IN THIS CHAPTER

- Making money with mining: transaction fees and block subsidies
- Understanding how mining builds trust
- Discovering how mining ensures the six characteristics of cryptocurrency
- Choosing the winning miner through proof of work and proof of stake

Chapter 1
Understanding Cryptocurrency Mining

Although not all cryptocurrencies require mining, Bitcoin and other mineable cryptocurrencies rely on miners to maintain their network. By solving computationally difficult puzzles and providing consent on the validity of transactions, miners support the blockchain network, which would otherwise collapse. For their service to the network, miners are rewarded with newly created cryptocurrencies (such as Bitcoin) and transaction fees.

When a miner sends a transaction message across the cryptocurrency network, another miner's computer picks it up and adds the transaction to the pool of transactions waiting to be placed into a block and the blockchain ledger. (You can find the details about cryptocurrency and blockchain ledgers in Book 2.) In this chapter, we explore how cryptocurrencies use mining to create trust and make the cryptocurrency usable, stable, and viable.

Understanding Decentralized Currencies

Cryptocurrencies are *decentralized* — that is, no central bank, no central database, and no single, central authority manages the currency network. Conversely, the United States has the Federal Reserve in Washington, D.C., the organization that manages the U.S. dollar, the European Central Bank in Frankfurt manages the euro, and all other fiat currencies also have centralized oversight bodies. (A *fiat* currency is legal tender supported by governments via a central bank. See Book 5, Chapter 9 for more about fiat currencies.)

However, cryptocurrencies don't have a central authority; rather, the cryptocurrency community and, in particular, cryptocurrency miners and network nodes manage them. For this reason, cryptocurrencies are often referred to as *trustless*. Because no single party or entity controls how a cryptocurrency is issued, spent, or balanced, you don't have to put your trust in a single authority.

REMEMBER

Trustless is a bit of a misnomer. Trust is baked into the system. You don't have to trust a single authority, but your trust in the system and fully auditable codebase is still essential. In fact, no form of currency can work without some form of trust or belief. (If nobody trusts the currency, then nobody will accept it or work to maintain it!)

SO WHY IS THE PROCESS CALLED MINING?

When you compare cryptocurrency mining to gold mining, why the process is referred to as mining becomes clear. In both forms of mining, the miners put in work and are rewarded with an uncirculated asset. In gold mining, naturally occurring gold that was outside the economy is dug up and becomes part of the gold circulating within the economy. In cryptocurrency mining, work is performed, and the process ends with new cryptocurrency being created and added to the blockchain ledger. In both cases, miners, after receiving their reward — the mined gold or the newly created cryptocurrency — usually sell it to the public to recoup their operating costs and get their profit, placing the new currency into circulation.

The cryptocurrency miner's work is different from that of a gold miner, of course, but the result is much the same: Both bring a new money supply to the market. For cryptocurrency mining, all of the work happens on a mining computer or *rig* connected to the cryptocurrency network — no burro riding or gap-toothed gold panners required!

In the trustless cryptocurrency world, you can still trust the cryptocurrency community and its mechanisms to ensure that the blockchain contains an accurate and *immutable* — unchangeable — record of cryptocurrency transactions. Cryptocurrencies are established using a set of software rules that ensure that the system can be trusted, and the mining process is part of this system that allows everyone to trust the blockchain.

Cryptocurrencies have no central bank printing new money. Instead, miners dig up new currency according to a preset coin-issue schedule and release it into circulation in a process called *mining.*

Exploring the Role of the Crypto Miner

Cryptocurrency miners add transactions to the blockchain, but different cryptocurrencies use different mining methods, if the cryptocurrency uses mining at all. Different mining and consensus methods are used to determine who creates new blocks of data and how exactly the blocks are added to the blockchain.

REMEMBER

How you mine a particular cryptocurrency varies slightly depending on the type of cryptocurrency being mined, but the basics are still the same: Mining creates a system to build trust between parties without needing a single authority and ensures that everyone's cryptocurrency balances are up to date and correct in the blockchain ledger.

The work performed by miners consists of a few main actions:

- Verifying and validating new transactions
- Collecting those transactions and ordering them into a new block
- Adding the block to the ledger's chain of blocks (the blockchain)
- Broadcasting the new block to the cryptocurrency node network

The preceding mining process is essential work, necessary for the continued propagation of the blockchain and its associated transactions. Without it, the blockchain won't function. But why would someone do this work? What are the incentives for the miner?

The Bitcoin miner actually has a couple of incentives (other cryptocurrencies may work in a different manner).

- **Transaction fees:** A small fee is paid by each person spending the cryptocurrency to have the transaction added to the new block; the miner adding the block gets the transaction fees.
- **Block subsidy:** Newly created cryptocurrency, known as the block subsidy, is paid to the miner who successfully adds a block to the ledger.

Combined, the fees and subsidy are known as the *block reward*. In Bitcoin, the block subsidy began at 50 BTC. (BTC is the ticker symbol for Bitcoin.) The block subsidy at the time of this writing is currently 6.25 BTC. The block subsidy is halved every 210,000 blocks, or roughly every four years; sometime around spring 2024, it will halve again to 3.125 BTC per block.

Figure 1-1, from the BlockChain.com blockchain explorer (`https://www.blockchain.com/explorer`), shows a transaction with the block subsidy being paid to an address owned by the miner who added the block to the blockchain. A reward of 12.5 BTC is being paid as the subsidy because this transaction was before the most recent reward halving in 2020; the actual sum received by the miner (the full reward, 13.24251028 BTC) is larger, because it also includes the transaction fees for all the transactions in the block.

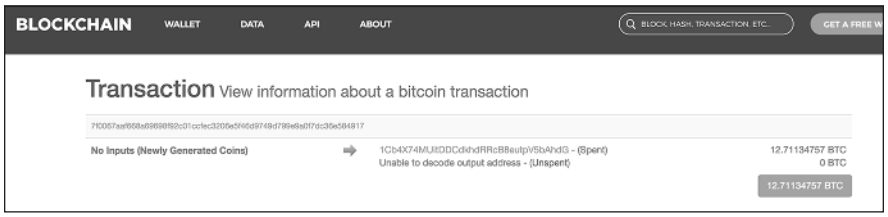

FIGURE 1-1: The block subsidy and transaction fees being paid to a miner, from the BlockChain.com blockchain explorer.

Making Cryptocurrency Trustworthy

For a cryptocurrency to function, several conditions must be met by the protocol. We like Jan Lanksy's six-factor list (Jan is a cryptocurrency academic, teaching at a university in the Czech Republic). Mining (in the mineable cryptocurrencies; non-mineable currencies have different mechanisms) is an integral part of making sure these conditions are met:

- **The system doesn't require a central authority and is maintained through distributed consensus.** That is, everyone agrees on the balances

associated with addresses in the blockchain ledger. Mining is an integral part of adding transactions to the blockchain and maintaining consensus.

- **The system keeps track of cryptocurrency units and their ownership.** Balances can be proven at any point in time. Mining adds transactions to the blockchain in a way that becomes immutable — the blockchain can't be changed. If the blockchain shows your balance is five Bitcoin, then you absolutely do own five Bitcoin!
- **The system defines whether new cryptocurrency units can be created, and, if so, the system defines the circumstances of their origin and how to determine the ownership of these new units.** A fixed issuance or inflation rate is predefined. Mining provides a way to release new cryptocurrency into circulation at a predetermined, controlled rate, with ownership being assigned to the miner.
- **Ownership of cryptocurrency units is proved through cryptography.** The three conditions of authenticity, nonrepudiation, and immutability are met, through the use of cryptography. Miners, using cryptography, verify that transaction requests are valid before adding them to a new block. The miner verifies that the transaction request is for a sum that is available to the owner of the crypto, that the owner has correctly signed the request with their private key to prove ownership, and that the receiving address is valid and able to accept the transfer.
- **The system allows transactions to be performed in which ownership of the cryptographic units is changed.** Transactions can be submitted only by senders who can prove ownership of the cryptocurrency being transferred. Cryptocurrency owners prove ownership by signing transactions using the addresses associated with a private key. Mining is the process through which transactions are accomplished, and miners verify ownership before adding the transaction to the blockchain.
- **If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system performs at most one of them.** Double-spending the same unit is not possible. The problem of double-spending was one that weakened earlier digital currencies. But with modern cryptocurrencies, miners vet transactions, searching the blockchain record of transactions to determine whether the owner actually has sufficient balance at that moment. If a sufficient balance isn't accounted for within the spend address (the Input address) in the transaction request, the transaction will be rejected by the node software and never mined onto the blockchain. Also, if the same sender has two or more pending transaction requests, but doesn't own enough cryptocurrency to cover them all, miners can decide which of the requests is valid. Additional transactions will be discarded to avoid *double-spending* the same currency.

If even one of these six conditions isn't met, a cryptocurrency will fail because it can't build enough trust for people to reliably use it. The process of mining solidifies and satisfies every single one of these conditions.

Reaching Agreement through Consensus Algorithms

A mind exercise known as the *Byzantine Generals' Problem* (or the *Byzantine Fault*, the *error avalanche*, and by various other names) illustrates the problem that cryptocurrency consensus algorithms seek to solve.

The overall problem? You're trying to reach consensus; in cryptocurrency, you're trying to reach agreement over the history of currency transactions. But in a cryptocurrency network, a distributed computer system of equals, you have many separate computers (nodes); the Bitcoin network, at times, has 50,000 to 200,000 nodes connected. Out of those thousands of systems, some are going to have technical problems: hardware faults, misconfiguration, out-of-date software, malfunctioning routers, and so on. Others are going to be untrustworthy; they're going to be seeking to exploit weaknesses for the financial gain of the people running the node (they are run by "traitors"). The problem is that for various reasons, some nodes may send conflicting and faulty information.

So to deal with this problem, a sort of parable or metaphor was devised, called the Byzantine Generals' Problem. (Three guys — Leslie Lamport, Robert Shostak, and Marshall Pease — first told this story in 1980, in a paper related to general issues of reliability in distributed computer systems.) Originally named the *Albanian Generals' Problem*, it was renamed after a long-defunct empire so as not to offend people from Albania! (Although in this interconnected world of constant social media offense, there must be at least some offended residents of Istanbul.) Apparently, distributed-computing academics like to sit around and devise these little metaphors. You may have heard of the *dining philosopher's problem*, the *reader's/writer's problem*, and so on. In fact, the *Byzantine Generals' Problem* was derived from the *Chinese Generals' Problem*.

Anyway, here is the idea, as described in their original paper:

We imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals can communicate with one another only by messenger. After observing the enemy, they must decide upon a common plan of action. However, some of the generals may be traitors, trying to prevent the loyal generals from reaching

agreement. The generals must have an algorithm to guarantee that A. All loyal generals decide upon the same plan of action [and] B. A small number of traitors cannot cause the loyal generals to adopt a bad plan.

(Search online for *byzantine generals' problem leslie lamport robert shostak marshall pease* if you're interested in seeing the original paper.)

That's the problem that cryptocurrency *consensus algorithms*, as they're known, are trying to solve: how the generals (the computer nodes) come up with consensus (all agree on the same plan of action — or transaction ledger), and avoid being led astray by a small number of traitors (faulty equipment and hackers).

Looking at the Cryptocurrency Miner

To have a chance at the mining reward, miners must set up their mining rigs (the computer equipment) and run that cryptocurrency's associated mining software. Depending on how many resources the miner is committing, they will have a proportional chance of being the lucky miner who gets to create and chain the latest block; the more resources employed, the higher the chance of winning the reward. Each block has a predetermined amount of payment, which is rewarded to the victorious miner for their hard work to spend as they wish.

So how is the winning miner chosen? That depends. In most cases, one of two basic methods is used (see Chapter 2 of this minibook for more about these and other methods).

- **Proof of work:** Under this method, the miner has to carry out a task, and the first miner to complete the task adds the latest block to the blockchain and wins the block reward, the block subsidy, and transaction fees. Bitcoin and other cryptocurrencies, such as Ether (for now; it plans to switch to proof of stake at some point), Bitcoin Cash, Litecoin, and Dogecoin, use proof of work.
- **Proof of stake:** In this system, the software is going to choose one of the cryptocurrency nodes to add the latest block; to be in the running, nodes must have a stake, generally meaning that they must own a certain amount of the cryptocurrency. The cryptocurrency network chooses the miner who will add the next block to the chain based on a combination of random choice and amount of stake — for example, with some cryptocurrencies, the more cryptocurrency owned and the longer it has been owned, the more likely the miner is to be chosen. (It's like owning lottery tickets: the more you own, the more likely you are to win.) With other cryptocurrencies, the choice is made sequentially, one by one, from a queue of preselected miners.

When Bitcoin first started, anyone with a simple desktop computer was able to mine. The would-be miner simply downloaded the Bitcoin mining software, installed it, and let the BTC roll in! As time went on, though, competition increased. Faster and more powerful computers were built and used for mining. Eventually, specialized processing chips called Application Specific Integrated Circuits (ASICs) were developed. An ASIC, as the name implies, is a computer chip designed for a specific purpose, such as displaying high-resolution graphics quickly, running a smartphone, or carrying out a particular form of computation. Specific ASICs have been designed to be highly efficient at the forms of computation required for cryptocurrency mining — for example, for Bitcoin mining. Such a chip can be 1,000 times more efficient at Bitcoin mining than the chip in your PC, so in today's Bitcoin mining environment, it's go ASIC or go home!

For high-difficulty cryptocurrencies, such as Bitcoin, the ideal mining environment requires the following conditions.

- **Low hardware costs:** Those mining rigs aren't free.
- **Low temperatures:** Lower temperatures make cooling your mining rigs easier.
- **Low electricity costs:** Mining rigs can use a lot of power.
- **Fast, reliable Internet connections:** You need to be communicating with the cryptocurrency network rapidly with minimal downtime because you're in competition with other miners.

Fear not, though! With many different copies and mimicry of Bitcoin running rampant, Bitcoin is no longer the only game in town, and you can find lots of alternative mining choices, with varying levels of required computing power. Today, some of the most profitable cryptocurrencies to mine are less known and can be mined using off-the-shelf computer hardware due to less stringent difficulty levels that are associated with lower popularity and adoption.

ASIC SCHMASIC

An ASIC is, technically speaking, an *application specific integrated circuit*: an incredibly specialized computer chip that is good at doing one operation very efficiently. However, you'll likely hear cryptocurrency people refer to the specialized mining box they've purchased as an ASIC, or an *ASIC box*. An ASIC is only good for a specific mining algorithm. For example, if you've got an ASIC built to mine Bitcoin, which uses the SHA-256 algorithm, you're not going to be mining Litecoin with it because that would require an ASIC built for the Scrypt algorithm.

TECHNICAL STUFF

Historically, during the years 2013 to 2020, a large portion of global cryptocurrency mining was claimed to take place in China, at perhaps three times the rate of the next-closest nation (the United States). A combination of cheap electricity and easy access to cheap computer components for building mining rigs gave China an edge that Chinese miners have leveraged and maintained, even with their government's apparent disapproval of cryptocurrencies. Recently, China has gone as far as to outright ban the trading and mining of Bitcoin and other cryptocurrencies, but the fact that the network hardly noticed a disruption during this debacle is a testament to how resilient and difficult to shut down distributed cryptocurrency systems such as Bitcoin are.

Making the Crypto World Go 'Round

A cryptocurrency has value because a large number of people collectively believe that it does. But why do they believe cryptocurrency has value? The answer is trust. (For more on trust, see the earlier section, "Making Cryptocurrency Trustworthy.") A holder of Bitcoin can trust that their Bitcoin will be in their wallet a day from now or 10 years from now. If they want to research how the system works, they can audit the code base to understand the system on a deeper level to see how trust is maintained. However, if they do not have the skillset or the computer science knowledge to audit code, they can choose to trust that other people, more knowledgeable than them, understand and monitor the system; they can trust the overall blockchain community that is managing the particular cryptocurrency.

Without the mining functionality underpinning the distributed peer-to-peer cryptocurrency system, this collective trust (based on the proof of collective work towards the chain) would not exist. (How the pre-mined cryptocurrencies or other weak-consensus mechanisms manage to exist is another story that we're not discussing in this book; we're focusing on mined cryptocurrencies, of course.)

REMEMBER

Mining makes sure that your balances won't change without your authorization. It incentivizes everyone to behave correctly and punishes those who don't. It creates a digital form of value transfer that can be trusted by each individual user as an equal peer in the network because every part of the system is aligned for one purpose: to provide a secure way to create, verify, and transfer ownership of digitally scarce cryptographic units.