign collective. DXdao leverages reputation-based governance and holographic consensus to coordinate and manage funds. You can't buy your way into it.

Understanding smart contracts

Ethereum smart contracts are like contractual agreements, except there is no central party to enforce the contract. The Ethereum protocol "enforces" smart contracts by attaching economic pressure. They can also enforce implementation of a requirement if it lives within Ethereum, because Ethereum can prove certain conditions were or were not met. If it doesn't live within Ethereum, it's much harder to enforce.

WARNING

Ethereum smart contracts are not yet legally enforceable and may never be because the perception is that you don't need outside authorities enforcing agreements. Legal systems are controlled by governments. As they stand now, governments are central authorities — some with more or less consent and democratic principles. Within an Ethereum smart contract, each participant has an inalienable vote.

Ethereum smart contracts do not include artificial intelligence. This is a cool possibility in the near future. But for now, Ethereum is just software code that runs on a blockchain.

Ethereum smart contracts are not safe. The DAO hack is a great example of the type of dangers that can occur. It is still early days, and putting a lot of money into an unproven system isn't smart. Instead, experiment with small amounts until all the bugs have been worked out of new contracts.

Discovering the cryptocurrency Ether

Ether is the name of the cryptocurrency for the Ethereum blockchain. It was named after the substance that was believed to permeate all space and make the universe possible. In that sense, Ether is the substance that makes Ethereum possible. Ether incentivizes the network to secure itself through proof-of-work mining, like how the token Bitcoin incentivizes the Bitcoin network. Ether is needed to execute any code within the Ethereum network. When utilized to execute a contract in Ethereum, Ether is referred to as *gas.*

Executing the code within a smart contract also costs some amount of ether. This feature gives the token added utility. As long as individuals want to use Ethereum for applications and contracts, ether will hold a value beyond speculation.

The wild growth in the value of ether has made it a popular token to speculate on. It's widely traded on exchanges around the world. Some new hedge funds are looking at it as an investment vehicle. However, the volatile nature and low market depth make ether a risky investment.

Getting Up and Running on Ethereum

In this section, I walk you through how to get started in the Ethereum blockchain ecosystem. Before you can build anything on Ethereum, you need an Ethereum wallet.

REMEMBER

Your wallet will hold your Ethereum tokens called *ether.* Ether is the cryptocurrency that allows you to create smart contracts inside Ethereum. This is sometimes referred to as *gas.*

Downloading the Ethereum wallet can take some time, but the interface is very intuitive and the instructions provided throughout the process are easy to follow.

TIP

Within the Ethereum wallet, you can win test ether to build your test contracts and organizations. You don't need to mine ether to learn how it works.

Mining for ether

Ethereum is kept running by a network of computers all over the world that are processing the contracts and securing the network. These computers are sometimes referred to as *nodes,* and they're mining crypto ether.

In order to reward individuals for the time and cost involved in mining, there is a prize of five ethers about every 12 seconds. The prize is given to the node that was able to create the latest block in the Ethereum blockchain.

All new blocks have a list of the latest transactions. The proof-of-work consensus algorithm guarantees that prizes are won most often by nodes with the most computational power. Computers that aren't as powerful can win, too — it just takes longer. If you want to try your hand at mining ether, you can do it with your home computer, but it will take a very long time to successfully mine a block and win ether.

WARNING

Mining ether is not for the technical novice. You need to be familiar with command line. If you don't have a clue what command line is, you probably want to skip this process. Also, be sure to follow the most up-to-date instructions on the Ethereum GitHub (`http://github.com/ethereum`).

Setting up your Ethereum wallet

To set up your Ethereum wallet, follow these steps:

1. **Go to `www.ethereum.org`.**
2. **Click the Download button.**

   You have to scroll down the page a bit to find the button.

   TIP

   Be sure to save the Ethereum wallet download someplace you can find it later.
3. **Open the Ethereum wallet.**

   You may need to check for updates to the software under Help.
4. **Choose Develop in the drop-down menu.**
5. **Select One of the Test Networks such as Robsten or Rinkeby.**

   Here you get set up to mine test ether. This process is much less time-consuming than real ether mining, but it still takes some time — currently, it's about two hours.
6. **Create a strong password.**

   Don't forget to save your password someplace safe.
7. **Click through the startup menu.**

   The Ethereum team has a few tutorials that are interesting to review while you're waiting on your test net to download. The download may take ten minutes or so.
8. **Choose Develop ➪ Start Mining.**

   Don't skip this step. You need the ether for later projects.

You've just set up your wallet, and you're earning test ether for your future smart contract projects.

Building Your First Decentralized Autonomous Organization

DAOs will change how the world does business in the future. They allow anyone in the world to create a new type of company online that is governed by pre-agreed-upon rules that are then enforced through the blockchain network. Creating a DAO is easier than you might think. In this section, you build your first test DAO. I break this project into three sections: build, congress, and governance.

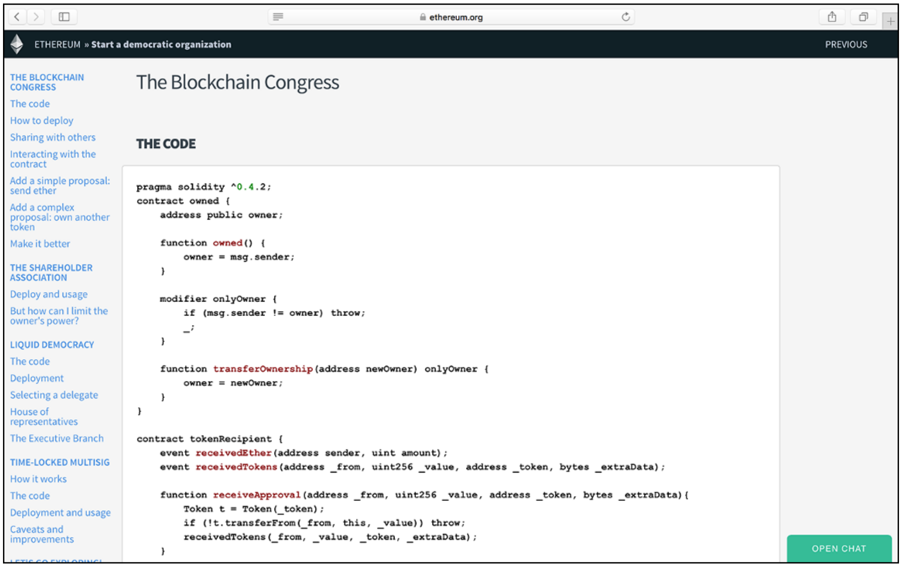
REMEMBER

In order to successfully complete your test DAO, you need to have set up your Ethereum wallet and done some mining on the Ethereum test net (see the preceding section).

Follow these steps to create your first test DAO:

1. **Go to `www.ethereum.org/dao`.**
2. **Scroll down the page to the Code box (shown in Figure 5-3) and copy the code.**
3. **Open the Ethereum wallet you made earlier.**

   You'll develop your DAO in your Ethereum wallet.



The Blockchain Congress

THE CODE

```
pragma solidity ^0.4.2;
contract owned {
    address public owner;

    function owned() {
        owner = msg.sender;
    }

    modifier onlyOwner {
        if (msg.sender != owner) throw;
        _;
    }

    function transferOwnership(address newOwner) onlyOwner {
        owner = newOwner;
    }
}

contract tokenRecipient {
    event receivedEther(address sender, uint amount);
    event receivedTokens(address _from, uint256 _value, address _token, bytes _extraData);

    function receiveApproval(address _from, uint256 _value, address _token, bytes _extraData){
        Token t = Token(_token);
        if (!t.transferFrom(_from, this, _value)) throw;
        receivedTokens(_from, _value, _token, _extraData);
    }
```

FIGURE 5-3: The Code box.

Test net and congress

The next phase of your DAO project is setting up the framework for your DAO. Follow these steps:

1. **In your Ethereum wallet, choose Develop ➪ Network ➪ Test Net.**
2. **Click the Contracts tab and then click New Contract.**

   The Ethereum team has set up a few test templates for DAOs.
3. **Paste the code you copied in the preceding section into the Solidity code box.**

   Make sure you're selecting Solidity Contract Source Code on the tab and not Contract Byte Code.
4. **From the Contract Picker, choose Congress.**
5. **Pick some variables when prompted to do so.**

   Here are your options:

   - The *minimum quorum* for proposals is the fewest votes a proposal needs to have before it can be executed.
   - The *minutes for debate* is the shortest amount of time, in minutes, that needs to pass before it can be executed.
   - The *margin of votes* for a majority. Proposals pass if there are more than 50 percent of the votes plus the margin. Leave it at 0 for a simple majority.

Governance and voting

Now you're going to name and set up the governance of your DAO. You need to set up a *minimum quorum* for proposals (how many votes a new proposal needs to have before it is passed). You also set up the *margin of votes for a majority* (how many votes a plan needs to pass) and the time allotted for discussing new plans.

1. **Name your new DAO.**

   This is kind of like naming a company.
2. **For Debate Times, select 5 minutes.**

   This is how long new proposals are open for conversation.
3. **Leave Margin of Votes for Majority set to 0.**

   This sets up how the democracy of your contract works.

4. **Confirm the price of the DAO.**

   You've mined some Ether in the test net via your wallet when you first set it up. If you skipped that step, go back and do it now. You need a little of the test net Ether to build your DAO.

5. **Click Deploy and type your password.**

   The DAO may take some time to deploy. When you arrive at your new dashboard, scroll down, and you'll be able to see your DAO being produced.

6. **Click the New icon.**

   A new unique icon will generate that represents your DAO.

Congratulations! You've created your first DAO.

Uncovering the Future of DAOs

Smart contracts and decentralized organizations hold a lot of promise. The pure democratic and hyper-rational nature of them is very appealing. However, at this point, there are more possibilities then knowns, and each contract that is created could be groundbreaking or a massive flop.

If you approach Ethereum as the new frontier that it is, you'll have more success. The Ethereum network has more benefits than drawbacks if you're careful. But expecting everything to work flawlessly and all the participants to act with integrity will open you up to greater losses. Ethereum has its share of bandits, not to mention those friendly enthusiasts who would like you to succeed.

The smart contract hacks of 2016 have highlighted the importance of security and properly reviewing contracts. It also illustrated that there are people with integrity who fight to fix issues.

Reading this book is only the beginning. It will give you a sound base to build your knowledge of Ethereum, but as with all new technologies, Ethereum is quickly evolving. Keep reviewing best practices and security measures.

In the following sections, I mention some things to keep in mind as you build your first few DAOs, build smart contracts, and debug your new blockchain systems.

Putting money in a DAO

Don't trust large sums of money to untested contracts and contracts that haven't been fully vetted. Large contracts are more often targeted by hackers. The DAO hack described earlier in this chapter (see the sidebar "With great power comes . . . great power") showed that even well thought-out contracts have unexpected weaknesses.

REMEMBER

Although smart contracts and blockchains let you conduct business with anyone around the world, it's still the early days. You can mitigate your risk by working only with known and trusted parties.

TIP

The security landscape will constantly be evolving with new bugs. Reviewing all new best practices is imperative. Manage the amount of money you're putting at risk and roll out contracts slowly and in phases. Ethereum is a new technology, and mature solutions are not yet built.

Building smarter smart contracts

Smart contract programming requires a different mind-set than standard contract writing. There is no third party to make things right if the contract executes in a way that you didn't expect or intend. The immutable and distributed nature of blockchains makes it tough to change an unwanted outcome.

REMEMBER

Your contract will have flaws and may fail. Build safety valves into your contracts so you can respond to bugs and vulnerabilities as they come up. Smart contracts also need an off switch that let you pull the plug and pause your contract when things are going wrong.

TIP

If your contract is big enough, offer bug-hunting bounties that incentivize the community to find vulnerabilities and flaws in your contract.

As with many things, the complexity of your contract also increases the likelihood of errors and attack vectors. Keep your contract logic simple. Build out small modules that hold each section of the contract. Creating a contract in this manner will help you compartmentalize any issues.

Finding bugs in the system

Don't reinvent the wheel by building your own tools such as random number generators. Instead, leverage the work that the community has already done and that has been well tested.

WARNING

You can only control for things within your own contract. Be cautious of external contract calls. They can execute malicious code and take away your control.

The Ethereum community has an excellent known bug list and even more helpful tips on how to build secure smart contracts on its GitHub page at `https://github.com/ethereum/wiki/wiki/safety`.

Uncovering DAOhaus on Ethereum

DAOhaus is a no-code platform for creating and managing a DAO. The DAOhaus app allows you to:

- Create a DAO.
- Add members to the DAO.
- Coordinate proposals with a user-friendly interface.

The DAOhaus app has three components: the smart contract, the subgraphs, and the client.

- **Smart contract:** DAOhaus uses Moloch DAO's smart contracts to facilitate on-chain DAO functionalities. For example, you can add members via proposals and treasury. Because DAOhaus is a no-code platform, it interfaces with Moloch contracts for all on-chain actions and features so you don't need to. Currently, the DAOhaus app supports Moloch v2 DAOs using the following contracts:

  - Moloch v2.1 and 2.5 are multi-summoner capabilities, plus a register function for metadata and EIP-1167 proxy pattern to reduce gas costs.
  - Minion gives you the ability to interact with your smart contracts while keeping funds safe in a third-party vault called Gnosis Safe.

  The DAOhaus app is scheduled to be using Moloch v3 (Baal) by the end of 2023.

- **Subgraphs:** DAOhaus uses The Graph, an indexing protocol for querying networks like Ethereum and IPFS. You can build and publish open application programming interfaces (APIs), called *subgraphs,* making data easily accessible and monetizable. The subgraphs ensure that on-chain data is indexed and available for querying. An indexing protocol incentivizes and coordinates the indexing of public blockchain data. You can find data on all compatible DAOs instantly using The Graph. You can find out more about The Graph at `https://thegraph.com`.

- **Client:** The client is software that allows you to access and interact with the DAO. It's built using the React framework, which is a popular JavaScript library for building user interfaces. The client allows the user to reference on-chain data from subgraphs, which are data structures that store information about a blockchain in a more organized and easily accessible way. Subgraphs can be used to index and query data on the blockchain, making it easier to work with and analyze. The client can also be used to perform on-chain functionality, which refers to actions that take place on the blockchain itself. For example, the client can be used to interact with Moloch smart contracts, which are self-executing contracts with the terms of the agreement between the buyer and seller being directly written into lines of code. The client allows the user to execute these smart contracts and interact with them on the blockchain.

Building and configuring your own DAO club on DAOhaus

In this section, you build and configure your own DAO on DAOhaus, a platform that provides tools and resources for creating and managing DAOs.

REMEMBER

A DAO is a type of organization that is run on blockchain technology and is governed by a set of rules encoded in a smart contract. DAOs allow individuals or groups to collaborate and make decisions in a decentralized manner, without the need for a central authority.

The DAOhaus platform offers a variety of features and tools for managing a DAO. It allows members of a DAO to comanage funds in a shared treasury and monitor fund transfers. The platform provides share-based voting, allowing members to create and vote on a variety of proposal types. It also includes a marketplace of community-developed "boosts" that provide custom functionality for DAOs. Because humans don't always get along, the DAOhaus allows grace periods and "ragequit" functionality to protect the investments of DAO members. DAOhaus is owned and operated by community members and provides opportunities for you to get involved in the cultivation of the platform.

You can set up your DAO by visiting the DAOhaus website and logging in using your MetaMask wallet. You'll also need to add the addresses of the members who will be participating in the DAO with you. If you're doing this on your own, you can just create a second address. If you have other people that you want to add, you'll need to get their Ethereum addresses first. When you're done, you and the other members will be able to start making decisions and participating in the organization.

Follow these steps to set up your DAO:

1. **Go to** `https://app.daohaus.club`**.**
2. **Click your MetaMask wallet to log in.**
3. **Click Clubs.**

   If you don't see this option, go to `https://app.daohaus.club/summon`.
4. **Click Add Multiple Summoners.**

   Make sure that there is one address populated. You can add more if you want.
5. **Click Summon.**
6. **Within your MetaMask wallet, click Confirm.**

TIP

Set your gas fee to the lowest level to cut your cost of setting up your DAO. You can do this from within your MetaMask wallet.

Configuring a DAO involves setting up the rules and governance structure for the organization. This includes determining how decisions will be made, who can participate in decision-making, and what actions can be taken by the DAO. There are various ways to configure a DAO, and the specific approach will depend on your needs and goals in the future. Some common elements include:

- **Voting rules:** How votes will be conducted and what percentage of the vote is needed to pass a decision
- **Membership rules:** Who you deem is eligible to join the DAO and how someone can become a member
- **Token distribution:** How ownership in the DAO will be distributed among members
- **Funding rules:** How you'll fund the DAO and how the funds will be allocated to different projects or initiatives
- **Decision-making process:** The process you'll follow when making decisions, and who will have the authority to make decisions on behalf of the DAO

After a DAO has been configured, it can be used to facilitate decentralized decision-making and enable your members to collaborate and work toward shared goals.

To configure your DAO club, follow these steps:

1. **Click Configure.**

   A new window opens allowing you to update the information about your organization.

2. **Enter the details for your club in the form.**

   You can go back and edit these details — they aren't part of the smart contract.

3. **Click Save.**

Now you have a fully functional DAO club.

Creating Your Own ERC20 Tokens

In this section, I show you how to create your own token using Polymath. Polymath is a security token service that is built on the Ethereum blockchain. It has taken the hard work out of programming your own token on Ethereum. Polymath offers a point-and-click interface that anyone can use.

Before you read through this section, make sure that you've set up MetaMask. If you haven't, refer back to Chapter 3, where you find detailed instructions for setting up your computer and downloading MetaMask.

You also need to get your hands on some Kovan Test Ether (KETH) in order to set up the smart contracts for your new token. KETH is the test Ether from the Kovan test network, a test network for developers working on Ethereum applications. KETH has no market value. You can obtain it for free if you have a GitHub account.

In this section, I walk you through how to set up your GitHub account, how to request KETH, and how to create your tokens.

Seeing up your GitHub account

GitHub is a development platform for storing code you develop. GitHub offers free accounts for open-source projects. So, if you're comfortable sharing the code you've developed, GitHub is a fantastic source for managing your projects and building software. GitHub also offers a paid version if you want to keep your code private. For the purposes of this section, a free account will work great.

To open a GitHub account, follow these steps:

1. **Open the Brave web browser.**

   If you don't yet have the Brave browser, go to Chapter 3.

2. **Navigate to** `https://github.com`**.**
3. **Enter your desired credentials.**
4. **Click Sign Up for GitHub.**

You're all set.

Requesting KETH on the Gitter Faucet

To request KETH, follow these steps:

1. **Open the Brave web browser.**
2. **Navigate to** `https://gitter.im/kovan-testnet/faucet`**.**
3. **Click Sign In to Start Talking.**
4. **Select Sign In with GitHub.**

Next, you'll grab your MetaMask account address so you can paste it into the social chat window and allow one of the community members to send you some KETH. Follow these steps:

REMEMBER

1. **Open your MetaMask account.**

   To open your MetaMask account, click the fox icon in the upper-right corner of your Brave browser window.

2. **From your MetaMask account, click the pull-down tab.**
3. **Select Kovan Test Network.**
4. **Copy your MetaMask address by clicking Account 1.**

Now you're ready to request some test Ether called KETH form the Kovan community. You'll take your Kovan Ethereum address from your MetaMask account and post it in the chat window. Make sure to only post your address. Follow these steps:

1. **Navigate back to** `https://gitter.im/kovan-testnet/faucet`.
2. **Paste your copied address into the chat window.**

Now you'll need to wait because one of the community members will check out your GitHub account and make sure you aren't spamming the network. This may take some time because the process of sending you KETH is done manually. You'll see the KETH in your MetaMask account after the transaction is complete. This process took me three days, but I worked on it over a holiday weekend.

To set up your Polymath account, follow these steps:

1. **Open the Brave web browser.**
2. **Navigate to** `https://tokenstudio.polymath.network`.
3. **Click Create Your Security Token.**
4. **Navigate to the fox icon for your MetaMask wallet.**
5. **Click Sign from within MetaMask.**

Creating your tokens

Now that you have the prerequisite KETH needed to create your own token, you can finally get started. In this section, you use the Polymath smart contract to build a custom Ethereum ERC20 token.

Reserving your token symbol

Polymath allows you to reserve your token symbol for 60 days. This reservation process is essential for setting up your token. You can check what names have already been taken by going to Etherscan (`https://etherscan.io/token`) and searching for the name you're thinking about using.

TIP

Reserving your name with Polymath only protects you within the Polymath system. It will not prevent someone else from issuing a token of the same name on Ethereum.

Go into your Jaxx wallet and use the Shapeshift service to exchange some of your BTC or Ether for POLY. After you've done this, move your new POLY tokens from your Jaxx wallet to your MetaMask account. (Chapter 3 gives instructions on how to move tokens from one address to another.)

To name your token, follow these steps:

1. **Enter your desired Token ticker name.**

   This needs to be five characters or less.

2. **Enter the name of your token.**
3. **Click Reserve Token Symbol.**

   This is a few letters that will represent your token on the network.
4. **Click Confirm.**
5. **Navigate to the fox icon for your MetaMask wallet.**
6. **Click Approve on Contract.**
7. **Click Approve on Fee.**

If your transaction will not approve, check to make sure you have enough Ether in your wallet to pay the Ethereum mining fee. It will take some time for your contract to be approved. This is because of the latency inherent in blockchains.

Creating your tokens

Now that you've reserved the name that you want to use for your token, you can create your new token. Polymath will have sent you an email with a link to your token creation dashboard.

WARNING

Your dashboard is integrated with several service providers that provide advisory, legal, KYC/AML, marketing, and custody service that you may need if you plan on making your token available to the public. KYC (Know Your Customer) is an anti-money laundering procedure used to identify customers that would like to move money. It's part of a global effort to fight money laundering and terrorism called AML (Anti-Money Laundering) and Combating Financing Terrorism (CFT). Always do your due diligence and seek your own legal counsel. If you choose to work with these integrated providers, the information you enter in each form will be sent automatically to the firms you selected. The firms will reach out to you to help you through the next steps.

In the following steps, I'm assuming that you are *not* going to offer your token to the public.

1. **Navigate to the Polymath email you received.**
2. **Click the link Click Here to Continue with your Token Creation.**
3. **Open your MetaMask wallet.**
4. **Click Sign.**
5. **Click I Have My Own for each of the service providers.**

Now that you've confirmed that you have your own service providers, you can start specifying your token. The left side of the page has several icons that let you know where in the process you are.

1. **Click Token on the left side of the page.**
2. **Under My Security Token Must Be, click Divisible.**
3. **Click Create My Security Token.**
4. **Open your MetaMask wallet and click Confirm.**
5. **Click Confirm.**
6. **Wait a minute, and open your MetaMask wallet again and click Confirm for the mining fee.**

If the page is stuck on approving your contract for more than five minutes, refresh the page and use MetaMask to sign on again. Also, from inside your MetaMask wallet, you can see the status of your contract. You can increase the mining fee and have it processed faster. This can skyrocket the cost of the transaction, though, so be thoughtful if you choose this option.

Polymath has built-in distribution for tokens for those who are using them as a means of raising capital. On your Polymath dashboard, this is referred to as STO, short for *Security Token Offering.* In the instructions I've provided, I made the assumption that the token you're creating will not be used for raising capital, so you can click Skip Minting and then click Confirm.

Polymath has created templates for the creation of security tokens. In these instructions, you use the smart contract that creates a hard cap of the number of tokens generated by the smart contract. You set a time and number of tokens that you would like to create. Because these tokens will be going to your own address, use minimum numbers so as not to waste your Ether.

Now you'll create a capped custom security token. The cap refers to the fact that the total number of tokens created is a fixed number that you choose at the time of its creation. Follow these steps to get started:

1. **Select the current time.**

   Give yourself a few hours to input the transaction just in case something happens that stalls you.
2. **Under Raise In, select ETH.**

3. **Under Hard Cap, enter the number of tokens you would like.**
4. **Under Rate, enter 1000.**

   TIP

   Think of this as the fee for generating your new tokens. You'll be "buying" them from the smart contract. If you enter 1000 under Rate, then the cost to produce your new tokens will be 1 ETH for 1,000 new tokens.

5. **Under ETH Address to Receive the Funds Raised during the STO, enter your MetaMask address.**
6. **Click Deploy and Schedule STO.**
7. **Click Confirm.**
8. **Navigate to your MetaMask wallet.**
9. **Click Confirm.**

Getting your hands on your tokens

You'll receive an email from Polymath letting you know that you have successfully set up your token. When you get this email, follow these steps:

1. **Navigate to** `https://tokenstudio.polymath.network`**.**
2. **Sign on via MetaMask.**
3. **Click Token on the right side.**
4. **Under Mint Your Token, download the sample CSV file.**
5. **Open the CSV file.**
6. **Remove the dummy data.**
7. **Input your own Kovan Test Network address in its place.**
8. **Save your new CSV file.**

Now that you've inputted your address to receive your token, you can upload it to the same page that you downloaded the sample from:

1. **Navigate back to** `https://tokenstudio.polymath.network`**.**
2. **Sign on via MetaMask.**
3. **Click Token on the right side.**
4. **Click Upload File.**

5. **Click Confirm.**
6. **Open MetaMask.**
7. **Click Confirm.**

Congratulations! You've created your own test security token. Ethereum is a powerful tool, and with tools like Polymath, it's easier and faster to create the blockchain applications you want.

IN THIS CHAPTER

- **Getting acquainted with the Cardano blockchain**
- **Seeing how Cardano's blockchain consensus works**
- **Getting your hands on ADA, the native token of Cardano**
- **Creating a no-code smart contract with Marlowe**

Chapter 6

Uncovering the Cardano Blockchain

In this chapter, I introduce you to the Cardano blockchain, a relatively new blockchain with extraordinary capabilities. The Cardano team worked for years researching, building, and testing new technologies to create an easy-to-use, friendly, and reliable blockchain. It's exciting for developers to build because it has smart contract functionality and uses a next-generation consensus algorithm called *proof of stake* (PoS), giving it some of the highest speeds for a public blockchain. But you don't need to know how to code to get something out of Cardano.

This chapter is essential if you're interested in creating smart contracts or want to earn more cryptocurrency through staking. Here, you find out how to secure your web wallet, buy ADA (the native token of Cardano), earn cryptocurrency through leasing out your assets, and create your very own smart contract.

Getting to Know Cardano

Cardano is a decentralized, open-source smart contract platform secured by a PoS consensus mechanism. Created in 2015 by Ethereum founding team members Charles Hoskinson and Jeremy Wood, Cardano was created as a blockchain platform that allows you to store, transform, and manage things you value, including your identity. Cardano has positioned itself as a "research first" blockchain.

TIP

PoS is a way that some blockchains, like Ethereum and Cardano, reach consensus and validate transactions. In a PoS system, people who hold cryptocurrency (also known as *stakers*) can earn rewards for validating transactions and adding new blocks to the blockchain.

It took two years of research before the team wrote the first code. The reason behind this thoughtful start was that the founders wanted Cardano to be the financial operating system for billions of people. The team did cryptographic research and dug into game theory, identity management, and programming language. All their research was documented in more than 100 academic and peer-reviewed papers.

Cardano is different from most blockchains. For example, you create tokens on Cardano without smart contracts. Tokens are governed and accounted for the same as ADA, Cardano's native token. When you move your tokens, they all use the same core infrastructure. Cardano has removed a layer of extra complexity and human error. That said, you can also use a smart contract on Cardano for more complex use cases like decentralized autonomous organizations (DAOs).

Here are six things you can do with Cardano:

- Send and receive tokens.
- Delegate your ADA to a pool and earn rewards.
- Vote on community-driven proposals.
- Earn ADA rewards by voting.
- Contribute to improving Cardano.
- Create smart contracts.

There are several reasons you may want to consider Cardano as the back end for your decentralized application (dApp):

THE CARDANO FOUNDATION

The Cardano Foundation is a nonprofit organization responsible for overseeing and promoting the development of this Cardano blockchain protocol. It works with stakeholders across industries to ensure that both legal and commercial standards are aligned to grow global adoption. Its most important responsibility is driving platform adoption.

The Cardano Foundation has a governing council that includes two entities — EMURGO (`https://emurgo.io`) and IOHK (`https://iohk.io`). EMURGO develops, supports, and incubates commercial opportunities and integrates businesses. IOHK is contracted to design, build, and maintain the Cardano platform.

- **It offers a peer-reviewed infrastructure.** This can be a better experience than some purely community-led projects. It has faster, more secure, and more cost-effective infrastructure with a dedicated team.
- **It offers accurate cost predictability because it doesn't auction for transaction fees.** This feature is essential when you're building enterprise infrastructure. Most software development needs outside capital, and Cardano has a venture fund. Every few weeks, new projects are picked from the proposed applications. The Cardano community discusses and votes on proposals. If you're considering building an application on Cardano, check out the community-led fund at `https://cfund.vc`.
- **It was built with a high-assurance formal development method.** The consensus mechanism, called Ouroboros, was peer-reviewed and published in top-tier publications in cybersecurity and cryptography. I cover Ouroboros in more detail in the next section.

Understanding Ouroboros: Cardano's Blockchain Consensus

Ouroboros is a PoS protocol that aims to improve the security of the blockchain and reduce energy consumption. It uses cryptographic techniques, math, and game theory to ensure that transactions on the blockchain are accurate and efficient. The protocol is considered secure as long as a majority (51 percent) of the staked ADA is held by honest participants. It also rewards users who contribute to the network in positive ways. Overall, Ouroboros aims to provide similar security guarantees as proof-of-work (PoW) protocols, but with lower energy costs.

The Ouroboros PoS protocol has two exciting features:

- **It distributes network control across stake pools of ADA.** That means almost anyone can be rewarded for supporting the protocol.

  Staked pools are operated by nodes that control the vote for the ADA that they have been granted. The more ADA the node controls, the more likely it will be rewarded and selected to create the next block. Ouroboros has put some limits on this to help make sure everyone has a fair chance. When a node is assigned as the slot leader, it will be rewarded with ADA for adding a block to the chain. The reward is also distributed to the owners of the pool.

- **Cardano's most significant advantage over PoW blockchains is that it can securely, sustainably, and ethically scale.** It claims to have four million times the energy efficiency of Bitcoin.

Meeting ADA: The Native Token of Cardano

ADA is the cryptocurrency for Cardano. It was named after Ada Lovelace, an English mathematician who is credited with inventing computer programming in the 19th century.

ADA is used as a digital currency and a block reward for nodes on the Cardano blockchain. Like most cryptocurrencies, they allow anyone to exchange value without requiring a third party, like a bank, to facilitate the exchange. Each transaction is recorded permanently, securely, and transparently on the Cardano blockchain.

Every ADA holder has a stake in the Cardano network. You can also take the ADA that is stored in a wallet and delegate it to a stake pool to earn rewards. I explain how to do that in the "Delegating your ADA in a stake pool" section, later in this chapter.

Buying and selling ADA

You can buy or sell ADA for money or other cryptocurrencies using cryptocurrency exchanges or from within the two supported Cardano wallets: Daedalus (`https://daedaluswallet.io`) and Yoroi (`https://yoroi-wallet.com`). You can find all the other places you can purchase ADA by heading to CoinMarketCap at `https://coinmarketcap.com`.

WARNING

Be sure to keep your private keys private to keep your funds secure. For more on keeping your cryptocurrency safe, turn to Chapter 3.

REMEMBER

Avoid keeping your cryptocurrency in an exchange longer than necessary. The FTX scandal of 2022 is an important reminder of the dangers of even a popular and secure exchange. Instead, use a cryptocurrency wallet to protect your ADA.

Swimming in the ADA stake pools

Stake pools can be public or private. A public stake pool is a Cardano network node with a public address to which other users can delegate their ADA (see “Delegating your ADA in a stake pool,” later in this chapter). As the name suggests, private stake pools can be accessed only by their owners.

A reliable operator that stays up and running 24 hours a day is more likely to have a successful pool. These operators tend to be individuals with the knowledge and resources to run the node 24 hours a day. As an ADA holder, you can delegate to public stake pools if you want to participate in the protocol and receive rewards. You don’t have to operate a Cardano network node yourself.

The more ADA delegated to a stake pool, the greater chance the pool has of being selected. Each time the pool is picked, it will write all the transaction and produces a block that will be recorded onto the Cardano blockchain. The pool is rewarded for doing this work, and the ADA it receives is shared between the stake pool operator and stake pool delegators.

Pledging your ADA

Cardano pools have no required minimum pledge amount, but most exchanges have a minimum order amount that you should keep in mind. At the time of this writing, it was $30 for Moonpay (a third-party payment provider used later in this chapter).

Often pool operators will pledge some or all of their ADA to their pool to make it more attractive. The more ADA pledges, the more rewards the pool will receive.

Picking an ADA pool

You can measure the desirability of a pool by its pool ranking. The number is generated by taking the pledged owner’s stake, costs, and margin and combining it with the size and pool performance. This number is used to rank pools in Daedalus and Yoroi wallets. The wallets will indicate and order the pools by how “desirable” the pool is to stake your ADA.

SATURATION OF ADA STAKE POOLS

When a stake pool is *saturated,* it has more ADA stakes delegated to it than is ideal for network health. When a pool reaches the point of full saturation, it will have diminishing block rewards. The saturation mechanism prevents centralization by prompting ADA holders to delegate their ADA to different stake pools. It also increases the demand for stake pools and incentivizes operators to set up new pools to continue earning maximum rewards.

Cardano created a saturation metric to maintain the welfare of both ADA holders and stake pool operators. It does this by disincentivizing a pool from becoming too big.

Delegating your ADA in a stake pool

Delegation is the process by which you, as an ADA holder, can send your money into a pool with other ADA holders. This is called a *delegated stake.* It allows you to gain the benefits of staking without the work of staking yourself.

ADA held on the Cardano network represents a stake in the blockchain. The size of your stake is proportional to the amount of ADA you hold. Holding more than 500 ADA allows you to vote on Cardano matters.

You can also delegate or pledge your stake to another party. This is essential to how Cardano operates. You have two ways to earn rewards by holding ADA:

- You can delegate your stake to a stake pool run by a third party.
- You can run your own stake pool.

THE DECENTRALIZATION PARAMETER

Cardano operates by federated nodes, which ensure that transactions on the network run smoothly and stay up. The number of federated nodes changes depending on the decentralization of the network. The ratio of slots created by the federation of nodes is balanced relative to the number of stake pool nodes.

This feature may change in the future. All block rewards are distributed to operating stake pools. At this time, federated nodes do not receive a reward. When Cardano has stabilized, this decentralization measure may go away.

ADA STAKED INCENTIVES

Incentives are given to ADA holders to ensure the longevity and health of the Cardano network. At the time of this writing, you could earn around 4 percent annualized by staking your ADA. The creators of Cardano use an incentive mechanism that incorporates mathematics, economic theory, and game theory.

You have three options for staking your ADA:

- **You can delegate staking to a pool via the Daedalus wallet.** Daedalus is a full-node wallet developed by IOHK.
- **You can delegate staking via the Yoroi browser-based wallet that EMURGO created.** I explain how to do this in the "Setting up your system for staking" section.
- **You can set up your own staking pool.** This option is more time-consuming and technical — beyond the scope of this book.

The amount of stake delegated to a pool is the primary way the protocol chooses who will be allowed to add the following block to the Cardano blockchain. Pools compete for the opportunity to add blocks so they can receive more ADA. The block reward is shared among everyone who delegated their stake to that pool.

Setting up your system for staking

In this section, you set up a wallet to hold ADA, secure your wallet, purchase a minimum of $30 of ADA (the minimum required at the time of this writing), and stake your ADA within a pool.

You'll need two pieces of clean paper, a non-smudging pen, an Internet connection, and the Brave (`https://brave.com`) or Chrome (`www.google.com/chrome`) web browser installed on your computer. ***Note:*** The web wallet you use in this section works with all popular browsers, but the instructions were written for the Brave browser.

REMEMBER

This tutorial is for a web wallet. Web wallets are not as secure as hardware or paper wallets, so don't leave a significant amount of cryptocurrency in your wallet. How much is "a significant amount"? That number is different for everyone. I think of it the same way I would my physical wallet: I never keep more than I'm willing to lose on a night out.

TIP

Yoroi is a hot wallet that plugs into your favorite browser. It's simple, fast, and secure. IOHK created Yoroi as part of its EMURGO product, and it follows best practices for software in the industry. IOHK has done comprehensive security audits, too. Yoroi is a great place to start with ADA. The wallet can be used as your daily wallet for Cardano.

Step 1: Get your ADA wallet

The first step is to get a wallet to keep your ADA. Follow these steps:

1. **Go to the Yoroi website at** `https://yoroi-wallet.com`.
2. **Click Download and pick your preferred browser.**

   You'll be directed to a new page.

   TIP

   If you're using the Brave browser, select the Chrome option — it'll work for Brave.
3. **From the new page, click the Add to Browser button and click through to add the extension.**

Step 2: Making sure you don't lose your wallet

After you've added Yoroi to your browser, you can access it from your browser's extension icon. In the following steps, you make a few configurations to your wallet.

1. **Open your browser.**
2. **Click the extension icon.**
3. **Select the Yoroi icon.**

   A new page opens.
4. **Click Continue.**
5. **Read and agree to the terms of use.**
6. **Click Continue.**
7. **Click Allow Cardano Payment URLs.**
8. **Click Allow again.**
9. **Click Finish.**

Great job! You're now ready to set up your wallet.

Step 3: Setting up your Yoroi wallet

If you just finished the preceding section, you should have your browser open on a Yoroi page for creating and restoring wallets. If you aren't on that page, click the Yoroi extension in your browser. Then follow these steps to set up and secure your Yoroi wallet:

1. **Click Create Wallet.**
2. **Click Cardano.**
3. **Click Create Wallet.**
4. **Name your wallet and create a unique password.**

   REMEMBER

   Write down your password on a piece of paper and store it somewhere you won't forget. If you lose your password, you lose your money!

5. **Click Create Personal Wallet and click through the warning page.**
6. **Write your seed phrase in order on a new clean piece of paper.**
7. **Click Yes, I've Written It Down.**
8. **Reenter your seed phrase in order.**
9. **Click through the warning page and click Confirm.**

Congratulations! Your wallet has been set up and secured. Consider laminating the papers on which you wrote your password and seed phrase. Treat the password and seed phrase with as much care as you would the money your wallet secures.

Step 4: Getting your hands on some ADA

Now that you have a secure wallet, you can purchase some ADA. This section starts with the page you left off on in the previous section. If you closed your browser, open it up again and click the Yoroi browser extension. Then follow these steps:

1. **Navigate to your Yoroi wallet.**
2. **Click the pull-down arrow in the upper-right corner of your Yoroi wallet.**
3. **Select Buy ADA.**
4. **Select your ADA wallet address.**
5. **Enter the amount of ADA you would like to purchase.**
6. **Click I Agree with the Terms of Use and click Exchange.**
7. **Click Continue.**

8. **Click Here to Redirect**

   You're directed to a third-party payment provider called Moonpay.

9. **Enter your email address.**
10. **Retrieve the verification code from your email and enter it on the Moonpay page.**
11. **Agree to the terms of use and click Continue.**
12. **Enter your details and click Continue.**
13. **Click through the rest of the pages to complete the transaction.**

TIP

If you're in a region that Moonpay does not support, you can purchase ADA via Coinbase (`www.coinbase.com`) or another exchange.

Step 5: Staking your ADA

Now that you have a balance of ADA in your wallet, you can stake your ADA. Staking your Ada allows you to receive additional ADA and helps keep the Cardano network healthy. Follow these steps:

1. **Navigate to your Yoroi wallet.**
2. **Click the Delegation List tab.**
3. **Select a stacking pool.**

   When selecting a stacking pool, pay attention to the fixed cost and return on assets (ROA). The ROA is the percentage return on ADA. Each pool's ROA is different.

4. **Enter the amount you would like to stake.**
5. **Enter your wallet password.**
6. **Click Delegate.**

You can check your staked ADA by clicking the Transactions tab in your Yoroi wallet.

Congratulations! You've successfully secured your wallet, purchased ADA, and gotten set up to earn ADA via a delegated staking pool.

Building Smart Contracts with Marlowe

Smart contracts are programs that can be built on blockchains; they're often used to automate various processes. However, creating and deploying smart contracts usually requires a skilled developer and can be complex and costly, because they're often written in specialized programming languages.

Marlowe is a product suite that makes it easier to build smart contracts on the Cardano blockchain, even for people who aren't experienced programmers. Marlowe includes a set of preprogrammed templates that can be used with low- or no-code solutions, as well as a programming language called Plutus that can be used to write contracts in JavaScript. Marlowe also has a tool called Blockly that allows users to create contracts by simply dragging and dropping predesigned blocks.

In this tutorial, you use Marlowe's no-code tools to build smart contracts on the Cardano blockchain. Follow these steps:

1. **Go to** `https://marlowe-finance.io`.
2. **Click Marlowe Run.**
3. **Click Try Demo.**
4. **Click Generate Demo Wallet.**
5. **Name your wallet.**
6. **Click Connect Wallet.**

   You're now set up to do a no-code demo on Marlowe Run.

   TIP

   On the Marlowe Run dashboard, you have three options for smart contracts. In the following steps, you use the Loan template, but the other two are also easy to use, and you should give them a try later.

7. **Click the Choose a Template button.**
8. **Select Loan.**
9. **Click Setup.**
10. **Name your contract TEST.**
11. **Name the parties for your contract.**
12. **Enter** 5 **in the Interest field.**
13. **Enter** 100 **in the Loan Amount field.**

14. **Click Review.**

    You've now set the terms for your loan, and you can execute the contract.

15. **Click the Pay and Start button.**
16. **Click Deposit for the Lender.**
17. **Click Deposit again.**

    Now that the funds have been transferred, they have a few minutes to deposit the amount plus interest back into your account.

18. **Click Deposit for the Borrower.**
19. **Click Deposit again.**

You can now explore some of the other tools the Marlowe team has made. I suggest the smart contract builder tool called Playground as your next step.

IN THIS CHAPTER

- » Uncovering the growing Polkadot ecosystem
- » Diving into nominated proof of stake
- » Getting started on Polkadot
- » Voting in new distributed democracy
- » Earning DOT for participating as a nominator

Chapter 7
Finding the Polkadot Blockchain

The Polkadot blockchain is now being called a layer-0 protocol. A layer-0 protocol is responsible for maintaining the integrity and security of the underlying data structure and for enforcing the rules and consensus mechanisms that govern the system.

The Polkadot blockchain provides the underlying infrastructure for building decentralized applications (dApps) and other distributed systems on top of them. In the case of Polkadot, it's a blockchain of mini specialized blockchains. Polkadot also is a green blockchain that uses a new kind of consensus called *nominated proof of stake.*

Polkadot and its ever-growing ecosystems are rapidly evolving. But despite this rapid growth, the platform has some incredibly approachable, user-friendly tools. Polkadot's easy accessibility has helped propel its popularity and usage.

In this chapter, I explain how to get your hands on DOT, the native cryptocurrency for Polkadot, and how to turn your DOT into more DOT. You do this by participating in a pool, voting on community projects, and nominating validators for the network.

After reading this chapter, you'll not only have a deep working knowledge of the Polkadot blockchain, but you'll probably have more DOT than at the beginning. With this information, you'll better understand the implications of building on Polkadot and investing in DOT. This will save you time and money as you explore other blockchains.

Understanding the Polkadot Ecosystem of Specialized Chains

Polkadot was founded by Gavin Wood, the cofounder and former chief technology officer (CTO) of Ethereum and inventor of the Solidity smart contract language. Gavin started working on Polkadot in 2016 as a sharded version of Ethereum. (To *shard,* by the way, within this context means to distribute data.)

In 2017, Gavin founded the Web3 Foundation (W3F), a nonprofit entity created to support the research and development of Polkadot and raise capital to build it. W3F raised $145 million in two weeks via a token sale and chose Gavin's development company, Parity Technologies, to create Polkadot. This made a lot of sense, given the fact that Gavin had designed the blockchain system and was in the best position to execute on its development.

Ten days after this substantial capital raise, a multi-sig wallet bug froze $90 million of ETH from Polkadot's token sale. Despite the massive loss, Polkadot and W3F pushed through and met the development milestones. W3F raised an additional $60 million in a token sale in 2019. These funds have gone into finishing the network deployment and supporting ecosystem growth.

Polkadot's first significant release was in 2019 with the launch of Kusama, a high-functioning testnet that was designed to stretch and strain governance, staking, and sharding under actual usage.

From what the Polkadot team learned from Kusama, it created the first mainnet chain candidate, Phase 1, which was launched in 2020. It operated as a proof of authority (PoA) network managed by six validators controlled by W3F. (Baby blockchains are vulnerable and need a lot of updates as they get up off the ground.) The mainnet transitioned to nominated proof of stake (PoS) later that year as planned. Polkadot also unlocked governance functionality, and control of the protocol was handed over to the community. Now W3F funds ecosystem initiatives and backs projects built on Polkadot.

Digging Deeper into Polkadot: The Blockchain of Blockchains

Polkadot is a foundational building block for Web 3.0 applications that enable developers to create private and secure applications that don't rely on a third party. It's considered a layer-0 protocol and multichain network. Multichain networks are not new in the blockchain space.

The Polkadot blockchain network was designed to support interconnected, application-specific subchains. The idea behind this is that each chain could specialize and tool itself relative to the application it was being used for and also be able to communicate with other applications that needed blockchain backends. Polkadot's goal was to enable scalability by allowing specialized blockchains to communicate with others in a secure, trust-free environment.

It uses a sharded model where transactions are processed in parallel instead of sequentially. Polkadot is the main chain of the system. To make it slightly confusing, Polkadot's main chain is referred to as a *relay chain.* So, if you're reading about Polkadot elsewhere, and you see *relay chain, main chain,* or *Polkadot,* they're most likely referring to the same thing.

Instead of having all applications connect and share the same ledger (the way Bitcoin, for example, works), Polkadot uses a structure called *parachains* (short for *parallelized chains*). Parachains define their logic and interface, and the relay chain validators execute it. Polkadot is the first fully sharded blockchain that splits the data into smaller partitions, known as *shards.* Shards comprise their own distinctive and independent data.

On Polkadot, each shard hosts core logic, the shards are executed in parallel, and Polkadot can send cross-shard asynchronous messages. However, each Polkadot shard (or, in Polkadot terminology, *parachain*) has a unique state transition function (STF). Applications can exist within a single shard or across shards by using the same logic. A shard's STF can be abstract if the validators on Polkadot can execute it within a WebAssembly (Wasm) environment. As long as each of Polkadot's parachains follows the same logic and rules, they'll work and speak with other parachains.

Polkadot is also developer-centric in its use of Parity Technologies' Substrate modular framework. What it means is that developers can select specific components that suit their application-specific chain needs when they're building their decentralized applications (dApps). Custom blockchains built on top of Polkadot focus on performing one task well (like gaming, finance, or insurance). This is a bit different in the blockchain world, where many blockchains try to solve every problem with the same tooling and store all the data in one place.

Polkadot doesn't support application functionality; instead, it provides security to the network's parachains, consensus, finality, and voting logic. This allows developers to contribute to the ecosystem's growth by designing and contributing to the parachains they're working on.

In the following sections, I dive into substrate, a framework for building blockchains. I also cover parachains that govern the network and explain some of the rules that hold the network together.

Substrate: The framework of the Polkadot blockchain

Polkadot's blockchain-building framework is called Substrate. All Substrate-based chains are seamlessly compatible with Polkadot, which means they're all interoperable within the ecosystem of parachains, applications, and other resources.

The Polkadot network's native token, called DOT, powers its substrates, and serves various functions within the network. These functions include covering transaction fees, staking, participating in governance, and purchasing parachain slots. DOT is an essential component of the Polkadot network and plays a crucial role in its operations.

REMEMBER

The minimum balance required to have an active account on Polkadot Network is 1 DOT. If your account balance is less then 1 DOT, your account will be slashed. *Slashing* is where the network takes your DOT. I haven't encountered other blockchains that do cleanup of *dust accounts* (accounts that have very low balances), so it's something to keep in mind regarding your own account.

You may also want to note some other unusual DOT requirements:

- The minimum contribution required to do crowd loans is 5 DOTs; staking requires 10 DOTs.
- When you have 20 DOTs, you can register an on-chain identity and vote.

These arbitrary minimums can change. Unfortunately, the community still needs to keep up with documentation that lets you know the requirements for different activities.

In the following sections, I cover the various ways in which Polkadot's native token, called DOT, is used to power its decentralized platform. These include building parachain chains, staking, participating in governance, and more. By understanding the role of DOT in these processes, you can gain a deeper understanding of how Polkadot's decentralized ecosystem functions.

Uncovering parachains

Parachains construct and propose blocks to validators on Polkadot. Each block undergoes availability an validity checks before being added. The nodes are responsible for adding the new data and checking to make sure that the information conforms to the rules and is correct. Full nodes for parachains are called *collators.*

Collators play a crucial role in the maintenance of Polkadot's parachain chains. They're responsible for gathering and aggregating transactions from users and creating block candidates that are then used to produce state transition proofs for the relay chain validators. To fulfill these duties, collators must maintain full nodes for both the relay chain and their respective parachains, as well as keep track of all necessary information for block authorship and transaction execution. Essentially, collators perform many of the same tasks as PoW nodes to maintain the integrity and functionality of the parachain chains.

Polkadot bridges parachains and offers two-way compatibility so transactions can flow between different parachains. The Cross-Consensus Messaging Format (XCM) allows parachains to send messages of any type to other parachains. This is how Polkadot has created a multichain model with infrastructure robustness so different dApps can seamlessly communicate messages and value to one another.

Here's a simplified way to view this: Polkadot is the primary source of information, truth, and logic. It also spawns subchains with specialized tools and logic tailored to their applications. Gluing the whole affair together are layers of validating nodes that ensure everything runs smoothly.

Seeing what nominated proof of stake has to offer

Proof of stake (PoS) was first introduced in a paper by Sunny King and Scott Nadal in 2012. It was proposed as a way to address the proof of work (PoW) consensus mechanism's inefficiencies and lower the computational resources required to run a blockchain network. PoS is based on the existence of a verifiable stake in the ecosystem and has become one of the most popular consensus mechanisms for blockchain networks, given the push for more green infrastructure.

The distinction between PoW and PoS is that, whereas PoW requires miners to expend energy to solve complex mathematical problems to validate transactions on the blockchain network, PoS does not require "work." Instead, with PoS, users need to show that they own a certain quantity of cryptocurrency. The ownership implies that they have a vested interest in ensuring that all transactions are valid.

The benefit of using PoS over PoW is that it doesn't require any significant computational resources or energy expenditure. This means using PoS instead of PoW can significantly reduce costs associated with running a blockchain network. Additionally, because users don't need expensive mining rigs or large amounts of electricity in order to participate in staking activities, it's more accessible than mining for casual users who can't afford mining rigs. Finally, because so many users are staking coins instead of just a few miners performing work, more diversity is created within the system, which leads to greater security and stability overall, at least in theory.

Proof of stake is an increasingly popular consensus mechanism for blockchains due to its convenience and cost savings compared to other options like proof of work. By requiring users to show that they own a particular quantity of cryptocurrency tokens native to their network, it reduces costs associated with running a blockchain network while also creating greater diversity within its ecosystem, which leads to better security and stability overall. For these reasons, many other blockchain networks are beginning to use this consensus mechanism instead of traditional methods like PoW. Ethereum is a notable new PoS user. For website owners and crypto enthusiasts alike looking for an efficient way to participate in distributed networks without wasting significant energy or money resources on mining rigs and electrical bills, PoS offers an attractive solution.

Polkadot has a unique PoS called *nominated proof of stake* (NPoS). The NPoS incentivizes DOT holders to participate in the network's day-to-day operation by picking the validator nodes, voting on network business, and staking assets.

DOT holders have the right to select nodes that validate network transactions. DOT holders who select nodes are known as *nominators;* a nominator must have a minimum of 10 DOT in order to nominate. The nodes are called *validators.* A validator indicates its intention to be a validator candidate. All candidacies are made public, and nominators then submit a list of up to 16 candidates they support. Polkadot distributes the stake among selected validators to maximize economic security for the network. On Polkadot, at the time of this writing, there is a maximum of 1,000 validators.

WARNING

In order to incentivize nominators and validators to act in the network's best interests, Polkadot's nominated proof of stake (NPoS) mechanism allows for the stake of both parties to be *slashed* if they engage in behavior that would harm the network. (Slashing is when the network takes away a portion of their DOT.) By creating real economic consequences for bad behavior, NPoS encourages nominators and validators to work toward the overall stability and security of the network.

Getting Up and Running on Polkadot

You need to purchase at least 11 DOT in order to set up an account and participate in staking while also making sure that Polkadot doesn't remove your account for having less than 1 DOT. The easiest way to get your hands on DOT is by buying some at your favorite exchange, such as Coinbase (`www.coinbase.com`). At the time of this writing, 11 DOT cost approximately $60 (but this number fluctuates).

REMEMBER

If you need help buying DOT, turn to Chapter 3. There you'll find detailed instructions on how to set up your account and connect to Coinbase or another exchange.

After you've obtained some DOT, you're ready to set up a browser extension that will act as a basic account injection and signer. The browser extension will protect you against all community-reported phishing sites and make it a little easier to use your DOT. Before proceeding to the following sections, grab two clean pieces of paper and a non-smudging pen, and make sure you have at least 11 DOT ready to transfer.

Step 1: Download the DOT browser extension

The recommended extension for DOT is the Polkadot{.js} extension. This extension injects the account's data and allows the signing of messages and transactions without making the account secrets available to the calling applications. Follow these steps to set up the Polkadot{.js} extension:

1. **Using the Brave web browser (available at** `https://brave.com`**), go to** `https://polkadot.js.org/extension`**.**
2. **Click Download for Chrome.**
3. **Click Add to Brave.**
4. **Click Add Extension.**

Now that you've installed the Brave browser extension, you will set it up to use on Polkadot in the following section.

Step 2: Configuring the DOT browser extension

Follow these steps to configure the extension and add DOT to your new address:

1. **In the Brave web browser, click the Extensions icon.**
2. **Click Polkadot{.js}.**
3. **Read the warning and click Understood.**
4. **Click the plus sign (+) to add an account.**
5. **Write down your 12-word mnemonic seed.**
6. **Name your account and create a unique password.**
7. **Write your password on another piece of paper for safekeeping.**
8. **Click the gear icon.**
9. **Under Display Address Format, select your account.**
10. **Click the Polkadot Relay Chain.**

Now that your Polkadot{.js} extension is set up, it's time to transfer in some DOT. To do this, you need to retrieve your new address from your Polkadot{.js} extension and initiate a transfer from the exchange where you purchased your DOT. If you need guidance on how to do this, refer to Chapter 3. After the transfer is complete and your DOT has been transferred to your new address, you're ready to stake your DOT on the Polkadot network in the next step.

Step 3: Joining a nomination pool

In this step, you stake your DOT to earn more DOT. As I mention earlier, Polkadot has an NPoS consensus in which nominators select a decentralized network of validators to secure Polkadot's entire multichain ecosystem. To help secure the network, you'll be rewarded with a fraction of the block reward. The nomination pool allows you to risk less DOT. You also don't have to manage your nominations. You can join a nomination pool with 10 DOT. Pool members split rewards and penalties proportionally.

WARNING

Old documentation you may see online says that the minimum is 1 DOT. This is no longer true and may change in the future.

Follow these steps to join a nomination pool:

1. **Go to** `https://polkadot.js.org/apps/#/staking`**.**
2. **Select Pool from the navigation bar.**

   You'll have a lot of choices so take a moment to review a few of them. Look to see if the pool is "open" and make sure it has selected 16 validators at a minimum.
3. **Select a pool to join.**
4. **Enter the amount of DOT you will assign to the pool and click Join.**

   Pay attention to the transaction fees before you sign.
5. **Click Sign and Submit.**
6. **Enter your password in the new window that pops up.**

REMEMBER

The funds nominated to a pool won't be visible in your account balance on Polkadot JS Apps UI. This is because your funds are transferred to the pool's account. This pool account is not accessible by anyone, including the pool operator — only the pool's internal logic can access the account.

After staking your DOT in a pool, you can claim your share of any rewards earned in the eras since you joined. Each era is 24 hours long. In the following sections, you claim your rewarded DOT from the pool you used in the previous section.

Step 4: Claiming your rewards

In this section, you remove your funds from the pool and claim your portion of the rewards. You can exit the pool at any time, but if you leave a pool, you'll be subject to an unbonding period of 28 days on Polkadot.

The *unbonding period* is the amount of time that must pass before an individual can withdraw their stake from a blockchain network or pool. In this case, the unbonding period is 28 days, which means that an individual must wait 28 days before they can withdraw their stake. This is often implemented as a security measure to ensure that individuals don't rapidly move their stake in and out of the network, which could potentially harm the stability and security of the network. The unbonding period can vary from one blockchain network to another, and it's often set by the network's governance mechanisms.

1. **Go to** `https://polkadot.js.org/apps/#/staking/actions`**.**
2. **Click Accounts.**

3. **Click Pooled.**

   This brings up the pool and the DOTs that you staked.

4. **Under the pools listed on the page, click the three-dot icon on the right.**
5. **Select Withdraw Unbonded.**
6. **Select Withdraw Claimable (if you have any rewards to claim).**
7. **Click through the pop-ups until you're done.**

In the following sections, you uncover how DOT is used to govern the Polkadot network.

Uncovering Governance on Polkadot

Polkadot has a governance mechanism that allows it to evolve in the direction of its interested stakeholders. It also has an economic democracy that allows everyone a voice weighted by the number of DOTs they control. Right now, you need more and more DOT even to have a voice on Polkadot, but hopefully this flaw will be rectified so the network is accessible to all who would like to participate. The founders' goal, however, seems to be benevolent — they want to ensure that the stakeholders can always control the network.

One of the ways that Polkadot has worked to ensure stakeholder control is in how the network uses several on-chain voting mechanisms, such as referenda with adaptive super-majority thresholds and batch-approval voting. Stake-weighted referenda are used to make all changes to the protocol. This means all changes to how the network works are put up for a vote by the stakeholders. Polkadot's founders incorporated a lot of lessons from the previous blockchain wars that Bitcoin and Ethereum endured. Fights over the structure and utility of the networks led to the fracturing of those networks, often between token holders, node operators, dApp developers, and core development. (You can learn more about the history and challenges of those networks throughout this book.)

Polkadot has a relatively civilized and organized way of balancing the need of all stakeholders. For example, all active token holders and the Polkadot council collaborate to administrate any network upgrade decision. The public token holders or the council can make a proposal, but it has to go through a referendum to allow all interested parties time to decide. Each vote is weighted by the amount of DOT that the individual controls.

There are four types of referenda:

- Publicly submitted proposals
- Proposals submitted by the council
- Enactment of a prior referendum
- Emergency proposals from the technical committee

In the following sections, you dive into the mechanics of referendums and their role in the governance of Polkadot.

Proposing a referendum

Anyone, including you, can propose a referendum. You deposit the minimum number of tokens for a certain period and if someone endorses the proposal, they may deposit the same amount of tokens to support you. The proposals with the highest number of bonded supporters are selected for the next voting cycle. Your bonded tokens will be released after the proposal is brought to a vote.

Every 28 days, new referenda are voted on. There are two queues — one for council-approved proposals and another for publicly submitted proposals. The referendum to be voted on alternates between the top proposal in the two queues. The top proposal is the one with the largest stake bonded behind it. Emergency referenda take precedence and are voted on right away.

If you vote, you must lock up your tokens until after the referendum has been enacted. This policy is meant to dissuade vote selling.

In the following sections, you use your DOT to participate in the governance of the Polkadot network and have a say in its future direction. You also discover how to cast your votes on various proposals and play a role in shaping the future of the decentralized platform.

Blockchain democracy in action

In this section, you find out how to vote on essential referenda that are being put forth on the Polkadot blockchain. To follow these steps, you must hold at least 2 DOTs in your account. Also, be prepared to lose access to the DOTs you'll use to stake your vote until after the referendum has been enacted. If you still need to set up your Polkadot browser extension, go back to the “Getting Up and Running on Polkadot” section to get set up.

1. **Go to** `https://polkadot.js.org/apps/#/democracy`**.**
2. **Review the current referenda that are up for a vote.**

   By clicking on each one, you can review the number of days it has left and how many people have voted.
3. **On the right side of the screen, click the Vote button.**
4. **Select Vote Nay or Vote Aye as you please.**
5. **Click Sign and Submit.**

Congratulations! You just voted, and in doing so, you supported the Polkadot ecosystem. Your vote helped shape the future of the network and has allowed it to continue to evolve through a new type of online democracy.

Nominating Your Validators

One of the most critical roles within the Polkadot network is that of a validator. Validators are responsible for keeping the network nodes in consensus (in other words, all the nodes agree to the same reality). They do this by verifying state transitions. As of the writing of this book, the number of validators is limited to 1,000, but Polkadot may update this number in the future. Also, although their goal is 1,000 validators, they may not get that many. Why? Here are a few reasons:

- **Validators are responsible for being online and faithfully executing their tasks 24/7 with no downtime.** That’s a big commitment.
- **Being a validator means receiving a payment from the network.** Dividing this payment too much could disincentivize participation or even introduce new game theory that centralizes the network.
- **Validators have to risk their own capital.** The minimum stake to be elected as an active validator is dynamic and changes over time, but as I was writing this, there were around 600 validators, and the staked DOT was worth more than $2,000 on most of them. The Polkadot team plans to change this as the network grows.

- **Validators must protect their signing keys from third parties.** This way, attackers can't take control and commit slashable behavior that causes them to lose their deposit.

REMEMBER

Slashing is where the network takes all or a portion of DOT for bad behavior.

If you want to have a look at the validators on Polkadot, you can view all of them and the amount each has personally risked at `https://ipfs.io/ipns/polkadot.dotapps.io/#/staking/targets`.

In the following sections, you find out how to earn DOT as a reward for network participation as a nominator. As a nominator, you're responsible for selecting trustworthy validators. At the time of writing this, you need 176 DOTs to complete this tutorial and earn a reward. You can still nominate a validator if you have at least 10 DOT to bond.

WARNING

Before you start, keep in mind that you may lose a portion of your staked DOT if a chosen validator misbehaves.

If you still need to set up your web extension for Polkadot and obtain some DOT, head to the "Getting Up and Running on Polkadot" section, earlier in this chapter.

In the following sections, you uncover Polkadot's staking dashboard and use it to manage your DOT.

Step 1: Getting connected to the staking dashboard

To access the dashboard for staking and use your Polkadot{.js} to log in, follow these steps:

1. **Go to** `https://staking.polkadot.network/#/overview`**.**
2. **Click Connect.**
3. **Select your Polkadot{.js} account.**
4. **Click and agree to the prompt that pops up with a disclaimer.**
5. **Click Connect again and select your address.**

Step 2: Nominating a Polkadot validator

To select a validator node on the Polkadot network, follow these steps:

1. **To begin, navigate to your dashboard from the previous step. On the left navigation bar, make sure that the network selected is Polkadot under the Network option.**

   If it isn't, click the current network and switch it to Polkadot.
2. **Click Nominate in the navigation on the left.**
3. **Click Start Nominating.**
4. **Select your controller account.**
5. **Under Reward Destination, select To Controller.**

   This will rerun funds to your account.
6. **Under Nominate, select Optimal Selection and click Continue.**
7. **Under Bond, enter the amount you want to bond and click Continue.**
8. **Review the summary and click Start Nominating.**
9. **Verify your transaction in your Polkadot{.js} account.**

You'll need to wait for one Polkadot era, which is approximately 24 hours, before checking on your nominations.

You can use the staking dashboard to manage your other activities on Polkadot, such as the staking pool you join earlier in the chapter. The dashboard has a more user-friendly interface than the explorer you use earlier (`https://ipfs.io/ipns/polkadot.dotapps.io/#/explorer`), but as you may have also noticed, it doesn't have all the same functionality.

IN THIS CHAPTER

- » **Getting to know Solana**
- » **Creating a decentralized application on Solana**
- » **Building a decentralized autonomous organization on Solana**

Chapter 8
Examining the Solana Blockchain

The developers of Solana are hoping to create an infinity scalable blockchain that is low-cost and green. Solana (SOL) is one of the most popular cryptocurrencies trading today. The development company behind Solana has raised a total of $315.8 million in funding. Given this significant funding, you'd be wise to keep an eye on the Solana project — it will most likely grow beyond any other project in the blockchain space.

The defining difference between Solana and Ethereum — and why you may want to learn more about the Solana system — is Solana's consensus algorithm, a new system called proof of history.

This chapter dives into the practical applications and future of the Solana blockchain and explains uses for its technology. You find out how to create your own decentralized application (dApp) and decentralized autonomous organization (DAO).

Uncovering Solana

Solana is a decentralized and open-source blockchain platform designed to be scalable, fast, and secure. It was created in 2017 by Solana Labs, a software development company based in San Francisco, California.

One of the main features of Solana is its high performance and scalability. It can process a significantly higher number of transactions than other popular blockchain platforms like Ethereum and Bitcoin.

Solana uses a combination of two consensus mechanisms to secure its network: proof of history (PoH) and proof of stake (PoS). Even with two consensus mechanisms, Solana is energy-efficient and environmentally friendly.

Solana has a native programming language called Move, which is used to write smart contracts and decentralized applications (dApps). It is a statically typed language that is designed to be easy to learn and use while also being highly secure.

Overall, Solana is a powerful and innovative blockchain platform that is well-suited for many use cases, including decentralized finance (DeFi), gaming, and supply chain management.

Solana's proof of history

Solana is an open-source, high-performance blockchain project that is built on a unique consensus algorithm called PoH. PoH enables Solana to keep accurate time across its decentralized network, even when the computers that make up the network don't trust one another. This allows Solana to process transactions quickly and securely without sacrificing decentralization or security.

Solana uses PoH to timestamp hashes of past blocks using a cryptographic hash function. These timestamps are then arranged into Merkle trees, with each node in the tree containing the hash of its child nodes. By sharing these timestamps with other computers on the network, each computer can build up a "history" of what has happened on the network over time.

This data structure has two advantages over traditional blockchain architectures:

- **It reduces storage requirements.** Each node needs to keep track of only a small amount of data (the hashes of past blocks).
- **It speeds up synchronization.** Each node needs to download only a small amount of data (the timestamps) from other nodes instead of needing to download the entire history of the blockchain.

Solana claims to process 710,000 transactions per second on an adversarial network, making it one of the fastest blockchain platforms in the world. Its unique consensus algorithm and high-performance capabilities make it well-suited for use cases such as supply chain management and identity verification.

Solana's PoH is a unique consensus mechanism that allows the Solana blockchain to achieve high transaction throughput and low transaction fees. It works by using a verifiable delay function (VDF) to secure the network, instead of relying on PoW like many other blockchain platforms do.

In a PoW system, miners compete against each other to solve complex mathematical puzzles in order to validate transactions and add them to the blockchain. This process consumes a lot of energy and can be slow, making it difficult to scale. In contrast, Solana's PoH system uses a VDF to randomly select the validators (called *validator nodes*) who will add the next block of transactions to the blockchain.

The VDF is a cryptographic function that takes a long time to compute, but is easy to verify after it has been computed. This means that the validator nodes can use the VDF to generate random numbers in a way that is secure and verifiable by the rest of the network. The validator nodes use these random numbers to determine which node will add the next block of transactions to the blockchain.

This process is much more efficient than PoW, because it doesn't require miners to compete against each other and consume large amounts of energy. It also allows for much higher transaction throughput and lower transaction fees, making it well-suited for large-scale decentralized applications. Additionally, because the VDF is easy to verify, the Solana network can reach consensus quickly and securely.

THE MAN BEHIND PROOF OF HISTORY

In November 2017, Anatoly Yakovenko published a whitepaper about PoH, a technique for keeping time between computers that don't trust each other. This technique was intended to make it possible for blockchain systems to scale up to the level of centralized payment systems like Visa.

Yakovenko implemented the technique in a private codebase using the C programming language. Greg Fitzgerald, a core developer fore Solana, encouraged Yakovenko to switch to the Rust language, and Yakovenko did so in just two weeks. Fitzgerald then began prototyping the open-source implementation of Yakovenko's whitepaper, publishing it on GitHub under the name Silk.

In 2018, the team behind the project created a company called Loom. However, to avoid confusion with another project called Loom Network, they rebranded as Solana and published a 50-node test net that consistently supported bursts of 250,000 transactions per second.

Overall, Solana's PoH consensus mechanism is a key feature that sets it apart from other blockchain platforms and allows it to achieve high levels of scalability and performance.

Solana's native token

SOL is the native token of the Solana platform. It can be used to pay nodes in a Solana cluster for running on-chain programs or validating their output. The system also uses micropayments called lamports, which are fractions of a SOL. These lamports are named after Solana's biggest technical influence, Leslie Lamport, a famous American computer scientist. Each lamport has a value of 0.000000001 SOL.

The value of SOL is determined by market forces, just like any other cryptocurrency. SOL can be traded on cryptocurrency exchanges, and it can be used to make payments for goods and services at merchants that accept it.

Accounts on Solana

Solana accounts are a fundamental part of the Solana blockchain, serving as the basic unit of storage for data and code. In many ways, they're similar to files in operating systems like Linux, because they're able to hold arbitrary, persistent data and they can be used in a wide variety of ways.

One of the key uses of Solana accounts is to store the platform's native token, SOL. As with other cryptocurrencies, SOL can be used to transfer value on the Solana network and can be bought and sold on exchanges. However, Solana accounts are not limited to just holding SOL; they can also be used to store custom data structures and executable code.

These data structures and code are used to create dApps on the Solana platform. When an account contains code, it can be run as a program on the Solana network, allowing it to interact with other accounts and data on the blockchain. This makes Solana accounts a powerful tool for building a wide range of dApps and decentralized systems.

Overall, Solana accounts are an essential part of the Solana ecosystem, and they're involved in nearly everything that users do with the platform. Whether you're using SOL to transfer value, building a dApp, or storing custom data, Solana accounts are at the heart of it all.

Rent on Solana

One important thing to keep in mind about Solana is that storing data in accounts costs SOL to maintain. This is called *rent.* The good news is that if you maintain a minimum balance equivalent to two years of rent payments in your account, you'll be exempt from paying rent. You can also get your rent back by closing the account and sending the lamports back to your wallet.

You need to pay rent once an epoch (every two days). The cost of rent on the Solana blockchain depends on various factors, including the size of the data being stored, the length of time it will be stored, and the current demand for storage on the network.

In general, the cost of rent on the Solana blockchain is calculated based on the amount of storage space and the duration you need. You can choose to rent storage for a specific period of time, or you can choose to pay on a recurring basis.

The cost of rent is also influenced by supply and demand. If there is a high demand for storage on the network, the cost of rent may be higher. Conversely, if there is a lower demand for storage, the cost of rent may be lower.

It's important to note that the cost of rent on the Solana blockchain is not fixed and can change over time. Users should carefully consider their storage needs and budget accordingly.

A percentage of rent collected by Solana is destroyed. The rest of the rent is distributed to vote accounts at the end of every slot. If your account doesn't have enough SOL to pay rent, your account will be deallocated and the data will be removed.

Public keys and Solana

Public keys, also known as addresses, are a crucial part of the Solana blockchain. They're the unique identifiers that point to accounts on the network, and they're necessary for interacting with those accounts. If you want to run a program or transfer SOL on the Solana network, you'll need to provide the appropriate public key(s) to do so.

Public keys on Solana are 256-bit values, which are typically represented as base-58 encoded strings. This means that they're composed of a combination of letters and numbers, and they look something like this:

```
7C4jsPZpht42Tw6MjXWF56Q5RQUocjBBmciEjDa8HRtp
```

These strings are long and complex, but they're necessary to ensure the uniqueness and security of each public key on the network.

In addition to being used to identify accounts on the Solana network, public keys are used to verify the authenticity of transactions. When a transaction is signed with a private key, the corresponding public key is used to verify that the transaction is valid and came from the correct account. This ensures the security and integrity of the Solana network.

Overall, public keys play a crucial role in the Solana ecosystem, providing a unique and secure way to identify accounts and verify transactions. Whether you're running a program, transferring SOL, or interacting with a dApp, you'll need to use public keys to do so.

Solana's clusters

A *Solana cluster* is a group of independently owned computers that work together to verify the output of user-submitted programs. The cluster can be used to preserve a record of events and their programmatic interpretations, as well as to track the possession of assets and the computers performing meaningful work to maintain the cluster.

The Solana cluster produces a *ledger,* which is a record of all events that is preserved for the lifetime of the cluster. As long as a copy of the ledger is maintained, the output of the cluster's programs can be reproduced and will remain independent of the organization that launched it.

Getting Up and Running on Solana

Solana Playground is a browser-based integrated development environment (IDE) for Solana. It allows you to develop and deploy Solana programs without having to install any software on your computer. Simply open Solana Playground in your web browser, and you're ready to start writing and deploying Solana programs.

In this section, you use Solana Playground to develop and deploy a basic Solana program. This will help you get started with Solana Playground and give you a taste of what it's like to develop on the Solana platform.

After finishing this section, you'll have a basic understanding of how to use Solana Playground and how to develop on the Solana platform. This will set you up for success as you continue to learn and explore the world of blockchain development.

Creating a Playground wallet

When developing on the Solana platform using Solana Playground, you don't need to create a file system wallet using the Solana command-line interface (CLI). Instead, you can create a browser-based wallet with just a few clicks.

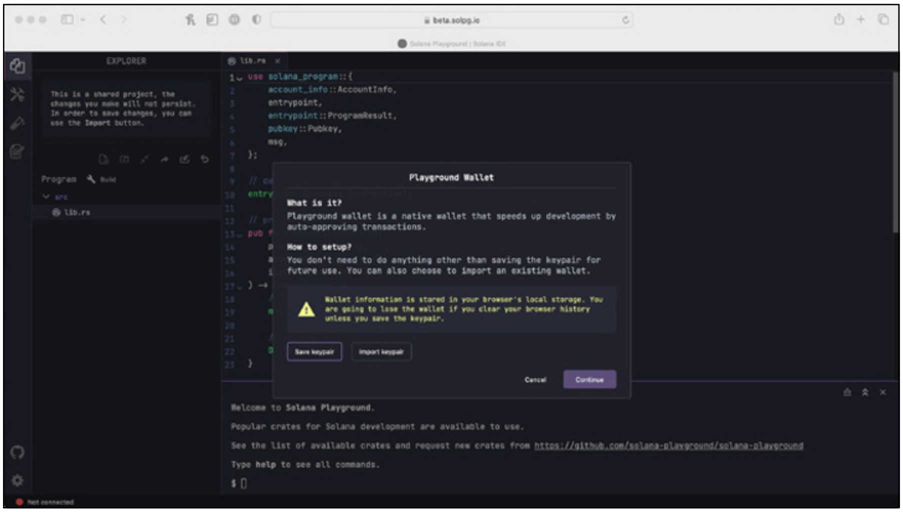
To set up your Playground wallet, follow these steps:

1. **Go to** `https://beta.solpg.io/6314a69688a7fca897ad7d1d`.
2. **Click the red status indicator in the lower left (where it says Not Connected).**

   A popup window appears (see Figure 8-1), giving you the option to save a local copy of your wallet's keypair file.

   WARNING

   Your Playground wallet is saved in your browser's local storage. If you clear your browser cache, your saved wallet will be removed. Therefore, it's important to make sure to save a local copy of your wallet's keypair file for backup. This will ensure that you can access your wallet even if you need to clear your cache.
3. **Click Save Keypair.**
4. **Click Continue to create your wallet.**



This is a shared project, the changes you make will not persist. In order to save changes, you can use the Import button.

```
use solana_program::{
    account_info::AccountInfo,
    entrypoint,
    entrypoint::ProgramResult,
    pubkey::Pubkey,
    msg,
};
```

Playground Wallet

What is it?
Playground wallet is a native wallet that speeds up development by auto-approving transactions.

How to setup?
You don't need to do anything other than saving the keypair for future use. You can also choose to import an existing wallet.

Wallet information is stored in your browser's local storage. You are going to lose the wallet if you clear your browser history unless you save the keypair.

```
Welcome to Solana Playground.

Popular crates for Solana development are available to use.

See the list of available crates and request new crates from https://github.com/solana-playground/solana-playground

Type help to see all commands.

$
```

FIGURE 8-1: Decide whether to save a local copy of your wallet's keypair file for backup.

After your Playground Wallet is created, you'll see your wallet's address, your SOL balance, and the Solana cluster you're connected to at the bottom of the screen. By default, you'll be connected to the Devnet cluster, but you can also connect to a localhost test validator if you prefer. Consider using testnest when experimenting because it's free.

Creating a Solana program

Solana uses Rust, a systems programming language that is designed to be fast, safe, and concurrent. It was created in 2010 by Graydon Hoare and is sponsored by the Rust Project, a collaborative effort of volunteers.

The code for your Rust-based Solana program lives in the `src/lib.rs` file within Solana Playground. This file is where you'll import your Rust crates and define the logic of your program. In Rust, a *crate* is a compiled binary or library that can be used as a dependency in other Rust projects. Crates are published to a central package registry called `crates.io`, which allows developers to easily discover and reuse existing code.

The `solana-program` crate provides the necessary tools and functionality for developing Solana programs in Rust. The Solana team has helpfully added the code with comments on the page when you load it, so it's easy for you to look back at it to check your work.

Importing the solana-program crate

Follow these instructions to guide you through the process of creating a new Rust program that uses the `solana-program` crate.

1. **Go to `https://beta.solpg.io/6314a69688a7fca897ad7d1d`.**
2. **Click the file icon in the upper left to create a new file.**
3. **Name the file `test.rs`.**
4. **Add the following code to the top of your `test.rs` file:**

```
use solana_program::{
    account_info::AccountInfo,
    entrypoint,
    entrypoint::ProgramResult,
    pubkey::Pubkey,
    msg,
};
```

The code you just added imports the `solana-program` crate and brings the needed items into the local namespace, allowing you to use them in your program. With this code in place, you're ready to begin writing the logic of your Solana program.

Writing your program logic

Every Solana program must define an `entrypoint`, which tells the Solana runtime where to start executing your on-chain code. The `entrypoint` is a public function named process_instruction that takes three arguments: program_id, accounts, and instruction_data.

You'll use the process_instruction function to log the message "Hello, world!" to the blockchain and then gracefully exit with the Ok(()) result. This tells the Solana runtime that the program executed successfully without any errors.

After you've written the code for your Solana program, you can build it using the Build & Deploy tab in the left sidebar of Solana Playground.

1. **Go to** https://beta.solpg.io/6314a69688a7fca897ad7d1d.
2. **Input this code in the** test.rs **file from the preceding section:**

```
// declare and export the program's entrypoint
entrypoint!(process_instruction);

// program entrypoint's implementation
pub fn process_instruction(
    program_id: &Pubkey,
    accounts: &[AccountInfo],
    instruction_data: &[u8]
) -> ProgramResult {
    // log a message to the blockchain
    msg!("Hello, world!");

    // gracefully exit the program
    Ok(())
}
```

3. **Click the Build button.**

   Your program begins to compile.

If the build is successful, you'll see a success message in the Playground's terminal. You may receive some warnings about unused variables, but these won't affect the build of your program — you can safely ignore them.

Deploying your program

After you've successfully built your Solana program (see the preceding section), you can deploy it to the Solana blockchain using the Deploy button (it looks like a wrench and hammer) on the Build & Deploy tab of Solana Playground. Your program is deployed to the selected Solana cluster, such as Devnet or Testnet.

When you deploy your program, you'll see your Playground wallet balance change. By default, Solana Playground will automatically request SOL airdrops on your behalf to ensure that your wallet has enough SOL to cover the cost of deployment. If you need more SOL, you can airdrop more by typing **solana airdrop** in the Playground terminal, followed by the amount of SOL you want to airdrop, like this:

```
solana airdrop 2
```

This command airdrops 2 SOL to your wallet, allowing you to deploy your program and interact with it on the Solana blockchain.

Initializing your client

You'll use Solana Playground to create a client for your Solana program by using the `run` command in the Playground terminal to create a `client` folder and a default `client.ts` file. This is where you'll work for the rest of the "Hello, world!" program.

From where you left off at the end of the "Writing your program logic" section, you're now ready to run your program.

Step 1: Running your program

To run your "Hello, world!" program, follow these steps:

1. **Open the Solana Playground in your web browser by going to** `https://beta.solpg.io`**.**
2. **In the Playground terminal, which is the black box at the bottom of the screen, enter** run**.**

In Solana Playground, there are many utilities that are globally available for you to use without having to install or set up anything. The most important ones for the "Hello, world!" program are `web3` for `@solana/web3.js` and `pg` for Solana Playground utilities. You can access these utilities by pressing Ctrl+Space (Windows) or ⌘+Space (macOS) inside the editor.

FINDING YOUR PROGRAM ID

When you're executing a Solana program using web3.js or from another Solana program, you'll need to provide the program ID, which is also known as the public address of your program. You can find your program ID on the Build & Deploy sidebar in Solana Playground, under the Program Credentials drop-down.

Step 2: Creating your transaction

To execute your on-chain program, you must send a transaction to it. Each transaction submitted to the Solana blockchain contains a listing of instructions and the programs that these instructions will interact with. To create a new transaction and add a single instruction to it, use the following code:

```
// create an empty transaction
const transaction = new web3.Transaction();

// add a hello world program instruction to the transaction
transaction.add(
  new web3.TransactionInstruction({
    keys: [],
    programId: new web3.PublicKey(pg.PROGRAM_ID),
  })
);
```

Each instruction must include all the keys involved in the operation and the program ID that you want to execute. In this example, `keys` is empty because your program only logs "Hello, world!" and it doesn't need any accounts.

Step 3: Signing your transaction

After you've created your transaction, you can submit it to the Solana cluster using the following code:

```
// send the transaction to the Solana cluster
console.log("Sending transaction...");
const txHash = await web3.sendAndConfirmTransaction(
  pg.connection,
  transaction,
  [pg.wallet.keypair]
);
```

It's worth noting that the first signer in the `signers` array is the transaction fee payer by default. In this case, you're signing with your `pg.wallet.keypair`.

Running your application

You can use the `run` command in Solana Playground to run the client application you've written. After your application completes, you'll see output similar to the following:

```
Running client...
  client.ts:
   My address: GkxZRRNPfaUfL9XdYVfKF3rWjMcj5md6b6mpRoWpURwP
   My balance: 5.7254472 SOL
   Sending transaction...
   Transaction sent with hash: 2Ra7D9JoqeNsax9HmNq6MB4qWtKPGc
 LwoqQ27mPYsPFh3h8wignvKB2mWZVvdzCyTnp7CEZhfg2cEpbavib9mCcq
```

You can use `solana-cli` directly in Solana Playground to get information about a transaction. Run the following command, replacing *`TRANSACTION_HASH`* with the hash you received from calling the "Hello, world!" program:

```
solana confirm -v TRANSACTION_HASH
```

You should see `"Hello, world!"` in the `Log Messages` section of the output.

You're now a Solana developer! You can try updating your program's message and rebuilding, redeploying, and re-executing your program to see how it works.

Building a DAO on Solana

Realms is a platform on the Solana blockchain that allows users to easily create and manage DAOs. With Realms, you can create custom DAOs, manage your members, vote on proposals, and allocate your *treasury* (funds you have put inside a smart contract). The platform is designed to be flexible and can be used to create a variety of different types of DAOs, including multisig, nonfungible token (NFT) community, and community token DAOs. An NFT community could be used, for example, by an artist to help them distribute their music first to their super-fans. A DAO uses tokens to give its members voting rights in its governance. For example, a DAO could be used to manage a charity.

Realms also serves as the front end for SPL Governance, a standard for building and maintaining DAOs on Solana that is agnostic to both DAO type and asset type. This makes it easy for builders to create DAOs that are tailored to the specific needs of their communities.

At its core, a DAO is a community with a shared bank account that is run and governed by smart contracts on a blockchain. Members of a DAO can use it to make decisions in a transparent and decentralized way, with smart contracts executing those decisions. For example, a member may create a proposal suggesting an investment of the DAO's treasury or a program upgrade. The other members of the DAO can then vote on the proposal, and if a predefined quorum votes in favor of it, the proposal is accepted and executed by a smart contract.

This structure provides a flat organizational structure, where every member of the DAO has an equal say in the direction of the organization. This allows for more democratic and decentralized decision making, which can be beneficial for a variety of different types of communities.

To set up your Solana DAO, you'll need two clean pieces of paper to write down your password and seed phrase. You'll also need to purchase some SOL. The minimum purchase with the Phantom wallet is $50.

Creating a Solana wallet

To create a Solana wallet, follow these steps:

1. **Go to `https://phantom.app`.**
2. **Click Download.**
3. **Click Brave.**
4. **Click Add to Brave.**
5. **Click Add Extension.**
6. **Click Create a New Wallet.**
7. **Write down your password on a clean piece of paper.**
8. **Write down your seed on the other piece of paper.**
9. **Click through to finish.**

You now have a secure place to keep your SOL and interact with the Solana blockchain. Don't forget to keep your password and seed phrase safe. You may even consider laminating the paper so it's harder to damage.

Getting your hands on SOL

Now you need to load your wallet with SOL so you have the required amount to build your contract. Follow these steps:

1. **Open the Brave web browser, and navigate to your browser extensions.**
2. **Open your Phantom wallet.**
3. **Click Buy.**
4. **Click Solana.**
5. **Enter a minimum of $50.**

6. **Click Next.**
7. **Click Coinbase.**
8. **Click Authorize.**
9. **Click Preview Buy.**
10. **Click Confirm.**

Now you have your wallet loaded with SOL, and you can move on to building your DAO.

Creating a DAO on Realms

Creating a DAO on Realms is a simple and straightforward process that involves a few key steps. By following these steps, you can create your own custom DAO and start using it to make decisions in a decentralized and transparent way:

1. **Go to** `https://app.realms.today`**.**
2. **Click the Create DAO button.**

   Your Phantom wallet appears.
3. **Click the Connect button.**
4. **Select the Community Token DAO.**
5. **Enter the name of your community.**
6. **Under Do You Have an Existing Token for Your DAO's Community, select the No, Let's Create One radio button.**
7. **Under What Is the Minimum Number of Community Tokens Needed to Manage This DAO, enter** 10**.**
8. **Set your community approval quorums to 60%.**
9. **Under Do You Have an Existing Token for Your DAO's Council, select No.**
10. **Click the next arrow.**
11. **Click Create Community Token DAO.**
12. **When your Phantom wallet pops up, click Approve.**

3

Powerful Blockchain Platforms

IN THIS PART . . .

Ascertain the largest business blockchain consortium, Hyperledger, and what benefits and impact it will have for your industry and organization.

Understand Microsoft's blockchain efforts and core tools available to you through its network offerings.

Evaluate the IBM Bluemix project and the implications of blockchain technology combined with artificial intelligence.

IN THIS CHAPTER

- » Uncovering Hyperledger Foundation
- » Discovering key Hyperledger projects
- » Uncovering Hyperledger Besu
- » Mining on the Ethereum development network with Besu

Chapter 9
Getting Your Hands on Hyperledger

Hyperledger is a foundation that supports a community of software developers and technology enthusiasts who are building industry standards for blockchain frameworks and platforms. Hyperledger's work is crucial because they're creating blockchain technology that fits the needs of businesses. Cryptocurrencies on public blockchains have regulatory implications and liabilities that prevent many companies from utilizing these networks. Hyperledger has many of the same benefits of public blockchain technology but operates without a cryptocurrency. With big supporters such as Intel and IBM, Hyperledger is the "trusted" deployment platform for enterprise teams.

Hyperledger and its unique project are growing every day. As of this writing, it has more than 100 member companies and several blockchain applications in incubation. Hyperledger's first few projects include Fabric, Iroha, and Sawtooth. These are frameworks that developers can use to build private blockchains, create smart contracts, and build distributed identity for people and things.

In this chapter, I explain how to create an asset tracking and a smart auction application using Hyperledger's Composer tool. I also introduce you to the Fabric, Iroha, and Sawtooth projects. You gain a deep understanding of what the future of commercialized blockchain will hold for your company and industry. This knowledge will help you as you explore which technologies to utilize and which to avoid, saving you development time and resources.

Getting to Know Hyperledger

At the end of 2015, the Linux Foundation formed the Hyperledger project to develop an enterprise-grade and open-source distributed ledger framework. They hoped to focus the blockchain community on building robust, industry-specific applications, platforms, and hardware systems to support businesses.

The Linux Foundation saw that there were many different groups building blockchain technology without a cohesive direction. The industry was duplicating effort, and the tribalism was leading teams to solve the same problem twice. The foundation members saw similarities between the birth of the Internet and the emergence of blockchain technology: If blockchain was going to realize its fullest potential, an open-source and collaborative development strategy was desperately needed.

The Hyperledger project is led by Executive Director Brian Behlendorf, who has decades of experience dating back to the original Linux Foundation and Apache Foundation, as well as being a chief technology officer (CTO) of the World Economic Forum. So, it's not surprising that Hyperledger has been well received. Many of the top business and industry leaders have joined the project, including Accenture, Cisco, Fujitsu Limited, IBM, Intel, J.P. Morgan, and Wells Fargo. It has also attracted many of the top blockchain organizations.

Hyperledger's technical steering committees ensure robustness and interoperability between these different technologies. The hope is that the cross-industry, open-source collaboration will advance blockchain technology and deliver billions of dollars in economic value by sharing the costs of research and development across many organizations.

Hyperledger is identifying and addressing the critical features and requirements missing from the blockchain technology ecosystem. It's also fostering a cross-industry open standard for distributed ledgers and holding open space for developers to contribute to building better blockchain systems.

Hyperledger has a project life cycle similar to that of the Linux Foundation. A proposal is submitted, and then the accepted proposals are brought into incubation. When a project has reached a stable state, it graduates and is moved into an active state. As of yet, all Hyperledger projects are in the proposal or incubation stage. Each of the projects is led by a large corporation or startup. For example, Fabric is led by IBM, Sawtooth by Intel, and Iroha by the startup Soramitsu.

TIP

Hyperledger, like many open-source projects, uses GitHub (`www.github.com/hyperledger`) and Slack (`https://slack.hyperledger.org`) to connect with teams working on each of the projects. These are great places to get the latest updates and to check on the progress that these projects are making in development.

Identifying Key Hyperledger Projects

Hyperledger has several revolutionary projects under incubation. In this section, I fill you in on the three most prominent and well-developed projects. These blockchain technologies include distributed ledger frameworks, smart contract engines, client libraries, graphical interfaces, utility libraries, and sample applications.

Focusing on Fabric

Fabric was the first blockchain implementation on Hyperledger. It has become the foundation for developing most blockchain applications. Fabric is unique within the blockchain ecosystem because it allows developers to use pieces of Fabric without committing to all the functionality — a truly tailored plug-and-play experience. Fabric also can create smart contracts called *chaincode.*

Fabric is a permissioned blockchain and does not utilize a cryptocurrency. This means that all the participants are known (as opposed to on a typical public blockchain where all the participants are anonymous by default). Fabric works like most blockchains in that it keeps a ledger of digital events. These events are structured as transactions and shared among the different participants. The transactions are executed without a cryptocurrency (in contrast, a public blockchain uses its native cryptocurrency to pay the network to operate and to allow all the participants to remain anonymous). To dive deeper into the subject of Fabric, go to `https://trustindigitallife.eu/wp-content/uploads/2016/07/marko_vukolic.pdf`.

All transactions are secured, private, and confidential. Fabric preserves its integrity by only allowing updates by consensus of the participants. When records have been inputted, they can never be altered.

Fabric is an enterprise solution interested in scalability and complying with regulations. All participants must register proof of identity to membership services to gain access to the system. Fabric issues transactions with derived certificates that are unlinkable to the owning participant, thereby offering anonymity on the network. Also, the content of each transaction is encrypted to ensure only the intended participants can see the content.

Fabric has a modular architecture. You can add or take away components by implementing its protocol specification. Its container technology can handle most of the mainstream languages for smart contracts development.

Looking at the Inter-American Development Bank's work on Fabric

The Inter-American Development Bank (IDB) has been working with Fabric to support its cross-board innovations. IDB's efforts include forming an innovation lab called IDB Lab.

The IDB Lab was formed to find solutions to the problems of regulatory compliance, support, and governance. As it investigated the problem, IDB Lab formed LACChain, a permissioned public blockchain infrastructure. LACChain is a scalable and sustainable network for the Latin America and the Caribbean (LAC) region, implementing neutral, accountable, and robust governance.

Double-checking identity

LACChain addressed a major problem by developing a system that ensures compliance with regulations that require accountability for transactions. To achieve this, LACChain implemented two signature levels:

- The first level is permissioned, which means that access is granted only to individuals or organizations that have been vetted and identified.
- The second level allows for greater anonymity, because it separates the identity of the signer from the transaction, preventing the general public from knowing who signed it.

The permissioned layer of this system is built on Hyperledger Besu, while the public layer is based on Ethereum.

Anyone can join the LACChain networks by deploying a node. Each node can be a validator, boot, writer, and observer. You choose your deployment environment, which can be cloud or on-premises.

Entities must comply with the terms and conditions for LACChain testnets and the Adscription Agreement for LACChain Mainnet. The terms and conditions agreement requires that every node operator is responsible for the transactions it sends to the network and their content. The LACChain Mainnet requires each node that broadcasts transactions to sign them and the anonymous end-user signature.

LACChain implemented protocols for self-sovereign identity. This is a type of identity that the individual creates for itself versus one issued by a third party like a government or corporation.

Quantum-proofing LACChain

One of the existential threats blockchains face is quantum computers that are faster than classical computers. Quantum computers use the rules of quantum mechanics to do calculations and solve problems. They work differently from regular computers because they use qubits instead of regular bits to store and process information.

Classical computers store and process information using bits that can only be in one of two states (0 or 1), whereas qubits can exist in multiple states simultaneously. This property, known as *superposition,* allows quantum computers to perform certain types of calculations, such as breaking encryption, much faster than classical computers. The more qubits a computer has, the faster it can solve problems. Quantum computers are still being developed and have some challenges to overcome before they have enough accuracy and qubits to crack public key encryption used in blockchain technology.

Public key encryption is used by much of the Internet's infrastructure, so it will be a way bigger problem than someone having the ability to steal your Bitcoins.

TECHNICAL STUFF

IDB Lab, Cambridge Quantum Computing, and Tecnológico de Monterrey joined forces to address a specific problem using new post-quantum cryptography algorithms for public-key encryption and key establishment. With the help of the National Institute of Standards and Technology (NIST), a U.S. government agency that promotes innovation and industrial competitiveness, IDB Lab is able to test two new candidate algorithms called CRYSTALS-Dilithium and FALCON to add an extra layer of protection to the LACChain blockchain that is resistant to attacks from quantum computers in the future.

Economic sustainability

One of the trade-offs of using a public blockchain is that each transaction has a hard cost. You probably remember that there are transaction fees paid to nodes on public networks. Every blockchain has a different fee that will change over time and network congestion. The reason for this structure is to prevent individuals from spamming the network. When too many transactions hit the network simultaneously, it creates a denial of service (DoS) to legitimate users.

LACChain found a workaround that allowed it to solve this issue while still providing free transactions to users. It developed a new gas Distribution Protocol using smart contracts. It assigns gas per block to permissioned writer node accounts. The distribution of gas is dynamic to the stress of the network. More gas is available if fewer entries are being made; less gas is available if the network is saturated.

The Gas Distribution Protocol is a smart contract–based solution. The smart contracts evaluate all the transactions sent to the network and analyze how much gas is used per block. It also checks that the nodes sign the transactions and have enough gas.

Future governance of LACChain

LACChain created LACNet as an international nonprofit with the backing of Red Clara, another nonprofit that supports the academic community in Latin America. LACNet also has the support of the Internet Addresses Registry for Latin America and the Caribbean (LACNIC). Together these organizations will support the future of LACChain.

When this book was written, 60 projects were using the LACChain networks. With the innovations in quantum proofing and supporting free transactions not subject to DoS attacks, LACChain may become an essential innovation in the future of permissioned blockchains.

Investigating the Iroha project

Hyperledger's Iroha project is building on the work completed in the Fabric project. It's meant to complement Fabric, Sawtooth Lake, and the other projects under Hyperledger. Hyperledger added the Iroha project to incubation because the other projects didn't have any infrastructure projects written in C++. Not having a C++ project severely limited how many people could benefit from the work on Hyperledger and the number of developers who could contribute to the project.

Besides, most blockchain development at this point has been at the lowest infrastructure level, and there has been little to no development work on user interaction or mobile applications. Hyperledger believes that Iroha is necessary for the popularization of blockchain technology. This project fills the gap in the market by bringing in more developers and providing libraries for mobile user interface development.

At the time of this writing, Iroha is a very new project and has not integrated with Fabric or Sawtooth Lake. Hyperledger has plans to expand functionality to work with the other blockchain projects soon. Its iOS, Android, and JavaScript libraries will provide supportive functions like digitally signing transactions. It will be handy for commercial app development, and it will add new layers of security and business models only possible with blockchain technology.

Introducing Sumeragi: The new consensus algorithm

Blockchains have systems that allow them to first agree on a single version of the truth and then record that agreed-upon truth in their ledger. An agreement system is called a *consensus.* A consensus is complicated. Grasping the nuances of how and why consensuses act in the way they do is well beyond the scope of this book. It's also far more than you'll ever need as a business professional. What *does* matter for you are the consequences of different consensus mechanisms and how they affect what you're doing on that particular blockchain. I'm highlighting Iroha's consensus, Sumeragi, because it's very different from traditional blockchains.

Here are a few key things that make Sumeragi different:

- **Sumeragi does not have a cryptocurrency.**
- **Nodes that start consensus are added into the system by the Fabric member services.** Nodes build a reputation over time based on how they've interacted with the ledger. This is a permission blockchain run by known entities.
- **New entries are added to the ledger in a unique way.** The first node that starts consensus, called the *leader,* broadcasts the entry to a group of other nodes; those nodes then validate. If they don't validate, the first node will rebroadcast after a predetermined duration of time.

Depending on your use case for blockchain, Iroha may be positive or negative. If you're worried about censorship, Iroha may not be right for you. In this case, you'll be better off looking at a blockchain that is censorship resistant. If you're worried about other players on the network committing arbitrage, Iroha may also not be right — further investigation is needed. If you want to know all the players in your blockchain, Iroha may be exactly what you're looking for.

Developing mobile apps

TIP

Skip this section if you aren't part of the app development space.

Iroha is built for the web and mobile app developers so they can access the strengths of the Hyperledger systems. The Iroha team saw that having a distributed ledger wasn't useful if there were no applications utilizing it.

Iroha has a development path for the following encapsulated C++ components:

- Sumeragi consensus library
- Ed25519 digital signature library

- SHA-3 hashing library
- Iroha transaction serialization library
- P2P broadcast library
- API server library
- iOS library
- Android library
- JavaScript library
- Blockchain explorer/data visualization suite

One of the major hurdles of the blockchain industry has been in making systems user-friendly. Iroha has created open-source software libraries for iOS, Android, and JavaScript and made common application programming interface (API) functions convenient to call. It's still early in development, but Iroha is a good resource to explore for business use cases.

Diving into Sawtooth Lake

Sawtooth Lake by Intel is another distributed ledger project in Hyperledger. It's focused on being a highly modular platform for building new distributed ledgers for companies.

WARNING

As of this writing, the release version has software that is only *simulating* the consensus. It doesn't provide security for your project and should only be utilized for testing out new ideas.

Sawtooth Lake does not operate with a cryptocurrency. It maintains the security of the platform by allowing businesses to create private blockchains. These businesses running private blockchains then share the burden of computational requirements of the network. In its documentation, Sawtooth Lake states that this type of setup will ensure universal agreement on the state of the shared ledger.

Sawtooth Lake has taken the basic model of blockchains and turned it on its head. Most blockchains have three elements:

- A shared record of the current state of the blockchain
- A way of inputting new data
- A way of agreeing on that data

Sawtooth Lake merges the first two into a signal process it calls a *transaction family.* This model is best in use cases where all the participating parties have a mutual benefit to having a correct record.

Intel has allowed its software to be flexible enough to accommodate custom transaction families that reflect the unique requirements of each business. It also built three templates for building digital assets:

- **EndPointRegistry:** A place to record items in a blockchain
- **IntegerKey:** A shared ledger that is used for supply chain management
- **MarketPlace:** A blockchain trading platform for buying, selling, and trading digital assets

The consensus algorithm for Sawtooth Lake is called Proof of Elapsed Time (PoET). It was built to run in a secure area of the main processor of your computer, called a *trusted execution environment* (TEE). PoET leverages the security of the TEE to prove that time has passed by time-stamping transactions.

Other consensus algorithms have some kind of time-stamping element as well. The way they ensure that the records have not been changed is through publicly publishing their blockchains as proof that they have not been altered. The published ledger acts as a public witness that anyone can roll back and check. It's sort of like publishing an ad in a newspaper to prove something happened.

PoET also has a lottery system that works a bit differently from other blockchains using proof of work. It randomly selects a node from the pool of validating nodes. The probability of a node being selected increases proportionally to how much processing resources that node contributed to the shared ledger. Measures may be put in place to prevent nodes from gaming the system and corrupting the ledger.

Working with Hyperledger Besu

Hyperledger Besu is an Ethereum client that supports smart contract and dApp development, deployment, and operational use cases, using tools such as Truffle, Remix, and web3j. It was developed under the open-source Apache 2.0 license and written in Java. You can run Besu on the Ethereum public network or your own private permissioned network. It also works on the Ethereum test networks Rinkeby, Ropsten, and Görli.

Besu's Core features include an Ethereum virtual machine (EVM). The EVM is the Turing environment that allows you to deploy and execute smart contracts on the Ethereum blockchain.

One of the main reasons you may consider Besu is because it has implemented several consensus algorithms. Consensus is how the network agrees on the state of its blockchain and the transaction's validity. The consensus algorithm will dictate the cost, speed, and scalability of your software.

Here are two popular options that Besu offers:

- **Proof-of-authority (PoA):** PoA consensus protocols are used when participants are known to each other. The transactions and blocks on a POA network are validated by approved validators. Validators take turns creating the next block and don't compete for block rewards.
- **Proof-of-work (PoW):** POW consensus protocols are used when participants are not known. The transaction and blocks on POW networks are validated by the nodes that win each block.

Besu uses a RocksDB database to store chain data locally. This type of database is excellent for fast and low-latency storage. It allows you to quickly pull the blockchain's ordered transactions and the metadata for each transaction.

Besu allows you to monitor node and network performance using a tool called Prometheus or via the debug_metrics JSON-RPC API. You can also keep an eye on performance with another tool called Alethio.

Besu also allows you to keep your transactions private. This means that third parties cannot access the transaction content, sending party, or list of participating parties.

Overall, Besu lets you both build and deploy smart contracts on the most popular smart contract platform, Ethereum, while also giving you some of the benefits of private enterprise blockchain software.

Setting up your system for Besu

You can use the Hyperledger Besu on all systems with a Docker image to run a node in a container. If you're a moderately proficient developer, it's easy to follow the documentation on the Docker website and the Hyperledger website for Besu.

In the following sections, you find out how to set up Besu for your iOS system and how to deploy your own network. You'll need the following:

- A Mac running macOS 10.13 (High Sierra) or a more recent version of macOS
- A web browser
- An Internet connection
- Experience accessing your computer's Terminal application
- Java 17, which will be the minimum requirement in the next Besu version series

You'll also be downloading Teku, an open-source Ethereum consensus client. Teku lets you run a full beacon node implementation and a validator client for participating in proof-of-stake consensus.

TIP

You can also install Java using brew install OpenJDK.

Step 1: Preparing your system to install Besu

The first step is to install Homebrew:

1. **Go to the Homebrew website at** `https://brew.sh`**.**
2. **Under Install Homebrew, copy the command line code.**
3. **Open the Terminal application on your Mac.**

   Terminal is in the `Applications/Utilities` folder.
4. **Paste the code into Terminal.**
5. **If your system requests your password, enter it.**
6. **Press Enter.**
7. **Press Enter again when Terminal prompts you.**

Step 2: Installing Java

To install Java, follow these steps:

1. **Go to the Oracle website at** `www.oracle.com/java/technologies/downloads/`**.**
2. **Select your computer's operating system.**
3. **Click the Installer option.**
4. **Click through to complete the download process.**

Getting up and running on Besu

In this section, you connect to the Ethereum development network and start mining test ETH.

Step 1: Installing Besu

To install Besu, follow these steps:

1. **Open the Terminal application.**
2. **Type the following command line code into Terminal:**

```
brew tap hyperledger/besu
brew install hyperledger/besu/besu
```

3. **Check your Besu version by entering this command in Terminal:**

```
besu --version
```

Step 2: Installing Teku

To install Teku, follow these steps:

1. **Open the Terminal application.**
2. **Type the following command line code into Terminal:**

```
brew install ConsenSys/teku/teku
```

3. **Check your Teku version by entering this command in Terminal:**

```
Teku --version
```

Step 3: Starting Besu

To start Besu and join the development test network, follow these steps:

1. **Open the Terminal application.**
2. **Type the following command line code into Terminal.**

```
besu --network=dev --miner-enabled --miner-coinbase=0xfe3b5
   57e8fb62b89f4916b721be55ceb828dbd73 --rpc-http-cors-
   origins="all" --host-allowlist="*" --rpc-ws-enabled
   --rpc-http-enabled --data-path=/tmp/tmpDatdir
```

Congratulations! You're now up and running on the Ethereum development test network using Hyperledger's Besu. If you enjoyed this tutorial and want to learn more about building a private network or creating smart contracts, head to `https://besu.hyperledger.org/en/stable/private-networks/tutorials`.

IN THIS CHAPTER

- Building new applications
- Bridging your systems
- Authenticating new systems
- Deploying private Ethereum

Chapter 10
Applying Microsoft Azure

In this chapter, you get a preview of the exciting innovations that are taking place inside of Microsoft's Azure platform and how these changes can improve your business's efficiency and create new opportunities for products and services.

This chapter helps you compete for, collaborate with, and service customers in a global economy. Blockchain technology is opening new markets and changing business models. Microsoft is working hard to make it an accessible technology for traditional business.

This chapter also explains innovative blockchain bridges that are being built to allow you to connect and scale your existing systems. You find out how to deploy your own blockchain inside Azure and the keys elements to making a safe and hassle-free transition to blockchain systems for your business.

Bletchley: The Modular Blockchain Fabric

Project Bletchley concentrates on offering architectural building blocks for enterprise customers within a *consortium blockchain ecosystem* (a members-only, permissioned networks for members to execute contracts). Bletchley's blockchain fabric platform is powered by Azure, the cloud computing platform for Microsoft. Project Bletchley addresses the following:

- Digital identity
- Private key management
- Customer privacy
- Data security
- Operations administration
- System interoperability

In Project Bletchley, Azure provides the cloud layer for blockchain, serving as the platform where applications can be built and delivered. It will be availability in 24 regions globally. Azure is combining its traditional products such as hybrid cloud capabilities, extensive compliance certification portfolio, and enterprise-grade security to various blockchains. Microsoft wants to make it easier for the existing clients to quickly adopt blockchain technology, especially in controlled industries such as healthcare, financial services, and government.

Figure 10-1 shows project Bletchley's Blockstack Core v14, a new decentralized web of server-less applications where users can control their data.

Azure will work with several blockchain protocols. They are part of Hyperledger project and unspent transaction output (UTXO)–based protocols. This means that the Azure platform doesn't utilize a cryptocurrency and may be more appealing to enterprise customers. They'll also have integrations with more sophisticated protocols, including Ethereum, that do utilize a cryptocurrency to secure the network.

Cryptlets for encrypting and authenticating

Project Bletchley is built around two ideas:

- **Blockchain middleware:** Cloud storage, identity management, analytics, and machine learning
- **Cryptlets:** Secure execution for interoperation and communication between Microsoft Azure, Bletchley's ecosystem, and your own technology

Cryptlets are built as off-chaincode components, written in any language, executed within a trusted container, and communicated over a secure channel. Cryptlets can be used in smart contracts and UTXO systems, when additional functionality or information is needed.

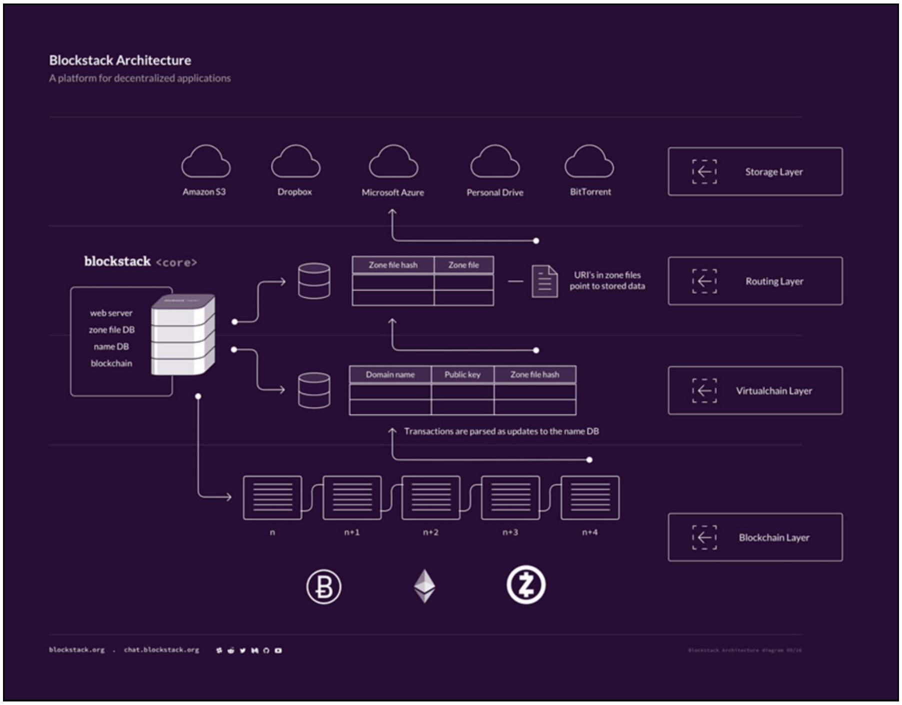


FIGURE 10-1: Blockstack Core v14.

Cryptlets bridge the gap in security between on- and off-chain execution of programs, operating when additional secure information is needed. They're what lets your customer relationship management (CRM) or trading platform connect with your cloud storage and then be secured with Ethereum, for example.

Bletchley's middleware works in tandem with Cryptlets and existing Azure services, like Active Directory and Key Vault, and other blockchain ecosystem technologies, to deliver a complete solution and ensure the reliable operation of your blockchain integration.

Table 10-1 shows the difference between an oracle and a Cryptlet from the Devcon 2 presentation on Bletchley.

Cryptlets are built by developers and sold in Bletchley's marketplace. They address many different functionality sets that are essential to building distributed ledger-based applications. The market is growing to meet the demands of customers who need the necessary functionality, such as secure execution, integration, privacy, management, interoperability, and a full set of data services.

TABLE 10-1 Cryptlets vs. Oracles

	Cryptlets	Oracles
Verification requirements	Requires trust with verification with a trusted host (HTTPS), a trusted Cryptlet key, and a trusted enclave signature.	Requires trust but no formal verification.
Infrastructure	Standard infrastructure. You achieve hardware-based isolation and attestation via enclaves available globally in Azure. Bletchley Cryptlet software development kit (SDK) frameworks (Utility and Contract) are available to help you get started quickly creating and consuming Cryptlets.	Customized infrastructure. You can write and host separately. Establishing trust is difficult. Oracles have been platform specific, and documentation is currently very sparse.
Developer use	Many language options are available, and they are blockchain agnostic.	Tied to their own blockchain and few language options.
Marketplace availability	A marketplace is available for publishing and discovery.	No common marketplace is available for publishing and discovery.

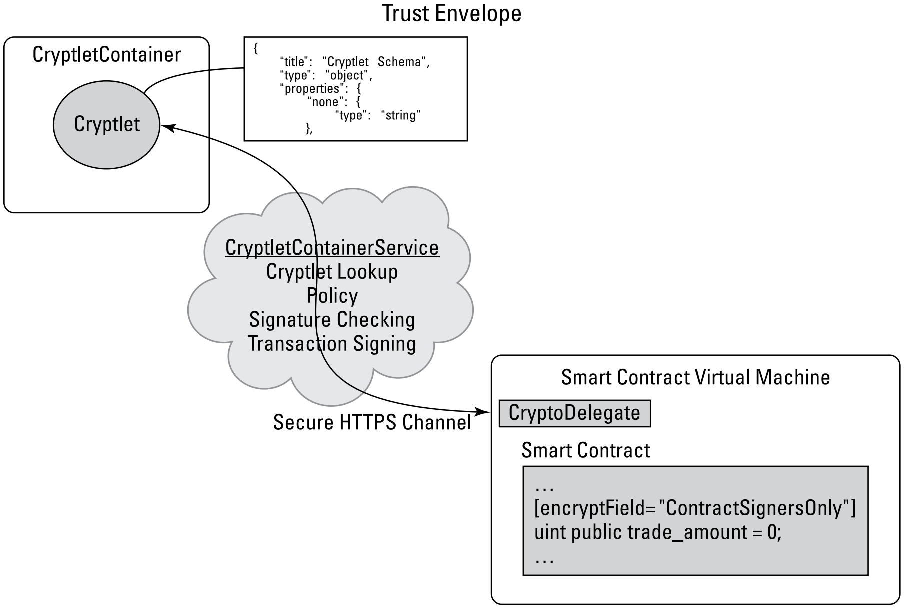
Utility and Contract Cryptlets and CryptoDelegates

There are two types of Cryptlets:

- **Utility:** Utility Cryptlets provide encryption, timestamping, external data access, and authentication. They create more sound and trusted transactions.
- **Contract:** Contract Cryptlets are full delegation engines. They can function as autonomous agents or bots. They provide all the execution logic that a smart contract normally does but outside of a blockchain.

Contract Cryptlets are tied to smart contracts and are created when your smart contract is published. They run in parallel with your virtual machine and have greater performance over traditional smart contracts built inside blockchains because they don't require a mining fee to execute your contract. They're most attractive to noncryptocurrency blockchains users where chaincode and smart contracts are signed by known parties.

Figure 10-2 shows a depiction of a Cryptlet container and the secure communication path to your smart contract.



```
{
    "title":  "Cryptlet  Schema",
    "type":  "object",
    "properties":  {
        "none":  {
            "type":  "string"
        },
```

```
. . .
[encryptField="ContractSignersOnly"]
uint public trade_amount = 0;
. . .
```

FIGURE 10-2: A Cryptlet container.

CryptoDelegates allow Utility and Contract Cryptlets to function. They act as adaptors by creating functional hooks in your smart contract virtual machines. They call the Cryptlet from the code of your smart contract, which in turn creates a secure and authentic envelope for transactions.

Building in the Azure Ecosystem

Azure is a digital ecosystem and cloud computing platform. It connects enterprises directly with their cloud partners and SaaS. This, in turn, allows enterprises to transfer their data in an interconnected, reliable, and secure way.

The Azure cloud platform is the second largest Infrastructure as a Service (IaaS) platform in the world. It's a reliable and safe haven for your cloud computing and data storage. In Azure, there is a service known as ExpressRoute, which provides consumers a way to directly connect to Azure. This, in turn, prevents the performance and security issues that are widely seen in the public Internet.

In 2015, Microsoft decided to expand its Azure ecosystem using the Ethereum and Hyperledger blockchain systems. The first offering of Azure Blockchain as a Service is powered by Ethereum. Ethereum is a Turing-complete blockchain framework for build applications, and you can read about it in depth in Chapter 5 or in *Ethereum For Dummies*, by Michael G. Solomon (Wiley). Microsoft aims to build more offerings based on the blockchain technology and Hyperledger. It's also growing the Azure marketplace, while transitioning to a portal for customers on Azure.

Microsoft's Azure Stack program incorporates Azure Quickstart Templates, which deploy the various Azure resources with the help of the Azure Resource Manager in order to help you get more work done. The Azure Resource Manager allows customers to work with their business resources as a group. It enables them to deploy, delete, or update all the resources in their solution in a coordinated and single operation.

Azure Quickstart Templates can work for various environments, like production, staging, and testing. Through Azure Resource Manager, customers get several features for tagging, auditing, and security. These features help consumers to manage their resources after deployment.

Microsoft's Project Bletchley is their blockchain architecture that is merged with established enterprise technologies they were already offering. It gives Azure a blockchain backend and marketplace.

Bletchley's ecosystem is an approach taken by Microsoft in order to bring forward blockchain or distributed ledger networks to a wider audience in a safe and effective manner. They want to help build authentic solutions and address actual business problems.

CHOOSING YOUR TEMPLATE

The Quickstart Template is a tool that is designed to make it easier for the users of Project Bletchley to spin up a private blockchain group. Currently there are about a dozen blockchain templates that allow you spin up blockchain applications in Azure. In the future, more templates will become available.

The Ethereum private version is one of the best at automating the process. step-it is a step-by-step process where you can select the members of the your consortium, determine the number of nodes each user will have on the network, and then geographically distribute those nodes using the Azure cloud to boost resilience.

Deploying Blockchain Tools on Azure

Azure has several other useful implementations of blockchain technology and tools that you might find useful. I cover four of Azure's core blockchain tools and projects in this section, including its Ethereum implementation; Cortana, an analytics machine learning tool; Azure's data visualization tool, Power BI; and its Active Directory (AD) tool. The last three are not specifically blockchain tools, but they can be used with your Azure blockchain project.

This section gives you an idea of what you can build with Azure and some of the tools available to make your project a success.

Exploring Ethereum on Azure

Ethereum Blockchain is now available as a service on Microsoft's Azure platform. This initiative is offered by ConsenSys and Microsoft in partnership. Solidity is a new project that they created that allows you to start building your decentralized application on Ethereum. Find out more at `https://marketplace.visualstudio.com/items?itemName=ConsenSys.Solidity`.

Ethereum Blockchain as a Service (EBaaS) enables enterprise developers and clients to develop a blockchain environment on the cloud and can be spun up with one click.

When you're deploying Ethereum blockchain on Azure, Azure offers two tools initially:

- **BlockApps:** A semiprivate and private Ethereum blockchain environment
- **Ether.Camp:** A built-in developer environment

BlockApps can also be deployed into the public environment of Ethereum. These tools allow rapid development of applications based on a smart contract.

Ethereum is a flexible and open system, which can be customized to meet the varied needs of customers. Read more about Ethereum in Chapter 5.

Cortana: Your analytics machine learning tool

Cortana is a powerful analytics machine learning tool based on cloud systems. It's a fully managed cloud service that enables users to easily and quickly build, organize, and share predictive analytics solutions. It provides many benefits to consumers.

By reviewing the analytics provided by Cortana Intelligence, you can take action sooner than your competitors by predicting the next big thing. This flexible and fast software allows you to build quick solutions for your industry, which are tailored to your particular needs.

Furthermore, the Cortana learning tool is secure and scalable. Cortana offers data value, irrespective of the complexity and size of the data. And, most of all, Cortana allows you to interact with smart agents, so that you can get closer to your consumers in more natural, practical, and useful ways. The Cortana Intelligence Suite is helpful in various sectors, including manufacturing, financial services, retail, and healthcare.

Visualizing your data with Power BI

Power BI, which is offered by Microsoft, is a powerful service based on the cloud system. It covers the latest business intelligence services and tools of Microsoft. This service assists data scientists in envisioning and sharing insights from the data of their organizations.

The Power BI data visualization course, which is provided online by edX, is part of the Microsoft Professional Program Certificate in Data Science. This cloud-based service is rapidly gaining popularity among data science professionals.

Power BI helps you to visualize and connect your data. In this course, students learn how to connect, import, transform, and shape their data for business intelligence. Additionally, the Power BI course teaches you how to create dashboards and share them with business users on mobile devices and the web.

Managing your access on Azure's Active Directory

Azure Active Directory (AD) is a broad access and identity management solution. It provides a wide set of facilities, which allow you to supervise access to cloud and on-premises resources and applications. This includes various Microsoft online services, such as Office 365, in addition to numerous non-Microsoft SaaS applications.

One of the main features of Azure AD is that you can handle access to its resources. These resources can be external to the directory, like Software as a Service (SaaS) applications, on-premises resources or SharePoint sites, and Azure services, or they can be internal to the directory, such as permissions for managing objects through directory roles.

Getting Started with Chain on Azure

Chain, which provides blockchain technology solutions, released its Chain Core Developer Edition on Azure. Chain Core Developer Edition is an open-source and free version of the company's distributed ledger platform. It enables you to issue as well as transfer assets on authorized blockchain networks.

Through its test net, your developers can join or start a blockchain network, access in-depth technical tutorials and documentation, and build financial applications. They can also run their own prototypes on the Chain's test net or create their own personal network on Azure.

Using financial services on Azure's Chain

Chain launched its open-source and free developer platform. It includes a test network, which is operated by Microsoft, Chain, and the Initiative for Cryptocurrencies and Contracts (3CI). 3CI is the platform launched by Chain, which provides blockchain technology solutions.

This platform enables you to issue as well as transfer assets on authenticated blockchain networks. It's an effort among leading financial companies and Chain. Various financial applications can be developed via Chain Core.

Many new innovative products are planned to be launched on this platform. The range covers payments, banking, insurance, and capital markets. Additionally, Visa has partnered with Chain in order to develop a secure, fast, and simple way to process business-to-business (B2B) payments worldwide.

Chain's three-pronged approach to distributed ledger

Chain makes tools for building apps on the Internet using blockchain technology. They have three products: Sequence, Chain Token, and Chain Cloud.

Sequence is a digital ledger that helps keep track of money and other things online. It's good for storing a lot of information, and it's easy to use, even for big companies.

Chain Token and Chain Cloud are tools for building and running apps on the Internet. Chain Token is used to run the Chain Protocol, and Chain Cloud is a way to develop and run decentralized apps in the cloud.

Overall, Chain is a helpful tool for people who want to build blockchain-based applications. It's easy to use, scalable, and secure, making it worth exploring as you consider blockchain platforms for your application.

Building your own ledger with Sequence

Getting up and running on Sequence is very easy. And after you've set up your ledger, they have a user-friendly user interface (UI) to help you create your first transactions. Each ledger that you create with Sequence is a discrete, append-only, cryptographically linked system of record.

Follow these steps to set up your ledger:

1. **Navigate to** `https://sequence.chain.com/start`**.**
2. **Click Create Team.**
3. **Enter your email address.**
4. **Enter the verification code that was sent to your email.**
5. **Name your team.**
6. **Enter a password.**
7. **Name your ledger.**
8. **Click Create Ledger.**

Congratulations! You've created your own ledger on Chain!

Chain Protocol's native cryptocurrency

Chain Token, or XCN, is the native cryptocurrency of the Chain Protocol. XCN is a utility-based token that is used for discounts, premium access, and to pay for commercial fees on Sequence. XCN is also used for on-chain governance for various community-driven programs through Chain DAO. In March 2022, XCN was upgraded and re-denominated to enable native governance features inherent in the token smart contract.

XCN has a few different uses. On Sequence, a ledger-as-a-service designed for enterprises, XCN is used to pay commercial fees. XCN can also be used on other Chain products. In addition, XCN stakers can participate in the Chain DAO to vote on Chain Improvement Proposals (CIPs), earn rewards for securing the protocol, and vote for grant recipients.

XCN was upgraded in March 2022 so it could be used for native governance features inherent in the token smart contract. This upgrade enables XCN stakers to participate in decisions about the future of the Chain Protocol through on-chain voting.

Chain Token plays an important role in the Chain Protocol ecosystem by providing a way to pay for fees, access premium features, and participate in on-chain governance. If you're looking for a cryptocurrency with utility, XCN may be a good choice for you.

Chain's cloud for Web 3.0

Chain Cloud Services is a one-stop shop for Web 3.0 developers. It provides free, public remote procedure call (RPC) endpoints for developers, alongside Premium and Enterprise plans packed with advanced developer tools. The Chain Cloud is powered by a globally distributed and decentralized network of nodes, making it a reasonable choice for blockchain developers and projects that need access to on-chain data. The Standard application programming interface (API) is available to all and free to use at the time of this writing. Developers can use their RPC endpoints to access Bitcoin, Ethereum, BSC, and Solana without needing to input any user info or login credentials.

As a leading provider of blockchain infrastructure services, Chain is uniquely placed to help you with all your needs when it comes to developing Web 3.0 applications, including the following:

- Chain offers free public RPC endpoints so that developers can access Bitcoin, Ethereum, BSC, and Solana without needing to input any user info or login credentials. All you need is an API key.
- Premium and Enterprise plans have advanced developer tools, making them useful for those who need a little extra help when building their applications.
- Their globally distributed and decentralized network of nodes ensures that you always have access to the data you need when you need it.

If you're looking for a provider of blockchain infrastructure services, explore Chain Cloud Services. They have everything you need to build Web 3.0 applications. You can do this by navigating to `https://docs.chain.com`.

IN THIS CHAPTER

- » Preparing for artificial intelligence blockchain apps
- » Building your IBM Fabric
- » Creating smart contracts
- » Deploying an Internet of Things solution

Chapter 11

Getting Busy with IBM

In this chapter, I introduce you to IBM's blockchain initiatives, which IBM is merging with its other groundbreaking technologies, such as Bluemix, a full Platform as a Service (PaaS) for application building, and Watson, its super computer.

Blockchain technology creates a near-frictionless value exchange. Artificial intelligence accelerates the analysis of massive amounts of data. The merging of the two capabilities will be a paradigm shift that affects the way we do business and secure our connected electronic devices.

If you're involved in the Internet of Things (IoT), health care, warehousing, transportation, or logistics industries, you will benefit from the information in this chapter. Also, if you're an entrepreneur and would like to learn about the new capabilities that come with the integration of artificial intelligence (AI) and blockchain on a scalable app platform, this chapter is for you.

IBM Blockchain Platform

The IBM Blockchain Platform is a cloud-based platform for building, running, and managing blockchain networks. It's designed to make it easier for organizations to adopt and use blockchain technology in their operations.

The IBM Blockchain Platform provides a range of tools and services for developing and deploying decentralized applications (dApps) on top of a blockchain network. It supports a variety of popular blockchain technologies, including Hyperledger Fabric, Ethereum, and Corda, and it can be used to build networks with different levels of complexity and scalability.

The platform also includes features such as automatic smart contract generation, real-time analytics, and network management tools, which can help organizations to more easily design, deploy, and maintain their blockchain applications. In addition, the IBM Blockchain Platform offers a range of security and compliance features to help protect against threats such as hacking, fraud, and data breaches.

Overall, the IBM Blockchain Platform is intended to provide organizations with a comprehensive, easy-to-use platform for building and running blockchain networks, with the goal of helping them to more effectively leverage the benefits of blockchain technology in their operations.

Supply chain

IBM has a Blockchain Solution for supply chain transparency. They understand that moving freight is a complex process involving different parties with different priorities. Modern supply chains are monitored through a network of IoT devices that scan products as they move from production to shipping and finally make it into the hands of the end user. IoT-enabled blockchain can store the temperatures, position, arrival times, and status of shipping containers as they move. Immutable blockchain transactions help ensure that all parties can trust the data and take action to move products quickly and efficiently. You can enable supply-chain transparency by leveraging an enterprise blockchain platform to transact with your supply-chain partners in a more trusted and efficient way.

IBM's blockchain can help you share data with other parties. Sharing data across a blockchain can be good for business because it allows parties to collaborate and share transparently, with a clear record of what happened when. But if you do that publicly on a blockchain, it can be problematic because your competitors can use the data to get a leg up on your company. Sharing data on an enterprise blockchain platform is better because you decide who can see your data. With a supply-chain transparency solution, you can create an immutable, distributed, and shared ledger to transact with your supply-chain partners in a more trusted and efficient way. In a world where speed, accuracy, and compliance are paramount, blockchain provides a solution that can help you meet your goals.

Enterprise blockchain platforms like IBM Blockchain offer unique benefits for supply chain management, including:

- The ability to track goods throughout the supply chain from supplier to customer
- A shared view of the supply chain that all members can trust
- Enhanced visibility into the location and status of goods in transit
- Priority access to shipping container temperatures, positions, and arrival times
- Improved compliance with food safety regulations
- The ability to quickly resolve disputes with improved transparency into all aspects of the shipment

World trade

IBM has also developed a blockchain solution for trade finance. The world is currently in *end-state globalization* where nearly all countries and cultures are completely interconnected and interdependent. You experience this as having a distributed workforce, where you may be working with teams in China, India, and Europe as a regular part of your day. Your company may be completely reliant on the work done in another country. For example, 90 percent of the world's advanced semiconductors are made in Taiwan. Without the work of people in Taiwan, the world would no longer be able to produce cheap electronics. The COVID-19 pandemic revealed one of the other characteristics of total globalization: the free movement of people across borders.

IBM is leaning into how the world is increasingly reliant on cross-border trade. Having a solution that fosters greater trust and transparency is more important than ever. That's where IBM Blockchain's experience in strategy, rapid product development, governance and regulation helps blockchain networks expand membership — an essential part of building a successful network. IBM Blockchain also offers a new class of transparent, risk-mitigated, and standardized trade finance and trade credit insurance solutions that can help you find new opportunities and markets while lowering risk and operational costs.

With IBM Blockchain, businesses can enjoy greater trust and transparency in cross-border trading. That's because blockchain creates a shared, immutable record of all transactions within a network. This means that every member of the network can see every transaction that has taken place — which helps to foster transparency and trust. In addition, blockchain enables businesses to verify the authenticity of documents quickly and easily — such as bills of lading, contracts, and invoices — which can help to reduce fraud and save time and money.

Another way that IBM Blockchain is helping to establish leadership in the new era of trade is by helping to create new trading hubs around the world. By convening new trade networks and bringing together buyers and sellers from different geographies, IBM Blockchain is helping to create new opportunities for cross-border trade. In addition, by lowering the barriers to entry for small businesses, IBM Blockchain is opening up new markets and creating more inclusive global supply chains.

Finally, with its transparent, risk-mitigated and standardized solutions for trade finance and credit insurance, IBM Blockchain is helping businesses find new opportunities while lowering risk and operational costs. For instance, companies can save time and money by automating the entire credit application process on the blockchain while reducing the risk of fraud. In addition, by using blockchain to track transactions from start to finish, companies can gain insights into client financial positions and transaction histories — which can help to lower risk or optimize financing terms.

In today's interconnected world, cross-border trade is more important than ever. But with this increased reliance on cross-border trade comes increased pressure on businesses to foster greater trust and transparency. So, as you're considering a solution to meet your needs in trade finance, you should look at what IBM can do for you.

Health care

IBM's blockchain technology has been used in the health care and life sciences industries to address various challenges, including the lack of interoperability between different systems, concerns about data privacy, and the need for better traceability in supply chains. These issues have become even more pressing with the COVID-19 pandemic, as health-care organizations have had to adapt their supply chains to meet the demand for protective equipment and have worked to develop treatments, tests, and vaccines. IBM's blockchain technology has been used to help address these challenges by providing a secure, decentralized platform for storing and sharing data. It has also been used to facilitate communication between different electronic health record systems and to help combat drug counterfeiting.

The growing healthcare market using blockchain technology is expected to be worth $126 billion by 2030. There are many ways that it can be used in health care, such as helping to prevent drug counterfeiting, making it easier to share and manage medical information, and tracking shipments of medical supplies. It has also been used during the COVID-19 pandemic to help with things like contact tracing and sharing research data. IBM has four primary ways they are supporting healthcare tech using blockchain:

- IBM is helping to secure personal protective equipment (PPE) supply chains by tracking the provenance and authenticity of PPE products.
- IBM is working on a project to allow patients to control access to their health data.
- IBM is collaborating with pharmaceutical companies and distributors to address counterfeit drugs.
- IBM is helping to streamline the clinical trial process by validating participant identity and ensuring regulatory compliance.

Blockchain is particularly well-suited for addressing health-care and life-sciences challenges because it's secure, tamper-proof, decentralized, and transparent. It can help to ensure the authenticity of PPE products, track the provenance of drugs, protect patient privacy, and streamline clinical trials.

The pandemic highlighted the many challenges faced by the health-care and life-sciences industries. But it also showed the potential for blockchain technology to help address some of those challenges. IBM Blockchain is just one example of how this technology can be used to secure supply chains, protect patient privacy, streamline clinical trials, and more. As we continue to grapple with the pandemic, it's important that we explore all the ways that blockchain can help us overcome these challenges.

IBM Blockchain has the potential to transform the healthcare and life sciences industries by solving some of their most pressing challenges. Blockchain technology can create a decentralized database of patient health information, a traceable medication supply chain, and digital credentials for healthcare professionals. This would improve interoperability, privacy, and supply-chain traceability while also ensuring that patients receive safe and effective medicines.

Business Blockchain on Bluemix

IBM is now offering blockchain technology that integrates with its traditional offerings, such as IBM Bluemix. Bluemix is an open-standards, cloud-based PaaS for building and managing applications. IBM has integrated a blockchain stack from Hyperledger, which is part of the Lynx foundation and is establishing best practices in blockchain technology.

You'll want to prepare for rapid and fundamental changes within IBM's blockchain initiatives. The technology is very new and still under incubation, both within IBM and Hyperledger.

Hyperledger has several different subprojects in development. As of this writing, IBM is using Fabric, but it may open up Bluemix to other projects. Fabric is open source and under active development within Hyperledger. You can start testing Fabric on Bluemix by using Hyperledger Fabric v0.6. However, IBM warns against running any valuable transactions directly on Fabric v0.6 or any earlier version.

Bluemix is the newest cloud offering from IBM. It's an implementation of IBM's open cloud architecture based on Cloud Foundry, an open-source PaaS.

Bluemix enables you to rapidly and easily come up with applications, deploy them, and manage them. Bluemix offers enterprise-level services that can integrate with applications without needing to know how to install or to configure them.

Figure 11-1 shows how IBM relates different aspects of blockchain and IBM systems. You can find out more at `https://goo.gl/12Q6no`.

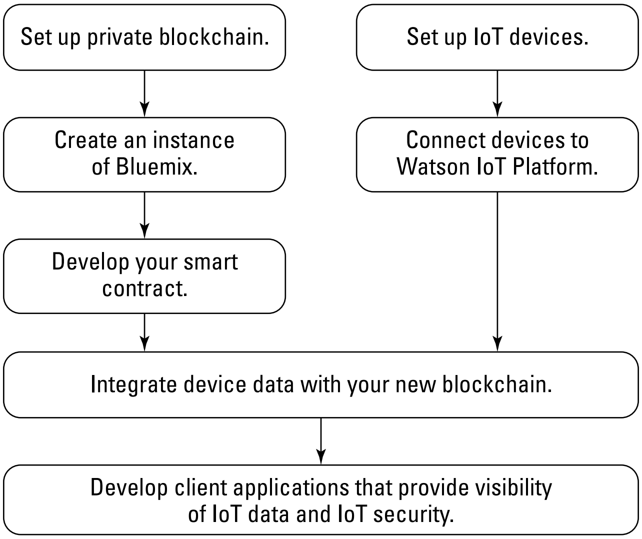

Set up private blockchain.
Set up IoT devices.
Create an instance of Bluemix.
Connect devices to Watson IoT Platform.
Develop your smart contract.
Integrate device data with your new blockchain.
Develop client applications that provide visibility of IoT data and IoT security.

FIGURE 11-1: How IBM Bluemix and IoT are merged with IBM Watson.

IBM Bluemix provides four core things:

- Computing infrastructure based on your apps' architectural needs
- The ability to deploy apps to a Bluemix public or dedicated cloud

- Dev tooling, such as code editors and managers
- Access to third-party open-source tools in their service section

Bluemix gives you everything you need to build your app. It's now offering blockchain infrastructure to test as well.

They have a service for integrating your applications with the Bluemix blockchain. As of this writing, there are two pricing models. A free account gets you what you need to test your idea. You get four peers and a cert authority to sign transactions, as well as a dashboard with logs, controls, and APIs.

The enterprise plan is priced at $10,000 a month and offers higher security and speed than the free model.

Two remarkable entrepreneurial pioneers are using Bluemix and the Hyperledger Fabric integration:

- **Wanxiang:** The largest China-based automotive components company, Wanxiang is working with IBM to deploy a private blockchain. They're embedding property rights into things like electric cars. The goal is to reduce the costs to consumers for leasing equipment. Wanxiang will use its blockchain technology to track the lifespan of the components and refurbish used batteries. Bluemix will take care of everything else.
- **KYCK!:** The financial technology (fintech) startup KYCK! is utilizing IBM's blockchain integration as a novel way to address Know Your Customer (KYC) needs for brokerages. This expense is limiting and costly for banks and other financial services. KYC is done to prevent money laundering and illicit trade, and to combat terrorism. KYCK! is building a video conference and encrypted document submissions platform. It will allow brokers to work with and authenticate clients the company has not met in person.

IBM has also built out three simple Chaincode applications that let you play with the IBM Blockchain network:

- **Marbles:** Marbles is an application that demonstrates transferring marbles between two users. It lets you see how you can move assets on a blockchain.
- **Commercial Paper:** Commercial Paper is a blockchain trading network implemented on IBM Blockchain. You can create new commercial papers to trade, buy and sell existing trades, and audit the network.
- **Car Lease:** Car Lease is a lot like the Marbles demo. It's designed to allow you to interact with assets. You can create, update, and transfer. It also allows a third party to view the history.

Watson's Smart Blockchain

IBM's supercomputer, Watson, is also available on the Bluemix platform. Watson is a cognitive computing artificially intelligent computer system. It can analyze structured and, more impressively, unstructured data at incredible speed.

WARNING

This technology is still developing, and customers have complained about its true ability to understand unstructured written language.

Watson can answer questions posed to it through natural language and learn as it absorbs more information. The implication of this technology, when married with blockchain technology, is astounding. One of the first implementations is within the IoT space. There is a strong need to secure data that is emitted from these devices and then make it actionable and intelligent.

Watson's cognitive computing is simulating human thought processes and using the MQTT protocol. Like a human mind, it grows over time. Its self-learning systems use data mining, pattern recognition, and natural language processing to mimic the way your brain works. Watson processes at a rate of 80 teraflops per second (one teraflop is a trillion floating-point operations). To put this into context, that replicates — and in some cases surpasses — a high-functioning human's ability to answer questions. Watson is able to do this by accessing 90 servers with a combined data store of more than 200 million pages of information, which it processes against six million logic rules. Watson is about the size of ten refrigerators, but it's been getting smaller and faster.

Figure 11-2 shows how IBM Watson relates different aspects of blockchain and IBM systems. Dive deeper at IBM `https://goo.gl/12Q6no`.

IBM is applying these amazing capabilities to IoT data feeds that utilize Chaincode implementation. Chaincode is a Hyperledger smart contract system. Here's how Watson-enabled blockchain for IoT devices will work:

- IoT devices send data to your private blockchain ledgers for inclusion in shared transactions as a tamper-resistant record marked in time.
- Partners and third-party service providers can access and supply IoT data as well, without the need for central control and management.
- All parties can sign and verify data, limiting disputes and ensuring each partner is held accountable for their individual performances.

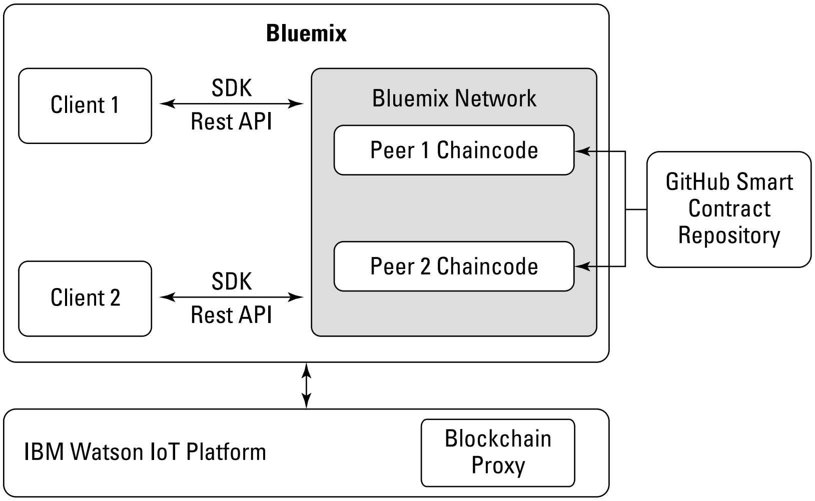


FIGURE 11-2: How Bluemix integrates clients, peers, and IBM Watson.

This is a simple implementation that does not take advantage of all the functionality and capabilities of Watson. Watson's ability to learn and make suggestions, and update out-of-date information will truly make it a powerful blockchain-enabled application in the future.

You can integrate Watson's IoT Platform with Fabric from Hyperledger. This integration allows you to execute Chaincode contracts through cognitive computing oracles. Watson's IoT platform has built-in capability that lets you add selected IoT data to your own private blockchain to create an oracle. This helps you protect the data from being viewed by unauthorized third parties.

When you've established a Bluemix workspace, you can add selective services, including the IoT Platform that integrates several technologies. Fabric is the blockchain technology that provides the private blockchain infrastructure for distributed peers that replicates the device data and validates the transaction through secure contracts.

Watson IoT Platform translates existing device data, from one or more device types, into the format needed by the smart contract APIs. Watson's IoT Platform filters out irrelevant device data and only sends the required data to the contract. Figure 11-3 shows how IBM Watson integrates with IoT devices and APIs. Watson acts as the Chaincode oracle and allows you to control what information is known to the parties involved in the contract. This functionality is important for privacy.

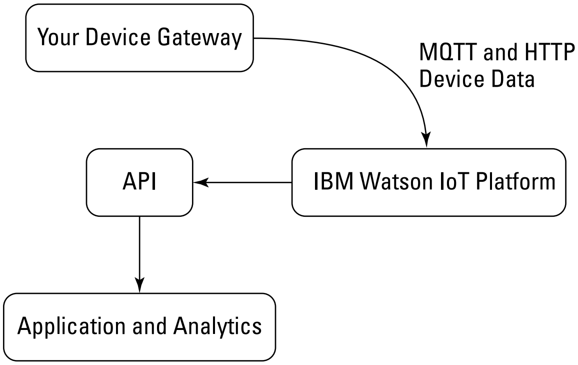


FIGURE 11-3: The Watson/API/device flow.

Building Your Starter Network on Big Blue

IBM's blockchain technology and IoT Platform offer new promising tools and can be leveraged to address many problems facing companies that are trying to scale:

- **Security:** The huge volume of data that's collected from millions of devices raises information privacy concerns. Also, hacked IoT devices have been used by nefarious organizations to cripple websites with distributed denial of service attacks.
- **Cost:** The high volume of messages, data generated by the devices, and analytical processes are going up as more devices come online and utilize that data.
- **Architecture:** Centralized cloud platforms remain a bottleneck in end-to-end IoT solutions and a central point of attack.

IBM's open-standards-based distributed IoT networks can solve many of the problems associated with today's centralized, cloud-based IoT solutions. Connected devices communicate directly with distributed ledgers. Data from those devices is then used by third parties to execute smart contracts, reducing the need for human monitoring.

The IBM Watson IoT Platform with a Fabric integration replicates data across a private blockchain network and eliminates the need to have all IoT data collected and stored centrally. Decentralized blockchain networks also improve the security of IoT devices. Unique digital identities are built for each device over time. This new way of creating and securing identity is exceptionally hard to spoof.

These new blockchain identities allow IoT devices to sign transactions that allow smart contracts to execute. A practical application of this would be an insurance product that was fed data from a smart car on the driving behavior of different individuals. The car would send data to be published in Fabric; the insurance product built with Chaincode would then recognize the new data and the identity of your car and update your policy.

The possibilities are nearly endless, and IoT has introduced huge opportunities for businesses and consumers, especially in the areas of healthcare, warehousing, transportation, and logistics.

There are three main tiers of IBM cloud-supported IoT solutions that meet the needs of different IoT business problems:

- **Device Gateway:** Device Gateway is for smart devices or sensors that collect data about the physical world. This could be things like weather sensors, temperature monitoring for refrigerated containers, or vital statistics data for a patient. These IoT devices send their data through the Internet for analysis and processing.
- **IBM Watson IoT Platform:** IBM combines its supercomputer with its IoT Platform to collect data from IoT devices and then analyze the data and take subsequent actions to solve problems. Watson provides machine learning, machine reasoning, natural language processing, and image analysis that enhance the ability to process the unstructured data collected from the sensors.
- **IBM Bluemix:** Bluemix is an open-standards-based cloud platform for building, running, and managing applications and services. It supports IoT applications by making it easy to include analytical and cognitive capabilities in those applications.

You can learn more about the IBM solution at `https://developer.ibm.com/technologies/blockchain`.

4 Industry Impacts

IN THIS PART . . .

Understand the future of the financial services industry when it utilizes blockchain technology to move money around the world quickly and inexpensively.

Clarify your knowledge of global real estate as it relates to blockchain technology.

Identify opportunities in the insurance industry to reduce fraud and increase profits through new insurance instruments.

Examine the large-industry implications of permanent systems within government organizations and legal frameworks.

Clarify other large global trends in blockchain technology and how they'll shape the world you live in and the everyday tools you use.

IN THIS CHAPTER

- » Discovering future global bank trends
- » Uncovering new investment vehicles
- » Exposing risk in the banking blockchain
- » Developing new financing strategies

Chapter 12 Financial Technology

The first to adopt blockchain technology were banks, governments, and other financial institutions — and they're the fasting-growing blockchain users, too. The powerful tools that are being built to manage and move money will reshape our world in new and unexpected ways, so it makes sense that financial technology (fintech) would jump onboard.

This chapter gives you the inside scoop on what governments are currently doing with blockchain technology and how it will affect you. Fintech touches your life every day, whether you're aware of it or not.

In this chapter, I introduce you to future banking trends, new regulations, and the new tools that can help you move money faster and cheaper. I also explain new types of investment vehicles and other blockchain innovations. Finally, I warn you about potential risks of investments involving virtual currency and new blockchain-technology-enabled financial products.

Hauling Out Your Crystal Ball: Future Banking Trends

Banking was the first industry to recognize the threat of Bitcoin and then the potential of blockchain to transform the industry. The banking sector is highly regulated, and the fees to organize and operate as a bank are expensive. These heavy regulations have been an insulating and protective shield for the whole industry, as well as a burden. The application of fast, efficient, digital money that doesn't carry the cost of handling cash and that is traceable as it moves through the financial system was an intoxicating and threatening proposal. The idea that value can be held outside the control of central authorities also piqued the interest of financial institutions and governments that back currencies.

Initially, these financial institutions and governments tried to squelch blockchain with regulation. Today, they're embracing blockchain through investment across the board.

In 2013 and 2014, the U.S. Securities and Exchange Commission (SEC) issued a warning to investors about the potential risks of investments involving virtual currency. The warning was that investors might be enticed with the promise of high returns and would not be skeptical enough of the new investment space that was so novel and cutting-edge. According to the SEC, digital currency was one of the top ten threats to investors. Today, the SEC stands ready to engage with companies and investors as cryptocurrency gains traction within all industries.

Not even two years later, countries around the world — including the UK, Canada, Australia, Japan, and China — began investigating how they could create their own digital currencies, seizing cryptocurrency for themselves and put money on the blockchain. In 2018, Venezuela launched a cryptocurrency called the Petro. The launch of the Petro is a significant turning point for cryptocurrency because Venezuela was the first sovereign nation to issue its own cryptocurrency. The Petro was unfortunately used to defraud Venezuelan citizens. However, the future may hold an oil backed digital currency for Venezuela.

Blockchain's promise of an uncompromisable ledger has been an appealing system to try for governments that are seeking to reduce fraud and improve trust. Innovations in blockchain technology promised to be able to handle the billions of transactions need to support economies, making a cryptocurrency feasible at scale.

Blockchains are in themselves permanent and unalterable records of every transaction that is inputted into them. Putting a country's money supply on a blockchain controlled by a central bank would be utterly transformative because there would be a permanent record of every financial transaction, existing at some level within their blockchain record, even if they weren't viewable to the public. Blockchain technology and digital currencies would reduce risk and fraud and give them ultimate control in executing monetary policy and taxation. It would not be anonymous like Bitcoin was at first. In fact, quite the opposite: It would allow them a full and auditable trail of every digital transaction made by individuals and companies. It might even allow central banks to replace commercial banks' role in circulating money.

The question of what the future for banking will look like can be scary and exciting. Consumers can now pay friends through their phones almost instantly in almost any type of currency or cryptocurrency. More and more retail stores have begun utilizing cryptocurrency as a way to pay for goods and accept payment from customers. In Kenya, using cryptocurrency is more normal than not. But this is still not the mainstream option for most of the world. Western markets are still in the early adoption phase.

Given that most individuals have their wealth locked into legal tender issued by governments or locked into assets that are within existing government systems, fintech innovations must merge with these existing systems before we see the mainstream utility of blockchain or digital currencies. If regulators find ways to tax and register accounts, mass adoption of customer-facing wallets with digitized tokens is two or three years down the road.

The business-to-business market will start utilizing blockchain much quicker. A production-hardened system with the associated policies and operations is being tested. Ripple and R3 among others have been hard at work making this possible. These systems will first focus on the institutional creation of digitized representations of deposits. These are IOUs between internal organizational departments and between trusted partners, like vendors. Regulators, central banks, and monetary authorities are all investing heavily in making this possible. Canada and Singapore have been moving very quickly.

Know Your Customer (KYC) and Anti-Money-Laundering (AML) regulations require banks to know who they're doing business with and ensure that they're not participating in money laundering or terrorism. Banks issuing cryptocurrencies still have significant challenges to overcome first. In order to stay compliant with KYC and AML regulations, they need to know the identity of all the individuals utilizing their currency. In many cases, people's bank accounts are already debit and credit service of transactions, like distributed ledgers in blockchains, except for centralized. The first candidates in this area are going to be regions where regulators, banks, and central banks work together. Singapore and Dubai are good candidates that already have blockchain initiatives.

Moving money faster: Across borders and more

Assessing the transaction volume needed to be met by a blockchain handling the currency of an economy like the UK or U.S. is difficult. The U.S. alone is processing billions of transactions a day and over $17 trillion in value a year. That's a lot of responsibility for a new technology! The nation would be crippled if its monetary supply were compromised.

The International Monetary Fund, the World Bank, the Bank for International Settlements, and central bankers from all over the world have met to discuss blockchain technology. The first step toward faster and cheaper money would be adopting a blockchain as the protocol to facilitate bank transfers and interbank settlement. Official digital currencies that ordinary citizens use on a daily basis would come much later.

Individual consumers wouldn't directly feel the cost reduction from utilizing a blockchain for interbank settlement. The savings would be seen in the bank's bottom line as cost reductions for fees charged by intermediaries.

Consumers will still want retail locations and commercial banks for the foreseeable future. But millennials have already adopted app-activated payments through PayPal, Venmo, Cash, and more. A new way of paying through their phones won't faze them.

The great challenge is that if all money is digital, compromising it could be catastrophic. It's possible that the architecture of blockchain systems could be strong enough. The issue might be instead that the code within the system is executed in an unexpected manner, as happened in the decentralized autonomous organization (DAO) hack on Ethereum (see Chapter 5). If the cryptocurrency were operating on a traditional public blockchain, then 51 percent of the nodes in the network would have to agree to fix the issue. Getting an agreement in place might take a lot of time, and it wouldn't be practical for businesses and people who need stable and secure money at all times.

REMEMBER

Many blockchains operate as democracies. A majority (51 percent) of a blockchain's nodes network are needed to make a change.

Creating permanent history

Data sovereignty and digital privacy are going to be huge topics in the future. Fraud prevention will be easier because if the whole economy is utilizing a cryptocurrency, there will always be an auditable trail inside the blockchain that secures it. This is enticing for law enforcement, but a nightmare for consumer privacy.

From a customer perspective, there's already an audit trail for everything you purchase with a credit or debit card. From an institution perspective, it's beneficial to have audit trails because it increases transparency of documentation and life cycles of the movements of these assets between different regions. It adds legitimacy to the trading of assets and allows them to bake compliance into their day-to-day transactions.

The “right to be forgotten” rules in Europe, which allow citizens the right to not have their data forever propagated on the Internet, are a difficult challenge for blockchains, because blockchains can never forget. Governments and corporations would have permanent historical records of every transaction, which could be devastating to national security if they were exposed to the public. Or in a company’s case, it may allow their competitors to have an inside scoop on how their competitors are investing.

The biggest challenge to using a permissionless blockchain such as Ethereum or Bitcoin would be guaranteeing that you haven’t sent money to an OFAC country to support terrorism. The answer is that you can’t because they are somewhat anonymous and anyone can open a wallet. It is possible to create algorithms to trace transaction movement — the U.S. government has been doing this for years — but anyone can move value in a permissionless world.

TECHNICAL STUFF

The Office of Foreign Asset Control maintains sanctions on specific organizations or individuals in what are considered high-threat countries. The government is unable to track the history of transactions when using permissionless platforms anonymously.

The need for KYC and AML makes a case for the permissioned blockchain in the shared ledger space. The software company R3 developed Corda, a private and permissioned blockchain-like platform to meet many of these challenges directly. They specifically do not globally broadcast the data from their participants. This keeps the data within the Corda blockchain private and was the primary nonfunctional requirement requested by the more than 75 banks that worked with R3 to adopt blockchain technology. They need to maintain their privacy and meet strong regulatory demands.

Going International: Global Financial Products

Blockchains will usher in many new types of securities and investment products. New markets will be opening with more efficient ways of calculating risk because collateral will be a lot more transparent and fungible across institutions when accounted for within a blockchain-backed system.

Blockchain technology also has applications in helping reduce scams within the global warehouse market for fraudulent double-sold goods. Blockchain entries enable manufacturers and regulators to document the provenance of products and, in turn, allows buyers to check the authenticity of what they’re buying. There are several solutions in the market, including Everledger and Provenance.

TIP

Hernando de Soto, the famous Peruvian economist, estimates that providing the world's poor with titles for their land, homes and unregistered businesses would unlock $9.3 trillion in assets. This is what is meant by the term *dead capital.*

It is imaginable that countries that can free their dead capital, the unfinanceable real property they own, will be able to bundle and sell these interests in these assets across a global marketplace. This would be things like transparent mortgage-backed securities for new real estate developments in Colombia or Peru.

In the future, countries will be able to free up their dead capital. Owners of properties, undeveloped land, and un-financeable properties will now have the opportunity to sell the interests in these assets across a global marketplace.

These assets will be appealing because asset managers will be able to actively parse underperforming assets given the transparency and capability of one being substituted in place of another through blockchain-based technology. The use of blockchains to manage these assets will give managers the power always to own top-performing securities, removing the rotten apples, reclassifying them, and selling them as new securities.

For non-institutional customers, micro-investments will be an attractive outlet enabled globally and locally through blockchain trading platforms. Using blockchain technology will also give them the means of investing in companies and their specific activities without having minimums or going through intermediaries that take a percentage of the investment.

Decentralized autonomous organizations (DAOs) are already out there and making DAO investment pools happen for a few risk-tolerant and more technically savvy investors. It may be some time before an institutional investor utilizes one or a portfolio manager recommends putting money into a DAO-based vehicle for her clients.

DAOs remove a lot of the necessary paperwork and bureaucracy involved in investing by creating a blockchain-based voting system and giving shares to those who invest in their product. To any blockchain, the "code as law" concept makes it unforgiving. The risks are many, particularly when there is poorly written code that executes in unintended ways. The consequences are that hacks to this system can be severe. The transparent nature of the original system, the poor code, gives hackers a wider attack vector and allows them to attack multiple times as they gain more and more information each time.

In the following section, I discuss the effects and benefits of blockchain technology on the world economy.

Border-free payroll

Our world is global, and companies don't have borders. Instant and nearly free payroll is enticing and would save a lot of headaches for organizations. But there are drawbacks, too.

The largest risks will be with the loss of funds through hacking. If you're compensated in cryptocurrency, and you were hacked, it would be impossible to retrieve your funds. There's no dispute resolution center. There's no customer service to complain to for the loss of these funds. Thieves of digital currency have global access while being somewhat anonymous. The hacker could be anywhere.

With the current structure of blockchains, the consumer is responsible for his own security. Currently, customers don't have the main burden of protecting and insuring themselves from a loss. Larger companies and governments offer protection and insurance, and they have for as long as anyone can remember. Regular individuals haven't had to protect themselves in this manner since they stopped holding their own gold during medieval times (more or less).

These challenges haven't stopped companies from processing payroll using cryptocurrency. Bitwage and BitPay are both competing in the market for payroll processing via Bitcoin. Bitwage allows employees and independent contractors to receive part of their paychecks in cryptocurrency, even if their employers don't offer the option. BitPay, on the other hand, has payroll service providers Zuman and Incoin integrated into its payment and payroll APIs. Again, early adoption is happening in areas that had nonexistent or inadequate solutions before.

Faster and better trade

Blockchains will facilitate faster and possibly more inclusive trade. Global trade finance has been restricted in recent years. Some banks like Barclays have even pulled out of growing African markets. They leave behind a vacuum for financing trade. Companies still need capital to ship their goods.

DAOs and micro investments could meet that need and give investors more profitable returns than are currently available on the market. Transparency of all the goods being sold, secure identity, and seamless global tracking that is all connected to a blockchain would open up this opportunity for small investors.

The interoperability between currencies, which companies like Ripple facilitate, will also allow for more trade because they offer flexible ways of calculating foreign exchange rates than through the transfer mechanisms. The introduction of more popular digital currencies into foreign currency exchanges will add to the adaptability and integration of underserved markets.

Aza Finance, formally called BitPesa, is a company that converts M-pesa phone minutes from Kenya into Bitcoin. With this technology, it offers businesses a faster and cheaper way to send or receive payments between Africa and China. The trade between Africa and China is a market of over $170 billion. It takes days to settle payments across borders, and the fees are high. When you use Aza Finance's digital platform, payments are instantaneous and cheap.

Guaranteed payments

Guaranteed payments that are permitted through blockchain-backed transactions will increase trade in places where trust is low. Poorer countries can compete on the same playing field as wealthier nations within these types of systems. As this happens over the next ten years, the global economies will shift. The cost of commodities and labor may increase.

Global companies pay their employees based on competitive pricing, as well as on employees' previous salaries. If blockchains allow for equality across economic divides, it won't happen overnight. Developers and other knowledge workers would be the exception because it'll be easier for them to support themselves based on anonymous work.

Financial inclusion and equal global trade are very important topics for governments. Adoption of digital currencies will more likely be done nationwide in small and developing countries. Most large countries have decentralized power structures that prevent quick changes to vital systems like money.

The central power structures of small countries will allow them to leapfrog over legacy infrastructure and bureaucracy. For example, most African and South American countries don't have landlines or addresses, but they all have smartphones and ability to create cryptocurrency wallets. The missing piece is overall trade liquidity and capacity to pay for basic needs such as utilities, rent, and food through a cryptocurrency.

Micropayments: The new nature of transactions

Micropayments are the new form of transactions. Credit card companies may use blockchain technology to settle the transaction, reduce fraud, and lower their own costs.

Global institutions like Visa and MasterCard, which provide the benefit of delayed payment, will always be needed by consumers in capitalistic societies. Even if the backend changes, you still have the same access points for customers. But physical cards will go away. In fact, that's happening now, even without blockchain technology. With blockchain technology, the customer identities behind payments will be more hardened against theft.

People still need credit to operate a business and get by personally. Credit card companies will keep making money through transaction fees. Credits run the world, and capital markets will always exist in our current social structure. The cost of sending money between groups will decrease, but that's a good thing for financial institutions. They want to focus on the service of providing their customers with the best choices in their investment or banking markets.

Squeezing Out Fraud

Bitcoin was created as an answer to the financial crisis, where fraud and other unethical actions caused the world economy to collapse. It shifts from a "trust or doesn't trust" view of the world to a trustless system. This subtle difference is lost to most. A *trustless system* is one in which you equally trust and mistrust every person within the network. More important, the blockchain provides a framework that allows transactions to occur without trust.

These same types of frameworks can be used for more than just exchanging value over the network. Let me share an example that will help illustrate the potential.

I go to a bar and the man at the door stops me and asks to see my ID. I reach into my wallet and hand him my driver's license. My license has a lot of information on it that the bouncer doesn't need, nor should he have access to (like my address). All he needs from the ID is that I'm over the age of 21. He doesn't even need to know how old I am — just that I meet the regulation requirements.

In the future, blockchain ID systems will let you choose what information you expose to what person and at what level. The more anonymous data it has, the safer it will be. Blockchain systems will help curb the theft of identity and data by not sharing information with those who don't need it or have permission to see it.

Another aspect of blockchain technology is that it will shift fraud from where it happened (past tense) to where it is currently happening in real time. Within our current system, audits are fractional post-mortems of what has happened. A group of outside auditors comes, pulls a few random files, and sees if everything is in place. Doing anything beyond this is too costly and time-consuming.

Record systems that have blockchain technology integrated within them will be able to audit a file as it's created, flagging incomplete or unusual files as they're created. This will give managers the tools they need to proactively correct files before they become a problem.

Another feature of blockchain systems will be the ability to share the data with third parties transparently. In the future, sharing data will be as easy as emailing a zip file, except the receiver will then have access to the original copy, not a copy if the file sent across email. When someone sends a file, he has a version on his computer and the receiver has a version. With blockchain technology, the two people will only be sharing one version.

Blockchains act as a third party that witnesses the age and creation of files. They can tell at a granular level each person who interacted with a file across systems, internally and externally. They can show what is missing from a file, not just the data that is contained in it now. Blockchain files can also be shared in a redacted fashion that does not compromise the validity of documents.

What this means is that you'll be able to see the age of a file, the complete history of a file, and what it looked like over time as it evolved. More interestingly, you'll also be able to see if anything is missing from a file. This concept is called *proving the negative.* Most file systems at this point can only tell you what they have within them. But you'll be able to tell what a file *doesn't* have.

Auditing will be less expensive and more complete. Updating audit rules could be done in a more centralized way. When regulatory nodes within a blockchain network have a shared and transparent view into asset transactions, the reporting of these transactions can be done through the regulator's location, without mandating 100 or more other institutions to adhere to the same rule set.

Blockchain-based systems that are fully integrated across an organization will be able to know where every penny was spent. The last mile of how money is spent is the most difficult to account for across organizations and governments. Because it's so difficult to account for, those wishing to steal funds have the opening they need.

The last mile could become a company's greatest opportunity to save wasted resources and identify corrupt individuals. Nonprofits that have strict guidelines on accounting for how they spend their money could benefit from this type of system the most. They could meet their needs for auditing and accountability to their donors without impeding them in their greater missions for good.

One system that has been explored would integrate directly into the workflow of aid workers. This system was originally designed to track medical records but could also track back all the supplies that are used with each medical patient. The benefits of this system would be monumental, given that so much fraud and theft occurs within the NGO world.

IN THIS CHAPTER

- Evaluating global real estate trends
- Discovering dead capital and ways to fix it
- Uncovering how Fannie Mae will fit in a blockchain world
- Revealing how China will evolve with blockchain technology

Chapter 13

Real Estate

Real estate will be one of the industries most impacted by innovations in blockchain technology. The impact will be felt in every country in a slightly different way. In the Western world, we might see the advent of things like transparent mortgage-backed securities traded on blockchain-enabled exchanges. In China, blockchain integration is already happening with things like notarization, an essential component of real estate transactions. In the developing world, blockchains hold the most promise because they may be able to free capital and increase trade.

This chapter dives into the innovations that are already happening around the world in the real estate industry. I also fill you in on possible changes coming down the road and the significant implications of blockchain technology.

Real estate holds much of the world's wealth and economic stability. The industry will be changing very quickly over the next few years, and knowing where these changes will occur and how you and your company can take advantage of them will be a benefit.

Eliminating Title Insurance

Title insurance is compensation for financial loss from defects in your title for a real estate purchase. It's required if you take out a mortgage on your home or if you refinance it. Title insurance protects the bank's investment against title problems that might not be found in the public records, are missed in the title search, or occur from fraud or forgery.

Title insurance is necessary in places that use common law to govern their title systems. The buyer is responsible for ensuring that the seller's title is good. Within these systems, a title search is done and insurance is bought. In areas that use a Torrens title system a buyer can rely on the information in the land register and doesn't need to look beyond those records.

Blockchain technology has been proposed as a supplement to help consumers in common law title systems. The idea is simple: Blockchains are fantastic public record-keeping systems; they also can't be backdated or changed without a record. In theory, blockchains could transform common law systems into distributed Torrens title systems.

In 2022, Future House Studios, a metaverse content creation company, became the first to mint the ownership of its corporate office as an NFT. The company's office real estate title will remain and transact permanently on a blockchain. TruMint, a blockchain real estate company, guided Future House Studios through the process and hopes blockchain and NFT technology will become a natural part of real estate. TruMint was created by a group of Harvard-trained attorneys and blockchain software engineers. They made it possible to sell real estate legally, as easy as transferring an NFT. Their team created added security measures to satisfy all real estate purchase requirements in all 50 U.S. states. TruMint works as a legal lockbox that puts real-world titles into cold storage, allowing an NFT "digital deed" to transact indefinitely on-chain. At any point, the NFT holder can retrieve the real-world title by returning the NFT "key" to the lockbox. This method will substantially reduce the cost and hassle of selling and purchasing real estate. It's as straightforward as e-signing transfer documents and then moving the NFT from one wallet to another wallet.

Protected industries

Every industry has self-protecting systems to keep new competition out. It might be a high regulatory burden, government-granted monopolies, or high startup costs. The industry that has built up around the buying and selling of real estate hasn't changed much in the last 40 years and is ripe for disruption. Many different parties contribute to the process.

Here are the different industries that are built around the buying and selling of homes:

- **Real estate agents:** A real estate agent helps you compare different neighborhoods and find a home. He often helps you negotiate a price and communicates with the seller on your behalf. This service is valuable, and it's not likely to be displaced by blockchain technology. You can already buy a home without a real estate agent — people choose to work with them because they improve the process.
- **Home inspectors:** Home inspectors uncover defects with the house before you buy it — defects that could cost you money down the road. The defects home inspectors find can be used to negotiate with the seller for a better price. In the future, homes will continue to have wear and tear — that'll never change. But blockchain technology could be used to record repairs to property and defects found in the inspection.
- **Closing representatives:** At closing, the final step is settlement. The closing representative supervises and coordinates the closing documents, records them, and releases the money to the appropriate parties. Closing representatives may be displaced by blockchain technology — the functions performed by closing representatives could be built into smart contracts or chaincode.
- **Mortgage lenders and servicers:** Mortgage lenders and servicers provide funds for a mortgage and collect the ongoing mortgage payments. They won't be displaced with blockchain software, but they may use blockchain technology to help them reduce costs with record keeping and auditing.
- **Real estate appraisers:** The real estate appraiser's job is to look at a property and determine how much it's worth. The appraisal process is done every time a property is bought or refinanced. Companies like Zillow have taken a lot of the legwork out of knowing the market value, but each home is unique and needs to be assessed periodically. Even in the real estate mortgage process, multiple appeals may be called for to meet everyone's needs. It might be useful to record this data within a blockchain as a public witness.
- **Loan officers:** Loan officers use your credit, financial, and employment information to see if you qualify for a mortgage. They then match what you're eligible for with products that they sell. Like a real estate agent, a loan officer helps you get the best option across a spectrum of choices. Blockchain software may be used to help loan officers keep track of documents that they give you and audit the process for fair lending law compliance.
- **Loan processors:** A loan processor assists loan officers in preparing mortgage loan information and the application for presentation to the underwriter. Software that pulls the buyer's source information is being explored. It's not blockchain technology, but it could be disruptive for this position.

- **Mortgage underwriters:** A mortgage underwriter determines whether you're eligible for a mortgage loan. She approves or rejects your mortgage loan application based on your credit history, employment, assets, and debts. Organizations are exploring automating the underwriting process using artificial intelligence. It's not blockchain technology, though.

Each of these agents serves a core purpose that helps protect the buyer, seller, and mortgage provider. In most industries, the cost of doing business goes down over time — improvements in efficiency brought about by competition and innovation contribute to driving down cost. The mortgage industry is attractive as a candidate for blockchain innovation, because the opposite has occurred: The cost of business has gone up. The typical U.S. mortgage is over 500 pages and costs $7,500 to originate. This is three times what it cost ten years ago. Blockchain technology can meet the needs of protecting the buyer, seller, and mortgage provider while reducing the cost to do so.

Consumers and Fannie Mae

The Federal National Mortgage Association (known as Fannie Mae) is both a government-sponsored enterprise and a publicly traded company. It's currently the leading source of financing for mortgage lenders and has dominated the market post-recession as private money left.

Since the recession, 95 percent of all home loans made in the United States have come through Fannie Mae. This is about $5 trillion in mortgage assets. With few exceptions, loans that are not done through Fannie Mae or its close cousin, Freddie Mac, are jumbo loans (typically more than $417,000 each). These loans are still funded through private money.

Fannie Mae has an automated program used by loan originators to qualify a borrower. It helps them navigate guidelines for a conventional loan. Lenders run your loan application through Fannie Mae's computer system, and it spits out an answer of either approve or decline for your loan. Online platforms are using this new software to reach consumers, allowing them to bypass traditional retail locations. Fannie Mae and Freddie Mac are exploring blockchain technology to even further streamline this process and reach customers directly.

Mortgages in the Blockchain World

A mortgage in a blockchain world won't seem that much different than a mortgage in the traditional world. The part that you'll notice is that a blockchain mortgage will be less expensive at closing.

Given that most people only ever buy a few homes in their lifetimes, the difference may not seem like a big deal. But the money does add up. Blockchain technology could lower the cost to originate a mortgage back to pre-2007 levels.

Reducing your origination costs

Mortgage origination costs have increased, and the reason is simple: Banks fear fines that they can incur if they mess up any part of the mortgage process. So, the industry has put in steps to help make sure that they meet all the requirements at the time of origination and years later when they're audited. Big banks have paid billions in fines from the mishandling of documents. They're now required not only to have all the essential documents, but also to prove that they followed the correct process and sent you all the necessary documents.

Blockchain-based products reduce the redundancy that banks began incorporating into their process after the recession. Record keeping and auditing expenses have skyrocketed since the introduction of the Dodd–Frank Wall Street Reform and Consumer Protection Act, and blockchain technology could reduce that cost.

Companies wanting to meet the needs of banks with a blockchain solution would need to let banks prove that they followed the guidelines set out in Dodd–Frank. It would also help banks document why they made certain decisions on loans, and help them locate documents that were used in origination, even if they aren't in possession of them.

Blockchain applications could put close to $4,000 back on the table for the average home purchase. The mortgage industry is a lot like the car loan industry and the credit card industry. Similar applications could reduce the administration cost that these industries have due to consumer protection laws, while at the same time letting companies meet those requirements.

Knowing your last-known document

One of the largest cost drivers in the mortgage origination process often comes years after the loan was first made. Sometimes those facilitating the loan process add unneeded documents into client files, or old files that aren't used to originate a loan are left in the folder. Also, duplicate records may occur. When it comes time to audit the file, there is too much information to sift through. Banks pay money to outside firms to check their records and try to determine what documents were used in the final dissection on your loan.

Blockchain software can solve this problem in an elegant way. Blockchains are distributed record-keeping systems that allow for multiple parties to collaborate on data over time without losing track of what that data looked like at any given point along the way. This means that the half dozen individual organizations that collaborate to help you buy your home can now all interact on the same chain.

A chain in this use case would start with you. Your chain would then have subchains added to it over time, such as the purchase of a home. You could then authorize others — such as banks, employers, credit agencies, appraisal companies, and the like — to write against the chain. They would each add their data to your chain, and the other authorized parties could read this data and add their own.

Blockchains would change the need for central repositories for files. It would automate some of the processing of the paperwork, and would always give a clear history of your loan, reducing the need to audit and prepare documents to be verified.

This is a big idea, but it doesn't require the whole ecosystem to collaborate. Each branch that does would strengthen the system and add value, much like the way each additional person who owned a fax machine made the power of having one that much more useful.

Forecasting Regional Trends

Blockchain has been fighting an uphill battle to become a mainstream software solution. It is often met with fear because many people don't understand how it works or what the actual implications are for its widespread implementation. Also, many of the early advocates, like early adopters of any new technology, were seen as a little "out there." Blockchain gets caught up in the bad PR of Bitcoin and illicit and illegal things being done with the technology.

However, 2016 was a turning point for the industry. It became clear that blockchain would be disruptive and that those who wanted to be on the positive side of that equation had to come up with a blockchain strategy.

Every major bank began programs to investigate and experiment with blockchain or joined a consortium. Many moved first to interbank settlement and cross-border transfers, which are relatively straightforward applications for blockchains. The next and more transformative evolutions will be the systems and data that are secured through decentralization.

In the following sections, I cover the trends in blockchain technology in the United States, Europe, China, and Africa.

The United States and Europe: Infrastructure congestion

The United States and European countries may take longer to implement blockchain technology than other countries. Even though companies in these countries spend billions of dollars on infrastructure maintenance, it's just that: maintenance. There are already existing solutions to the problems that blockchains want to solve. It's not just a matter of saying that blockchains would offer a better solution — that solution must be ten times better than an existing system or be able to implement through integration.

One of the main challenges that the United States faces is that it's decentralized in the distribution of power and decision-making. Each county and each state will come up with its own rules for how to implement or use blockchain technology. This process has already begun.

Blockchains can trigger money transmitter laws and regulations. In the United States, it's clearer at a federal level what types of businesses are considered money transmitters. Given that all the essential public blockchains currently use a cryptocurrency token to drive security, the issue is clouded, which has given rise to private and permission blockchains that operate without tokens.

State licensure requirements are ambiguous for companies using blockchain technology for applications other than payments. Regulations and laws will be enacted to protect consumers. Europe already has laws around "being forgotten." Compliance with these rules could be tricky when data entered into blockchains is around forever and can't be removed by anyone, even if they wanted to.

Being engaged in money transmission in many U.S. states is a felony if you aren't properly licensed. The hard consequences of overstepping law through innovation compel blockchain companies to spend significantly more money and time on compliance — to the tune of an average of $2 million to $7 million per year per company because they must meet regulatory requirements in all 50 states. The legal fees are heavy burdens for these technology startups.

The legislation of each state as applied to the blockchain industry is not clear yet. New York and Vermont have begun integrating this technology into law. New York has increased the cost to be in compliance and driven innovation to move to friendlier locations. Vermont, on the other hand, passed a law that makes blockchain records admissible in court.

Luxembourg created a legal framework for electronic payment establishments in 2011 and was early on the idea of "electronic money." Luxembourg and the UK have become home to many blockchain companies because the regulatory environment is easier for them to navigate and afford. For less than $1 million, blockchain businesses can obtain a payment instrument license in the European Union. This license grants companies access to 28 EU countries. This approach has allowed the EU to advance beyond the United States in fintech innovation.

China: Uncertain state

Bitcoin and other cryptocurrencies have had bipolar standing in China for years. The country took its first hostile stance against crypto industry since 2013 when it rolled out its first set of crypto restrictions. In 2017, the government issued a ban on initial coin offerings (ICOs). As a result, many crypto entrepreneurs have fled China for fear of arrest. The crackdowns are part of a broader pattern of tightening and then losing regulation in China. This ebb and flow have made it difficult for blockchain companies to operate in the country, and many have been forced to shut down or relocate. Given this history, it's not surprising that so many of the early blockchain companies in China have disappeared.

Bitcoin and other cryptocurrencies have long been seen as a threat to China's economy and financial stability. In 2021, the Chinese government took action to crack down on cryptocurrency trading and mining in what is seen as one of the most intense crackdowns in the world. The move significantly impacted the global cryptocurrency market, as China has been a major player in Bitcoin mining and trading. However, the Chinese government is not entirely opposed to blockchain technology and is instead pursuing other uses for it, such as supply chain management and nonfungible tokens (NFTs). The key difference is that these applications must be under the control of the government, which goes against blockchain's decentralized and unrestricted nature.

It remains to be seen how this crackdown will affect China's role in the global cryptocurrency market, but it's clear that the government is intent on maintaining tight control over the use of blockchain technology within its borders.

The developing world: Roadblocks to blockchain

The future is here — it's just not distributed. This is especially true in developing countries, which often have a greater need for technology, yet don't have the same resources or the right political environment to allow those innovations to take root. Some small countries try protectionist measures that block the importation of goods that could be made within their borders; other countries mistrust the quality and benevolence of products and services that come from the outside sources as well. On a darker note, some political systems benefit too greatly from the inefficiencies and ambiguities that their legal system has in place to change.

Hernando de Soto Polar is a Peruvian economist and author who has spoken widely on an informal economy and the importance of business and property rights. One of the prominent issues that keeps the developing world undeveloped is *dead capital.* The property that is informally held and not legally recognized with the current systems in place cannot be trusted. For owners of this land, it is difficult or impossible to finance and sell. The uncertainty also decreases the value of the assets. The Western world has been able to borrow against assets and sell them relatively freely. This has driven innovation and economic prosperity.

The technology that is enabled by blockchains could change that reality for developing countries very quickly. Clear ownership records for land would mean that it would be sellable and financeable. This would make the beachfront property of Colombia irresistible. Irreversible payments and true known identity would open credit and commerce in new ways.

Many startups and hackers have come together to try to make this future vision a reality. Even larger global players like the World Bank have had repeated meetings about blockchain and its impact in the developing world. Bitcoin and blockchain are making inroads in Africa where local currencies and infrastructure are deeply mistrusted. AZA Finance, a payment and trading platform servicing many countries in Africa, has begun expanding to the UK and Europe. It has also started widening its service offerings to things like payroll.

As many roadblocks as developing countries have toward development and innovation, they also have advantages that Western countries will never overcome. The lack of existing infrastructure in developing countries makes it easier for them to leapfrog Western nations. This was evident in the proliferation of cellphones in developing countries. Developing countries also don’t have the same regulatory bodies and consumer protections. This is particularly attractive for blockchain startups that fall into the gray zone in Western countries. Developing countries often have fewer decision makers, making it easier to meet people who have the power to change.

IN THIS CHAPTER

- Building new business
- Tailoring individual insurance
- Creating new insurance markets
- Cutting costs in unexpected ways

Chapter 14 Insurance

Blockchain insurance technology is situated to change how individuals and companies buy and obtain insurance coverage, and it's being tested by companies you may know, like Toyota. You need to understand the implications of these new technologies that are just now on the horizon.

In this chapter, I explain how these new technologies work and their core limitations. I show you how Internet of Things (IoT) devices will collaborate with insurance providers. I also describe how self-executing blockchain contracts will shape policies and company structures.

This chapter prepares you for the fundamental changes in technology that may shift the burden of proof. After reading this chapter, you'll be able to make more educated decisions about blockchain-based insurance coverage and payments. You'll understand how the cost of coverage will affect you and the different types of coverage that will become available to you in the future.

Precisely Tailoring Coverage

IoT devices, immutable data, decentralized autonomous organizations (DAOs), and smart contracts are all shifting the development of insurance for consumers. The convergence of all these technologies is possible because of the development of blockchains.

Blockchains do a few things really well that will allow for two major shifts in how insurance will be bought and sold in the future: Individuals will be able to gain more custom coverage, and new markets will open up that weren't possible before due to costs.

Insuring the individual

Insurance built around the individual will allow for a significant shift of priorities. Asset management will be less critical, and the insurers will be able to focus on risk calculation and matching supply and demand.

You could create a marketplace platform that insures customers. There are many ways that you could organize this new business. One possibility would be an on-demand marketplace where users post their requests, either standardized by custom smart contract or by chaincode contract. If you haven't read about these types of new self-executing digital contracts, check out Chapter 5 on Ethereum and Chapter 9 on Hyperledger.

With this type of model, you, as the insurer, could calculate the premium for the specific demand, based on historical data and other risk calculation factors in your risk model. If the customer is satisfied with the offer, the customer can bid or subscribe, depending on the demand model being utilized.

This new type of insurance could be adopted by peer-to-peer (P2P) or crowd-funded insurance or a traditional insurance company that adopts the technology. Either way, both are created in a decentralized cryptocurrency ledger with the use of smart contracts/chaincode, which guarantee the payment from the customer to the investor and vice versa if an incident occurs. Blockchain is key here, because it enables a few things that weren't feasible or secure a few years ago.

Blockchains create near frictionless transfer of value meaning micropayments are feasible because the transaction fees are so low. You can now open up new markets that did not have a working monetary system or legal system or instances where the cost of transactions and disputes outweighed the benefit of offering coverage.

You can use DAOs, with smart contracts, to govern large groups at a fraction of the cost and time. You could use this model to incorporate and administer your new company, and possibly crowd-fund insurance platforms.

The self-executing nature of smart contracts could also illuminate many of the costs of claims adjustment and third parties that help with the processing and collection of funds.

The legality of all this is still in question. Determining privacy concerns and consumer rights is difficult. Each country has its own regulations and disclosures for the insurance industry. That said, consumer rights and disclosure requirements may be better executed using blockchain technology. Decentralized insurance (also known as "Insurance 2.0") is a type of insurance built on blockchain technology and operates decentralized, without the need for a central authority or intermediary. It aims to improve upon traditional insurance models by providing more transparent, flexible, and secure insurance products and services.

One of the main benefits of decentralized insurance is the use of *smart contracts*, which are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. Smart contracts can be used to automate the buying and selling of insurance and facilitate the payment of claims. This can make buying and using insurance more efficient and transparent, because all parties involved can see the terms of the contract and the conditions under which claims will be paid.

Decentralized insurance can also be more flexible than traditional insurance, because it allows users to customize their coverage and choose from a variety of insurance products. It can also offer more diverse coverage, because it isn't limited by geographic boundaries or regulatory frameworks.

Overall, decentralized insurance has the potential to provide more accessible, transparent, and secure insurance products and services and is an emerging area of interest in the blockchain industry.

Here are some of the promising innovators within the space:

- **InsurAce (`www.insurace.io`):** InsurAce is a decentralized multi-chain insurance protocol that provides insurance services to decentralized insurance users. It allows you to secure investment assets like smart contracts, custodian risk, and token offerings. InsurAce claims to lower its premium by creating portfolio-centric products that embrace risk diversification.
- **Harpie (`https://harpie.io`)** is an interesting decentralized insurance company that offers crypto protection plans for cryptocurrencies, tokens, nonfungible tokens (NFTs), and other digital assets. Harpie connects directly to your Ethereum wallet, giving Harpie a clear insight into your asset holdings and enabling Harpie to monitor anything that may happen to your assets. Harpie provides coverage for theft, hacks, natural disasters, and more. It's conveniently compatible with most crypto wallets, allowing you to secure more than one wallet at a time. Harpie is also launching an on-chain firewall it claims will prevent hacks, scams, and other types of theft.

- **Tidal (`https://tidal.finance`)** is interesting within the smart contracts space because new technologies being built in decentralized insurance are vulnerable to manipulations and hacking. Tidal seeks to build trust in blockchain protocols by creating a decentralized insurance market for decentralized insurance that lets the new financial pioneers offload some of the inherent risks of building software on the Internet. It connects buyers and sellers to crowd-source coverage for smart contract hacks. Tidal also allows you to create specific insurance pools for one or more protocols. The platform's primary purpose is to maximize capital efficiency while offering competitive insurance premiums.

The new world of micro insurance

Micro insurance is insurance to protect low-income people against risk, such as accident, illness, and natural disaster. It has become more feasible through blockchain technology.

When thinking about micro insurance, pay attention to two categories (which can go hand in hand):

- Insurance targeted to low-income households, farmers, and other entities where the insurance is designed around specific needs — typically, a low-premium and index-based insurance
- Insurance that deals with low-value products or services

The biggest issue with these types of contracts within traditional insurance models is that their handling costs are disproportionately high and make it unattractive to serve these markets.

The low-friction attribute of blockchains allows them to move value at extremely low cost, nearly instantly anywhere in the world, with no charge backs, opening up the opportunity of serving more people and at lower costs.

The key advantage of blockchain is that the creation of smart contracts allows for secure transactions without any middleman, so insurance has significantly lower costs.

The blockchain micro insurance principle is simple and consists of four steps:

1. Lending/insuring agreement proposal

   A person can offer to lend his property through his insurance provider, if the property is digitally registered. The offer can be sent to the potential user, either through the insurance company channels or via a public platform such as Facebook.

2. Agreement review

   The borrower can then review the proposal that he received and accept or decline it. The offer is kept in the public records, and if the borrower accepts the proposal, he can purchase the insurance through standard payment channels, and the process moves to the third step.

3. Agreement signature and notarization

   If both parties are on the same page, the insurance is paid for and the borrower receives the property in question, and the agreement is digitally signed and notarized onto a blockchain. This makes it virtually tamper-proof. All the transaction information is safely stored with a clear audit trail if it's ever needed.

4. Confirmation tokens

   Both parties receive special digital tokens that serve as the proof of identity for the agreement in question. These tokens are used to cryptologically confirm that both parties have signed the agreement.

Besides this ease of use, smart contracts allow for index-based insurance, which is very useful for agricultural insurance and other fields where the values depend greatly on dynamic factors that can be accurately documented by trusted third parties. In this particular case, insured farmers can receive automated payouts when particular conditions, such as drought, are reported by verified meteorological databases, thus further reducing potential service cost.

This sector of decentralized insurance, micro insurance, has been slow to grow. Systems built on blockchain technology have more expense and additional risk than traditional software. A shortage of competent developers and privacy concerns have slowed commercialization of some pretty good ideas. However, the promise of decentralized and open-source financial applications, like self-executing insurance contracts, has kept investment dollars coming. These applications, often called *smart contracts*, can be used for a variety of purposes such as lending, borrowing, trading, and more.

A startup called Yas Microinsurance (`https://yas.io`) has started to make waves. It's a Hong Kong–based insurance on-blockchain provider that raised $4.5 million in 2022 to provide insurance for things like special events or even just going for a walk. Yas Microinsurance claims its product is autonomous insurance and micro-insurance on the blockchain. It's still in the early days of commercialization.

Witnessing for You: The Internet of Things

Blockchains enable the creation of a new type of identity for both people and things. They build on a traditional model where a certificate authority issues a certificate. For people, that certificate would be a document such as a birth certificate or a driver's license. But "things" have similar certificates that help consumers validate quality and authenticity.

These types of certificates have been knocked off for years. More and more sophisticated security has gone into their creation, but this increases the cost. Blockchains allow for the recording of these traditional certificates in an unalterable history that anyone can look up and reference. An added feature is the ability to update those records as new events occur.

IoT devices can now publish all kinds of data autonomously to their records and update the current state they're in. Now that IoT devices can speak for themselves and have their histories and identities published and sharable with third parties, insurance will be just one of the many industries affected.

IoT projects in insurance

IoT will likely have significant impact in three areas of your life: the connected car, the connected home, and the connected self.

The IoT is, at its core, a disruptive technology and, as such, it'll change the shape of a broad range of industries, such as automotive original equipment manufacturers (OEMs), home security, and cable and mobile providers. In that mix are insurance companies — in particular, the ones that work with property and casualty (P&C) policies.

The data gathered by the sensors in the new appliances and devices, along with the automation and additional control options, will lead to new possibilities when it comes to new companies emerging in the insurance industry. Combined with the blockchain decentralized ledgers and smart contracts, the whole process could be automated to a level that would've been impossible before.

WARNING

The new, always online, lifestyle that comes with such a radical shift in technology removes some of the existing risks, but it introduces new ones, the most important of which is information security. All this means that the risk factors will have to be recalculated. For example, self-driving cars will have reduced risk of accident due to the absence of human error, but the reliability of the technology will be in question until we have enough data from real-world application.

Implications of actionable big data

Big data has been a thing since 2000, and nowadays it's a $200 billion industry and of particular importance to the financial sector. However, big data comes with a number of problems that only grow with its presence in the everyday world:

- **Control:** If you have a big multinational enterprise or a consortium, the issue of data sharing becomes fairly significant. Version control is imperfect, and it can sometimes be really difficult to tell which is the latest, most up-to-date copy.
- **Data trustworthiness:** How do you prove if you're the creator of said data, or someone else is? What happens with corrupted data?
- **Data monetization and transfer:** How can you transfer, buy, or sell rights to any data, and be sure that it's the only copy there is?
- **Data changing:** How do you ensure that data is not being changed when it's not supposed to?

All these problems are solvable using cryptocurrency and blockchain. The large challenge that the industry is working through now is scaling blockchain technology to accommodate the cost and data storage demands of enterprises.

Taking Out the Third Party in Insurance

One of the greatest advantages that blockchain tech introduces into the modern finance world is the smart contracts that allow for business transactions without the involvement of a third party, such as banks or intermediaries. Removing third parties allows for things like micropayments and reduction in cost associated with repetitive human labor.

Put simply, a *smart contract* is a protocol that allows for two parties to record their transaction into a blockchain. These contracts can be used for pretty much anything, from exchange of physical goods (that have digital signatures) to exchange of information or money.

The key security feature here is that, unlike the ordinary financial database, the information is distributed to and verified by all the computers in the network, making it decentralized. The data is unique and not able to be copied; the audit trail is immutable.

Self-driving cars present a compelling use case for blockchain technology. There is a dilemma in assessing fault without a human to witness. Determining who is to blame — was it a failure of the car's navigation, a manufactured part, or the other driver?

One interesting group working in insurance automation is Squirrel Finance (`https://squirrel.finance`), a decentralized insurance platform for yield farming on BNB Smart Chain (BSC), previously Binance Smart Chain. Squirrel instantly and automatically compensates you if your funds are stolen. It works by checking whether you've received your expected deposited amount when you withdraw. If the amount doesn't match, Squirrel will automatically compensate you with the withdrawal transaction amount from your contract in the form of NUTS, the Squirrel token. There is no human involvement after setup. Squirrel's governance token is also used to manage the protocol and earn farm insurance fees.

Decentralized security

At the core of current business models is something that could be called the *centralized trust paradigm*, in which middlemen such as bankers, brokers, and lawyers coordinate and ensure the veracity of financial transactions and exchanges of goods.

Centralization comes with certain inherent security risks, such as data corruption and theft. Blockchains combat this by creating a decentralized system that is based on mutual distrust of all the participants that keep each other in check.

In order to create such a system, you create a distributed ledger that uses cryptocurrency (like Bitcoin, Ethereum, or Cardano), where each participant is both the user of the system and responsible for its maintenance and upkeep.

Crowdfunded coverage

Similar to standard crowdfunding initiatives, the idea is to pool resources from numerous entities or persons in order to cover for an unexpected shortcoming in an insurance plan. For example, a retirement insurance plan could kick in only at the age of 65, but a person could be forced to retire early because of unforeseen circumstances, and additional funds would be needed by the unfortunate individual.

Economic disparity has grown over the years, and numerous underinsured or uninsured people could benefit from such a system. Crowdfunding can potentially provide benefits to all three parties in question:

- **Insurers** gain increased revenue because more people are interested in their plans. They gain access to a greater portion of the underinsured population. In addition, the insuring company could improve its brand recognition — it could be seen as a company that cares.
- **Donors** could benefit from possible tax exemptions, if the structure of the campaign allows it, or they could gain other benefits, such as discounts or free services.
- **Seekers** (those looking for insurance) obviously stand to gain the most, as they can get better protection and more affordable coverage.

Cognizant proposed interesting insights to crowdfunding insurance in its white-paper. You can find it at `https://goo.gl/u3Kd3U`.

The implications of DAO insurance

DAOs are corporate entities that have no full-time employees, but are able to perform all the functions that a standard corporation can. The ability to create such an entity stems directly from the improvement in blockchain algorithms, which has happened over the last few years and has created what is commonly known as blockchain 2.0.

A DAO is, in essence, a form of an advanced smart contract. The DAO is able to treat DAO as a corporation where all its individual policy users are shareholders, while the corporation itself never is in direct control of any particular group or individual.

In the same manner, a DAO is never under control of the developers, and they don’t issue or deny policies. It’s strictly a peer-to-peer insurance model. Although vulnerabilities regarding identity verification still exist, this system will be improved, and in reality, the same issues exist even in the current, centralized insurance systems.

IN THIS CHAPTER

- » Reading blockchain documents
- » Building smart cities
- » Creating hack-proof identity

Chapter 15
Government

In this chapter, I introduce you to the exciting innovations that are taking place inside governments. Web 3.0 applications and other blockchain innovations, such as Bitcoin, are affecting the lives of everyday citizens globally, thanks in part to the technological revolution of Web 3.0 and the final stage of globalization, known as *end-state globalization.*

This chapter explains how governments will meet the challenges of porous borders and unbound citizens that can move freely and operate outside of traditional financial institutions. This chapter also explains how governments fight against cybercrime and identity theft thanks to the rising number of cases linked to token offerings and cryptocurrencies.

After reading this chapter, you'll have a clear understanding of regulatory changes and smart city initiatives that will be critical to economic growth and sustainability. Many governments are using blockchain technology to bridge technological gaps.

Global Regulatory Action

The cryptocurrency industry has moved into a new stage of development, called *Web 3.0.* Artists from around the world have flocked to blockchain technologies to create art that is digitally transferable and programmable. Most artists are using nonfungible tokens (NFTs) to represent the ownership of their art or fungible membership tokens that allow fans to special access to the artist. The mass adoption of blockchain has created internal pressure for governments to come together to regulate the flow of value over the Internet. Smaller countries are facing an existential crisis regarding blockchains, given that most citizens can now access blockchain tech and both hold and create value with nothing more than a smartphone and an Internet connection.

Governments like El Salvador have leaned into the blockchain revolution. In a global first, El Salvador adopted Bitcoin as its currency in 2021. The president of El Salvador, Nayib Bukele, believes that Bitcoin is the path to financial freedom. Economic experts and many Salvadorans worry the change may threaten the country's sovereignty. An interesting side effect of El Salvador's move is that other countries may have to recognize Bitcoin as a legal tender.

Ninety-five percent of the world's population now has access to cryptocurrencies. Most people in the world can buy and trade new financial products. Almost every person on the planet could start using a sovereign identity they create for themselves.

Sovereign identity refers to a person's ability to control and manage their own digital identity, instead of relying on third parties to do so on their behalf. In a sovereign identity system, individuals have the ability to create and manage their own digital identities, which may include personal information, credentials, and other types of data. These identities are typically stored on a decentralized platform, such as a blockchain, which allows individuals to control and access their identity information without relying on a central authority.

The goal of sovereign identity is to give individuals more control over their personal data and to enable them to securely and privately interact with various systems and services online. It's also seen as a way to protect against identity theft and other types of online fraud, because individuals have more control over their own identity information and can verify their identity using cryptographic techniques.

Sovereign identity paired with open markets and art platforms allow anyone to make money selling their digital creations. It also makes it possible for people to avoid taxation and launder money. All this new global economic activity has brought together many countries to create and enforce regulations and taxation in a group known as the Financial Action Task Force (FATF). If you've ever opened a wallet or exchange account, FATF affects you. The group is focused on combating money laundering and terrorism financing. It includes 37 of the most influential and powerful countries in the world and has cooperation from many more. The list includes big economies like the United States, Russia, China, most of Europe, and India.

The FATF has announced that transactions involving cryptocurrencies and NFTs need to adhere to the Travel Rule, Which requires each member country to enforce Anti-Money Laundering (AML) and Know Your Customer (KYC) verification and that financial institutions must pass on the information to the next financial institution.

That may sound like no big deal, because all banks have been compliant with this rule for years. But these rules are now being enforced on cryptocurrencies that live entirely outside traditional financial institutions. Enforcement is difficult because cryptocurrencies are anonymous and permissionless. Every country that is part of the FATF must follow these rules and make cryptocurrency service providers like wallets and exchanges collect information about their clients and send it to governments. You will need to be known to send and receive cryptocurrency.

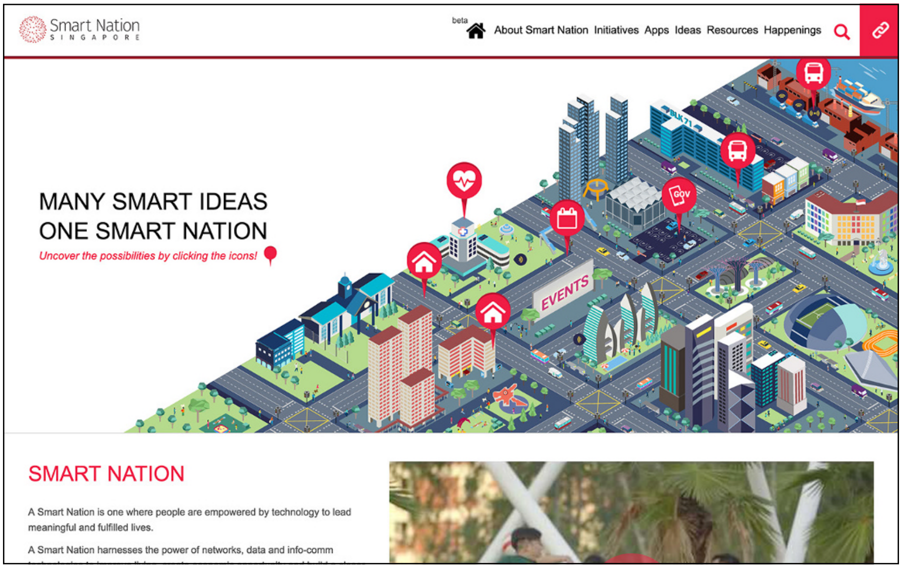
The Smart Cities of Asia

Smart cities are taking advantage of modern technology to enhance infrastructure function, and safety, and improve things like traffic and air quality. The business of becoming a smart city is booming, and almost every larger municipality has embraced the smart city concept.

Blockchain is especially useful when integrated with the Internet of Things (IoT) used by smart cities. Several interesting projects are being piloted now for commercial deployment. The U.S. Department of Homeland Security is exploring securing IoT devices used by Customs and Border Protection (CBP). Companies such as Slock.it are allowing connected objects to use the blockchain to enter smart contracts; its first product was a blockchain-enabled smart lock, which could be used by Airbnb customers. The integration of these technologies allows devices to use their sensors to set up smart contracts. This same technology could be used by city parking meters.

Figure 15-1 shows the home page of Singapore's Smart Nation project. Singapore has been courting startups from around the world to develop new technology in its "regulatory sandbox." It's a welcome invitation to blockchain technology companies that have been operating in the *gray zone* (where there is not a clear regulatory framework established); however many countries, like Singapore are taking direct action to define the space and let companies know what is allowed and not allowed.

Blockchain technology could also be used to share information between networks in a smart city securely. Many cities are exploring how to use blockchain to alleviate traffic jams. Singapore's Smart Nation project hopes to use the mobile phones of its citizens to measure the conditions of their bus rides, and then analyze the data to see when roads need to be upgraded. Singapore has been a leader in smart city development and has begun developing smart cities in other countries.



MANY SMART IDEAS
ONE SMART NATION

Uncover the possibilities by clicking the icons!

SMART NATION

A Smart Nation is one where people are empowered by technology to lead meaningful and fulfilled lives.

A Smart Nation harnesses the power of networks, data and info-comm

FIGURE 15-1: Singapore's Smart Nation project.

In this section, I walk you through some of the many blockchain efforts that are taking place in Asia.

Singapore satellite cities in India

The Indian government launched its Smart Cities Mission in 2015, with the intention of building 100 new smart cities and more than 6,000 projects. Many of these developments will be in the Delhi Mumbai Industrial Corridor, which is a 620-mile (1,000km) stretch between Delhi and Mumbai. Infrastructure worth $11 billion has already been planned across 33 cities, and much of the development will be funded through a public–private model. The project is expected to attract $90 billion in foreign investment, which will be used to create business parks, manufacturing zones and smart cities, all of which will be situated along a delegated rail freight corridor.

These smart cities are being developed as India's economy industrializes and the population becomes more urbanized. State intervention in the form of centrally planned cities is necessary in order to prevent the existing cities from becoming overcrowded and unlivable. India is particularly vulnerable to climate change because of its immense and impoverished population. Because of this, it's important that these cities are sustainable and smart. They need low-energy housing materials, intelligent grids, planned transportation, integrated IT systems, e-governance, and innovative water harvesting.

Singapore is a prime example of an intelligently planned city. Despite the high population density, it has excellent infrastructure and a high quality of life. Many of Singapore's private organizations have the knowledge and resources that are needed to develop India's smart cities. In collaboration with the Indian government, the private sector would be able to provide the capital, skills, and technology that are necessary for such large plans.

Andhara Pradesh and the Monetary Authority of Singapore have announced a financial technology (fintech) innovation partnership, with a primary focus on blockchain and digital payments. Singapore aims to develop a marketplace for fintech solutions in India.

Singaporean leadership has shown interest in partnering with India to develop a smart city as well as a new capital for Andhra Pradesh, a state in the southeast. It's setting up committees to analyze the potential for collaboration in India's plan to build 100 new cities, as well as further developing the infrastructure across 500 existing towns and cities.

India's minister of urban development has been in talks with both Singapore's current prime minister and its former prime minister. He has been seeking Singapore's expertise in smart cities, particularly focusing on intelligent transport systems, enhanced water management, and e-governance. The minister of urban development has also been examining Singapore's public housing schemes, as well as their private housing regulations. Funding structures for transport infrastructure have been looked at as well.

Indian authorities have also engaged a team of Singaporean experts to assist the development of a satellite town in Himachal Pradesh. The 49-acre (20-hectare) project aims to help decongest Shimla, a town that has had a massive population rise in the past few decades. The Singaporeans will assist in educational, residential, and commercial aspects of the town under development.

Both Singapore and Malaysia have shown interest in investing in another satellite town near Jathia Devi. The Singaporean government is undertaking a study that will assess various options. The state government of Himachal Pradesh is looking at developing five satellite towns near existing cities, using a private–public funding model.

Singapore’s Ascendas-Singbridge launched its eighth IT park in India. The 59-acre (24-hectare) International Tech Park Gurgaon is expected to have its first building completed in the middle of the year. The $400 million project aims to offer 8 million square feet of business space to help accommodate India’s burgeoning IT sector.

China’s big data problem

Blockchain technology is widely being discussed in China as a way to enhance the reliability of big data. People are looking at it as a way to solve the trust issue involved in sharing data between two or more parties that don’t have aligned incentives. Blockchain technology offers many new solutions to track ownership, origin, and authenticity.

Peernova is a promising U.S. company that is tackling big data problems. It previously focused on Bitcoin mining but pivoted into the blockchain space and raised $4 million from Zhejiang Zhongnan Holdings Groups, a construction company from China. Peernova plans to use blockchain technology to query traditional databases and track changes.

The use cases are to verify any changes to subsets of large data stores and use the more efficient and complete cryptographic audits instead of a traditional auditor to provide a reference point for a company. It hopes to help hedge funds calculate the tax liability of their investments by using blockchain to trace the history of money that has been invested over the years.

Dalian Wanda, the biggest real estate developer in China, is also getting into the blockchain game. It has teamed up with big data software company Cloudera to launch a blockchain project called Hercules. It sees the potential to use blockchain technology to make predictions derived from big data actionable for managers as they’re occurring, moving managers from reactive to proactive in situations like modifications to their protocols, as well as monitor user behavior within their systems.

Dalian Wanda and Cloudera aim to keep developing Hercules and integrate their technology into a variety of industries that rely on IT and big data. Project Hercules will act as an open-source suite that supports the needs of businesses. It makes it easier for organizations to deploy and manage blockchain apps on large data clusters.

You might find it odd to see a digital mining company partner with a traditional construction company to tackle auditing issues for hedge funds, or real estate companies working with big data to solve issues for system administrators, but this is the wild west of the blockchain world. The shortage in blockchain talent and the high demand for blockchain projects and investment are fueling this environment.

The Battle for the Financial Capital of the World

Blockchain technology has come into its own since breaking into the public consciousness with a plethora of news coverage in 2015. Many startups have been working on beta and pre-launch builds since then, with nearly 2,000 new blockchain startups forming overnight in 2016. Many of these finally went to market in 2017 and 2018 in Singapore, Dubai, and London where the regulatory bodies welcome innovation and compete to be the financial mecca of the world. This isn't just about fintech and smart cities for these leaders. It's a race for relevance in a world shifting to borderless and financially fluid global citizens.

London's early foresight

In 2016, the central government of the United Kingdom put out a report called "Distributed Ledger Technology: Beyond Block Chain" (`https://goo.gl/asIz6L`), which asserted that distributed ledger technology (blockchains) could be used to reduce corruption, errors, and fraud, and make various processes more efficient. They also stated blockchains could change the relationship of citizens with their government by bringing about more transparency and trustworthiness. But London has been very friendly to the technology since at least 2014. Many early blockchain startups incorporated or worked in London because it was the unofficially safest place to build a business. This was a big deal at that time because many cryptocurrency entrepreneurs were being arrested in 2014 and 2015.

Since this report came out, blockchains have been approved for use across government applications in the UK, including Whitehall departments (non-ministerial departments such as Land Registry, Forestry Commission, and Food Standards), local authorities, and delegated governments.

Here are several interesting projects and experiments that are happening in the UK:

- **Blockchain-based welfare distribution:** The Department of Work and Pensions has partnered with Barclays, RWE, GovCoin, and the University of London in an experiment that will use blockchain technology to distribute welfare with a phone app. The trial was designed to see if payments could be sent and tracked using blockchain technology.
- **Government DLT:** Credits, a blockchain platform provider, and the UK government are collaborating on a framework that allows UK government agencies to experiment with blockchain technology. (DLT stands for distributed ledger technology.)
- **Blockchain-based international payments:** Santander Bank has launched a trial of blockchain-based international payments. The staff pilot program involves an app that connects to Apple Pay. Users can use touch ID to transfer payments of between £10 and £10,000.
- **Using blockchain technology to trade gold:** The Royal Mint has teamed up with CME Group, a market operator, to use blockchain technology to build a gold market in the hopes of making London a more appealing city for gold sales. Blockchain technology is being adopted by the two entities because they see it as an efficient digital mechanism for trading gold.

These are all experiments to see if blockchain technology is the new platform to exchange value. The success or failure of this scheme will define the future course of the UK and the rest of the world.

The regulatory sandbox of Singapore

Singapore, like the UK, has gone out of its way to make working there as easy, friendly, and financially appealing as possible. In 2015, government officials traveled to San Francisco to announce and recruit entrepreneurs to come work in what they coined a "regulatory sandbox" — a play on the term *development sandbox*, which is a safe environment where developers can build software. Singapore had the same idea in mind for building software companies.

At that time, blockchain companies in the United States and many other places were still in the gray zone. The idea of a safe place to operate and invest money was very appealing to many entrepreneurs, myself included. If you've never been to Singapore, you should go! It's beautiful, clean, and safe.

Singapore is taking steps to explore the technology, and it's paying off. A Singaporean bank, OCBC, used blockchain technology for cross-border transfers. It sent money to its subsidiaries, OCBC Malaysia and the Bank of Singapore.

R3 has also been active in Singapore. It opened a lab for researching and developing digital ledger technologies alongside Monetary Authority of Singapore. R3 is working on an exchange to support interbank payments. The banks will deposit cash and be issued a digital currency.

Singapore's central bank also launched a pilot project, along with eight foreign and local banks as well as the stock exchange. This proof-of-concept project aims to use the blockchain technology for its interbank payments. The pilot project also aims to review cross-border foreign currency transactions.

It's not just blockchain companies that are going to experiment in Singapore. All the biggest players have gotten involved — Bank of America, Merrill Lynch, IBM, Credit Suisse, The Bank of Tokyo-Mitsubishi UFJ Ltd, DBS Bank Ltd, JP Morgan, The Hong Kong and Shanghai Banking Corp Ltd, OCBC Bank, United Overseas Bank, and the Singapore Exchange.

TIP

Every bank in the world must know who it's doing business with. The whole idea of Know Your Customer (KYC) helps combat money laundering and tourist funding.

The next phase will be determining foreign currency transactions and building on Singapore's KYC efforts. This could lead to the country forging the way in blockchain-based identity. Singapore already has a robust and modern digital identity system that could easily be connected to a blockchain.

The Dubai 2020 initiative

The government of Dubai had an ambitious plan to move all government documents and systems onto the blockchain by 2020. The scheme to go paperless was part of its initiative to become a global leader in blockchain technology and boost efficiency across all sectors.

The Minister of Cabinet Affairs and the Future detailed how the new scheme will enable users to update and verify their credentials through the blockchain. They'll only have to log in with their credentials once to have access to both government and private entities, such as insurance companies and banks. They also anticipate sharing their technology with other countries to allow simpler border crossings. Instead of passports, travelers could use pre-authenticated digital wallets, as well as pre-approved identification.

The Dubai government has estimated that its blockchain initiative has the potential to save 25.1 million hours in productivity. This boost in efficiency will also help to cut back on carbon emissions.

Dubai's Global Blockchain Council (GBC) announced seven new public-private collaborations, combining the skills and resources of startups, local businesses, and government departments. They'll apply blockchain technology to the following:

- **Healthcare:** The Estonian software company, Guardtime, will collaborate with one of Dubai's largest telecom operators, Du, to provide the technological expertise for digitizing healthcare records and moving them to the blockchain.
- **The diamond trade:** A pilot project will use blockchain technology for the authentication and transfer of diamonds. The Dubai Multi Commodities Center will be digitize *Kimberly certificates* (documents created by the UN to restrict the trade of conflict diamonds).
- **Title transfers:** Title transfers will be digitized and recorded on a blockchain. A Singaporean blockchain startup known as Dxmarkets has developed a proof-of-concept.
- **Business registration:** The GBC is trialing the use of blockchain technology for business registration. This is different from the decentralized autonomous organization (DAO) of Ethereum but could streamline identity verification through the Flexi Desk program. It's currently in the demo stage, with several entities working on a proof-of-concept.
- **Tourism:** Dubai Points is a pilot program that was launched in collaboration with Loyyal, using blockchain technology to help the tourism industry. It aims to incentivize travel by granting points to travelers who visit certain places. It will use smart contracts to facilitate the rewards. These points may work like a crypto token and be tradable an exchanges.
- **Shipping:** IBM is working with the GBC to use blockchain technology for improved shipping and logistics. The program aims to help regional players to collaborate on how they exchange goods. Smart contracts will be utilized as solutions for compliance and settlement issues.

Dubai, like Singapore, has put its money and talent into insuring that it will dominate the blockchain space quickly. This is one luxury of small government and central authority.

Bitlicense regulatory framework: New York City

If you're planning on operating a blockchain startup in New York City, plan for extra fees. In June 2015, the New York State Department of Financial Services

(NYDFS) put out the final version of Bitlicense, the regulatory framework for digital currency aimed to give the industry more clarity. In reality, it pushed many blockchain startups out of NYC. The license itself costs $5,000 and can be up to 500 pages. It requires the fingerprints of each company's leaders and an extensive background check on the applying businesses. The chief complaint is the roughly $100,000 in expenses associated with the application. This estimate includes time allocation, legal, and compliance fees. Bitlicense is in stark contrast to the efforts made by other financial centers such as London, Singapore, and Dubai.

The final Bitlicense was the result of almost two years of research and debate over how the technology should be regulated. It came about after it was deemed that the existing regulations were not suitable for digital currency companies.

On a positive note, NYC blockchain businesses no longer need approval from the NYDFS for new software updates or further rounds of venture capital funding. The framework states that digital currency firms only need approval for changes that are "proposed to an existing product, service, or activity that may cause such product, service, or activity to be materially different from that previously listed on the application for licensing by the superintendent."

The first company to receive a Bitlicense was Circle, the Bitcoin wallet providers. The license allows them to operate in New York under the regulatory framework. Circle is one of the few companies that can legally do so. Most blockchain startups are avoiding working in New York because the cost and effort of the license outweigh the benefit. Only the highest-funded startups are making an effort.

Ripple has been awarded its second license. This iteration of their license has allowed it to sell and hold XRP, which is the digital asset behind the Ripple Consensus Ledger (RCL). It will enhance Ripple's ability to deal with business customers who want to use its technology for international funds transfers.

Other U.S. regions have also put up similar bills to regulate digital currency and require licensing. California bill AB 1326, would have done that for the region but failed after the Electronic Frontier Foundation (EFF) was able to oppose it. (The EFF is a group based in San Francisco that defends consumer rights and new technology.)

Although New York City was early to regulate, it has been a difficult and dangerous place for blockchain-based companies to operate. NYC has banned some new financial products that were too competitive for traditional institutions, such as interest-bearing crypto accounts that often averaged 8 percent. It also levied a $100 million fine against BlockFi, a leading custodian of crypto accounts, destroying a once-promising fintech company.

Friendly legal structure of Malta

European Union member country Malta has taken drastic and direct steps to embrace blockchain technology. Moving much more quickly than other nations, Malta saw the potential of blockchain and took steps to secure itself as a hub for innovation. Most blockchain startups have faced a hostile environment, so many — including the mega-exchange Binance — have flocked to Malta to set up business.

After the United Kingdom exits the EU, Malta will be one of the few countries left in the EU that has English as an official language. Malta is also governed by continental law and common law, which makes them more favorable to business. This has positioned Malta well to support international blockchain and cryptocurrency-related companies that want to incorporate and have a legal structure.

TECHNICAL STUFF

Malta is a small island that has seen many different ruling regimes. Each established their own rules and some of them have stuck. Malta has a mixed legal framework now that includes Roman law, French law, British law, and their own laws enacted by the Maltese parliament after the 1964 Independence. But they are mostly known for civil or continental law (which has been codified over the years) and common law (which is established through court rulings).

Malta has passed two groundbreaking acts and one bill that have shifted the conversation around legal standing for blockchain companies, offering legal protection and a framework that more accurately governs distributed technology, blockchains, and all the innovation that has grown out of them. Here's a summary of these three pieces of legislation:

- **Virtual Financial Assets Act:** The Virtual Financial Assets Act regulates initial coin offerings (ICOs). The law requires any company raising capital through an ICO to publish a white paper giving a detailed description of the whole project. The ICO must also make the company's financial history public.
- **Malta Digital Innovation Authority Act:** The Malta Digital Innovation Authority Act creates regulatory procedures for cryptocurrency and the blockchain companies. It also establishes a regulatory body called the Malta Digital Innovation Authority (MDIA).
- **Technology Arrangements and Services Bill:** The Technology Arrangements and Services Bill allows blockchain companies and cryptocurrency exchanges to register and be certified by the Malta government.

These new acts and bill have opened Malta to new technology and will possibly be used as an example by other governments that also hope to attract innovation. The greatest benefit is giving companies a safe place to grow and experiment within known parameters.

Securing the World's Borders

Blockchain is being explored by many governments to secure borders. The UK has an ambitious goal of ensuring that travelers never need to break stride as they move through their airports. This is in contrast to the long security lines that are present now at almost every airport. The main hurdles that the UK must overcome for frictionless travel experience have to do with *passenger resolution* (the ability to know definitively any given passenger's identity, even if the passenger is from another country). Passenger resolution has been a problem for countries that are fighting terrorism.

The United States has opened up its technology for passenger resolution under the Global Travel Assessment System (GTAS). It's available for public collaboration on GitHub (`www.github.com/US-CBP/GTAS`).

Computers, cameras, and sensors involved in the noninvasive screening and authentication of passengers all need to be secured to ensure national security. Blockchains, with their underlying immutable properties, are a promising technology for this use case and are being tested now.

The other interesting thing that can be created through blockchains is biographical identities — identities that are built over time. Any data can be linked with a biographical identity, and the privacy and readability of the attributed data can be managed by publishers. Over time, identity is built by adding additional attributes. Attributes can be just about anything, from data off your personal device to instances that your documents were checked at a border crossing. These attributes are published to the individual's chain of identity by certificate authorities or those authorized by certificate authorities.

The Department of Homeland Security and the identity of things

The Department of Homeland Security under the Science and Technology Directorate explored securing IoT devices for the U.S. borders. It has worked with now-defunct Factom, Inc., an Austin, Texas–based blockchain startup to advance the security of digital identity for IoT devices.

Factom created identity logs that capture the ID of a device, who manufactured it, lists of available updates, known security issues, and granted authorities while adding the dimension of time for added security. The goal is to limit would-be hackers' abilities to corrupt the past records for a device, making it harder to spoof.

Passports of the future

ShoCard (`www.shocard.com`) is an application development company that is working with the blockchain company Blockcypher. It has built prototypes that allow you to establish your identity within a secure blockchain environment. ShoCard ID lives on an app on your phone and can be used to share all different kinds of credentials securely.

The new feeder document

You may not have heard of Smartrac, but it's more than likely that you touch a piece of its technology every day. Smartrac is the number-one provider of radio-frequency identification (RFID) tags and other identification chips that live inside of things like passports and ID cards.

One of the largest challenges that countries face while fighting identity fraud is in the authentication of the underlying documents used to build identities. These are things like Social Security cards, birth certificates, and diplomas, which are currently easy and cheap to knock off.

Smartrac has been battling this problem with more and more sophisticated technology. Its latest innovation, dLoc, is a software authentication solution that allows feeder documents to be checked against a blockchain record.

Document data is married to a unique ID of the near-field communication tag (NFC) to create a 32-bit hash value, which is only recognizable by the issuing agency using a private key. The hash value is stored in Smart Cosmos and backed up in a public blockchain. After that has happened, the document with the dLoc sticker can be verified using a desktop reader or a mobile app on an NFC-enabled phone.

What this does is create two amazing things that have never been possible with paper documents:

- An unalterable history of the document, showing its true age and ownership.
- Allowing certificate authorities to sign for the authenticity of a document cryptographically. So, even if the underlying paper used to create documents was stolen, it would not be adequately signed, or if a document was taken after it was issued, it could be marked as a stolen document.

IN THIS CHAPTER

» **Discovering the lean government foundations being built around the world**

» **Getting a head start on improved Internet infrastructure layers for your business and home**

» **Starting to make your own blockchain identity**

» **Monetizing your information through smart contracts**

Chapter 16
Other Industries

It's easy to focus on the most prominent blockchain projects and industry impacts, but blockchain technology has already begun to touch all aspects of society.

In this chapter, I lead you through some of the more interesting and unusual applications of blockchain technology that you may not have suspected. Some of the most exciting transformations will occur within government systems, new trust layers for the Internet, and new industries created by blockchains. Here, you discover the most impressive changes that are taking place now and how these transformations will affect your life and the industry you work in, as well as the governments and agencies that protect you.

Lean Governments

A few small nations have realized that if they are going to compete in a global economy, they have to offer more and do it in a way that does not burden their citizens. In order to compete, they've shifted many of the traditional ideas around what it means to provide citizenship. In a world that is moving from hard borders to very porous ones, where people have the power to choose where they live and what country they call home, these small countries are doing well.

Citizenship is becoming a commodity that can be purchased, with each nation offering different advantages. Countries are moving away from the passive citizenship model, where you're born a citizen of a country, to one where you choose citizenship based on the advantages that that country offers.

Under this new model, citizenship is no longer tied to a physical location. Government can exist without borders or a physical location. Old models see citizenship as a location that can be invaded and overruled by another nation or sources within, such as a revolution.

Blockchain technology and other top-grade innovations are being embraced in these areas — first, because they make it possible and, second, because they help reduce the weight on government by creating more efficient systems that citizens can access quickly anywhere in the world, even if the physical territory is overrun.

Singapore, Estonia, the United Arab Emirates (UAE), and China have all been market leaders in these types of initiatives. The Smart Nation project of Singapore and e-Residency of Estonia are unique systems that strive to reduce the paperwork and wait times of citizens and increase the efficiency of shared resources. The 2020 initiative that Dubai launched will remove all physical documents and replace them with blockchain-backed documents or systems. China's efforts to reduce fraud have changed the dynamics for the blockchain space.

Singapore's Smart Nation project

Smart Nation is Singapore's national effort to create a future of better living for all its citizens and inhabitants. People, businesses, and government are working together. The project spans from digital identity all the way to IoT sensors that optimize public records.

Singapore believes that people empowered by technology can lead more meaningful and fulfilled lives. It's exploiting new technologies, networks, and big data to its fullest and actively seeking innovation through regulator sandboxes and active recruitment and incentivizing innovation by startups.

You can see a depiction of the Smart Nation initiative at `https://goo.gl/EGmF4X`.

Singapore has been able to quickly test and deploy new technology because it has a single layer government. It coordinates policies and efforts across institutions quickly. Smart Nation is an excellent example of this philosophy that new technology trumps politics as usual.

Estonia's e-Residency

Estonia is a small country in the European Union with 1.3 million inhabitants. It has limited resources to meet the needs of its citizens, but through technology, it has been able to exceed the capabilities of many larger nations. Estonia launched digital ID cards for online services and was the first country to offer *e-Residency,* a digital identity, available to anyone in the world interested in operating a business online.

Signing up for an Estonia e-Residency takes a few minutes, and the background check costs about $100. Having an e-Residency card does not make you a citizen of Estonia, but it does give you a lot of benefits.

TIP

You can also become an Estonia e-Resident. Apply online at `www.e-resident.gov.ee/become-an-e-resident/`.

After it exited the Soviet Union, Estonia invested heavily in new technology. It shifted completely away from traditional government to one where it utilizes a *single-window principle* (one point of access for citizens). The single-window principle enables access to all tax and customs services for citizens with a single secure log-in anywhere in the world. Straightforward and paper-free transactions are made possible through this system. Everything, except marriage and real estate purchases, can be done completely online. Estonian citizens can make bank transfers or pay tax in a few minutes.

The Estonian people have come to expect their government to simplify and use more IT solutions. The active development of e-services has reduced the number of visits to the Estonian Tax and Customs Board service bureaus by more than 60 percent between 2009 and 2016, lowering the overall cost.

Estonia upgraded its income and social tax returns environment in 2015 and collected €125 million more in value-added tax (VAT) than the previous year due to the development and extensive usage of e-services. The Estonian government added a tax liability calculator that pulls data from incorporated banking systems of citizens. It also made it easy to submit invoices to the system.

The Estonians have embraced blockchain technologies. The next big development will be a blockchain-enabled cloud. Estonia has hired Ericsson, Apcera, and Guardtime to jointly develop and operate a hybrid cloud platform that will enhance the scalability, resilience, and data security of tax reporting and online health-care advice.

Nasdaq is developing blockchain services in Estonia as well. It's building a market for private companies that keeps track of the shares they issue and enables them to settle transactions immediately. It's focused on improving the proxy voting process for enterprises. It will be a way to register your business.

The Bitnation project is collaborating with Estonia to offer a public notary to Estonian e-Residents, which will allow Estonia's e-Residents, regardless of where they live or do business, to notarize their marriages, birth certificates, and business contracts on a blockchain. Blockchain notarized documents aren't legally binding in the Estonian jurisdiction, or in any other nation or state, but it will allow citizens to prove the age of these documents.

Better notarization in China

China has a love–hate relationship with cryptocurrency. On the one hand, Chinese citizens have been trying to use tokens as a means to launder money out of the country or hide profits from taxation. This has caused the Chinese government to tighten regulation around the use of cryptocurrencies. However, as the usefulness of the underlying blockchain technology has expanded beyond the movement of value, China has begun to embrace blockchain technology.

An interesting example of its early use was by Ancun Zhengxin Co., which is leading the shift to electronic data notarization services in China through partnerships with more than 100 traditional notarial offices in 28 provinces. It's also offering electronic data storage and blockchain notarization solution through traditional offices.

Ancun publishes thousands of records in a publicly searchable blockchain that allow users to go back and check the authenticity and age of notarized documents.

TIP

Many startups are working on similar concepts in the United States. For example, WordProof (`https://wordproof.com`) lets you hash and timestamp dates on your website.

The Trust Layer for the Internet

Over the last 30 years, the Internet has been built in layers — one layer on top of the next — making it easier and safer for the those using it. The blockchain is the next layer of the Internet. Think of it as the trust layer. It will likely fade quietly out of the public's consciousness and just start making your online interactions more pleasant. The implementation of blockchain technology will eventually do away with irritating problems that commonly occur online because there aren't sufficient ways to trust information.

There are two key areas where work has begun that you may not be aware of but will love: email with little to no spam and a new kind of identity online.

Web 3.0 email

Mailchain (`https://mailchain.com`) is a new blockchain-based email platform that allows you to send fully encrypted messages to other Mailchain accounts and to ETH and NEAR wallet holders. Mailchain gives you complete ownership of your data and is working to make the Internet a little more private. (Unencrypted email is a major vulnerability.)

All Mailchain messages are encrypted end-to-end by default. Your private keys used to encrypt your messages are never revealed to the Mailchain protocol. Your secret recovery phrase is used to create a series of private keys, each of which perform independent actions that allow you to register addresses and authenticate, store, and save messages privately.

The Mailchain application encrypts your data from within your web browser. The encrypted files are then stored in Mailchain. Only you can decrypt these files via your private keys. Mailchain can't decrypt your secret recovery phrase, messages, or registered addresses.

Mailchain uses a messaging key in place of your wallet key to encrypt and decrypt messages for each address. Messaging keys are more secure for encryption and mean you don't expose your wallet's private key.

When you register a wallet address with your Mailchain account, a new messaging key is created. With your wallet, you sign a confirmation to indicate that this key should be used for messaging. Signing this confirmation creates proof that users can independently verify. You only know the private key for messaging.

Registered addresses are encrypted before being stored, and you only need to verify ownership of your wallet address once. Mailchain disconnects your wallet after your wallet has created the proof. Your wallet private key is never exposed.

Each time an email is sent, a new encryption key is created to encrypt the message and its location. The encryption key is then uniquely encrypted for each address receiving the message. A new key is created for each recipient and for each new message. This is important to ensure that only the intended recipient reads the message's contents.

When a message is sent, the message is encrypted and stored on distributed storage. An encrypted "delivery request" holds information for the message recipient to be able to collect their encrypted message. Your messages are held on what is called an *ephemeral transport layer,* which is temporary and only exists until your message has been retrieved or your email expires.

When you receive a new message, it's saved in your private inbox. Before being stored, your new email is re-encrypted with a key that is specific to your inbox.

Your inbox is also secured via a private key. All IDs, filters, and metadata are encrypted. Mailchain can't identify relationships even if multiple addresses received the same messages.

If this looks like an interesting secure email option, navigate to `https://mailchain.com` to claim your free email account.

REMEMBER

No single Internet security solution is perfect. There are ways to view your data (for example, by using Pegasus spyware) even if you send fully encrypted messages. Developed by the Israeli cyber-arms company NSO Group, Pegasus is covertly installed on all types of devices running iOS and Android. It uses a *zero-click* attack that exploits existing loopholes in data verification. Pegasus is capable of reading text messages, tracking calls, collecting passwords, tracking your location, accessing your device's microphone and camera, and harvesting information from other apps.

Owning your identity in web3

The World Wide Web Consortium (W3C) is a nonprofit organization established in 2012 that helps develop protocols and guidelines that ensure the long-term growth of the web. The W3C developed the Modern Paradigm for Standards, which is intended to help radically improve the way people around the world develop new technologies and innovate for humanity.

An important initiative has been decentralized identifiers (DIDs). DIDs, also known as self-sovereign identity, are a new type of globally unique identifier. Driven by the flaws of centrally issued identity, these new self-issued IDs allow you to control your identity using digital signatures that use cryptographic proofs.

Most unique identifiers, or models of identity (such as your Social Security number), are not under your control. External authorities such as governments issue your IDs and decide what they mean. They're valid only in specific contexts and recognized by certain organizations. They may disappear or cease to be valid at any time. These IDs often reveal personal information about you that is not necessary. IDs are also fraudulently replicated by malicious third parties — all without your consent.

Because the generation and assertion of DIDs is entity-controlled by you, you can have as many DIDs as necessary to maintain the separation of personas and interactions online. One of the fundamental tenets that blockchain enthusiasts talk about is the personal responsibility of owning the data that you create and that identifies you uniquely. This concept may seem straightforward, but most people don't own or control the data that represents their identities.

Most of the control is held by centralized databases that are vulnerable to hacking. These databases hold the information, and certificate authorities validate that the information is correct and unaltered. In the information age, your data is your identity. The more distributed the data is, the greater the likelihood that it will fall into the hands of those who want to misuse it.

Blockchain-based identity places control of identity in the hands of the individuals or corporations that the identity represents. Central databases and certificate authorities aren't necessarily replaced. Data still needs a secure home, and it still makes sense to have third parties validate the authenticity of documents.

The value in changing the order of responsibility around identity is that it becomes harder to steal, hold hostage, or manipulate the underlying documents that represent your identity. Information is shared as needed without exposing unnecessary information. An irrevocable and globally accessible identity may not always be a good thing. Those building identity platforms will need to be mindful of consumer protection such as credit forgiveness, the right to be forgotten, and voter anonymity.

Oracle of the Blockchain

Blockchain technology doesn't solve for the problem that information must come from somewhere. It's also important that the information can be relied on. It's the human element that can't yet be removed from the equation when you want to act on a contract within a blockchain system.

There is no central authority to police or enforce honesty in a blockchain system. Predicting the future honesty of authors of information is impossible. The logical conclusion is that each transaction must cost less than the cost to rebuild reputation. The reputations of trusted authors are built over time, and the longer an author is honest and correct, the more valuable the author's reputation becomes. This concept is similar to the value of a name brand.

In this section, I explain how artists and creatives are using blockchain technology to monetize their work through blockchain technology.

Trusted authorship

Smart contracts and chaincodes have created a new opportunity for knowledgeable individuals and corporations to monetize their information. These types of systems need trusted sources of information to execute against. These trusted sources could be rating agencies, weather outlets, or just about anything else.

You could also connect IoT devices to a blockchain infrastructure and have them create their own voices and identities on a blockchain network. They need to build trust over time and can still be corrupted at any given point. Past honesty doesn't prevent future dishonesty or the corruption of a source of information.

Not all smart contracts or chaincodes are self-contained or execute against infallible sources. The more practical and applicable business use case requires information to be derived from sources outside the known universe of any given blockchain network. Several startups are attacking this problem from different angles.

OpenSea is a startup that is building a decentralized protocol for content ownership, discovery, and monetization. It does this via an NFT marketplace. Its system is designed to record and timestamp metadata and ownership information about creative assets, such as writing and music.

Factom has created Acolyte, a service that allows users to build a reputation over time for the information they provide to the network. Smart contract builders can subscribe and compensate oracles that are created. They can also rate them for their trustworthiness.

From a dramatically different angle, Augur, another blockchain startup, has pioneered the idea of prediction markets. Augur is a platform that rewards users for predicting future real-world events such as election or corporate buyouts. The bets are made by trading virtual shares in the outcome of events. Users make money by buying shares in the correct outcomes. The cost of the shares fluctuates based on how the community feels about the likelihood of the event acutely happening. Augur is similar to a betting website. Anyone can make a prediction. Anyone can create a prediction market for any given event. This would allow you as a business owner, for example, to take a poll on what people think is most likely to occur. It may also uncover inside information that authors would like to be able to capitalize on.

Intellectual property rights

One of the hardest-hit industries that is struggling with intellectual property rights is the music industry. Artists at the top are squeezed out economically by the many intermediaries that rely on their creative work. Small artists can't make music a primary source of income because they only see a small fraction of the revenue. Mega-stars make it on the sheer volume of fans.

The Internet has made it easier for artists of all sizes to share their work. At the same time, it has made it even harder for people to make a comfortable living doing what they love. The music industry food chain is long, and each intermediary takes a small piece of the pie and adds to the length of time that it takes for funds to finally reach the artist. Often, the artist will wait up to 18 months or more to see any money and may only get $0.000035 per instance of her music being streamed. This situation is a best-case scenario in our current market, with no one defrauding the artist.

Blockchain has been introduced as a way to help lighten the massive financial burden on creatives. Cryptocurrency could be used to reduce transaction fees associated with credit cards and fraud. It would also open up new markets in developing countries that don't have regular access to credit cards.

An even more interesting but less straightforward possibility would be migrating the whole music industry ecosystem onto a blockchain system that utilized smart contracts or chaincode to facilitate immediate payment for utilization. It could also clarify ownership of licenses and make it easier for consumers to license music for commercial use.

Several projects are working on this issue and looking to promote a healthy, sustainable, and frictionless ecosystem — one that does not displace market player but does allow artists to gain a bit more from their hard work.

UjoMusic is beta testing its platform that lets users sell and license music directly. It utilizes the Ethereum network, smart contracts for execution, and Ether (the Ethereum cryptocurrency) for payment. You can download a whole song or just the vocal and instrumental stems for commercial or noncommercial use. The musicians are then paid immediately with Ether.

Peertracks is an early blockchain startup that's working on changing the music industry. It's a music streaming website that allows users to download and discover new artists. It does this through its peer-to-peer network called MUSE and the creation of individual artist tokens. These tokens work like other cryptocurrency and fluctuate in value depending on the popularity of the artist. Since 2020 however there has been a proliferation of platforms that let you discover artists including OpenSea, SuperRare, Nifty Gateway, and Mintable just to name a few. Artists themselves have also gotten into the game, Snoop Dogg launching his own NFTs on MakersPlace.

Blockchain technology doesn't remove the need for music labels and distributors. However, they'll need to act quickly if they don't want to be displaced by new companies that adapt this more efficient model, just as Netflix disrupted Blockbuster.

5

The Part of Tens

IN THIS PART . . .

Discover ten free blockchain resources that will help you stay up to speed on the technology and the industry.

Identify ten rules to never break while working within the cryptocurrency and blockchain world.

Find out more on the top ten metaverse blockchain projects and organizations that are shaping the future of the industry.

IN THIS CHAPTER

- » Discovering free blockchain education resources
- » Getting involved in the blockchain community
- » Staying up to date on the latest blockchain news
- » Deepening your knowledge of other blockchain resources

Chapter 17
Ten (or So) Free Blockchain Resources

In this chapter, I outline interesting free resources across the blockchain ecosystem that will help you stay informed and get involved in the community. Here, you can find free tools for making *oracles* (the data feeds that allow smart contracts to execute), videos that will expand your knowledge, and organizations that are shaping the future of the industry.

Ethereum

Ethereum is an open-source crowdfunded project that built the Ethereum blockchains. It's one of the most important projects in the space because it has pioneered building a programing language within a blockchain. Due to its built-in programing language, the Ethereum network allows you to create smart contracts, create decentralized organizations, and deploy decentralized applications.

Ethereum 101 (`www.ethereum.org`) is a website started by the members of the Ethereum community. It's a curated repository for high-quality educational content about blockchain technology and the Ethereum network. Anthony D'Onofrio, Ethereum's Director of Community, oversees the project.

Got Minted

If you're new to nonfungible tokens (NFTs) and you're looking for an easy, hassle-free way to set up your wallet and start collecting unique digital assets, look no further than Got Minted. In five simple steps, the site walks you through creating your wallet, minting your first NFT, connecting your wallet to OpenSea, and exploring NFTs on the marketplace. You'll be ready to experience the exciting world of NFTs in about ten minutes. Whether you want to collect, you're a gamer, or you're just curious about this emerging digital trend, Got Minted makes it easy to get started with NFTs by simplifying the setup. Head to `https://gotminted.com` to get started.

Blockchain University

Blockchain University is an educational website that teaches developers, managers, and entrepreneurs about the blockchain ecosystem. It offers public and private training programs, hackathons, and demo events. Its programs are solution-oriented design thinking and hands-on experiential training. You can find Blockchain University in Mountain View, California, or at `https://theblockchainu.com` and `https://dlt.education`.

Bitcoin Core

Bitcoin Core (`https://bitcoin.org`) was originally used by Satoshi Nakamoto to host his whitepaper on Bitcoin protocol. It's home to educational material on Bitcoin core protocol and downloadable versions of the original Bitcoin software.

The site is dedicated to keeping Bitcoin decentralized and accessible to the average person.

REMEMBER

It's a community-run project, and not all the content is managed by the core team. Keep this in mind while perusing the site.

Blockchain Alliance

The Blockchain Alliance was founded by the Blockchain Chamber of Digital Commerce and the news organization Coincenter. It's a public-private collaboration by the blockchain community, law enforcement, and regulators. They share a common goal to make the blockchain ecosystem more secure and to promote further development of technology. They do this by combating criminal activity on the blockchain by providing education, technical assistance, and periodic informational sessions regarding Bitcoin and other digital currencies and those utilizing blockchain technology.

You can learn more about their events or join their organization at `www.blockchainalliance.org`.

Multichain Blog

Multichain is a company that helps organizations rapidly build applications on blockchains. They offer a platform that can issue millions of assets on a private blockchain and you can also track and verify activity on your network through their tools. Beyond their toolset and platform, they've been thought leaders in the blockchain space.

These are my favorite posts from their blog (`www.multichain.com/blog`):

- Four genuine blockchain use cases (`www.multichain.com/blog/2016/05/four-genuine-blockchain-use-cases/`)
- Beware the impossible smart contract (`www.multichain.com/blog/2016/04/beware-impossible-smart-contract/`)
- Smart contracts and the DAO implosion (`www.multichain.com/blog/2016/06/smart-contracts-the-dao-implosion/`)
- Understanding zero knowledge blockchains (`www.multichain.com/blog/2016/11/understanding-zero-knowledge-blockchains/`)

HiveMind

Paul Sztorc founded Truthcoin, a peer-to-peer oracle system and prediction marketplace for Bitcoin. It utilizes a proof-of-work sidechain that stores data on the state of prediction markets. Bitcoin can support financial derivatives and smart contracts through HiveMind, the platform developed out of the Truthcoin whitepaper. Check out their resources and education materials at `http://bitcoinhivemind.com`.

Smith + Crown

Smith + Crown is a blockchain research organization focusing on global trends, industry intelligence, and blockchain systems structure. They've created research tools to expand blockchain companies. Smith + Crown looks for impact, application, and accessibility. They've made most of their research publicly available and free of charge. You can take advantage of the research tools, countless reports, and databases of all noteworthy projects in the blockchain space. Smith + Crown are the researchers and advisors to several prominent blockchains and cryptocurrency advocacy groups, such as the Chamber for Digital Commerce, the Token Alliance, and Social Alpha. Check them out at `https://www.smithandcrown.com`.

Unchained and Unconfirmed Podcasts

The *Unchained* and *Unconfirmed* podcasts are amazing and up-to-date interviews with top industry folks in the blockchain and cryptocurrency space. *Unchained* is a weekly, hour-long podcast by Laura Shin, a former senior editor of *Forbes* and the first mainstream reporter to cover crypto assets full-time. Shin does impressive and well-thought-out deep dives into the people and companies building the decentralized Internet. She can help you get a better understanding of regulation, security, and privacy issues that are inherent in blockchain technology. You can listen to her podcast at `https://unchainedpodcast.com`.

Here are a few good episodes to listen to:

- **Ledger on How Consumers and Institutions Should Be Safeguarding Their Private Keys:** `https://unchainedpodcast.com/ledger-on-how-consumers-and-institutions-should-be-safeguarding-their-private-keys-ep-101/`

- **How Donating Crypto Can Help You Save on Taxes:** https://unchainedpodcast.com/how-donating-crypto-can-help-you-save-on-taxes-ep-94/
- **Naval Ravikant On How Crypto Is Squeezing VCs, Hindering Regulators, and Bringing Users Choice:** https://unchainedpodcast.com/naval-ravikant-on-how-crypto-is-squeezing-vcs-hindering-regulators-and-bringing-users-choice/
- **How Binance Became the Most Popular Crypto Exchange in 5 Months:** https://unchainedpodcast.com/how-binance-became-the-most-popular-crypto-exchange-in-5-months-ep-84/

IN THIS CHAPTER

- Discovering your legal vulnerabilities
- Understanding the technical shortcomings of blockchains
- Identifying thieves best points of attack on your systems
- Developing your security best practices

Chapter 18
Ten Rules to Never Break on the Blockchain

In this chapter, I dig into the things you should take into account while working with blockchain technology and the cryptocurrencies that run them.

REMEMBER

Always consult your CPA and attorney before making financial decisions. This technology is new, and the rules that govern it are not fully developed.

Don't Use Cryptocurrency or Blockchains to Skirt the Law

The legality and the legal zoning of cryptocurrencies are still fluctuating in many places of the world. I'm not kidding when I tell you to talk to your CPA and your attorney. It will be money well spent and will keep you out of trouble.

Here are three very silly questions that I get asked frighteningly often:

- **Can I use cryptocurrency as a way to hide money?** This idea is a dangerous one. ***Remember:*** Blockchains keep records of all transactions forever, so even if you think you came up with a clever way to hide some tokens, those looking for bad behavior have time to find it.
- **Can I use blockchains as a way to smuggle money out of my country?** Many countries have limitations on the funds citizens can take out of the country. You don't want to do this for the same reason as I just mentioned: Blockchains keep records of all transactions forever.
- **Can I use cryptocurrency to buy illicit goods?** The answer is — you guessed it — no! Blockchains keep a trail of your actions *forever!* Even law enforcement that stole Bitcoin from the infamous Silk Road marketplace got caught.

REMEMBER

Don't do anything with cryptocurrency and blockchains that would be illegal to do with real money.

Keep Your Contracts as Simple as Possible

Decentralized autonomous organizations (DAOs), smart contracts, and chaincode are all the rage at the moment. The promise of cutting administration and legal cost is very enticing to many corporations. A sometimes overlooked characteristic of this technology is that it is just code. That means that there is no human being interpreting the rules that you've laid out for everyone to follow. The code becomes law, and the law only stretches to what is incorporated into the blockchain contract. The "fat" that was cut can sometimes be very important.

There is no one to interpret the code. That means that if the code is executed in a fashion that you did not expect, there is also no one to enforce the intent of the contract. The code is law and nothing unlawful occurred. That's why you should keep your contracts simple and modular in nature to contain and predict the outcomes of contract fulfillment. It's also a good idea to have your contract tested and beaten up even by other developers who are incentivized to break it.

The reach of the blockchain you're building your project on matters, too. You can think of it like jurisdictions. Sure, a smart contract can execute on outside data, but the smart contract cannot demand funds from accounts that they do not have access to. That means that all the value must be set aside in some manner, which may encumber cash flow.

Another thing to think about is the source of information that your contract uses to execute against. If it's weather data for an insurance contract, do you trust and agree on the source? Is it possible to manipulate the source data? A lot of thought should go into the oracle source before implementation. When building a smart contract keep in mind that your data channels may be dynamic. For example, APIs are updated frequently, and if your contract is calling one that has changed it may break your smart contract.

Publish with Great Caution

The whole point of blockchains is that once data is put in, it's hard to take it out. That means that what you put in will be around for a long time. If you publish encrypted sensitive information, you need to be okay with the fact that the encrypted data may one day be broken and what you published may be readable to anyone.

TIP

Think about this before you publish:

- Would I be comfortable with this information being decrypted at some point?
- Am I comfortable sharing this information for all eternity with anyone who wants to review it?
- Is this data harmful to a third party and something that I could be liable for if published?

There is work being done in cryptography to make quantum proof encryption, but because both quantum computing and quantum proof encryption are still in the testing phase, it's difficult to say what the technology will be capable of 20 years from now.

Back Up, Back Up, Back Up Your Private Keys

REMEMBER

Blockchains are very unforgiving creatures. They don't care if you lost your private keys or passwords. Many a crypto nerd has been laid bare and given up countless tokens to the great blockchain oceans — treasure that will never be recovered.

The private keys that control your cryptocurrency often live inside your wallets, so it's important to protect and secure them. Be careful with online services that store your money for you. Many cryptocurrency exchanges and online wallets have had their funds stolen. Also, taking a screenshot or image and storing it on the cloud is the same thing as sending yourself an email. Whatever you do, do *not* do this. It will compromise your keys. You should make a plan so your loved ones can access your keys should something happen to you. A healthy 30-year-old CEO of a cryptocurrency exchange died and locked up $190 million worth of assets because he did not have a succession plan. Also, don't overlook Bluetooth connectivity as a hidden door to your cold storage. Make sure your device is completely inaccessible from the Internet.

TIP

Only store small amounts of tokens for everyday use online or in an Internet-accessible device. Think of cryptocurrency wallets like your cash wallet. Don't keep more money in it than you're willing to lose at any given time. More than a hundred known malware applications are looking to get ahold of your private keys and steal your tokens.

Keep the rest of your currency in *cold storage* — completely offline with zero access to the Internet. This could be in a paper wallet, on a computer that can't access the Internet, or in a unique hardware device built for securing cryptocurrency.

If you choose to use a paper wallet to secure your cryptocurrency, laminate it and make copies. Also keep in mind that printers often have access to the Internet and their data can be retrieved by third parties. The truly paranoid only use printers that have no access to the web. Keep your paper wallet copies in different locations such as a bank vault and a secure location in your home.

REMEMBER

Back up your digital wallets and store them in a safe place. A backup is in case your computer fails, or you make a mistake and delete the wrong file. The backup will allow you to recover your wallet in case your device was corrupted or stolen. Also, don't forget to encrypt your wallet. Encrypting your wallet allows you to set a password for withdrawing tokens.

WARNING

Encryption is a helpful measure to protect you against thieves, but it can't shield you against keylogging software. Always use a secure password that contains letters, numbers, punctuation marks, and is at least 16 characters long. The most secure passwords are those generated by programs designed specifically for that purpose. Strong passwords are harder to remember. You might consider writing down your password and laminating it like your private keys. There are limited password recovery options within cryptocurrency, and a forgotten password could mean lost tokens.

TOOLS TO KEEP YOUR TOKENS SAFE

You might consider using the BitGo wallet to secure your Bitcoin. Although it is an online wallet, BitGo requires both an online and offline signature to move your tokens. Because of this functionality, it's more secure than your standard online wallet.

BitGo wallets use three keys. They hold one, you hold one, and the other is held on your behalf by a third-party key recovery service (KRS). Two signatures are required on every transaction. Usually this is done by BitGo and you, unless you lose one of your keys; in that case, the KRS will help out. The BitGo wallet is not free — they require a small fee per transaction.

Check out the BitGo wallet at `www.bitgo.com/wallet`.

Triple-Check the Address Before Sending Currency

Cryptocurrency has attracted a fair number of scoundrels, so be careful when you send money. As soon as the money is out of your wallet, it's gone forever, and there is no way to get it back. There are no chargebacks and you can't call customer support. Your money is gone.

Triple-check the wallet address before sending. You want to make sure you're sending it to the right address. Also double-check the address even if you copy and paste it. There is malicious software out there that can swap your addresses for Ctrl+C/Ctrl+V commands.

Take Care When Using Exchanges

Cryptocurrency exchanges are central points that hackers like to target to steal tokens. They're seen as pots of gold just ripe for the picking, and more than 150 of them have been compromised.

Keep this in mind while using exchanges, and follow the best practices laid out in this book to keep your tokens safe. Do a little research on the exchange you're using to see what security measures it has in place.

Two-factor authentication is critical. You may also consider setting up a secret phrase with your telecom provider to help prevent social engineering. You don't want to be the victim of a SIM card swap. Your phone number doesn't have to be your backup; Google and several other companies also offer a two-factor authentication option (check out the Google Authenticator app).

Finally, just use exchanges to move your funds in and out. Don't use the exchange as a place to store value. Instead, hold significant amounts of crypto in cold storage or in a laminated paper wallet with several copies.

Beware Wi-Fi

If your router wasn't set up correctly, it's possible for someone to see a log of all your activity. Also, when you're on an unsecured or public portal, you may also be exposed to malware. You must assume that the owner of the network can see your activity.

WARNING

Only use trusted Wi-Fi networks and make sure you've changed the password on your router to something as secure as a password. Most Wi-Fi router passwords are set to a factory default of "admin" and can easily be taken over by a third party.

Identify Your Blockchain Dev

Blockchain technology is new, and there just aren't that many people who have a lot of experience when it comes to building blockchain applications.

If you're thinking about hiring a developer to help you with a project, check out her GitHub and see what work she's done before you get started. She may not need to be experienced with blockchain specifically, but if she isn't, she should be a very experienced developer outside of the blockchain world.

There aren't many resources out there yet to help developers when they get stuck. Inexperienced developers may struggle, and at this point most are inexperienced and will take longer to develop your application.

Don’t Get Suckered

The blockchain industry as a whole does not have the same protection and security measures that banks and other financial institutions have, and there are not the same laws for your protection and financial welfare. There is no consumer protection and no FDIC bank insurance of funds from the government. If you get robbed or conned, you may not be able to turn to anyone for help.

Also, the industry has had a lot of hype in the last few years without much delivery of things of real value. The year 2016 saw over a thousand new blockchain companies pop up overnight claiming expertise. When you’re looking at developing a project and trying to decide if it’s worth the investment, it’s always a good idea to take a minute and make sure it even makes sense. Ask yourself the following questions:

- Is there real value generated?
- Is the value created in the way that benefits you?
- Why hasn’t it been done already?
- Are there other more tested technologies that could be used to accomplish the same thing with the same efficiency or better?

Blockchain technology holds a lot of promise and power and, as such, should be approached thoughtfully and carefully.

Don’t Trade Tokens Unless You Know What You’re Doing

Cryptocurrencies are very volatile and will swing wildly in value at any given time and sometimes for no discernable reason. Many of the cryptocurrencies have little depth, and trading large amounts can crash the market value. Working with public blockchains means that you’ll likely need to hold some amount of the currency to utilize them.

Don’t get caught up in trading the tokens unless you take the time to understand the market well. A good rule of thumb is if you haven’t traded traditional assets like stock before, be sure to take extra time to understand cryptocurrency. You need to dive just as deep into it as you would to learn about the stock market before you get started. Consider reading *Cryptocurrency Investing For Dummies* by Kiana Danial (Wiley). If you do choose to trade the tokens and cryptocurrencies, don’t forget to report this activity to your accountant. You may need to report your gains or losses on your income tax return.

IN THIS CHAPTER

- Diving into novel metaverse worlds
- Uncovering immersive virtual education environments
- Discovering new virtual shopping malls

Chapter 19

Ten Top Metaverse Projects

New metaverse projects that are based on blockchain technology are emerging every day. Entrepreneurs have seen opportunities to capitalize on the very powerful tools blockchains offer to move money faster, secure computer systems, and build digital identities. They've combined these technologies with immersive 3D environments that allow you to explore and create whole new worlds.

In this chapter, I introduce you to some of my favorite metaverse projects that incorporate fun token economics, such as earn-to-play and voting. You also discover the world of virtual education and shopping malls.

After reading this chapter, you'll have an idea of some of the amazing things happening within the metaverse and know just where to start your next project. You may even make new friends online in one of these virtual worlds!

Decentraland

Decentraland is a decentralized virtual reality (VR) platform that allows users to fully control their experiences. It is powered by nonfungible tokens (NFTs), which enable users to access and trade unique digital assets that can be customized to meet their needs.

On Decentraland, users can create, experience, and monetize their own content. The platform is divided into parcels called LAND, which are 3D nonfungible digital assets that are maintained through an Ethereum smart contract. These parcels are identified by their coordinates (*x*, *y*) and are owned by members of the Decentraland ecosystem.

Ownership of these virtual properties is secured through the use of the cryptocurrency token MANA, which gives users full control over their LAND the way a title would for a physical property. Decentraland allows users to explore a variety of virtual worlds and scenes created by artists on different parcels of LAND. If you're interested in exploring Decentraland, you can navigate to `https://decentraland.org` to start your journey.

The Sandbox

The Sandbox is a virtual world that allows players to build and monetize their gaming experiences through the use of NFTs on the Ethereum blockchain. It's made up of three integrated products:

- **VoxEdit,** a 3D modeling and NFT creation software that allows users to create and animate 3D objects
- **The Marketplace,** where users can upload, publish, and sell their NFT creations
- **The Game Maker,** which allows users to build 3D games without coding using visual scripting tools

The Sandbox uses several types of tokens to facilitate transactions and interactions within the platform. SAND is the ERC-20 token used as the basis for all transactions and interactions within the Sandbox. LAND is a unique NFT representing a digital piece of real estate in the Sandbox metaverse that players can buy to build interactive experiences. ASSETS are NFTs created by players that can be traded on the marketplace and used as creation elements in the Game Maker. They utilize the ERC-1155 standard.

The Sandbox is based on the Ethereum blockchain and uses smart contracts to provide copyright ownership for user-generated content. It aims to disrupt existing game makers like Minecraft and Roblox by providing creators with full ownership and control of their creations and rewarding them for their participation in the ecosystem. The Sandbox has a large community of creators, having generated 40 million downloads across iOS and Android with its two mobile hits, The Sandbox (2011) and The Sandbox Evolution (2016). You can start making your own games by navigating to `www.sandbox.game`.

Axie Infinity

Axie Infinity is a fun new virtual world full of fierce and adorable pets called Axies. The gameplay is similar to the popular Pokémon Go mobile game. In this exciting new digital landscape, you can battle your Axies against other players, harnessing their unique abilities. You also earn cryptocurrency through your gameplay.

If you're ready for a truly immersive gaming experience that combines blockchain technology with cute avatars in a dynamic virtual world, hop online and download Axie Infinity at `https://axieinfinity.com`.

MetaStreet

MetaStreet is a decentralized interest rate protocol for the metaverse. It was built to grow the gross domestic product (GDP) of emerging virtual economies within the metaverse. The MainStreet protocol does this through a variety of algorithmic capital vaults that generate diversified yield through automatic underwriting, aggregation, and the execution of NFT-backed notes.

In decentralized finance (DeFi), you can think of vaults as pools of funds with an associated strategy to maximize returns for their investors. The capital vault enables secondary market liquidity for NFT-backed notes. Liquidity is important in creating market stability. Vaults are becoming attractive to investors because they can earn yield by investing capital into diversified portfolios of NFT-backed notes.

MetaStreet also offers education to investors to help them learn how to invest in these new types of new assets. You can discover more about MetaStreet by navigating to `https://metastreet.xyz`.

Enjin Coin

Enjin has had its ups and down with the NFT bubble of 2022. It built a multiverse of digital activities such as Enjin-powered games that let you earn NFTs. It also allows users to trade NFTs and build NFT-based games.

Enjin is also the first NFT company to be accepted into the UN Global Compact Membership. The Global Compact requires companies to align their business models with the ten principles derived from UN declarations on human rights, labor, the environment, and anti-corruption.

Enjin has also created JumpNet, a blockchain bridge that enables it to claim to be a carbon-negative blockchain system. JumpNet also lets Enjin remove gas fees for its users and reduce the cost of running its NFT smart contracts. You can find out more at `https://enjin.io`.

Metahero

Metahero is a platform that lets you create lifelike 3D avatars and virtual objects for gaming, VR platforms, social media, and fashion. It combines 3D technology with a marketplace and a token ecosystem. Metahero is also converting real-world art into ultra-high-definition NFTs, permanently preserving the art in digital form. Wolf Studio, a global leader in 3D scanning, is supporting these efforts.

The Metahero token, HERO, can be purchased with Binance Coin (BNB) on decentralized exchanges. Metahero is run on top of the Binance smart chain, a parallel smart chain running smart contracts on the Binance Exchange.

Interestingly the HERO token is a deflationary asset. The total circulating supply is reduced by burning up to 2 percent of each transaction. *Burning* is when tokens are sent to a wallet with no private key, in effect destroying them forever.

You can get started creating your meta world by navigating to `https://metahero.io`.

Star Atlas

Star Atlas is an immersive space-themed role-playing game. It uses real-time graphics technology on the Unreal Engine 5. It allows Star Atlas to have cinematic-quality video-game visuals.

Star Atlas has also integrated blockchain technology using the Solana protocol. It claims to run on a largely serverless infrastructure. Utilizing Solana's high throughput of 50,000 transactions per second enables gameplay interactions between assets to be recorded in real time and bypasses the need for a robust traditional server backend for online multiplayer games.

Start Atlas also incorporates NFTs obtained and traded within the game. Its economy mimics the tangibility of real-world assets and ownership. If you enjoy role-playing games and want to earn to play, you can get started by navigating to `https://staratlas.com`.

Bloktopia

The Bloktopia Metaverse is a 21-level virtual skyscraper that was developed in the Unity Engine. The 21 levels symbolize the 21 million Bitcoin that will be minted. Bloktopia has a lot of educational material and allows you to quickly get up to speed on new information about cryptocurrencies and NFTs.

Industry experts contribute educational materials on revenue models, playing games with friends, building networks, and taking advantage of other ways to get started in the metaverse.

Bloktopia allows crypto projects, exchanges, and influencers to showcase their content. The virtual skyscraper includes more than 200 virtual stores, an auditorium for live talks and seminars, a gaming floor, and virtual event spaces.

You can unlock multiple streams of passive and active income, access educational and learning tools about crypto, and participate in virtual events and gatherings within this virtual venue. To explore this new space, navigate to `www.bloktopia.com`.

Highstreet

The Highstreet world is a play-and-earn open-world metaverse. It incorporates shopping, gaming, and NFTs. The game has been able to attract traditional and new crypto brands to help support its massively multiplayer online role-playing game (MMORPG).

You can play to earn by completing quests, attending social events, socializing with players, and shopping for NFTs from real-world brands. This adds a fun element so that it doesn't just feel like a virtual mall for digital assets.

Highstreet also incorporates the HIGH token, a native utility and governance token for the Highstreet game. HIGH tokens are required to access some areas of the game and some special events. HIGH tokens can also be used to buy virtual real estate and products in the Highstreet Marketplace. HIGH token holders also vote on governance proposals to determine future features of Highstreet, with voting weight calculated in proportion to the number of tokens you have staked.

If you're interested in role-playing games, check out Highstreet by navigating to `www.highstreet.market`.

Voxels

Voxels is an Ethereum-based metaverse platform. The Voxels virtual world includes real-life infrastructure such as roads, land, and buildings. Like many other metaverse crypto games, you can buy virtual land, build on it, customize your avatar with wearable NFTs, and explore the open world.

Voxels is one of the most accessible virtual worlds to get started and build in. You can begin building by dragging and dropping blocks in real time. You don't need special equipment or software — only your favorite web browser.

The central city in Voxels is called Origin City, and it's where you begin playing the game. The original map of Origin City comprised 3,026 purchasable land parcels in a wide range of shapes and sizes. Now the game includes expansion and islands.

If you're ready to start, you can drop into Origin City right now by navigating to `www.voxels.com/play`.

Index

About the Author

Tiana Laurence is an author, investor, technologist, and teacher. She is passionate about ensuring that women have a voice in the future of technology. Tiana cofounded the first enterprise blockchain company that built data integrity software for the Department of Homeland Security and identity software for the Gates Foundation. She has spoken at the National Institute for Science and Technology, the Federal Reserve, the World Economic Forum, and numerous banks, insurance companies, and Fortune 500 companies about the impact of blockchain technology, Central Bank Digital Currency (CBDC), Web 3.0 marketing innovations, and tokenized assets. She is also the author of *NFTs For Dummies* (Wiley) and *Introduction to Blockchain Technology* (Van Haren Publishing), which is used in Europe for blockchain certification. Tiana also teaches fintech at Santa Clara University. Tiana is also a frequent contributor to *Forbes.* You can follow her on Twitter at @laurencetiana.

Dedication

This one is for my sisters. Thank you for all the support and encouragement you gave me as I was writing this book.

Author’s Acknowledgments

This book is the product of many people’s ideas and work. It would not have been possible without the open and supportive blockchain and cryptocurrency world. I’d like to specifically thank Scott Robinson, John Pigott, Ryan Fugger, Charley Cooper, Alyse Killeen, Jeremy Kandah, Clemens Wan, Greg Wallace, Tom Bollich, and Brian Behlendorf for the direction and guidance in the evolving blockchain space and for taking time out of their busy lives to review and sanity-check my work.

This book also took a lot of editing. I’m not kidding — it really took a lot of editing. My project editor, Elizabeth Kuball, did a great job keeping me on task and on schedule, and Steve Hayes, my executive editor, made the whole book possible. I’d also like to thank Danny Yang for his thorough technical review and excellent suggestions and all the other behind-the-scenes people, who did thankless jobs to bring this book about. I’m forever in their debt.

Publisher's Acknowledgments

Executive Editor: Steve Hayes
Development Editor: Elizabeth Kuball
Copy Editor: Elizabeth Kuball
Technical Editor: Danny Yang
Production Editor: Mohammed Zafar Ali
Cover Image: © phive/Shutterstock

Take dummies with you everywhere you go!

Whether you are excited about e-books, want more from the web, must have your mobile apps, or are swept up in social media, dummies makes everything easier.

Find us online!

dummies.com

dummies®
A Wiley Brand

Leverage the power

Dummies is the global leader in the reference category and one of the most trusted and highly regarded brands in the world. No longer just focused on books, customers now have access to the dummies content they need in the format they want. Together we'll craft a solution that engages your customers, stands out from the competition, and helps you meet your goals.

Advertising & Sponsorships

Connect with an engaged audience on a powerful multimedia site, and position your message alongside expert how-to content. Dummies.com is a one-stop shop for free, online information and know-how curated by a team of experts.

- Targeted ads
- Video
- Email Marketing
- Microsites
- Sweepstakes sponsorship

20 MILLION PAGE VIEWS **EVERY SINGLE MONTH**

15 MILLION **UNIQUE VISITORS PER MONTH**

43% OF ALL VISITORS ACCESS THE SITE **VIA THEIR MOBILE DEVICES**

700,000 NEWSLETTER **SUBSCRIPTIONS**

TO THE INBOXES OF

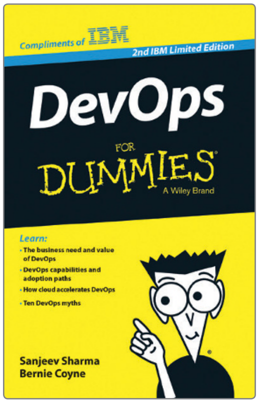
300,000 UNIQUE **INDIVIDUALS EVERY WEEK**

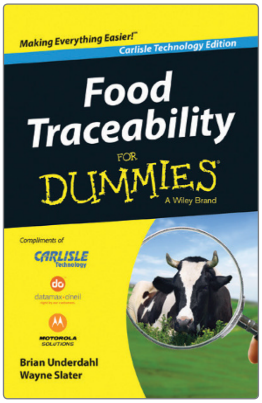
# of dummies

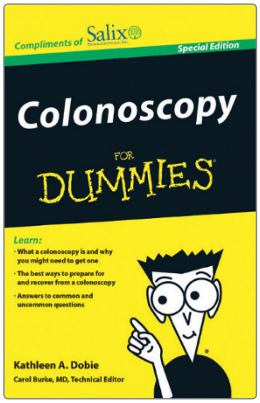
Custom Publishing

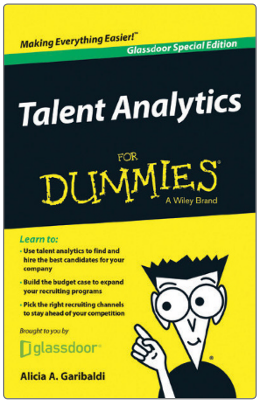
Reach a global audience in any language by creating a solution that will differentiate you from competitors, amplify your message, and encourage customers to make a buying decision.

- Apps
- Books
- eBooks
- Video
- Audio
- Webinars






Compliments of Salix
Special Edition
Colonoscopy
FOR
DUMMIES
Learn:
• What a colonoscopy is and why you might need to get one
• The best ways to prepare for and recover from a colonoscopy
• Answers to common and uncommon questions
Kathleen A. Dobie
Carol Burke, MD, Technical Editor


Making Everything Easier!™
Glassdoor Special Edition
Talent Analytics
FOR
DUMMIES
A Wiley Brand
Learn to:
• Use talent analytics to find and hire the best candidates for your company
• Build the budget case to expand your recruiting programs
• Pick the right recruiting channels to stay ahead of your competition
Brought to you by
glassdoor
Alicia A. Garibaldi

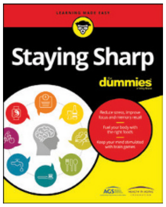
Brand Licensing & Content

Leverage the strength of the world’s most popular reference brand to reach new audiences and channels of distribution.

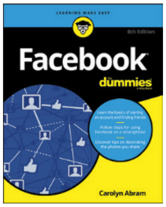
For more information, visit dummies.com/biz

dummies®
A Wiley Brand

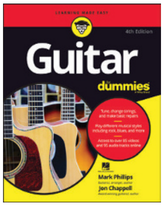
PERSONAL ENRICHMENT



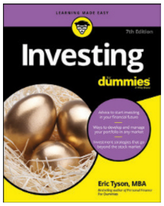
9781119187790
USA $26.00
CAN $31.99
UK £19.99



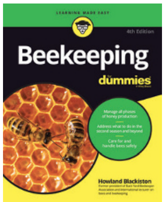
9781119179030
USA $21.99
CAN $25.99
UK £16.99



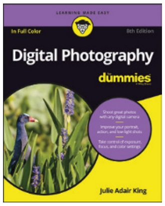
9781119293354
USA $24.99
CAN $29.99
UK £17.99



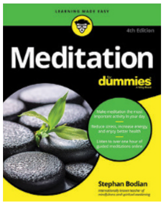
9781119293347
USA $22.99
CAN $27.99
UK £16.99



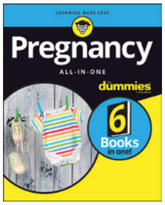
9781119310068
USA $22.99
CAN $27.99
UK £16.99



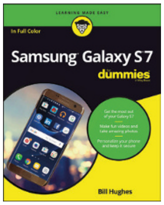
9781119235606
USA $24.99
CAN $29.99
UK £17.99



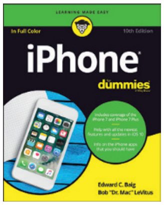
9781119251163
USA $24.99
CAN $29.99
UK £17.99



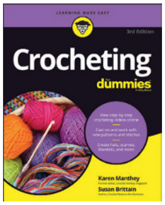
9781119235491
USA $26.99
CAN $31.99
UK £19.99



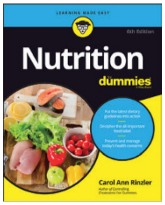
9781119279952
USA $24.99
CAN $29.99
UK £17.99



9781119283133
USA $24.99
CAN $29.99
UK £17.99

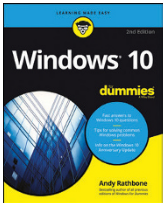


9781119287117
USA $24.99
CAN $29.99
UK £16.99

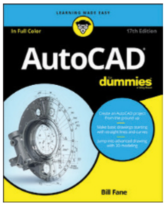


9781119130246
USA $22.99
CAN $27.99
UK £16.99

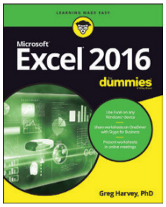
PROFESSIONAL DEVELOPMENT



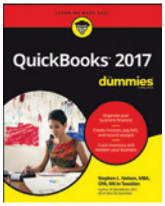
9781119311041
USA $24.99
CAN $29.99
UK £17.99



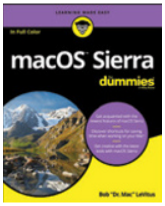
9781119255796
USA $39.99
CAN $47.99
UK £27.99



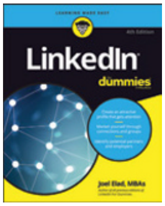
9781119293439
USA $26.99
CAN $31.99
UK £19.99



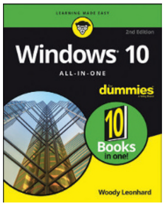
9781119281467
USA $26.99
CAN $31.99
UK £19.99



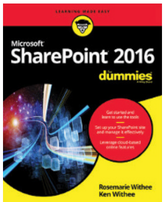
9781119280651
USA $29.99
CAN $35.99
UK £21.99



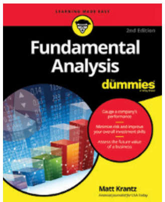
9781119251132
USA $24.99
CAN $29.99
UK £17.99



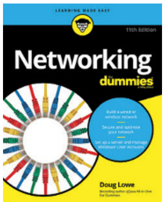
9781119310563
USA $34.00
CAN $41.99
UK £24.99



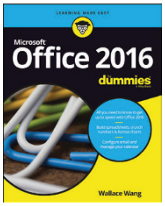
9781119181705
USA $29.99
CAN $35.99
UK £21.99



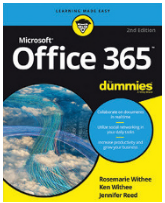
9781119263593
USA $26.99
CAN $31.99
UK £19.99



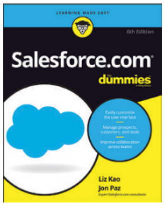
9781119257769
USA $29.99
CAN $35.99
UK £21.99



9781119293477
USA $26.99
CAN $31.99
UK £19.99



9781119265313
USA $24.99
CAN $29.99
UK £17.99



9781119239314
USA $29.99
CAN $35.99
UK £21.99

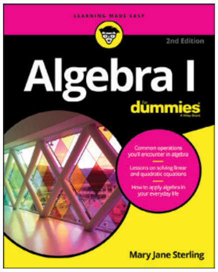
9781119293323
USA $29.99
CAN $35.99
UK £21.99

dummies.com

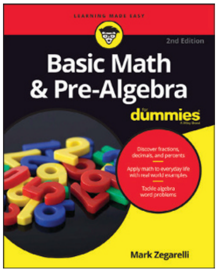
dummies®
A Wiley Brand

Learning Made Easy

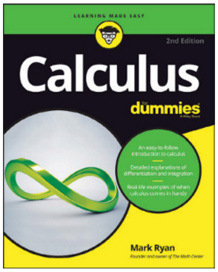
ACADEMIC



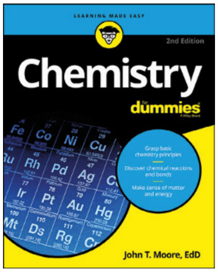
9781119293576
USA $19.99
CAN $23.99
UK £15.99



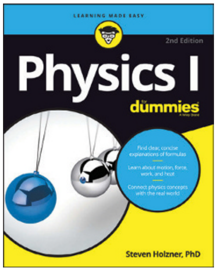
9781119293637
USA $19.99
CAN $23.99
UK £15.99



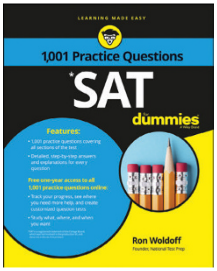
9781119293491
USA $19.99
CAN $23.99
UK £15.99



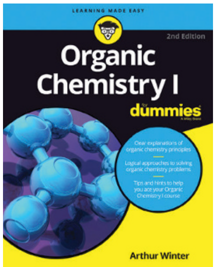
9781119293460
USA $19.99
CAN $23.99
UK £15.99



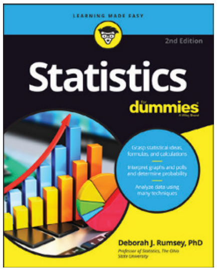
9781119293590
USA $19.99
CAN $23.99
UK £15.99



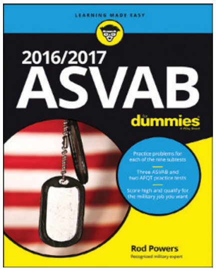
9781119215844
USA $26.99
CAN $31.99
UK £19.99



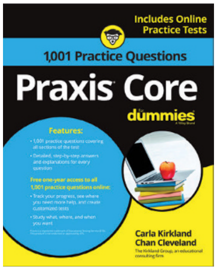
9781119293378
USA $22.99
CAN $27.99
UK £16.99



9781119293521
USA $19.99
CAN $23.99
UK £15.99



9781119239178
USA $18.99
CAN $22.99
UK £14.99



9781119263883
USA $26.99
CAN $31.99
UK £19.99

Available Everywhere Books Are Sold

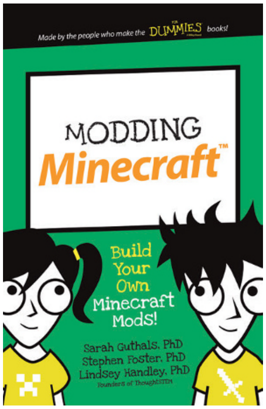
dummies.com

dummies®
A Wiley Brand

Small books for big imaginations

Made by the people who make the For Dummies books!
Getting Started with Coding
Get Creative with Code!
Camille McCue, PhD

9781119177173
USA $9.99
CAN $9.99
UK £8.99

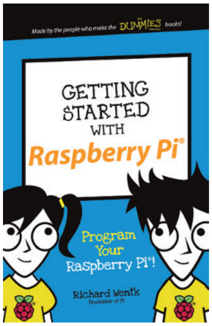

Made by the people who make the For Dummies books!
Modding Minecraft™
Build Your Own Minecraft Mods!
Sarah Guthals, PhD
Stephen Foster, PhD
Lindsey Handley, PhD

9781119177272
USA $9.99
CAN $9.99
UK £8.99

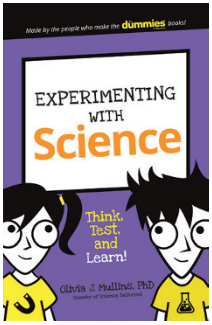
9781119177241
USA $9.99
CAN $9.99
UK £8.99

Made by the people who make the For Dummies books!
Designing Digital Games
Create Games with Scratch™!
Derek Breen

9781119177210
USA $9.99
CAN $9.99
UK £8.99


Made by the people who make the For Dummies books!
Getting Started with Raspberry Pi®
Program Your Raspberry Pi®!
Richard Wentk

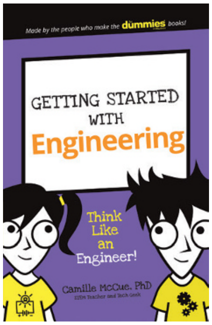
9781119262657
USA $9.99
CAN $9.99
UK £6.99


Made by the people who make the dummies books!
Experimenting with Science
Think, Test, and Learn!
Olivia J. Mullins, PhD

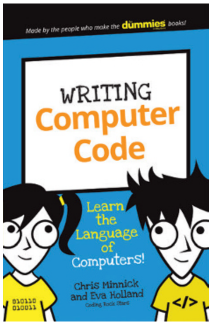
9781119291336
USA $9.99
CAN $9.99
UK £6.99

Made by the people who make the For Dummies books!
Creating Digital Animations
Animate Stories with Scratch™!
Derek Breen

9781119233527
USA $9.99
CAN $9.99
UK £6.99


Made by the people who make the dummies books!
Getting Started with Engineering
Think Like an Engineer!
Camille McCue, PhD

9781119291220
USA $9.99
CAN $9.99
UK £6.99


Made by the people who make the dummies books!
Writing Computer Code
Learn the Language of Computers!
Chris Minnick and Eva Holland

9781119177302
USA $9.99
CAN $9.99
UK £8.99

Unleash Their Creativity

dummies.com

dummies®
A Wiley Brand