# CERTIFIED BITCOIN PROFESSIONAL

# EXAM PREP

CBP

BROUGHT TO YOU BY

C4

# Certified Bitcoin Professional Exam Prep Book

This book is dedicated to all the current and future Certified Bitcoin Professionals.

In Bitcoin we trust. ₿

Text written by:
Jessica Levesque
Janine Römer

Thank you to CBP Committee Members:
Hunter Albright
Dirk S. Anderson
Rodney MacInnes
Janine Römer
Peter Warrack

Thank you to C4 Board Members:
Andreas. M. Antonopoulos
Joshua McDougall
Pamela Morgan
Michael Perklin

## ▼ Connect with C4

Join Our Newsletter for Monthly Announcements:

http://cryptoconsortium.org/

Watch C4's Free Educational Videos by Subscribing to Our YouTube Channel:

https://www.youtube.com/c/CryptoCurrencyCertificationConsortium

Connect with C4 on Social Media:

https://twitter.com/learnmorewithc4

https://ca.linkedin.com/company/crypto-currency-certification-consortium

https://www.facebook.com/CryptoCurrencyCertificationConsortium/

Take the C4 Udemy Course:
https://www.udemy.com/course/draft/3182666/?referralCode=E24FE661C09DB047BAC9

Learn More About C4 & Our Other Certifications:

https://cryptoconsortium.org/

# Table of Contents

# Introduction

## What Is the CryptoCurrency Certification Consortium (C4)?

Welcome to the official preparatory book for the Certified Bitcoin Professional (CBP) exam, brought to you by CryptoCurrency Certification Consortium, or C4.

C4 is a Canadian non-profit organization that provides certifications to professionals who have proven they understand cryptocurrency-related topics. Recipients of each respective certificate will have demonstrated comprehensive knowledge in various disciplines ranging from basic cryptography to low-level cryptocurrency development.

Volunteer committees of industry professionals, who themselves have taken and passed the CBP exam, update and improve C4's various certification exams. The release of this book was a joint effort of CBP committee members and C4 board members to provide educational resources and training for those who seek to become Certified Bitcoin Professionals. People like you!

This book is meant to focus your preparation, not provide an exhaustive list of all possible test materials. Bitcoin moves fast and our exams are updated regularly.  Be sure to spend some time learning about recent industry events before attempting the exam.

You can learn more about C4 on our website: https://cryptoconsortium.org/.

## What Is the Certified Bitcoin Professional Exam?

Before we can jump straight into the content, let's go over who a Certified Bitcoin Professional is and what the CBP exam looks like, so that you will know what to do with the material we provide.

Regardless of their professional area of expertise, CBPs earn their certificate by demonstrating high-level conceptual knowledge about the Bitcoin blockchain, bitcoin transactions, how the network operates, and key events in its history.

Think of it like your driver's license test: you need to demonstrate an understanding of how to set the car in motion and navigate roadways safely. You don't need to explain the physics and chemistry of internal combustion engines to pass.

Here is what to expect regarding the CBP exam:

The CBP exam has a time limit. **You will have 20 minutes to complete 75 multiple choice and true-or-false questions regarding various key knowledge areas about Bitcoin and the broader ecosystem.** The exam is designed to test core competencies which are valued within the industries that use and develop on Bitcoin and open blockchain infrastructures.

**A passing grade of at least 70% is required for the certificate.** If you fail the exam, you may pay to take the exam again.

While the exam itself is time-limited, there is no time limit between paying the exam fee and actually taking the exam. You are free to spend as much time as you want studying and preparing for the test, without fear of penalty.

## How Is This Book Structured? What Will I Learn?

In this book, you will learn what Bitcoin is, what it does, and why it matters.

There are seven sections that correspond to various content areas from the CBP exam.

1. History of Money
2. The Digital Economy
3. Cryptography Basics
4. Bitcoin Basics
5. Clients, Wallets, and Key Management
6. Mining
7. Bitcoin Commerce

Each section has headings and subheadings to help you manage the information provided.

You'll also notice that each section ends with a short quiz. The answers to all quiz questions are in the Quiz Answer Key section at the end of the book.

All of the content in this book was created, curated, or reviewed by CBP committee members who work in the Bitcoin and open blockchain industry.

## What Is Bitcoin?

It has now been more than a decade since a pseudonymous individual or group, going by the name of "Satoshi Nakamoto," first published the Bitcoin whitepaper to the cryptography mailing list in 2008. He / she / they described Bitcoin as "a purely peer-to-peer version of electronic cash [that] would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution."

Mathematicians and computer scientists have been experimenting with digital currencies since the 1980s. But they suffered from many of the same problems (and more) that the traditional banking system did, due to centralization of control. Bitcoin was revolutionary because it was the first decentralized digital currency.

In essence, bitcoin is a form of digital money where transactions are recorded in a hash-linked data structure called a blockchain, which is secured through a game-theoretical consensus mechanism called proof-of-work. If you are having trouble understanding any of the words or phrases you just read, don't worry, you're not alone! You will be exploring them in more detail, at your own pace, in this book.

While certain technical aspects of Bitcoin have since changed, the original inspiring idea of a peer-to-peer electronic cash system that is public, open-access, open-source, borderless, secure, decentralized, and censorship-resistant keeps growing stronger.

What started off as the "silly Internet money" used by a small group of developers and cypherpunks has expanded into a thriving digital economy worth hundreds of billions of dollars. Bitcoin still has a long way to go: in scaling to a capacity that accommodates the global market; in improving user interface design; in network robustness and security; and in privacy tools for safeguarding your financial life. None of these things will succeed without educating each other and the next generation. And our focus is on education, not speculation.

In this book, you will 'Learn More With C4'.

We also offer a CBP Udemy course that features video content from industry professionals if you're looking for a more comprehensive preparation path:

You can learn about all of our resources and learning materials on our website, https://cryptoconsortium.org/.

# History of Money

## The Functions of Money

Money is a way to express value across distance and time, and to make trade more efficient and scalable in a way that simple barter cannot.

If you have ever taken an economics class, you have probably been pulled through the historical timeline of how money has evolved from barter and debt-based systems, to primitive forms of money like shells, beads and livestock, to precious-metal coins. Before the shift from physical to digital forms of money, the last major transition in the evolution of money was from commodity money, like pigs and cows, to paper fiat money, like promissory notes.

But regardless of which era of the history of money you look at, it is clear that the most successful money of the time, or of a particular geographic area, was so because it fulfilled at least one or more of the three functions of  money. The three functions of money are: unit of account, store of value, and medium of exchange.

### Unit of Account

A unit of account is a common standard of measurement for the value of goods or services. The most familiar forms of money act as units of account within a specific location in which that currency is accepted in trade. For example, the U.S. dollar is a unit of account for goods and services in the United States; it is also used as a unit of account in other areas of the world because the U.S. dollar is currently considered a global reserve currency. In the European Union, the euro is considered the primary unit of account. In the U.K., the British pound sterling is the unit of account. And so on.

Two important factors in whether a form of money works as a good unit of account are stability and simplicity.

For stability the question is: ‘is the supply inflating?’ In other words, is its value as money increasing or decreasing wildly, requiring frequent shifts in the pricing of goods and services?

For simplicity, the question is: how easy is it to remember and express the value of goods and services?

### Store of Value

Another function of money is the store of value, which is a way to save and retrieve wealth by being able to accurately anticipate its future value. The term “store of value” might conjure up images of literally stashing something away in a box. However, store of value has to do with the predictability of value. In other words, will it retain its current value or increase in value. Determining that a money acts as a good store of value means that the demand and / or supply of that currency or asset is stable.

### Medium of Exchange

Finally, a medium of exchange is any tool that is used to solve the “double coincidence of wants.” The double coincidence of wants is when two parties engaging in trade both have what the other wants, making the trade mutually beneficial. For example, if Bob is selling coffee for $3, and Alice wants coffee and is willing to spend $3 on coffee, an exchange is likely.  Having a common medium of exchange increases the chances that a trade will be successful.

## The Properties of Money

Whether a form of money satisfies one or more of the three functions (unit of account, store of value, medium of exchange) depends on its properties. Properties of money include: scarcity, fungibility, durability, portability, divisibility, unforgeability, and universality.

### Scarcity

The supply of a given resource is limited, while our demand for that resource is unlimited. Scarcity can depend on factors like location. The classic example is a primitive money like seashells. In terms of scarcity, they may make good money for a mountain villager far inland, but they would be a terrible money for a coastal fishing village. A good money should be plentiful enough that there is enough supply to allow you to use it, but not plentiful enough that it stops being a useful measurement of value and wealth.

Are you wondering how digital forms of money achieve scarcity when, by nature of being digital, they should be easy to “copy and paste?” We will get to that in later sections.

### Fungibility

Units of money should be considered equally interchangeable, meaning that units of money should be able to be used in place of each other. This is where the concept of fungibility comes in.

When something is fungible, it means that it is able to replace or be replaced by another identical item. In other words, it is interchangeable. Keep in mind though that whether a unit of money is actually fungible may not necessarily affect whether it is legally fungible.

Here's an example to help you understand: a business or government shouldn't refuse to accept your dollar bill just because it has a small tear or crinkle in it; yet most of us, if given the option, would probably choose a freshly printed dollar bill over an old crinkled bill just because one looks nicer than the other.

While one bitcoin is equal to one bitcoin, there is a problem of fungibility in Bitcoin that breaks down to coin ownership. Unlike a dollar bill, which may have been "owned" by many people prior to you that you may never know, blockchain analysis tools exist which can trace the transaction history of bitcoin to the individuals who used them. If a coin was involved in something unethical or illegal, such as an exchange hack, people might not want to come into possession of it and risk associating themselves with that crime.

So while one bitcoin can be exchanged for one bitcoin, there's a little more to Bitcoin's fungibility story!

### Durability

Something is durable if it is able to withstand damage. Durability shows whether a unit of money can survive wear-and-tear over many years without needing to be fixed. This is why precious metals were popular materials for coins. The giant Rai stones of the Micronesian island of Yap are also a famous example of a durable system of money, because the stones could resist most weathering and damage. We say "set in stone" for a reason.

### Portability & Divisibility

When it came to portability and divisibility the Rai stones were not convenient. They weighed so much that moving them to their new owners was a difficult event. In a weird way, this lack of portability actually increased the value of stones that *were* successfully transported. Because of this, ownership of these stones was often passed down through an oral history, rather than being determined by its physical possession. Dividing the stones into pieces also wasn't practiced, just as people couldn't divide animals like cows and pigs that they were trading. This is a good example of how these properties can sometimes make a form of money good for one function, like a store of value, but not for another function, like a medium of exchange.

### Unforgeability

With the rise of coinage, debasement of those currencies through shaving, clipping, and forgery was combated in a variety of ways. Political leaders to this day have made an effort to increase unforgeability by stamping and inscribing images and symbols into their units of currency, to make them just that much harder to copy. Tests could also be conducted on these coins to determine whether they were real gold and silver or not, such as by weighing them, listening to the sounds they made when dropped, or even by melting them down and verifying that their elemental structure was pure. However there was a glaring problem with this model: what would happen when the centralized authority who issued and stamped the currency had an incentive to generate forgeries themselves, for example to pay off large debts? That same problem also affects centralized ledgers and digital forms of money, which we will discuss in the next section.

### Universality

Universality has to do with how broadly a form of money is accepted, across contexts, cultures, and even national borders. On the European continent, the euro is more widely accepted than the British pound sterling. As a global reserve currency, the U.S. dollar is not only accepted across all states in the union, but often by many governments and businesses around the world engaging in international trade. The digitization of national currencies over the last several decades means that your currency may be *practically* increasingly accepted anywhere online, due to conversion mechanisms behind the scenes.

With the digitization of money, a larger and larger portion of day-to-day commerce is being conducted online, recording transaction activity within centralized digital ledgers.

## Centralized Ledgers

By the end of this chapter, you should be able to answer the following questions: What is a ledger? What is the history of centralized ledgers?

### Ledgers

A ledger is simply an account or record of the transfer and /or ownership of assets, liabilities, income, expenses, and capital. It has been theorized by socio-economic historians that ledgers may have been one of the earliest use cases for the development of a formal written language.

Keeping track of ‘who owes who what and how much’ would have been an important aspect for any society, and even more so once it was no longer possible for individual members to form relationships with everyone in their group, and rely on informal promises. Ledgers were, and continue to be, maintained in a variety of contexts. There are ledgers for personal accounting, for businesses to track sales and purchases, for cities to track taxes and trade, and for governments to track national debts, among many other scenarios.

Throughout most of human history, the safekeeping of ledgers was complicated and politically charged. Who had permission to add, change, or remove entries? Where would the ledger be physically stored? How would its integrity be ensured? The answer to these questions was almost always the same: a centralized trusted authority.

### The Digital Age

The advantages and problems with ledgers carried over to the digital age. Just because machines took over tasks like organization, storage, and math calculations, the human element hasn't gone away.

The digitization of money and ledgers still faced the question of how to protect these systems against malicious actors in a safe and secure way. Custodians, brokers, accountants, and anyone else who manages their own ledgers this way, may need, at some point, to agree with everyone else. Each version of the record must align with the other copies. This requires a lot of time, work, and oversight to maintain, and for good reason.

Mathematicians and computer scientists began experimenting with the viability of non-state digital currencies in the 1980s, but were unable to solve the key issue of centralized control, and so digital currencies continued to suffer from the same problem.

Those who attempted to build distributed ledgers still had a coordination problem, regarding how to organize permissions among a slew of untrusted and unknown parties.

## The Bitcoin Whitepaper

By the end of this chapter, you should be able to answer the following questions: What is the Bitcoin whitepaper? What are the main points from the whitepaper?

On October 31st, 2008, a person or group of people named Satoshi Nakamoto published the Bitcoin whitepaper to the cryptography mailing list. The whitepaper has 12 sections, including the introduction and conclusion.

You can, and should, read the whitepaper at: https://bitcoin.org/en/bitcoin-paper

## Transactions

In the section on *Transactions*, Satoshi explains how ownership of coins is transferred from one person to the next using digital signatures. Keeping track of this chain of ownership across the distributed network is one way Bitcoin is able to prevent double-spending. This means that someone can't spend the same money twice. By contrast, the centralized model of previous experiments in electronic cash assumed that "only coins issued directly from the mint are trusted not to be double-spent."

## Timestamp Server

If you read the whitepaper in full, you may notice that at no point does Satoshi use the term "blockchain," even though the words 'block' and 'chain' are frequently used in the same sentence. This is because "blockchain" as a compound noun did not become a popular way to refer to Bitcoin's hash-linked data structure until many years after the fact. Instead, Satoshi simplifies the description of this system as a "*Timestamp Server*. "The timestamp proves that the data must have existed at the time… to get into the hash. Each timestamp includes the previous timestamp in its hash." The timestamps form a chain, and each new timestamp reinforces the ones before it.

## Proof-of-Work

In the section *Proof-of-Work,* Satoshi states that the integrity of the chain of blocks is protected by a requirement to contribute computing power. This proof that the computer is working and putting forth effort, known as proof-of-work, is necessary to build blocks into the future, as well as to modify the past should anyone attempt to do so. The longest chain represents the majority decision, or in other words the greatest proof-of-work effort.

## Network

In the section *Network,* Satoshi outlines the step-by-step process where nodes include transactions in blocks. A node is a unit of a data structure.  A block is where the data is permanently recorded. If different versions of a block are shared or broadcast at the same time, or if a block is missed, the network decides which chain to follow. The decision of which chain to follow is called consensus.

## Incentive

In the section *Incentive,* Satoshi describes what will come to be called the coinbase transaction. It is "a special transaction" that "adds an incentive for nodes to support the network." In other words they are rewarded with bitcoin. This incentive creates "a way to initially distribute coins into circulation, since there is no central authority to issue them."

The absence of a central issuer is a core feature of Bitcoin's monetary policy. The comment that this incentive mechanism is like gold miners is the original reason why terms like *miner* and *mining* have been applied to this computational work, despite no actual pickaxes or gold being involved.

## Reclaiming Disk Space

Keeping a record of all transactions and blocks can take up quite a bit of storage within a blockchain. In the section of the Bitcoin Whitepaper "*Reclaiming Disk Space,"* Satoshi offers a solution called the Merkle Tree Data Structure.

A merkle tree is a data structure that summarizes and verifies the integrity of large sets of data. With Bitcoin, a Merkle tree summarizes all the transactions in a block. It then creates a digital fingerprint of all the transactions, which allows a user to verify if a transaction is included in a block, or not.

Essentially, what the Merkle Tree structure does is compact old blocks to free up storage space.

## Simplified Payment Verification

Merkle Trees are also used in *Simplified Payment Verification* (SPV) proofs.

As Satoshi writes, "a user only needs to keep a copy of the block headers of the longest proof-of-work chain." The user can get the longest proof-of-work chain by requesting data "until he's convinced he has the longest chain" and getting the Merkle branch that links the transaction to the block where it was timestamped. Satoshi warns that "the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker."

What does all of this mean?  Simplified Payment Verification allows a user's bitcoin wallet to verify that a transaction is included in the Bitcoin blockchain, without having to download the entire blockchain.

## Combining and Splitting Value

*Combining and Splitting Value* illustrates the three common types of transactions:

1) One input and two outputs, one of which is change
2) Many inputs and one / few outputs (known as an aggregating transaction)
3) One / few inputs and many outputs (known as a distributing transaction)

What's important to know is that Bitcoin's blockchain uses a UTXO-based model. A UTXO is an unspent transaction. In other words it's the amount of bitcoin that remains after a transaction has occurred.

### Privacy

*Privacy* provides some vital advice to bitcoin users who want to protect their anonymity despite the fact that transaction records are public. As long as people don't give personal information to trusted third-parties, it is difficult to link transactions to your identity. As Satoshi writes, "a new key pair should be used for each transaction to keep them from being linked to a common owner." In other words, avoid reusing bitcoin addresses. A bitcoin address is the destination for a bitcoin payment.

### Calculations

Finally, *Calculations* explores the probability of a malicious attacker being able to "generate an alternate chain faster than the honest chain," and "change one of his own transactions to take back money he recently spent." This "race between the honest chain and an attacker chain" has come to be called a 51% attack.

### The Bitcoin Whitepaper Solved the Double-Spending Problem

The double-spending problem, previously mentioned in *Transactions*, is what Bitcoin was designed to prevent. The double-spending problem is the financial version of the Byzantine Generals' Problem, also known as BGP. BGP is a thought experiment which assesses the risk that a network participant is unreliable and transmits imperfect information, resulting in system failure.

The BGP was first written about like this: "a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement."

Predecessors of Bitcoin tried various ways to solve the BGP. While they were unsuccessful, all the research from distributed systems and cryptography eventually led to the creation of Bitcoin. Bitcoin solves the BGP because it found a way to stop double-spending. And this is why Bitcoin is the first decentralized digital currency!

## Predecessors & Notable Events

By the end of this chapter, you should be able to answer the following questions: Before Bitcoin, what did digital cash look like? What are major events affecting Bitcoin since its creation?

## Digital Cash Before Bitcoin

Before Bitcoin, there were many different ideas for systems of digital cash. In  the early 1980s, computer scientist and cryptographer David Chaum invented eCash. eCash, was designed to send digital money anonymously but it never took off.

In 1997, British cryptographer and cypherpunk Adam Back published “Hashcash” to the cypherpunks mailing list, proposing a solution to email spam. The plugin would add stamps to email headers as proof that the sender’s central processing unit (CPU) had performed computational work. This CPU work made it harder for spammers to generate this proof for all of their messages.

Within the same period, computer scientist Nick Szabo began to theorize about computer protocols that would allow negotiations and agreements without the need of third parties. Szabo reportedly proposed a system called Bit Gold in 1998, the same year that Wei Dai proposed “b-money” on the cypherpunk mailing list. Szabo wrote about a digital money where unforgeable bits could be created online and then stored and transferred without depending on a third party.

## Bitcoin

In October 2008, Satoshi published the Bitcoin whitepaper, citing Back’s *Hashcash*. While not explicitly cited in the whitepaper, Satoshi would later write in a 2010 forum post that the digital currency models proposed by Szabo and Dai were also inspirations for Bitcoin.

## Genesis Block & Pizza Day

On January 3rd, 2009, the first block, known as the genesis block, of the Bitcoin blockchain was mined. You will learn more about the genesis block in Section 4: Bitcoin Basics.

Around January 10th, developer Hal Finney became the second known person to join the Bitcoin network, even publicly tweeting “Running bitcoin.”

The first-known retail purchase using bitcoin wasn’t made until May 22nd, 2010, when Laszlo Hanyecz paid 10,000 bitcoin for Papa John’s pizzas. At the time, bitcoin was barely worth pennies. May 22nd is now celebrated annually as “Bitcoin Pizza Day” in the Bitcoin community.

## The Silk Road

In its early years, Bitcoin’s growing reputation as censorship-resistant digital money attracted those who were willing to operate at the nexus of highest risk and highest reward. Between 2011 to 2013, an online marketplace called the Silk Road used bitcoin as its primary method of payment. A wide range of items were sold on the Silk Road, including grey and black market goods that attracted the attention of law enforcement. The shuttering of the Silk Road in October 2013 stimulated a media frenzy around the misconception that bitcoin was just “drug money” and nothing more.

### Mt. Gox

Bitcoin’s reputation in the mainstream view worsened when Mt. Gox, the largest bitcoin exchange at the time, suspended all trading in February 2014, after a massive theft of more than 600,000 bitcoin. Despite the network itself being decentralized, many users fell victim to the pitfalls of trusting a centralized third party with their keys. Keys are like access codes. And it didn’t help that the price of bitcoin had been dropping massively from the all-time-high of over $1,200 in November 2013. This contributed to the narrative that bitcoin was just a speculative investment for gamblers and nothing more.

### Lightning Network

In January 2016, a paper on a second-layer protocol called the Lightning Network was published by Joseph Poon and Thaddeus Dryja. This was presented as a scaling solution that would help to grow Bitcoin’s capacity to accommodate greater and greater portions of the global economy.

### Scaling & Price

The Lightning Network was one scaling proposal among many, and a fierce debate raged within the online community between 2015 to 2017. After many months of arguments between various interests, the network activated Segregated Witness in August 2017. Segregated Witness, or “SegWit,” was an architectural change to bitcoin transactions that moved the witness data into its own Merkle tree data structure.

A few months later, in December 2017, the price of bitcoin reached a new all-time-high at close to $20,000. You may remember the excitement about bitcoin during this time. Even traditional news sources began to report on bitcoin! There was a massive influx of people and institutions into the industry, many of which were unfortunately misinformed that Bitcoin was just a “get-rich” scheme and nothing more. As a result, some naive investors learned the hard way that it could also be a “get-poor-quick” scheme if not approached responsibly.

A new all-time-high was reached in February of 2021 when bitcoin’s price skyrocketed to over $50,000.

After more than a decade, the lesson that we all should have learned is that Bitcoin is not just one thing. It is, and can be, many things to different people. Regardless of what it may come to mean to you, there is always something more to learn.

In the next section, “The Digital Economy,” we will begin by looking at the landscape of commerce on the internet and how Bitcoin has carved out its own niche.

## Quiz 1

1. Which function of money is gold most often used for?
    2. Medium of Exchange
    3. Unit of Account
    4. Store of Value
    5. Tax Collection
6. Which property of money is NOT necessary for an asset to be used as a medium of exchange?
    a. Scarcity
    b. Government Backing
    c. Ease of Transmission
    d. Fungibility
7. In order to accurately record balances and transactions, a trusted centralized party is required to curate the ledger.
    a. True
    b. False
8. When was the Bitcoin whitepaper published?
    a. October 31st, 2008
    b. October 31st, 2009
    c. January 3rd, 2008
    d. January 3rd, 2009
9. This person created HashCash, one of the Bitcoin precursors, and was cited in the Bitcoin whitepaper.
    a. Nick Szabo
    b. David Chaum
    c. Adam Back
    d. Both A and B
10. What is the Byzantine Generals' Problem (BGP)?
    a. A problem where network participants are unreliable or transmit imperfect information which causes system failure.
    b. A computer strategy game similar to Civilization, which pays winners in bitcoin.
    c. A set of problems that members of the Bitcoin community have submitted to improve Bitcoin.
    d. When several nodes have the same blocks in their locally-validated best blockchain.
11. When was the genesis block mined?

    a. January 3rd, 2009
    b. October 31st, 2009
    c. January 3rd, 2008
    d. October 31st, 2008

12. Mt. Gox was an early Bitcoin exchange that shut down because the Bitcoin network failed.
    a. True
    b. False

# The Digital Economy

## Centralized Versus Decentralized Systems

By the end of this chapter, you should be able to answer the following questions: How do centralized versus decentralized systems compare? What is decentralized consensus?

There are thousands of companies in the financial technology industry, each claiming to be different from the next, even “revolutionary.” But at the end of the day, almost all of them still operate within the same centralized system. PayPal, AliPay, Venmo, Apple Pay, and Google Pay are all very similar, although they may have slightly different colors and their user interface may look different.

The goal of Bitcoin, as Satoshi stated, was to do away with the “inherent weaknesses of the trust based model” and build a payment system based more “on cryptographic proof instead of trust.”

Creating such a system involves decentralizing control.

### Decentralizing Control

This mesh-like network graph is a decentralized network (Fig. 1). We know it is decentralized because the dots, known as nodes, are all connected directly to other equal peers. This is in contrast to connecting to a facilitator node as you see in this image (Fig. 2).

The important thing to remember with a peer-to-peer decentralized network is that there is no central point. All peers are equal.

Bitcoin, as a pure decentralized network, does not have any centralized administration points, or “coordinating entities,” for the purposes of registration, peer discovery, or facilitation. It is an entirely open-access network.

### Decentralized Consensus

Decentralized consensus is achieved when two or more nodes have independently reached an agreement on the state of the ledger. In Chapter 10 of ‘Mastering Bitcoin,’ Andreas M. Antonopoulos explains that “consensus emerges from the interplay of four processes that occur independently on nodes across the network:

- Independent verification of each transaction, by every full node, based on a comprehensive list of criteria;

- Independent aggregation of those transactions into new blocks by mining nodes, coupled with demonstrated computation through a Proof-of-Work algorithm;
- Independent verification of the new blocks by every node and assembly into a chain; and
- Independent selection, by every node, of the chain with the most cumulative computation demonstrated through Proof-of-Work."

## AltCoins

By the end of this section, you should be able to answer the following question: How are altcoins created?

Even though this book and the CBP exam focus on Bitcoin, it is still relevant to mention that other cryptocurrencies and blockchains have emerged since Bitcoin’s inception, and many people who use bitcoin will also encounter them within this new digital economy.

The term “altcoin” is short for “alternative coin.” An altcoin is a cryptocurrency that was created after and separate from bitcoin. The world “altcoin” can point to a few different types of cryptocurrencies.

1) One type of altcoins are cryptocurrencies that are copies of Bitcoin. These copies are also known as forks. These altcoins can have either little or no changes made. The small changes are made to the codebase.
2) Altcoins can also have big changes made to the codebase. An example of these changes could be using different types of security.
3) Some altcoins were created independently from the Bitcoin codebase, but still use a blockchain-based system. Ethereum is an example of this.
4) There are also cryptocurrencies that were created independently from Bitcoin, but don’t use a blockchain-based system.

We will discuss the different types of forks in the Bitcoin Basics section. But for the time being, just know that in the example of altcoins, a fork is like a copy of the Bitcoin codebase.

Altcoins are often created by those who want to experiment with different features or characteristics of Bitcoin. They may do this to appeal to different markets and demands. For example, several altcoins were created with the idea that people wanted faster transactions. Others were created to improve the privacy and anonymity of transactions or even to create a platform for smart contracts.

One important distinction to make is that a token is not the same as an altcoin. Altcoins are the native currency or asset that is essential to the function of that blockchain system. Tokens are created on top of the existing system and may not be used monetarily. Basically, a token could disappear tomorrow, and the underlying blockchain system would function as normal. That is the key difference.

There are a few special categories of altcoins that are not part of the exam, but are useful to know about if you are working in the industry. You may have come across projects such as Tether, Libra, and the term stablecoin.

Cryptocurrencies are known to fluctuate rather wildly in price. The goal of stablecoins is to keep consistent value, despite fluctuations in supply or demand for that coin. But in reality stablecoins are more like digital versions of national currencies, like the U.S. dollar. Whether based on a particular fiat currency or more than one national currency, stablecoins do still fluctuate in value within the global market.

## Exchanges

By the end of this section, you should be able to answer the following questions: What are exchanges? What is an example of an early exchange that failed?

Exchanges are marketplaces where assets and currencies can be bought and sold, or traded. It is also where price discovery is conducted, based on the crossover between supply and demand.

### Custodial Exchanges

When it comes to online exchanges, the most popular type is a custodial exchange. These exchanges take custody of your funds to let you trade with other users. Most custodial exchanges require their users to complete an identity verification process as part of ‘Know Your Customer’ or KYC rules. These identity checks are part of anti-money laundering, or AML, regulations.

Once an exchange completes these checks, users can then send their coins into the exchange to begin trading with other users. Because the exchange sits in the middle of every trade, they present a risk because they have full control over the keys to your assets. Remember the Mt. Gox issue we discussed where all the users lost their bitcoin?

Another risk of exchanges is that your personally identifying information could be exposed in the event the exchange suffers a data breach.

Every once in a while, you will probably hear about a custodial exchange that suffers a data breach, unauthorized access, a malicious insider, regulatory pressure, or some other compromising event. But here is a particularly famous example:

Between 2010 and 2014, Mt. Gox was the dominant fiat-to-bitcoin exchange, controlling up to 70% of the trading market, which was still relatively small compared to the traditional financial world. The exchange collapsed in 2014 after a series of breaches, concluding in the loss of more than 600,000 of their customers' bitcoin. The price of bitcoin crashed shortly thereafter.

A number of other exchanges have also lost their customers' money over the years. However, as the industry has grown, exchange breaches no longer have an effect on the price of bitcoin.

### Non-Custodial Exchanges

In contrast to custodial exchanges, there are decentralized non-custodial exchanges. The decentralized exchanges are also called DEXes. They allow you to have control of your coins, and rarely ask for personally identifying information, except if there is a dispute.

Crypto-to-crypto trades are the most secure against counterparty risk because they do not rely on any traditional banking mechanisms to settle. The coins being traded are usually locked into a type of multi-signature address, which is an address associated with more than one private key.

Someone may act as a go-between before the trade starts. Crypto-to-fiat trades are possible in many national currencies. With these trades there will always be the risk of transaction reversal on the fiat side if the trade involves bank accounts.

### OTC Desks

Over-the-counter, or OTC desks, are for conducting off-exchange trading directly between two parties, like two individuals or brokers. These trades are usually conducted online or over the phone. Smaller exchanges can offer this as a personalized service for institutional clients and high net-worth individuals, who may have large orders that could disrupt the market if they go through a large formal exchange.

### P2P Exchanges

Finally, in-person peer-to-peer (P2P) exchanges are when two or more people trade informally and directly without using any online exchange mechanisms, except perhaps for discovering their trading partners. They usually communicate over secure messaging platforms to set prices and amounts beforehand, then arrange a physical meeting place to conduct the trade. Crypto-to-fiat cash (or vice versa) trades are the most commonly done in this way. Before engaging in this type of trade, make sure to cross-reference the price of whatever is being offered, as sources of price discovery may vary. Unless you know and trust the person you're trading with, it is recommended to conduct these in-person trades in a semi-public setting for safety reasons. This is why Bitcoin meetups are often used for meeting interested parties.

## Quiz 2

1. In order to accurately record balances and transactions, a trusted centralized party is required to curate the ledger.
    a. True
    b. False
2. What is an altcoin?
    a. A token created by the Cambridge Centre For Alternative Finance.
    b. A cryptocurrency only issued by governments.
    c. A blockchain-based digital currency based on the concept of, but seperate from, Bitcoin.
3. Mt. Gox was an early Bitcoin exchange that shut down because the Bitcoin network failed.
    a. True
    b. False

# Cryptography Basics

## What Is Cryptography?

By the end of this section, you should have a basic idea of what cryptography is and what role it plays in cryptocurrencies like Bitcoin.

The term “cryptography” comes from the Greek word ‘kryptos,’ meaning “hidden,” and ‘graphie’ meaning “writing” or “recording.” Together, this translates to the art of secret writing.

Cryptography has been used for thousands of years. Once humans created a system of writing, they were also motivated to figure out how to protect their letters from nosy neighbors and spies.

A cipher is the instructions for performing encryption or decryption, including for the most primitive pen-and-paper ciphers. In modern times, these instructions are in the form of code algorithms run by computers.

Even if you’ve never gone out and deliberately used cryptography, you are probably using it multiple times a day. The hard drive and storage on your laptop or smartphone is likely encrypted. Most websites you visit use HTTPS, which uses cryptography to maintain the security of the webpage you’re using. Even to access this book! If you use a messaging app like Signal, Wire, or WhatsApp, they use encryption to keep your messages confidential. And if you use Bitcoin and other cryptocurrencies, you are in one of the newest experimental areas of cryptographic research!

### Functions of Cryptography

There are five primary functions of cryptography. To help you remember these functions, let’s use the acronym PAINT: ‘P’ for privacy. ‘A’ for authentication. ‘I’ for integrity. ‘N’ for non-repudiation, and ‘T’ for transfer of keys. While you don’t need to know this acronym for the exam, it’s important to have an underlying understanding of the functions of cryptography.

First, privacy and confidentiality. You may use encryption to ensure only the intended receiver can read a message you send.

Second, authentication. You may use encryption to prove who you are, or at least that you have the credentials to authorize a particular action.

Next, integrity. You may use cryptography to ensure that a message has not been modified from when it was originally sent.

Fourth, non-repudiation. This means that the sender of a message cannot deny that they sent this message. The authority of the message cannot be disputed, when authentication and integrity are both at play.

And finally, the transfer of keys, or key exchange. This is the process by which cryptographic keys are securely shared between the sender and receiver.

### Encryption & Decryption

The difference between "encryption" (Fig. 3) and "decryption" (Fig. 4) is simple. Encryption changes a plaintext message into unintelligible ciphertext. Decryption converts that ciphertext back into plaintext. These processes either use one key, in a symmetric cryptography scheme, or two different keys, in an asymmetric cryptography scheme.

## Symmetric versus Asymmetric Cryptography

In the last section you were introduced to cryptography, and the acronym 'PAINT' to help you to remember the five primary functions of cryptography: 'P' for privacy. 'A' for authentication. 'I' for integrity. 'N' for non-repudiation. And 'T' for transfer of keys.

By the end of this section, you should be able to answer the following questions: What is the difference between symmetric and asymmetric encryption, and how does asymmetric encryption impact key exchange?

### Symmetric Key Cryptography

As we mentioned in the previous section, symmetric key cryptography uses one key for both encryption and decryption. Asymmetric key cryptography, also known as public key cryptography, uses two keys, one for each operation (Fig. 5).

Symmetric key cryptography presents a problem because, to use it to communicate securely with another party, the same key must be available both to the sender and receiver. Therefore the key must be shared with the other party somehow without exposing it during the key exchange. Otherwise, all messages that have been encrypted with the key could be decrypted by anyone who manages to access it.

### Asymmetric Key Cryptography

In 1978 Ralph Merkle introduced one of the first protocols for asymmetric encryption to the public.

The two different keys in an asymmetric crypto-system are known as the public key and the private key. As is probably obvious from the name, the public key can be 'public,' and can be shared freely. The public key performs the encryption function, converting plaintext into ciphertext. The private key must be kept secret because it performs the decryption function, converting ciphertext back into plaintext (Fig 6.). Bitcoin uses the Elliptic Curve Digital Signature Algorithm (ECDSA) to generate these keys.

One very important part of public-private key pairs is that the public key can be derived from the private key. This means that if you know the private key you are able to figure out the public key. However the reverse is not true; the private key cannot be derived from the public key. If you have a public key, but no private key, you'd be unable to access the private information. We will explain more about how these keys are used in Bitcoin specifically in later sections

In the following example, two parties are trying to communicate with each other using an asymmetric key crypto-system. Bob, the sender, he has a public key belonging to Alice. When Bob sends a message to Alice, he uses Alice's public key to convert the message into ciphertext. The only person who can read it now is Alice, because she has the private key.

Eve, a bad actor, wants to snoop on the conversations between Bob and Alice. When Bob sends the ciphertext message to Alice, Eve attempts to read it. However, she only has Alice's public key, which can only be used for encryption, not decryption.

When Alice receives the ciphertext from Bob, she uses her private key to convert the ciphertext message back into plaintext. Now she can read what Bob wrote! Vice versa, if Alice wanted to respond to Bob, she would use Bob's public key to convert the message into ciphertext. Bob would then use his own private key to decrypt the message back into plaintext. The only way for Eve to read the messages is if she had access to the private key.

## Hash Functions

By the end of this section,  you should be able to answer the following questions: What is a hash function? How are hash functions used in Bitcoin?

Hash functions are a form of one-way, keyless cryptography. Hash functions are algorithms that scramble data into something called a hash. A hash is a fixed-length, alphanumeric reproducible checksum. In other words the length of a hash never varies. It is made up of letters of the alphabet, numbers, mathematical symbols, and punctuation marks. A checksum is a sum that compares the two sets of data to make sure they are the same. A checksum is also called a fingerprint.

These fingerprints ensure the integrity of data because any change to the input data results in a change to the output hash. This means someone could detect whether that data has changed in route or over time. The input data is called the plaintext. And this plaintext input can be any number of ‘bits’: a sentence, a novel, a spreadsheet, or an entire digital archive. This input, once scrambled, is called ciphertext.The plaintext input is not easily recoverable from the ciphertext. These hashes are primarily used for the third function of cryptography, message integrity.

For example, imagine that you are a software developer, and you want to make sure that software released to your users is not tampered with. It is becoming common practice for open-source developers to create a hash of the code for their software, to sign that hash of their code with their key, and to publish this hash and signature on their website. Let’s break that down a little more. A developer can create a hash of the code. Next the developer uses their private key to sign that hash of their code. And then they would publish the hash and signature to their website.

Using this system, when users download the software, they can build the software from scratch, compute a hash of the files, and compare it against the hash the developers published. If both hashes match, that user knows their download of the software is safe. And that it came from the developer who signed the hash.

## Hash Functions & Bitcoin

Bitcoin uses two hash functions: SHA-256 and RIPEMD-160.  “SHA” stands for ‘Secure Hash Algorithm’. RIPEMD-160 stands for ‘RACE Integrity Primitives Evaluation Message Digest’.

SHA-256 plays an important role in what is called the proof-of-work mining process. We’ll talk about proof-of-work later, but simply put it means that a system needs computing power to deter malicious attacks.

The RIPEMD-160 hash function is used to help turn public keys into bitcoin addresses.

We’ll continue to talk about keys and addresses as we progress through this book.

## Digital Signatures

By the end of this section,  you should be able to answer the following questions: What are digital signatures? How are digital signatures used in Bitcoin?

### Authentication

Although hash functions perform the third function of cryptography, integrity, they are key to digital signatures which are primarily used for the second function: authentication.

A digital signature algorithm is a mathematical way to show the 'authenticity' of a digital message. The signature takes the form of a seemingly random sequence of data. Digital signatures are like a handwritten signature. They are used to authorize an action or authenticate a statement. But unlike a handwritten signature, digital signatures cannot be easily forged. It is unique to the private key which generates it, and the particular message it is used to sign.

In Bitcoin, private keys are used to sign transactions. You do not need to be connected to the internet to sign transactions. By signing the transaction, you authorize the transfer of ownership of coins from one address to another.

### Integrity

In addition to authentication, digital signatures still serve the purpose of integrity.

Let's imagine a scenario with the same characters we used in the second section: Alice, Bob, and Eve. When Bob sends his encrypted message to Alice, he also signs the message with his private key. Signing with his private key proves to Alice that it came from him. However, Eve intercepts the message. Even though Eve can't decrypt Bob's message, she can replace it with a different encrypted message by using Alice's public key.

When Alice receives the message, she is able to decrypt the message. However, when she tries to verify the digital signature, it doesn't match Bob's public key. This means she can assume that someone changed the message to trick Alice into thinking that Bob wrote something he didn't. If Alice receives a message with a verified digital signature, then she can be confident that it was Bob who sent it. This is why it is so important to keep your private key safe and secure.

If this was a Bitcoin transaction, and Alice was running a bitcoin node, which verifies transactions on the Bitcoin network, it would check whether the bitcoin being sent is owned by Bob's public key and if it matches Bob's digital signature and bitcoin address. If it doesn't, then Alice's bitcoin node will reject the transaction as invalid.

### Non-Repudiation

Finally, digital signatures combined with hash functions can provide non-repudiation. Non-repudiation means that something is undeniable. So in this case, Bob cannot deny that the digital signature on a message was created using his private key. Bob also can't say that his message was changed, if the fingerprint matches.

If Bob wanted to deny that a message with his digital signature did not come from him, his only defenses would be: 1) "My private key has been stolen!" or 2) "The digital signature algorithm is broken!" The latter excuse would be a very big deal, if found to be true. While an unlikely excuse, cryptographic algorithms do have a shelf life; eventually, the hash functions and digital signature algorithms we use today -- including the ones used in Bitcoin -- will need to be upgraded with ones that are even more secure.

## Quiz 3

1. What is cryptography?
    a. Cryptography is the name of the algorithm that secures Bitcoin private keys.
    b. Cryptography is a routing mechanism.
    c. Cryptography is the science or study of the techniques of secret writing.
    d. Cryptography compresses the size of the Bitcoin blockchain.
2. In symmetric cryptography, the key is a piece of information that is used to encrypt a message
    a. True
    b. False
3. A private key can be derived from a public key.
    a. True
    b. False
4. Cryptographic hash functions are used in the Bitcoin protocol to ensure data integrity.
    a. True
    b. False
5. What basic components of a cryptocurrency provide security and anti-counterfeiting measures?
    a. Digital signatures
    b. Public key infrastructure
    c. Hash functions
    d. All of the above

# Bitcoin Basics

## Bitcoin & Blockchains

By the end of this section, you should be able to answer the following questions: What is the difference between Bitcoin with a capital B, bitcoin with a lowercase b, and a blockchain? What are the denominations of bitcoin and how are they related to each other?

### Bitcoin & bitcoin (upper and lower case)

You would be hard pressed to find an article or book about cryptocurrencies that didn't mention the words "Bitcoin" and "blockchain." You may be wondering, how are these terms distinct from each other, and why is 'Bitcoin' sometimes written with a lowercase 'b,' while elsewhere with an uppercase 'B'?

There is no official literary style guide for when to use upper- or lowercase 'b' in Bitcoin, but over time people have generally conformed to the following standard:

Uppercase 'Bitcoin' is used to refer to the software project, protocol, network, or community. Lowercase 'bitcoin' is used to refer to the unit of value that is transferred over the Bitcoin network. We send and receive bitcoin - with a lowercase b- just like we send and receive units of other currencies like the dollar and euro - which are also written in lowercase. Bitcoin as a unit can also be expressed using the symbol 'BTC', though some exchanges and financial services may use other symbols instead, like XBT.

Also notice how "bitcoin" is a plural noun, like water or police. Conversely, the word "dollar" is a singular noun, like a chair or a car. Over time it has become the norm to say 'sending bitcoin', with no -s, to someone rather than sending bitcoins.

### Bitcoin the Unit

As a unit, bitcoin has several subunits or denominations. One bitcoin is equal to 100 million satoshis, which is the smallest on-chain unit. Satoshis are abbreviated as Sats. In between the two is the millibit and bit. One millibit is equal to 100,000 satoshis, or one thousandth of a bitcoin. One bit is equal to 100 satoshis, or one millionth of a bitcoin.

With the arrival of the Lightning Network, a second-layer payment protocol, there is also the millisatoshi, which is one thousandth of a satoshi or one hundred billionth of a bitcoin. Lightning payments can be smaller than one satoshi, but the on-chain settlement transaction must be at least one satoshi, as that is the smallest usable unit on the Bitcoin blockchain. It's important to know that bitcoin has a supply cap of 21 million.

## Blockchains

The term ‘blockchain' refers to the public ledger and data structure in which the Bitcoin network records the history of valid transactions, spanning back to January 3rd, 2009. Unfortunately, a lot of companies and governments have used the word ‘blockchain' over the last several years to talk about digital ledger projects that aren't distributed and don't even use ‘blocks.'

It's very important to understand that blockchains are not magic. A blockchain is simply a database that can record data in a tamper-evident way, meaning it's obvious if it's been changed.

Blockchains themselves aren't cryptocurrencies. And blockchains don't have all of the other characteristics that Bitcoin has that make Bitcoin work well as a cryptocurrency. Characteristics such as decentralization, security, immutability, and censorship resistance are not parts of all blockchains, but they are part of Bitcoin. Bitcoin has these characteristics due to multiple technologies working together in harmony. In other words, Bitcoin is not powerful due to any one single factor.

In the Bitcoin network, these characteristics are determined by nodes that run the Bitcoin software. Nodes communicate with peers, verify information they receive, and broadcast new information. Nodes also organize what they know in data structures to conform to consensus rules. Consensus rules are the rules that all Bitcoin full nodes use to determine if a block, and the transactions in the block, is valid.

When you have enough nodes running in many countries, a system is more decentralized. When you have many sources of energy to power mining nodes, security is increased. The more energy being used for computation, the more difficult it becomes to change the ledger.

You can think of Bitcoin like a cake and its blockchain like eggs. Eggs are important for making a cake, but you can't make a cake out of just eggs. When people say “blockchain not Bitcoin” it's like saying “eggs not cake.” And just like you need more than eggs to make cake, you need more than just a blockchain to make a working cryptocurrency!

## Keys & Addresses

By the end of this section,  you should be able to answer the following questions:
What is the relationship between Bitcoin addresses, public keys, and private keys?
How are Bitcoin addresses generated?

### Private Keys

As we mentioned in the last section, Cryptography Basics, before you can receive, hold, and send bitcoin, you must first generate a private key(s).

A private key is a 256-bit number. A “bit” or binary digit is the smallest unit of measurement for computer data, with a value of 0 or 1. It is usually represented as an alphanumeric sequence. “Alphanumeric” just means numbers and letters. This private key format only uses numbers 0-9 and characters A-F.

These private keys are used to generate digital signatures, which means you can spend bitcoin that is controlled by that key. If you don’t have the correct private key, you cannot spend the bitcoin. Therefore, it is very important that these keys are generated in the proper manner, then stored in a safe and secure location.

### Entropy

Since your private key is essentially just a number, you want to generate a random number that someone else won’t be able to guess easily. Therefore you will need a strong source of entropy, or randomness. Think about the passwords that you use for your bank account. Hopefully you did not use the lyrics of a popular song, or the name of your dog -- unless, of course, your dog’s name happens to be J_!*Pw$^hPX.

Common methods of physically generating randomness include flipping coins, where heads is one and tails is zero. As explained earlier, to a computer, private keys are just binary numbers, 1s and 0s. Though it is difficult and nerdy, it is entirely possible to do the math from that point on with pen and paper, once you have found a source of randomness.

When you have successfully generated the private key, you can now derive the public key and then the addresses. Your wallet software will do this for you automatically, but you should probably know a little bit about how that happens.

### Public Keys & Addresses

In the last section, we introduced hash functions. When your wallet is generating public keys and addresses, the public key is double hashed using SHA-256 and

RIPEMD160. This public key hash is then encoded in Base58 format. Using Base58 format helps protect against errors by making it easier for humans to read. Once this is completed, you have a bitcoin address!

As you will learn about in the next section, Clients, Wallets, and Key Management, these keypairs and addresses used to be generated on an independent basis. If you wanted to use a fresh bitcoin address, you would need to generate another key pair, and back it up as well! Now keys are generated in a hierarchical tree structure, with master keys and child keys and grandchild keys. We will talk about that more later.

As long as you have your private key, you will be able to re-generate the public keys and addresses associated with it. However, the reverse is not true: you cannot derive the private key from a bitcoin address or public key. This is one of the great features of Bitcoin, because it means you can share your bitcoin address without risking the security of your funds, just like you can share your public key without compromising the security of your messages.

## ♦ Transactions & UTXOs

By the end of this section,  you should be able to answer the following questions: How are funds accessed and transferred on the Bitcoin network? What are transaction inputs and outputs? What is an Unspent Transaction Output?

### Transactions

As we talked about in the previous sections, a bitcoin address is ultimately derived from your private key, and the private key is used to generate digital signatures that authorize transactions. A transaction is the transfer of ownership of bitcoin from one address to another.

When you send bitcoin, your wallet will organize the information needed to make the transaction, which follows a standard format. One of the most important rules about transactions is that the transaction must be signed using the correct private key.

Then the transaction must be shared with the rest of the network until it reaches a mining node, which will often include it in the next block on the blockchain as long as it is a valid transaction.

If that miner's block and all its transactions are valid, it is added to the blockchain. The transaction now has one confirmation. It's important that the nodes show that they accept the block by creating the next block in the chain. They show this by using "the hash of the accepted block as the previous hash." A new block is added to the blockchain approximately every 10 minutes.

With one confirmation, the receiver of the bitcoin should be able to see the transacted amount in their wallet, and be able to spend it. Each additional block that references the hash of this block is counted as another confirmation for the transaction. A transaction with six confirmations means that a transaction was included in one block and referenced by five subsequent blocks. Although six confirmations does not mean that payment is guaranteed, six confirmations is considered a solid benchmark for irreversibility in Bitcoin. This is because it would take a lot of computing power to contradict and change the ledger after six confirmations. This relates to mining, which we will talk more about in the mining section.

## UTXOs

Another important thing to understand about bitcoin transactions is that they use what is called an “input-output” model. With a few exceptions, every transaction has at least one input and one output. When a transaction occurs, the outputs of a previous transaction become the inputs.

An output which is yet to be spent, but is available to be spent, is called an unspent transaction output, or UTXO. UTXOs are like chunks of bitcoin that can come in all shapes and sizes. Unlike dollar bills, which have fixed denominations ($1, $5, $10, $20, $100), bitcoin UTXOs can be sent in any denomination.

When you spend bitcoin, you or your wallet will select which UTXOs to spend. Most of the time, the UTXOs you will need to spend will be more than you need for the payment. This is why ‘change addresses’ are important - your wallet will divert the extra bitcoin as its own UTXO chunk change output back into your own wallet, so that you won’t overspend.

Imagine you need to pay someone $12.34. Just like with mixed bills and coins, there are different combinations of UTXOs you could use to pay that amount. The simplest option would be if you just happen to have a UTXO that is exactly $12.34 worth of bitcoin. But that is rarely the case.

Maybe you have a UTXO worth $30, which is too much. In this instance, your wallet would spend the whole $30 UTXO, and generate a change output to return the extra $17.66 back to your address.

Maybe you have a bunch of UTXOs worth $5 each. In this instance, your wallet would spend three of them, and generate a change output to return the extra $2.66 back to your address.

A common question from those new to Bitcoin is, “Why are fees not considered a UTXO?”

If you had to include an additional output to pay a fee, you would need to know ahead of time which address to send the fee to. In other words, you would need to know which miner would include your transaction in the blockchain. Such a requirement would put a wrench in the transaction process and require centralized coordination, which is not what the Bitcoin system is designed for.

## Fees

By the end of this section,  you should be able to answer the question: How do transaction fees work?

One of the popular and complicated discussions around how Bitcoin works has to do with transaction fees. Are fees too high? Too low? Why are there fees at all?

Because Bitcoin is an open network, anyone from anywhere can broadcast transactions to include in Bitcoin's blockchain.

Each block in the blockchain has limited space, up to about 4 megabytes in the case of bitcoin, and so the network must have a way to prioritize transactions.

Since miners are the ones who add transactions to the blockchain, it is up to them to decide, ultimately, which transactions to include. They make their choices based on the fees of the transactions.

Transactions effectively compete with one another for the attention of miners. Miners are incentivized to pick the transactions that pay the highest fee per byte, measured as "sats per byte."

Put more simply, the higher the fee you pay per byte, the more likely it is that a miner will include it. The value of the payment itself does not really matter to miners - it's the fee PER BYTE that they care about. This is why some transactions worth millions of dollars paid pennies in fees, and some small-value transactions paid more.

Another important thing to understand about fees is that they are not set by the network, like Visa or MasterCard or WeChat sets their fees. If Visa says that you must pay a certain fee, you can't really negotiate with them, you just have to pay it. In Bitcoin, it is the sender that sets the fee. Your wallet software will suggest an estimated fee based on the current conditions of the Bitcoin network, but ultimately it is up to the sender to decide what fee to include with their transaction.

Most Bitcoin wallets allow you to set your own fees, while suggesting recommended values based on the current network. Wallets make these recommendations using many factors including your transaction's size, network congestion, and what you choose as the priority of the transaction.

Priority simply means how quickly you want to send the bitcoin.

Larger, more complex transactions need to pay higher fees than smaller, simpler transactions. A complex transaction may have many inputs and outputs. A simple transaction uses few inputs and outputs.

The number of transactions waiting to be confirmed on the network rises and falls based on time of day, week, and even year. Congestion on the network happens when there are more transactions waiting to be confirmed than can fit in the next block. If you need your transaction to be confirmed quickly, you can increase the fee to make it more attractive to miners. On the other hand if it is low-priority and you have plenty of time, you can set the fee lower and save money. Your wallet should be estimating what is a “good” fee based on these factors.

### Fee Estimations

Unfortunately, many wallets use poor fee estimation algorithms. This means the wallets can be tricked into recommending fees that are higher than necessary. For example, if an attacker sends several very high sat-per-byte transactions, even if the network isn’t busy, other wallets may see that fee as evidence of congestion, and increase their own fees. This can create a vicious cycle, where a large percentage of Bitcoin wallets have their fee estimation thrown off. So when algorithms are making decisions like this, being able to set your own fees can be very useful.

If you come across a wallet that still calculates transaction fees based on the value of the payment, you should probably avoid it. Those kinds of calculations are carried over from the centralized legacy banking system, which does tend to make up fees based on the amount being spent.

We hope you now have a much better understanding of fees and how they are calculated. In the next section you will learn about consensus, Bitcoin Improvement Proposals, and forks.

## Consensus & BIPS

As we have mentioned in previous sections, the Bitcoin network is made up of nodes, which are computing devices that run the Bitcoin software and participate in the consensus process.

### Consensus Process

While Bitcoin nodes are operated by individuals and businesses, their participation in the Bitcoin network is interdependent, meaning that the nodes depend on peer connections to learn about new blocks and transactions. In other words, nodes need each other!  However, each node does independently verify information before accepting it.

Decentralization gets strength in numbers, but the network can practically function as long as at least two nodes agree on a common set of consensus rules. This is how Bitcoin was bootstrapped in the first place: Satoshi was the first miner, and then, he/she/they were slowly joined by others who wanted to participate in the experiment.

The genesis block that Satoshi mined on January 3rd, 2009 is the “common ancestor” of all blocks in the Bitcoin blockchain, as well as some of the “forks” of Bitcoin that split off from the original network. We will talk more about the meaning of “forks” in just a bit.

One of the key ways in which nodes maintain consensus is by checking whether any block they come across can be followed backward in time through the chain, until it eventually links to the genesis block: block 0. Since each block references a hash of the block immediately preceding it, there should be a clear, unbroken connection up to the latest block.

Each node is always regulating its relationship with peers. If another node is deemed dishonest, for example, because they have been relaying incorrect information, nodes will restrict communication with that node, up to and including blocking them entirely.

### BIPs

While a set of fundamental characteristics have remained exactly the same over the last decade, many other things have changed through what is called Bitcoin Improvement Proposals, or BIPs.

There is no official organization which is responsible for reviewing, approving, or implementing BIPs; like many open-source software projects, it is informal and community-driven. There is also no formal vote, or at least there is a vote only in the sense of consensus nodes running the software of their choice.

You will not need to memorize all BIPs as part of the CBP exam, as there are dozens, but you will need to have a basic understanding of a few of them, because you will probably encounter them often as a Bitcoin professional and end-user.

BIP-32 is the standard for creating hierarchical deterministic (HD) wallets, a type of deterministic wallet where keys and addresses are generated in a tree-like structure, with the “root” being the master extended key.

BIP-39 is the standard for generating mnemonic seeds which is a more readable and recoverable format for backing up private keys. It allows individuals to add a passphrase during the key derivation process.

BIP-44 is the standard for account hierarchies in deterministic wallets, allowing users to segregate funds for different purposes as well as hold other compatible cryptocurrencies.

BIPs 32, 39, and 44 are the BIPs most important for you to know.

If you don't quite understand the significance of these BIPs yet, or what they proposed, don't worry. You will learn more about these BIPs in the Clients, Wallets, & Key Management section. In the next section, we will talk about what happens when there is a disagreement or break in consensus, an event known as a "fork."

## Forks

By the end of this section, you should be able to answer the question: What are forks?

The term "fork" is carried over from software engineering, particularly open-source projects that use version-control management tools like Git. In that context, a fork is a divergence in software code. When it comes to blockchain systems, forks are also used to describe splits in a blockchain's history or network consensus.

### Soft Forks

A soft fork is a backwards-compatible change. It is backwards-compatible because it allows nodes who don't want to update to the latest version to ignore the changes if they want and continue operating without disruption. As Andreas M. Antonopoulos explains in the talk "Forkology: A Study of Forks for Newbies," soft forks are a 'tightening' of the rules. Therefore, miners that encounter transactions using the new features from a soft fork will still interpret those transactions as valid.

An example of a soft fork was the introduction of Segregated Witness in 2017, after being proposed through BIPs. Remember that BIP stands for Bitcoin Improvement Proposal. BIPs 141 and 144 were about scalability and malleability issues in Bitcoin. Segregated Witness changed the way data is stored on the blockchain. There are other examples of successful soft forks but we won't cover those in this book.

### Hard Forks

In contrast to soft forks, a hard fork forces nodes to make a choice about whether to accept or reject the changes to the network. While soft forks are a tightening of the rules, hard forks are a loosening of the rules. A miner that has not agreed to changes in the consensus rules will consider a transaction using the new features invalid. If a hard fork is controversial, it can become a network or consensus fork, where a portion of the network breaks away to continue with the new rules.

If the new rules continue, a long term chain-split happens, and the two halves of the network form separate blockchains going forward. Both of these blockchains do share a common history. An example of a Bitcoin consensus fork is Bitcoin Cash.

It's worth noting that it is possible for a chain-split to take place without there being any changes to the consensus rules. This is rare though and usually accidental, and the chain that split rejoins the original chain. These abandoned blocks are considered "stale" because they are no longer part of the longest greatest cumulative difficulty chain.

### Code Forks

The most common type of fork is a code fork, where someone copies a piece of software, makes changes, and runs it separately from scratch. The two blockchains may share much of the same software, but they have no common block history or network participants. They do not even share the same genesis block. The changes made may consist of faster average block times or different cryptography. Some examples of Bitcoin code forks include Litecoin, Dogecoin, and Zcash.

## Quiz 4

1. What is the name of the smallest unit of bitcoin?
    a. Nanobit
    b. Bitcent
    c. Millibit
    d. Satoshi
2. A digital signature is proof that the sender controls the correct private key for transacting those bitcoin.
    a. True
    b. False
3. After a block explorer website reports six confirmations for your transaction, your payment is guaranteed.
    a. True
    b. False
4. Transaction fees are usually paid by the recipient.
    a. True
    b. False
5. BIP is an acronym for:
    a. Bitcoin Improvement Protocol
    b. Bitcoin Improvement Proposal
    c. Bitcoin Interchange Protocol

    d. Bitcoin Integration Project

6. Which BIP builds on HD wallets to enable multi-account and multi-asset functionality?
    a. BIP-12
    b. BIP-44
    c. BIP-70
    d. BIP-98
7. Soft-forks force existing clients into changing the consensus rules.
    a. True
    b. False
8. Regarding hard forks, which of the following statements is true?
    a. The 21 million supply limit cannot be changed.
    b. The proof-of-work algorithm cannot be changed.
    c. The block reward cannot be increased.
    d. Anything could be changed in a hard fork.

# Clients, Wallets, & Key Management

## Types of Clients

By the end of this section, you should be able to answer the following questions: What are the different types of clients and how are they used? What is Simplified Payment Validation and how is it used in lightweight clients?

In the first two parts of this section, we will talk about the difference between a client and a wallet.

A Bitcoin client is the software program which acts as an interface – whether on a desktop, laptop, mobile phone, or specialized computing machine – to the Bitcoin network. A client is often bundled with Bitcoin wallet software, which helps private key generation and management. But we will talk more about wallets in the next section.

More advanced clients, especially those that cater to developers, businesses, and miners, may provide information about the state of the network and network events.

In general, there are two main types of clients: full clients and light clients.

### Full Clients

Full clients, also called full nodes, are clients that are able to validate transactions and blocks. A mining node is a full node that performs proof-of-work to produce new blocks.

Overall, full nodes have several purposes:

- Full nodes can look up historic blocks. This helps new nodes to download and organize their own local copy of the blockchain.
- Full nodes can look up transaction history for lightweight clients. Lightweight clients don't have the entire blockchain downloaded. So, full nodes make it possible for people to use lightweight clients, like mobile wallets.
- Full nodes check blocks and transactions to make sure that they are valid before relaying them to peers. The validity of a transaction has to do with Bitcoin's consensus rules. Remember that consensus rules are the rules that all bitcoin nodes must enforce when deciding if a block and the transaction in the block are valid.

An example of a full node client is Bitcoind (Bitcoin Core daemon), also known as the reference client. The original version of Bitcoind was built by Satoshi, and as we learned in the last section, it is maintained and improved upon through a community review process. Due to its stability and reliability, to this day it is still the most popular client with miners.

### Light Clients

In contrast to full clients, light clients store a minimal amount of blockchain data. They don't store enough data to validate transactions and blocks. That is why someone with a light client must either connect it to their own node, or to a node run by a third-party provider. Full nodes participate in the consensus process, whereas light clients rely on full clients to provide them with information about the blockchain and the state of the network.

However, light clients can still perform a minimal amount of validation. They can figure out whether a transaction has been confirmed without having to download the entire blockchain. This is done via Simplified Payment Verification or SPV. SPV is a technique that was originally suggested by Satoshi Nakamoto in the whitepaper.

A light client using SPV only needs to download the block headers, rather than the entire block. A block header is a summary of the rest of a block. The light client requests proof that the block was included and this proof is in the form of a Merkle branch. Remember, a Merkle tree is a data structure that summarizes and verifies large sets of data, and so a Merkle branch is one part of a Merkle tree. In other words, a light client using Simplified Payment Verification needs less trust than clients and wallets that are fully relying on third-party servers.

It's worth recapping what we just learned about full versus light clients. Full nodes participate in the consensus process. Light clients rely on full clients to provide them with information about the blockchain and the state of the network.

If you are still unsure of the difference between full and light clients, take another spin through this section.

## What Is a Wallet?

By the end of this section, you should be able to answer: What is a bitcoin wallet and how are they used?

As you know, bitcoin does not exist in a physical form like gold or paper bills do. It is a fully digital currency. But you may be surprised to learn that bitcoin also doesn't actually exist in a wallet, despite all the talk of "digital cash."

When you use a bank card, your dollars or euros aren't stored in your bank card. Rather, your bank card allows you to access and spend funds that are recorded on a centralized bank ledger, or, if you're lucky, backed by physical paper cash in a bank vault.

While Satoshi originally referred to a "wallet" as a single bitcoin address, later on a wallet became known as a collection of addresses and keys, and the software that manages them. While it may be useful to visualize wallets as a leathery object with pockets, bitcoin wallets are more like keychains. The keys allow you to access bitcoin that are ‘locked up’ on the blockchain, until you generate a digital signature that authorizes it to move to another address. A Bitcoin wallet holds access keys to unlock spendable funds that are recorded as belonging to your addresses on the Bitcoin blockchain.

One person can have multiple wallets. That shouldn’t be too surprising if you think of it in terms of bank cards and keychains. You can have multiple sub-accounts and bank cards, and you could have more than one keychain for different purposes or settings: a keychain for your home, a keychain for your workplace, etc.

Each address in a wallet can collect UTXOs (unspent transactions). From these collections of bitcoin, your wallet software will calculate and display a balance. To make the concept of UTXOs easier to visualize, imagine that each bitcoin address is like a pocket in a wallet. Each pocket can contain a practically infinite combination of these chunks of bitcoin. The balance displayed for that address shows the amount of bitcoin held within that “pocket.” The total balance for your entire wallet is the amount of bitcoin that is spendable by the private keys in your “keychain.”

However, not every wallet must have private keys in it. Some wallets are “watch-only,” meaning that they are used as an interface to keep an eye on certain addresses. They manage public keys, but not the private keys that can be used to spend funds.

## Types of Wallets

By the end of this section, you should be able to answer the following questions: What are the types of bitcoin wallets? What is the difference between deterministic and non-deterministic wallets? How do hierarchical deterministic wallets work?

As we discussed in the last section, a wallet is used to generate and manage keys for your bitcoin. The following is important to keep in mind when you go about choosing a wallet to use.

### Hot, Cold, & Warm Storage

To start, you should consider whether a wallet is “hot” or “cold” These qualifiers refer to whether the private keys are stored on a device connected to the internet or not.

A hot wallet runs on an internet-connected device. This makes hot wallets more accessible, but it also increases the risk that they are exposed to attackers.

A cold wallet stores private keys and signs transactions offline.

Some people also differentiate between “warm” consumer wallets and “hot” business or exchange wallets. A warm consumer wallet is used on an internet-connected device, but it is being used by one person who may turn off their phone or desktop computer now and then. A “hot” business wallet is used as part of a service, and therefore needs to be online most of the time so it can be used by customers. Many businesses in the space use a combination of hot and cold wallets for their funds: hot wallets for day-to-day operations, cold wallets for long-term holdings that don’t need to move frequently. It’s not recommended to put more money in a hot wallet than you would in the leather wallet you carry for fiat.

Now let’s take a closer look at the types of wallets.

### Paper Wallets

First, let’s discuss paper wallets versus software wallets. A paper wallet is literally a sheet of paper printed with a private key and the corresponding public address. They usually include QR codes (a two dimensional bar code) as an easy method for import into a software wallet.

Paper wallets were popular in the early days of Bitcoin, but they are no longer recommended. They aren’t recommended because they encourage address reuse, due to storing only one private key and address at a time. They also don’t handle change addresses, so users must be careful not to destroy paper wallets once they’ve spent bitcoin from them and accidentally lose access to change.  Remember, roses are red, violets are blue, with paper wallets, change often falls through.

The term paper wallet can also be misleading, as most users who generate paper wallets are using software to do so. Of course, you can generate and write down the private key by hand, without using any software, but this is very difficult for the average user and prone to error.

### Brain Wallets

A brain wallet refers to the practice of memorizing private keys. In the past, the term “brain wallet” also referred to people who generated private keys from a non-random set of words. Both of these methods are discouraged as users will lose access to their funds if they forget the private keys, or create private keys that are very easy to guess. In addition, should the owner die, access to the funds will not be recoverable by any designated heirs. And when generating brain wallets, users may fail to introduce sufficient randomness and therefore create private keys that are easy to guess. In 2019 it was shown that the number one password to be breached was 123456.

Paper wallets should not be confused with mnemonic seed backups. Paper wallets store one public-private key pair, whereas mnemonics are human-readable seeds for re-generating multiple keys and addresses.

### Web-based Wallets

In the category of software wallets, there are web-based wallets, otherwise known as browser wallets because they are accessed from a browser. The private keys are stored (hopefully encrypted) by the web wallet provider, and locally within your own browser. This type of wallet requires you to trust that the web wallet operator won't serve you malicious code that compromises your keys. Since browsers are very complex pieces of software that you use to navigate many websites, this is not a very secure way to store private keys. Web-based wallets are hot wallets.

### Desktop & Mobile Wallets

In the category of software wallets, there are also desktop and mobile wallets that run on your device as an application, rather than through a browser. Unless you have configured your desktop or mobile device to be air-gapped, these are almost always warm wallets. An air gapped wallet means the device has never touched the internet. Unless you are a security expert, an air-gapped wallet will require help from a security professional to do properly.

### Hardware Wallets

Hardware wallets are specialized devices that store private keys offline. They can be used in combination with a desktop or web wallet, by connecting them to a computer via USB. They often secure private keys using a PIN and optional passphrase. Popular hardware wallets include Trezor, Ledger, and Coldcard. If a hardware wallet malfunctions, is stolen, or destroyed, the private keys can be restored to a new wallet using the mnemonic seed backup.

### Multisignature Wallets

Finally, a multi-signature or “multi-sig” wallet is a wallet that requires several private keys to authorize transactions. These keys can be owned by the same person, stored across different devices, or held by multiple different people called co-signers. The purpose of a multi-sig wallet is to separate security and responsibility. In a multi-signature wallet, with for example a 2-of-3 scheme, at least two out of three keys are required to authorize a transaction. Multi-signature wallets are ideal for businesses and exchanges.

How you store your private keys matters. Stay safe out there, friends.

## Deterministic Wallets

By the end of this section, you should be able to answer the following questions: What is the difference between deterministic and non-deterministic wallets? How do hierarchical deterministic wallets work?

### Non-deterministic Wallets

In the early days of Bitcoin, there was only one wallet; the wallet that came with the Bitcoin Core daemon. That wallet was non-deterministic. That means that it randomly generated each private / public key pair separately. That meant that every time you created a new address, you had to make sure to back it up as well, or that new key could be lost if the program failed. This is why non-deterministic wallets are sometimes referred to as “just a bunch of keys” wallets, because there was no structure to the key generation process for ease-of-use.

### HD Wallets

The introduction of Hierarchical Deterministic, or HD, wallets after 2011 was a big improvement in recoverability. This is because you no longer needed to make regular backups to safeguard all of your keys. With a deterministic wallet, you only need to back up one master key and you will be able to re-generate all keys and addresses during recovery.

BIP-32 HD wallets have a common starting point for key generation called a root seed. It is ‘hierarchical’ because the relationship between the master private / public key pair and its child or grandchild key pairs forms a tree structure, similar to folders and sub-folders on your computer. That “root seed” or “master private key” is usually sufficient for a full wallet export or import, allowing for migration between different wallets that follow the BIP-32 and BIP-44 standards.

The root seed is made up of simple words to make it easier for people to write down and store and verify. This set of words is called a “mnemonic seed.” It is typically 12 or 24 words that come from standard word lists written in many available languages. We will talk more about how to make these mnemonic seed backups later.

Another advantage of HD wallets is that users can use the public receiving addresses without needing access to the private keys. This allows HD wallets to be used in receive-only scenarios (like on servers), using a different public key and address for each transaction.

BIP-44, “Multi-Account Hierarchy for Deterministic Wallets,” was a further extension of the BIP-32 standard that allows for handling multi-address, multi-account, and even multi-coin wallets. This means that for the same mnemonic seed backup, you could operate a wallet that holds bitcoin, ether, and zcash, for example.

Now you might be asking, what do these mnemonic seed backups look like? How do you go about making them? Where would you store them safely? These questions and more will be addressed in the next section about imports, exports, backups, and recovery.

## Imports, Exports, Backups, & Recovery

By the end of this section, you should be able to answer the following questions: What is a Wallet Import Format? How do you create backups of private keys? What is the recovery process?

### Wallet Import Format

The Wallet Import Format, or WIF, is a way to represent a private key as a base58 string. A base58 string is an encoding method that creates a sequence of numbers and letters which is easy to copy. This is the format used by the wallet in the Bitcoin Core reference client. The format has error-checking to make sure that the conversion was done correctly. There is support for WIF among other wallets, but it is not as popular as the BIP-32 and BIP-39 backup formats.

### Backups & Recovery

As we discussed in the last section, the BIP-32 and BIP-39 standards represent the seed or master private key as a mnemonic sequence of usually 12 or 24 words, built on a word list that was carefully vetted for word length and simplicity. For non-English users, there are currently also BIP-approved word lists available in many other languages.

After you generate a new wallet, the wallet software will often require you to write down your mnemonic seed, before you can send or receive any bitcoin using those keys. This is so that you can recover your wallet and it reduces the risk that you will lose access to your funds. It is very important that you follow these instructions.

This is not an exhaustive guide about how to create proper backups, but here is a short list of important aspects of the process to keep in mind:

- When you copy the list of 12 to 24 words, make sure that you copy all of them, with the correct spelling and the correct order. If you are using a hardware wallet, it should have come with a small blank sheet for your mnemonic seed words.

- Store that piece of paper in a safe, dry place, such as a tamper-evident bag inside a locked safe. For most people, the greatest risk of loss for their bitcoin is simply losing or misplacing their backup by accident. Don’t split up your seed words in different locations, as this increases your risk of accidental loss.
- Your wallet software will probably have you double-check the order of words after you have written them down. They also might have features in the wallet that allow you to test your backup at a later point in time. Take advantage of these features whenever you can. Always make sure to check that you are using the correct wallet software when doing so. You should never respond to a request from the wallet provider to share your mnemonic seed as it is likely coming from a phisher, an attacker who is trying to steal your money.
- Once you have set up your wallet, created your backup, and tested your backup, schedule dates to check that your backups are intact, and also re-test the recovery process.
- These tests may include what action you will take if your phone or hardware wallet is lost, broken, or stolen somehow. As long as you have your backup, you should be able to recover your wallet into any BIP-32 or BIP-39 compliant wallet.

Pamela Morgan’s book *Cryptoasset Inheritance Planning: A Simple Guide for Owners* takes you through this process, whether you are looking for a clear step-by-step guide for making backups, or want to create a bitcoin access plan for heirs.

Different wallets may implement different BIP standards, and even with the ones they share in common, they may have not implemented them consistently. This leads to wallet incompatibility, which can cause unnecessary confusion during recovery.

When you import your private keys or mnemonic seed words that were generated in one wallet, into another wallet, the two wallets may “see” your bitcoin balance differently. Most of the time, your coins are still there and your backup is correct. The problem is that the second wallet has trouble “finding” your coins based on the different way in which it regenerated your wallet. Also, if you were using a wallet with advanced features, some additional data backups may be required to fully recover it into other software.

If you are unsure about the recovery methods of a particular wallet, and which other wallets it may be compatible with, you can check out walletsrecovery.org.

In the event that you use a multi-signature wallet, as we discussed earlier, each private key will need to be backed up in a similar way, and you should still have a recovery plan.

Besides using cold wallets or a multi-signature wallet, there is another way to protect your bitcoin in the event that your mnemonic seed is compromised. In the next section, we will look at passphrases.

## Passphrases

By the end of this section, you should be able to answer the following questions: What are passphrase-encrypted wallets, and what advantages do they provide?

Private keys must remain secret for your bitcoin to be secure. This is very important! Because they must remain private, some people may want to add protection for their mnemonic seed backups.

The BIP-39 standard allows you to add a passphrase during the key derivation process. Most popular hardware wallets support this feature.

As BIP-39 says, “A user may decide to protect their mnemonic with a passphrase.” Passphrases can be a sentence, a string of random characters and symbols, and so on. Passphrases can serve as a form of two-factor authentication. This is because without the correct passphrase, an attacker who gets access to just the mnemonic seed would not have sufficient credentials to spend your bitcoin.

## Blockchain Explorers

By the end of this section, you should understand what a blockchain explorer is and how they can be used to examine blockchain data.

A blockchain explorer is like a browser for blockchain data. They are websites that allow for querying address and transaction information. The operator of a blockchain explorer usually needs to run a full node on the network. The node feeds their data into a database that divides the information based on certain criteria. They then make that information available to others. Some blockchain explorers are run privately by companies, and they may correlate off-chain with on-chain data to perform anti-fraud checks or compliance. Other explorers are available to the public, and vary in terms of the types of transaction information they display.

An average user of Bitcoin may want to use a blockchain explorer to find out more information about a particular transaction or block, whether it’s one of their own or someone else’s. “Has this transaction been confirmed? How many inputs and outputs were there? Which block was this transaction mined in?” These are just a few of the questions that could be answered using a blockchain explorer.

Because of blockchain explorers when you share a bitcoin address with someone they can look up every payment you've received or sent with that address. In other words it is possible to determine other addresses owned by the same person by investigating that address's transaction history.

However, it is important to remember that these blockchain explorers are run by other people using their copy of blockchain data and could be incorrect. Blockchain explorers and transaction APIs are trusted third-parties that could provide inaccurate and.or incorrect information. Because of this, even after a block explorer website reports six confirmations for your transaction, your payment is not guaranteed.

In the next section, we will begin Section 6: Mining, to learn about how bitcoin is actually created, how the blockchain is built, and why this process underpins the security of the network.

## Quiz 5

1. Bitcoind is a full Bitcoin client.
    a. True
    b. False
2. It is possible for people using lightweight clients to use Bitcoin wallets and broadcast transactions without having their own copy of the blockchain.
    a. True
    b. False
3. There is a limit of 25 Bitcoin addresses for every user on the Bitcoin network.
    a. True
    b. False
4. A hot wallet stores private keys and signs transactions offline.
    a. True
    b. False
5. Which BIP builds on HD wallets to enable multi-account and multi-asset functionality?
    a. BIP-12
    b. BIP-32
    c. BIP-44
    d. BIP-70
6. What is BIP-39?
    a. The implementation document for generating mnemonic seeds and passphrases.
    b. The implementation document for making hardware devices compatible with various software wallet interfaces.
    c. The implementation document for generating Reusable Payment Codes, or Paynyms.
    d. The implementation document for generating Reusable Payment Codes, or Paynyms.
7. It is possible to determine other addresses owned by the same person by investigating that address's transaction history.
    a. True
    b. False

# ▼ Mining

## What Is Mining?

By the end of this section, you should be able to answer the following questions: What is the basic value that miners provide to the Bitcoin network? How are new bitcoin created? What is a block reward? What is a coinbase transaction?

The use of the terms "mining" and "miner" in relation to Bitcoin security and consensus dates back to Satoshi Nakamoto's whitepaper itself. In part 6, *Incentive*, Satoshi wrote: "... the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block." This creates motivation for nodes that support the network, and is a way to get coins into circulation. Satoshi compared the "steady addition of a constant amount of new coins" to "gold miners expending resources to add gold to circulation."

This comparison to gold contributed to the perception of Bitcoin as "digital gold." However, this association can be confusing for people when it comes to understanding how Bitcoin mining actually works.

Mining serves three purposes: it provides network security, provides the method of issuing currency, and adds transactions to Bitcoin's public ledger.

### Security

Mining contributes to the security of the network, which is also known as its immutability. Mining impacts security because it requires proof-of-work when adding a block. Generating this proof-of-work involves spending energy to power specialized computing devices. Proof-of-work creates a cost for attackers who want to disrupt the network or reverse transactions. An attacker would have to expend, at the very least, an equal amount of computing power to compete with the longest, greatest cumulative difficulty blockchain.

### Currency Issuance

Mining also acts as a decentralized mint for bitcoin. When miners add a new block to the blockchain, they are rewarded with a set number of new bitcoin. They are also rewarded with the fees from transactions which were included in that block. As of the release of this book, the reward is 6.25 bitcoins per block. The reward started out at 50 new bitcoins per block, but there is a "halving" every 210,000 blocks, or about every four years. So it has been reduced over time to 25, then 12.5, and now at this book's release, 6.25 bitcoin. The reward motivates honest nodes to reach consensus about the state of the ledger. This is because the reward for following the rules and coming to consensus should be more attractive than the potential gain from disrupting the network. It should be more profitable to be honest than dishonest.

### Recording New Transactions

Mining also records new transactions into Bitcoin's public ledger. On average, a new block is produced every ten minutes, and so transactions are confirmed on average within ten minutes. This timing depends on congestion in the network.

As we talked about in the section "Transactions & UTXOs," a transaction is confirmed when it is included in a block. When a transaction has six confirmations it means it has been included in a block that was then followed by five additional blocks and that the transaction is six blocks deep. Therefore, if someone wanted to remove or reverse the transaction, they would need to create an alternative chain of blocks that were generated using an equivalent or greater proof-of-work than the original chain. This would be extremely expensive, and that is why we have not seen such an attack happen in Bitcoin's history to date.

You may also be asking how does someone actually receive the block reward when they mine a block? How do these new bitcoin enter the market?

When a miner builds a candidate block to add to the blockchain, they basically write themselves a check for whatever amount of bitcoin the current block reward is. If their block is verified and accepted by the rest of the network, they win the award of new bitcoin through what is called a coinbase transaction. Not to be confused with Coinbase the exchange, the coinbase transaction is the first transaction to be listed within the block. This first transaction listed in the block awards the miner the current block reward plus any transaction fees.

Miners are allowed to include a coinbase transaction which pays less than the reward, but their block will be rejected if they attempt to pay themselves more. Furthermore, the miner must wait until that transaction has at least 100 confirmations, or is 100 blocks deep, before they can spend the reward.

## Difficulty & Proof of Work

By the end of this section, you should be able to answer the following questions: What is difficulty? How is it adjusted? How are blocks "chained" together? What is proof-of-work?

In the last section, we talked about how proof-of-work is important to the immutability of the Bitcoin blockchain and its transactions. It's important to understand that while Bitcoin's proof-of-work capacity, the amount of energy being used to mine, has been increasing overall, those numbers are in constant flux. Miners join, leave, and rejoin the network due to a number of factors.

In the last section, we also talked about coinbase transactions, which reward miners for successfully adding a new block to the blockchain. But how are these blocks actually chained together?

### The Chaining of Blocks

Blocks are chained together, linking all the way back to the first block, the genesis block. This happens by each block referencing the hash of the previous block. The previous block is also called the parent block. The sequence of hashes linking each block to its parent creates a tamper-evident log. Altering even one block would mean that all of the blocks mined after it would no longer reference it correctly. For example, trying to remove a transaction would show all previous blocks as incorrect, making any tampering obvious. As we talked about in Section 3 “Cryptography Basics,” changing the input to a hash function even slightly will produce an entirely different output.

### Difficulty

Bitcoin uses the SHA-256 hash function in its proof-of-work algorithm. Difficulty is the measure of how much work it will take to find a hash below a given target. This means that a mining device would need to keep generating hashes over and over again until it found one that satisfied the target criteria. The higher the difficulty, the harder it is to reach the target.

In the past, difficulty was low enough that miners could use their home computers. There wasn’t much competition; just a bunch of computer scientists and cryptographers experimenting with a new form of digital money. Eventually, the difficulty rose high enough to make it impractical and unprofitable to mine using general-purpose computing devices. Miners now use special-purpose hardware called ASICs. But we will talk about that more in the next section.

### Hashrates & Difficulty Targeting

How is the hashrate measured? The hashrate is defined as the number of SHA-256 hash calculations per second being generated by miners in the network. At the time this section was recorded, the Bitcoin hash rate was over 100 hashes per second. That is 100 quintillion hashes per second. Here is what that number looks like: 100,000,000,000,000,000,000

As the global hashrate rises and falls, the difficulty is reviewed and adjusted roughly every 2 weeks. To achieve this, all bitcoin nodes analyze the previous 2,016 blocks to see how long it took for all 2016 blocks to be created.

We know that the Bitcoin network targets 1 new block every 10 minutes. That's 6 new blocks every 60 minutes, or 144 new blocks every day. 2016 blocks at an average of 10 minutes is 14 days - or two weeks. If the average block time for this period was less than 10 minutes, the difficulty is increased. If the average block time was more than 10 minutes, the difficulty is decreased.

The difficulty is adjusted to keep the average 10-minute block time as a constant. This helps us comfortably predict the issuance schedule of Bitcoin. At any given time, we not only know exactly what the total supply of bitcoin is, but we can very accurately know how many bitcoin will exist a year from now, ten years from now, and so on.

The difficulty adjustment cycle works like this: If the difficulty becomes too great for some miners, meaning they earn fewer rewards, they may leave the network. However they usually don't drop out entirely; instead they shut off their older, less efficient machines. If enough miners leave the network, block times will slow down, because the difficulty was set at a higher hashrate that has now decreased. When the next adjustment comes, the difficulty will be reduced. Therefore, the miners who previously left can now rejoin the network. If a lot of miners and hash power joins, then blocks may start being mined faster than the 10-minute average. When another adjustment comes, the difficulty will be increased, so that the block time falls back closer to the 10-minute average.

An easier way to visualize Bitcoin's proof-of-work algorithm is the Sudoku puzzle example used in Chapter 2 of 'Mastering Bitcoin.'

Imagine there is a Sudoku puzzle competition and whoever solves the puzzle first wins. A puzzle with a 9x9 grid is much easier to solve than a puzzle with a 27x27 grid. As more and more people apply to participate in the Sudoku puzzle competition, the organizers increase the complexity of the puzzle.

Now imagine that some of the contestants in the competition develop machines to automate the solving of Sudoku puzzles. Do you think you would be able to compete against a machine that specializes in solving Sudoku puzzles?

This is a simplification of the dynamic that has emerged over the last decade, as Bitcoin miners moved from CPU mining to ASIC mining.

## Mining Pools & Hardware

By the end of this section,  you should be able to answer the following questions: What is a mining pool? What are the advantages and disadvantages compared to solo mining? What mining hardware is used today? What are the differences between CPU, GPU, and ASIC?

As a miner, one of the decisions you make is whether to mine solo or participate in a mining pool. There are pros and cons to both, and depend on factors like your geographic location, access to cheap energy resources, and your ability to invest significant capital in a mining operation.

## Solo & Pooled Mining

A solo miner takes on all the costs of equipment, maintenance, and the associated operating responsibilities, like power usage. On the other hand, pooled mining has multiple clients contribute to the creation of a block.

In pooled mining, the reward is split based on how much hashrate each individual miner contributed. While your share of the reward will be much smaller, pooled mining can make these payouts much more consistent over time, as the combined hashrate of the pool can compete with large, solo mining operations. Pooled mining is more suitable for beginners and those with less capital.

## ASIC Mining

It’s important to note in the context of solo versus pooled mining that we are focusing on the current state of the network, but mining wasn’t always a multi-billion dollar industry. In the first couple years of Bitcoin’s existence, it was possible to mine bitcoin using your laptop or desktop’s Central Processing Unit or CPU. Satoshi wrote in the whitepaper: “Proof-of-work is essentially one-CPU-one-vote.”

However, this was not possible for very long at all. By the end of 2011, miners had already upgraded their setups multiple times. And by 2013, application-specific integrated circuits (ASICs) chips made specifically to mine bitcoin, became the foundation of this growing industry. Instead of college students mining out of their dorm rooms, entire companies were being set up in key locations around the world just to mine bitcoin. Incentivized by the reward that Bitcoin offers, there is a lot of research into mining hardware, energy sourcing, and efficiency.

With the success of ASIC mining, there was a growing concern about centralization. A significant portion of the mining industry was based in areas of China. Being based in China made these businesses very close to the chip manufacturers, giving them an advantage to get newer, better hardware and replacements faster than computers in the United States or Europe. Also, the distribution of energy in certain areas was underdeveloped or non-existent. Therefore, these mining companies used energy that would have otherwise been wasted, making it particularly cheap, an advantage over miners in countries with expensive electricity costs. This is why mining operations have also become popular in Iceland with geothermal energy, the Canadian province of Quebec with hydropower, and some South American countries where electricity is subsidized.

For a couple of years, there was a lot of fear and discussion about what would happen if one of these powerful mining companies managed to gain 51% or more of the Bitcoin network's hashrate.  What would it look like and how likely is it that such an attack could be launched, will be discussed in the next section.

## 51% Attacks

By the end of this section, you should be able to answer the following questions: What is a 51% attack? What could a potential attacker do with majority hashing power?

In the Bitcoin whitepaper, Satoshi wrote: "As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the  longest chain and outpace attackers."

They also wrote: "If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes."

### Honest versus Dishonest Nodes

The descriptor "honest" is used 15 times throughout the Bitcoin whitepaper. The definition of an "honest node" is not stated explicitly, but it is implied that an honest node is one which follows the consensus rules and only relays valid transactions to peers. By contrast, a "dishonest" node may try to disrupt its peers and the wider network by spreading false information. An example of this is if a dishonest node tried to double-spend. To double-spend means exactly what it sounds like- an attempt to spend the same money twice.

### Attacks

Throughout this section, we have talked a lot about incentives. Satoshi was careful about making promises about how resistant Bitcoin was to attack, but they believed that the block reward would encourage nodes to "stay honest."  Satoshi thought that miners would find it more profitable to follow the rules rather than undermine the system as that would invalidate their own wealth.

This type of attack came to be referred to as a 51% attack. A 51% attack is where one entity gains control of a majority of the hash rate on the Bitcoin network, and causes network disruption. The idea that some mining companies would have an advantage because of location during the same time as the increase of ASICs over CPUs, prompted many discussions about the potential for takeover.

If a majority of the hashrate was controlled by a single entity, they may attempt to prevent transactions from confirming, re-write transaction history, and double-spend.

It is very important to understand that controlling 51% of the hashrate does not guarantee an attack, although it does increase the probability that an attack may be successful. In fact, this sort of attack could be attempted with less mining power, but the odds of success would be extremely low.

A 51% attack doesn't give full power over the Bitcoin network. The older a transaction is, the more secure it is. It would be very expensive for an attacker to change transactions older than the last few blocks. Also, the attacker would still be held to the rule requiring at least 100 confirmations to spend the block reward.

Obviously, there is no central authority to stop these theoretical attacks. But, there is also no authority to force the rest of the network to continue using a co-opted chain. Therefore the long-term success of this takeover would be very unlikely and costly.

In summary, if a 51% attack was successful, the attacker could potentially:

- Prevent specific transactions from being confirmed
- Reverse recent transactions
- Double-spend their own bitcoin
- Prevent other miners from discovering blocks
- Reduce confidence in Bitcoin and deflate the currency’s value

In the next section, we will begin the seventh and final section of this book, “Bitcoin Commerce.”  The next section will be more of a practical guide on how to use bitcoin and interact with payment processors, merchants, and exchanges.

## Quiz 6

1. Which hashing algorithm is used in Bitcoin's proof-of-work scheme?
    a. HashCash
    b. AES
    c. SSL
    d. SHA-256
2. What does the acronym "ASIC" stand for?
    a. Application Specific Integrated Code
    b. Application Specific Integrated Circuit
    c. Application Summation Integrated Circuit
    d. Addition Summation Integrated Circuit
3. With 51% of the network hashing power a group of miners can double-spend any transaction only from the previous block.
    a. True
    b. False

# Bitcoin Commerce

## Using Bitcoin

By the end of this section, you should be able to answer the following questions: How do you get bitcoin? How do you use bitcoin? Where can you use bitcoin?

There are four main ways to acquire bitcoin, some more challenging than others: mining it, earning it, buying it, and winning it.

### Mining Bitcoin

As we discussed in the last section, mining a block on the Bitcoin network earns rewards: the new coins minted in that block, plus the fees for all transactions included in that block.

Once mined, these rewards can be spent after 100 confirmations. Mining can be a very direct and private way to earn bitcoin. However, it can require a lot of money to get started, and even more if you want to be profitable.

### Earning bitcoin

Another way to get bitcoin is to earn it through your work. Whether you are self employed, a freelancer, or an employee, you can offer your products and services in exchange for bitcoin. Ask your employer if they can pay your salary fully or partially in bitcoin. Your employer doesn't even need to have bitcoin themselves, as there are services now to convert payroll automatically into bitcoin or vice versa.

### Buying bitcoin

When you ask how to get bitcoin, a lot of people will say to buy it. There are dozens of exchanges in so many countries now where you can do so, with credit cards, debit cards, wire transfer, as well as cash. However, unless you are buying it directly from another person, you need to be very careful about which service you choose. As we talked about in the section about exchanges, most of them will require you to provide sensitive identifying information. And you have to trust that they will safeguard your personal information against cyber attacks.

This is why many people buy their first bitcoin from someone they know, or at a local meetup.

### Winning bitcoin

Finally, another way to acquire bitcoin is through donations, or as a prize for winning a contest or game. There are websites like satoshis.place and LN Games, which besides being a fun way to use bitcoin, has the secondary benefit of testing out the Lightning Network and helping developers to improve it.

### Pricing in bitcoin

Regardless of which avenue you use to acquire bitcoin, you will need to understand how it is priced, and the implications of price volatility in a given week, month, or year. As with many other goods and services, the price of bitcoin is determined by supply and demand.

The current price of bitcoin in any other currency is whatever a buyer was willing to pay, and a seller was willing to accept. The average of many such transactions, across many markets, is shown on various sites as the current price.

### Volatility

The price of bitcoin is still quite volatile, changing by hundreds or thousands of dollars sometimes, but over time, we've seen that its volatility has gradually decreased, As the economy that Bitcoin serves grows, bitcoin's price becomes more stable, or at least predictable.

Imagine that transactions and market events are like pebbles. Throwing a pebble into the puddle that was Bitcoin's economy in the early years would cause a great splash. Now that Bitcoin is more of a pond, the effect is not so great. And once it is more like an ocean, encapsulating trillions of dollars in economic activity and savings, any given buy or sell will become almost insignificant.

Similarly, the value of fiat currencies also fluctuate, depending on the political influence and stability of the governments that back them. Since the U.S. dollar is considered a global reserve currency, it is relatively more stable compared to many other national currencies. Despite its lack of official backing by any government, Bitcoin supports a digital economy in which many people are now able to earn a living and support their families in ways that they couldn't have before, due to all the hurdles on monetary transfers across borders or even accessing banking facilities.

## Payment Processors

By the end of this section, you should be able to answer the following questions: What is a payment processor? What services do they provide? Are products / services priced in bitcoin or fiat? How does volatility affect pricing?

Whether you are a bitcoin user, or someone who accepts bitcoin as part of your business, at some point you will come across a payment processor. A payment processor is a software or a service that accepts and manages incoming payments from customers. These payments can be in either bitcoin or fiat, but for the remainder of this section, we will focus on bitcoin being the form of payment.

From the customer's perspective, payment processors for bitcoin and other cryptocurrencies basically operate in the same way as fiat-based processors.

In the background, there are a variety of ways that the processor can handle bitcoin it receives on behalf of the client. The bitcoin can simply be forwarded to the business client's own bitcoin wallet. Or, with a third-party processor, the bitcoin can be converted into a particular national currency, and then forwarded to a fiat bank account. That way, a business could potentially accept bitcoin without ever needing to figure out how to manage it themselves.

Most payment processors are third-party, custodial software-as-a-service businesses. Just as you want to be careful about which exchange you choose to trust, you want to be aware of the important differences between payment processors, based on what is most important to you.

For example, what payment methods does the processor work with? Does it take Visa, MasterCard, or American Express? What about PayPal, Alipay, or WeChat Pay? Does it accept any other cryptocurrencies besides bitcoin?

You should also consider the processing steps: What percentage of the payments do they keep as processing fees? How long will your funds be locked before you can withdraw them?

Then there are security considerations: Does this payment processor have a good reputation for keeping clients' funds safe? How do they handle fraud protection? Do they have a good understanding of coin management techniques, such as batching, to avoid high on-chain fees?

If you don't want to trust your business funds with a third party, there is also self-hosted payment processing software that merchants can use without relying on third parties, like BTCPay Server. Though it may be a little scary and challenging to be responsible for handling your own setup and maintenance, with BTCPay Server, you will have full control not only over the money you receive from customers, but also potentially sensitive information about your customers.

Whichever path you take, you will have to deal with a very important question: How should your goods and services be priced, in bitcoin or in fiat?

Even though the price volatility of bitcoin is decreasing over the long-term, it will be a while before bitcoin can be an effective unit of account. Until then, most people will still judge its value in fiat terms. Products and services will almost always be priced in the local currency where the merchant is based, even if they accept bitcoin or other cryptocurrencies as payment.

There are two main reasons for this: price volatility, and tax accounting. As the price of bitcoin can fluctuate significantly in a short period of time, it'd be difficult to adjust the price of products to reflect that. Merchants want to prevent customers today being 'over-' or 'undercharged' compared to customers who visited your shop just yesterday. So when you are buying things with bitcoin, you will see the fiat price displayed, which is then converted into a bitcoin based on real-time price data when you go to finalize the purchase.

Ideally the payment processor you use should be keeping a record of the fiat value of bitcoin when they receive it. This also simplifies accounting and tax reporting obligations. Businesses must keep records of their payables and receivables in the currency that is recognized and accepted by tax authorities, regardless of whether they are accepting fiat or cryptocurrencies. That also goes for customers, as spending bitcoin can be a taxable event that needs to be reported.

This has been a brief look into the questions and challenges that Bitcoin payment processors have to deal with. In the next section, we will look at how merchants can use bitcoin in their businesses.

## Merchants

By the end of this section,  you should be able to answer the following questions: How can merchants begin accepting bitcoin for products and services? How many confirmations should it take before a payment is considered settled?

Since Bitcoin is peer-to-peer, and so much of the software tools are open-source, anyone can become a merchant. Accepting bitcoin payments in exchange for goods and services in your business is as easy as providing your customer with a payment request in the form of an address or QR code.

As we discussed in the last section, ideally you will want to use payment processors that record the time and date, amount, and fiat denominated conversion relevant to your jurisdiction. You will also want to establish a policy for refunds, as for the most part you would not want to return the bitcoin to the address it came from. Depending on the amount of time that has passed, you cannot always be sure that the customer still has the keys for previously used addresses, and it is also not a good idea to reuse addresses.

We've talked about how it becomes harder to reverse a transaction the more confirmations it has. When accepting bitcoin as part of your business, a very important question to ask is: How many confirmations should a transaction require before a purchase is considered "settled"? The answer will vary depending on the value of the purchase, and the general risk of fraud.

For example, it's not a good idea to transfer the ownership of your car based on a transaction with zero confirmations, sent by someone you don't know very well. It would also be tedious to wait for six confirmations on a cafe latte with a customer who is a regular. Online stores that accept on-chain bitcoin transactions tend to have you wait about 10 to 15 minutes for one confirmation before they consider your purchase order to be "settled." However 10 to 15 minutes can be a bit too long for physical stores. This is why Lightning, a second-layer micropayments network for Bitcoin, is becoming the preferred method of payment for relatively low-value purchases.

We will not be covering the Lightning Network in this book, but if you are interested in learning more about it, feel free to sign up for the C4 mailing list on the C4 website so that you can be notified when our Certified Lightning Network Professional exam is released. You can also find several sections on the Lightning Network on our YouTube channel.

So, why is it a bad idea for merchants to consider an on-chain payment "settled" before it is actually confirmed? Well, the answer is pretty simple. Until that transaction is included in a block, that bitcoin will not be spendable by your keys. You do not own that bitcoin yet because you do not control it. Between the time that a customer authorizes the transaction and it is recorded in the blockchain, some things could go wrong, especially if that customer is trying to defraud you.

In a Bitcoin race attack, a malicious actor could broadcast two transactions: one pays you, the merchant, and the other sends the bitcoin to another address they control. Both transactions are "racing" to be confirmed in the blockchain. If the transaction to you is confirmed first, then the sale goes through legitimately and there is no fraud. If the other transaction goes through first, then you would not receive the bitcoin. However, your wallet may have seen the first transaction appear on the network and accepted it as valid, even though it hasn't been confirmed. If you have already provided access to the product or service, then you've been defrauded.

Most wallets prevent their users from trying to spend the same coins twice, but this attack can still be possible. Keep in mind that this type of attack does not actually "reverse" a transaction. This type of attack creates two transactions at the same time, spending the same coins, where only one of them will go through. This attack requires no expenditure of energy or control of hashrate. It is not guaranteed to succeed either. Whether the attack is successful depends on which transaction propagates faster through the network, until it reaches a miner.

It is worth noting that there are legitimate reasons for a user to resend a transaction that attempts to spend the same coins. If a transaction's fee is too low, it may take longer than expected to confirm. Some wallets have a feature called "Replace-by-Fee" (RBF), where you can resend a transaction with a higher fee to incentivize miners to include it. Regardless of which transaction gets confirmed first, the coins will not be double-spent, the alternative transaction will simply be ignored as invalid, since those coins have now been recorded in the blockchain as spent.

## Exchanges

By the end of this section, you should be able to answer the following questions: What is a bitcoin exchange? Who uses them and why?

We have touched on exchanges a few times during this book, particularly in the section about the digital economy. But now we want to look at exchanges from an economic perspective rather than a technical one.

Exchanges are marketplaces where assets and national currencies can be bought and sold or traded. There are different types of exchanges that will appeal to different needs and use cases. The main types are: centralized custodial, decentralized non-custodial, over-the-counter (OTC) desk, and in-person peer-to-peer.

Exchanges are not only used by people who work as traders for a living, they are used by anyone who wants or needs to trade one asset or currency for another. New people who may just want to learn about this technology could sign up to an exchange to buy their first bitcoin, or even better visit a local meetup and conduct a peer-to-peer exchange with an organizer. Remote workers may use exchanges to regularly convert their bitcoin paycheck into their local currency because that is more reliable than using wire transfers. Citizens of countries experiencing hyperinflation may use exchanges to protect their savings from devaluation. There is nothing preventing someone from using more than one exchange, or more than one type of exchange, to fulfill different needs and use cases in their lives.

Regardless of which option you choose, many of the mechanisms and vocabulary you may encounter are very similar, even if the architecture differs between exchanges.

On many exchanges, the interface or terminal will display what is called an orderbook. This orderbook will list available bids and asks. Bids are quotes to buy at a particular price, while asks are quotes to sell at a particular price. Of course, those who are posting asks, orselling will want the highest price possible, while those posting bids, or buying will probably want the lowest price possible. The difference between these two prices is known as the "spread." For example, if the ask price is $10,000 while the bid price is $9,000, then that exchange has a spread of $1,000. Orders will start being filled as one side or the other agrees to compromise. This is known as "closing the spread," where bids and asks begin to converge closer and closer. If many trades are conducted successfully, it may be reported that the exchange has high volume, which is the amount of an asset, currency, or security that is traded in a given period of time.

We would once again like to remind you that it is important to understand the associated risks, especially when it comes to storing your bitcoin on an exchange. If the exchange suffers a cyber attack or loses the keys, there is no way to recover your bitcoin. This is where the phrase, "not your keys, not your coins" comes from. On the other hand, if you are unfamiliar with how Bitcoin works and how to secure your own keys, self-custody can seem like a daunting task. This is why customer support and educational services are vital

## Quiz 7

1. What is a Bitcoin payment processor?
    a. A high-security bitcoin storage service.
    b. A web-based application that allows you to buy/sell bitcoins.
    c. A service or application that accepts bitcoin payments from your customers, organizing (forwarding ) the received funds to you in either bitcoin, local currency, or both.
2. The only way for merchants to accept Bitcoin is through a third-party bitcoin payment processor
    a. True
    b. False

3. Which statement is NOT true regarding merchants who accept bitcoin for goods and services?
    a. Merchants can accept bitcoin without using any 3rd parties if they choose to manage their bitcoin themselves.
    b. Merchants can use Bitcoin payment processors to convert their local currency and/or bitcoin.
    c. Merchants who accept bitcoin should pay attention to local laws and regulations.

## Conclusion

Congratulations! You have now learned the relevant content areas of the CBP exam.

Once you feel confident that this book and your own studying has adequately prepared you to prove your knowledge, take the final step on the road to becoming an official Certified Bitcoin Professional and sign-up online.

There are some things money can't buy. For everything else, there's bitcoin!

We value your feedback. If you have any comments or suggestions about this CBP Exam Prep book, please share them with us here:
https://forms.gle/oCUynfXp2RqtnY1E6

## Figures

Fig. 1 Decentralized Network

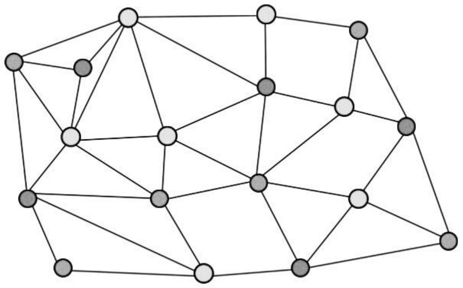


Fig. 2 Centralized Network

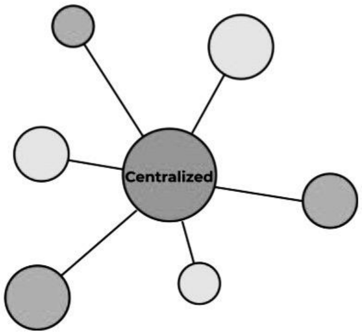


Fig. 3 Encryption

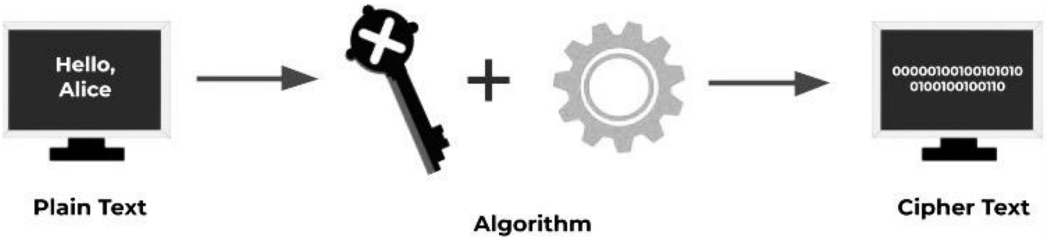


Fig. 4 Decryption

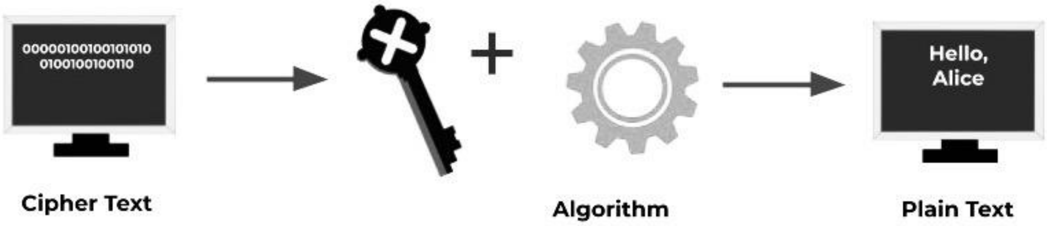


Fig. 5 Symmetric Cryptography

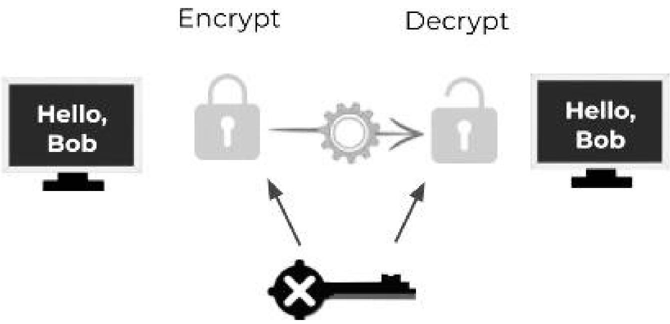
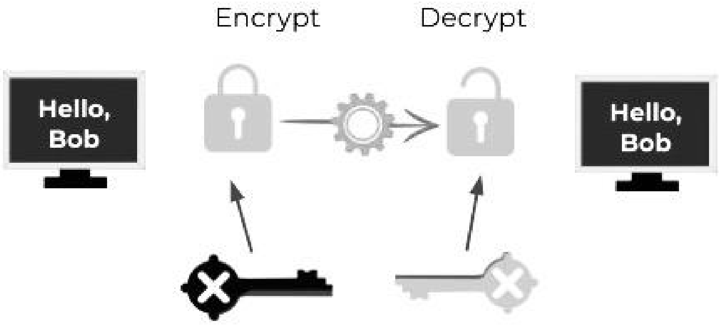


Fig. 6 Asymmetric Cryptography



## Glossary of Terms

During this CBP prep course you will encounter some complicated terms. To help clarify these terms, consistent icons are used in the course videos. Familiarize yourself with this alphabetized glossary and keep it handy as a reference.

**51% attack**

A 51% attack is where one entity gains control of a majority of the hash rate on the Bitcoin network, and causes network disruption.

**address**

A Bitcoin invoice address, or simply invoice, is an identifier of 26-35 alphanumeric characters, beginning with the number 1, 3 or bc1 that represents a possible destination for a bitcoin payment.

**bitcoin**

bitcoin with a lowercase 'b' is the name of the currency unit (the coin)

**BIP**

Bitcoin Improvement Proposals. A set of proposals that members of the bitcoin community have submitted to improve bitcoin. For example, BIP-21 is a proposal to improve the bitcoin uniform resource identifier (URI) scheme.

**block**

A grouping of transactions, marked with a timestamp, and a fingerprint of the previous block. The block header is hashed to produce a proof of work, thereby validating the transactions. Valid blocks are added to the main blockchain by network consensus

**Blockchain**

A list of validated blocks, each linking to its predecessor all the way to the genesis block.

**Byzantine Generals Problem (BGP)**

A reliable computer system must be able to cope with the failure of one or more of its components. A failed component may exhibit a type of behavior that is often overlooked—namely, sending conflicting information to different parts of the system. The problem of coping with this type of failure is expressed abstractly as the Byzantine Generals Problem.

**centralized**

A network where a central entity is necessary to provide parts of the offered services, such as coordination and discovery.

**coinbase transaction**

The first transaction in a block. Always created by a miner, it includes a single coinbase. Not to be confused with Coinbase.

**client**

Bitcoin software that manages connections and operations on the Bitcoin network

**cold wallet (cold storage)**

Cold storage in the context of Bitcoin refers to storing Bitcoins offline and spending without the private keys controlling them ever being online.

**consensus**

The decision of which chain to follow is called consensus.

**decentralized**

A network where no central entity controls, or is necessary to provide, parts of the offered services, such as coordination and discovery.

**difficulty**

Difficulty is a measure of how difficult it is to find a hash below a given target.

**difficulty target**

A difficulty at which all the computation in the network will find blocks approximately every 10 minutes.

**digital signature**

A digital signature algorithm is a mathematical way to show the 'authenticity' of a digital message.

**fees**

The sender of a transaction often includes a fee to the network for processing the requested transaction. Most transactions require a minimum fee of 0.5 mBTC.

**fork**

Fork, also known as an accidental fork, occurs when two or more blocks have the same block height, forking the block chain. Typically occurs when two or more miners find blocks at nearly the same time. Can also happen as part of an attack.

**genesis block**

The first block in the blockchain, used to initialize the cryptocurrency.

**hash functions**

Cryptographic hash functions are mathematical operations run on digital data; by comparing the computed "hash" (the output from execution of the algorithm) to a known and expected hash value, a person can determine the data's integrity. A one-way hash function generates an output that is practically impossible to reverse without knowing the input data.

Bitcoin uses SHA-256 and RIPEMD-160 hash functions.

**hot wallet**

A hot wallet refers to a Bitcoin wallet that is online and connected in some way to the Internet. It is a term that refers to bitcoins that are not being kept in cold storage.

**immutability**

the state of not changing, or being unable to be changed

**miner**

A network node that finds valid proof of work for new blocks, by repeated hashing.

**multisignature**

Multisignature (multisig) refers to requiring more than one key to authorize a bitcoin transaction.

**node**

Any computer that connects to the Bitcoin network is called a node.

Nodes that fully verify all of the rules of Bitcoin are called full clients.

**seed phrase (mnemonic seed)**

A seed phrase is a list of words which stores all the information needed to recover Bitcoin funds on-chain. Wallet software will typically generate a seed phrase and instruct the user to write it down on paper. If the user's computer breaks or their hard drive becomes corrupted, they can download the same wallet software again and use the seed words to get their bitcoins back.

### pooled mining

Pooled mining is a mining approach where multiple generating clients contribute to the generation of a block, and then split the block reward according to the contributed processing power.

### private key (secret key)

A private key in the context of Bitcoin is a secret number that allows bitcoins to be spent. Every Bitcoin wallet contains one or more private keys, which are saved in the wallet file.

### proof-of-work (PoW)

Satoshi states that the integrity of the chain of blocks is protected by a requirement to contribute computing power. This proof that the computer is working and putting forth effort, known as proof-of-work, is necessary to build blocks into the future, as well as to modify the past should anyone attempt to do so. The longest chain represents the majority decision, or in other words the greatest proof-of-work.

### public key

The public key is used to receive funds, similar to a bank account number. Digital signatures can be validated against the public key without revealing the private key.

### satoshi

A satoshi is the smallest denomination of bitcoin that can be recorded on the blockchain. It is the equivalent of 0.00000001 bitcoin and is named after the creator of Bitcoin, Satoshi Nakamoto.

### Satoshi Nakamoto

Satoshi Nakamoto is the name used by the person or people who designed Bitcoin and created its original reference implementation, Bitcoin Core. As a part of the implementation, they also devised the first blockchain database. In the process they were the first to solve the double-spending problem for digital currency. Their real identity remains unknown.

**timestamp server**

Satoshi writes in the white paper “The timestamp proves that the data must have existed at the time…to get into the hash. Each timestamp includes the previous timestamp in its hash.” The timestamps form a chain, and each new timestamp reinforces the ones before it.

**transaction**

In simple terms, a transfer of bitcoin from one address to another. More precisely, a transaction is a signed data structure expressing a transfer of value. Transactions are transmitted over the bitcoin network, collected by miners, and included into blocks, made permanent on the blockchain.

**unspent transaction output (UTXO)**

UTXO is an unspent transaction output that can be spent as an input in a new transaction.

**wallet**

A wallet is a collection of addresses and keys, and the software that manages them. Wallets are NOT always on a mobile device, but for this course we will use this icon to represent a Bitcoin wallet.

**wallet import format (WIF)**

WIF or Wallet Import Format is a data interchange format designed to allow exporting and importing a single private key with a flag indicating whether or not it uses a compressed public key.

*Definitions are pulled from Andreas M. Antonopoulos’ *Mastering Bitcoin*, Bitcoin Wiki, and Paige Peterson.

# Quiz Answer Key

## Quiz 1 Key

1. Which function of money is gold most often used for?
   a. Medium of Exchange
   b. Unit of Account
   **c. Store of Value**
   d. Tax Collection
2. Which property of money is NOT necessary for an asset to be used as a medium of exchange?
   a. Scarcity
   b. **Government Backing**
   c. Ease of Transmission
   d. Fungibility
3. In order to accurately record balances and transactions, a trusted centralized party is required to curate the ledger.
   a. True
   **b. False**
4. When was the Bitcoin whitepaper published?
   a. **October 31st, 2008**
   b. October 31st, 2009
   c. January 3rd, 2008
   d. January 3rd, 2009
5. This person created *HashCash*, one of the Bitcoin precursors, and was cited in the Bitcoin whitepaper.
   a. Nick Szabo
   b. David Chaum
   **c. Adam Back**
   d. Both A and B
6. What is the Byzantine Generals' Problem (BGP)?
   a. A problem where network participants are unreliable or transmit imperfect information which causes system failure.
   b. A computer strategy game similar to Civilization, which pays winners in bitcoin.
   c. A set of problems that members of the Bitcoin community have submitted to improve Bitcoin.
   d. When several nodes have the same blocks in their locally-validated best blockchain.
7. When was the genesis block mined?
   **a. January 3rd 2009**
   b. October 31st 2009
   c. January 3rd 2008

    d. October 31st 2008

8. Mt. Gox was an early Bitcoin exchange that shut down because the Bitcoin network failed.
    a. True
    **b. False**

## Quiz 2 Key

1. In order to accurately record balances and transactions, a trusted centralized party is required to curate the ledger.
    a. True
    b. **False**
2. What is an altcoin?
    a. A token created by the Cambridge Centre For Alternative Finance
    b. A cryptocurrency only issued by governments
    c. **A blockchain-based digital currency based on the concept of, but seperate from, Bitcoin.**
3. Mt. Gox was an early Bitcoin exchange that shut down because the Bitcoin network failed.
    a. True
    b. **False**

## Quiz 3 Key

1. What is cryptography?
    a. Cryptography is the name of the algorithm that secures Bitcoin private keys.
    b. Cryptography is a routing mechanism.
    c. **Cryptography is the science or study of the techniques of secret writing.**
    d. Cryptography compresses the size of the Bitcoin blockchain.
2. In symmetric cryptography, the key is a piece of information that is used to encrypt a message
    **a. True**
    b. False
3. A private key can be derived from a public key.
    a. True
    **b. False**
4. Cryptographic hash functions are used in the Bitcoin protocol to ensure data integrity.
    **a. True**
    **b.** False

5. What basic components of a cryptocurrency provide security and anti-counterfeiting measures?
    a. Digital signatures
    b. Public key infrastructure
    c. Hash functions
    d. All of the above

## Quiz 4 Key

1. What is the name of the smallest unit of bitcoin?
    a. Nanobit
    b. Bitcent
    c. Millibit
    d. **Satoshi**
2. A digital signature is proof that the sender controls the correct private key for transacting those bitcoin.
    **a. True**
    **b.** False
3. After a block explorer website reports six confirmations for your transaction, your payment is guaranteed.
    a. True
    **b. False**
4. Transaction fees are usually paid by the recipient.
    a. True
    **b. False**
5. BIP is an acronym for:
    **a.** Bitcoin Improvement Protocol
    **b. Bitcoin Improvement Proposal**
    **c.** Bitcoin Interchange Protocol
    **d.** Bitcoin Integration Project
6. Which BIP builds on HD wallets to enable multi-account and multi-asset functionality?
    **a.** BIP-12
    **b. BIP-44**
    **c.** BIP-70
    **d.** BIP-98
7. Soft-forks force existing clients into changing the consensus rules.
    a. True
    **b. False**
8. Regarding hard forks, which of the following statements is true?
    **a.** The 21 million supply limit cannot be changed.
    **b.** The proof-of-work algorithm cannot be changed.
    **c.** The block reward cannot be increased.
    **d. Anything could be changed in a hard fork.**

## Quiz 5 Key

1. Bitcoind is a full Bitcoin client.
    - **a. True**
    - b. False
2. It is possible for people using lightweight clients to use Bitcoin wallets and broadcast transactions without having their own copy of the blockchain.
    - **a. True**
    - b. False
3. There is a limit of 25 Bitcoin addresses for every user on the Bitcoin network.
    - a. True
    - **b. False**
4. A hot wallet stores private keys and signs transactions offline.
    - a. True
    - **b. False**
5. Which BIP builds on HD wallets to enable multi-account and multi-asset functionality?
    - **a.** BIP-12
    - **b.** BIP-32
    - **c. BIP-44**
    - **d.** BIP-70
6. What is BIP-39?
    - **a. The implementation document for generating mnemonic seeds and passphrases.**
    - b. The implementation document for making hardware devices compatible with various software wallet interfaces.
    - c. The implementation document for generating Reusable Payment Codes, or Paynyms.
    - d. The implementation document for generating Reusable Payment Codes, or Paynyms.
7. It is possible to determine other addresses owned by the same person by investigating that address's transaction history.
    - **a. True**
    - b. False

## Quiz 6 Key

1. Which hashing algorithm is used in Bitcoin's proof-of-work scheme?
    - a. HashCash
    - b. AES
    - c. SSL

    d. **SHA-256**
2. What does the acronym "ASIC" stand for?
    a. Application Specific Integrated Code
    **b. Application Specific Integrated Circuit**
    c. Application Summation Integrated Circuit
    d. Addition Summation Integrated Circuit
3. With 51% of the network hashing power a group of miners can double-spend any transaction only from the previous block.
    a. True
    **b. False**

## Quiz 7 Key

1. What is a Bitcoin payment processor?
    a. A high-security bitcoin storage service.
    b. A web-based application that allows you to buy/sell bitcoins.
    **c. A service or application that accepts bitcoin payments from your customers, organizing (forwarding ) the received funds to you in either bitcoin, local currency, or both.**
2. The only way for merchants to accept Bitcoin is through a third-party bitcoin payment processor
    a. True
    **b. False**
3. Which statement is NOT true regarding merchants who accept bitcoin for goods and services?
    a. Merchants can accept bitcoin without using any 3rd parties if they choose to manage their bitcoin themselves.
    **b. Merchants can use Bitcoin payment processors to convert their local currency and/or bitcoin.**
    c. Merchants who accept bitcoin should pay attention to local laws and regulations.