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`.

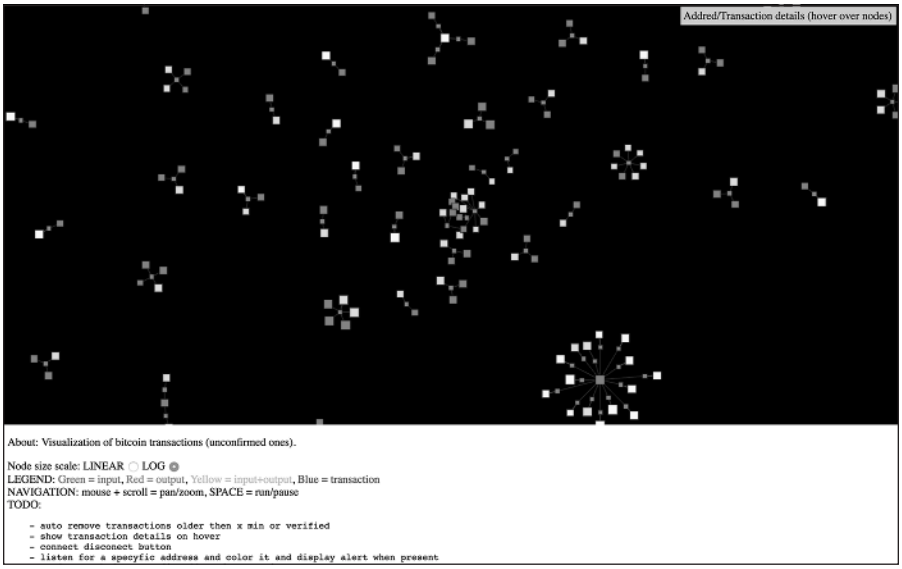

FIGURE 1-1: The structure of the Bitcoin blockchain network.

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.

  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

TECHNICAL STUFF

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.

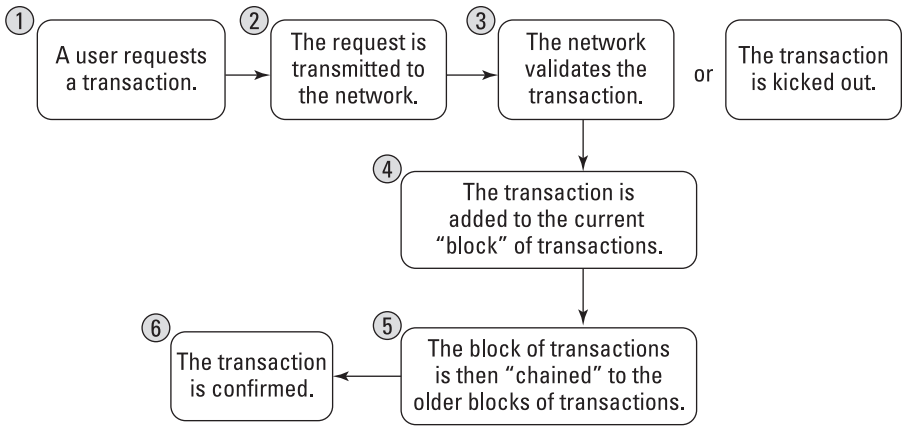

FIGURE 1-2: How blockchains work.

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.

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.