How Bitcoin Works

Everything You Need to Know

By Don Durrett

Second Draft (August 2019)

Introduction

The purpose of this book is to save you time. I have found that trying to understand Bitcoin is tedious and time-consuming. In fact, it can take hundreds and hundreds of Google searches. When I was doing my research, I found several references that Bitcoin was like a rabbit hole. Once you find an answer, it leads to more questions.

It was very frustrating researching Bitcoin, so I decided to write this book to save you time. It is written in a non-technical format, although if you are not computer literate, it could be somewhat challenging. I have added a glossary at the end so that you can look up some of the terms that are used.

While I have tried to make Bitcoin easy to understand, in some ways, that is not possible. Thus, some of the concepts will stretch your brain even with non-technical language. I did not want to write a simplistic book that does not explain how Bitcoin works. I wanted to provide something that gives you enough information that you can feel comfortable knowing how it works.

I am not a Bitcoin developer or Bitcoin expert. I am a layman who wants to understand how it works. The reason for my interest is from an investor's viewpoint, and also as a user of Bitcoin. If I am going to own and use Bitcoin, then I want to know how it works.

The title claims that it is everything you need to know. Of course, that is a bit of hyperbole. You could say that it is almost everything you need to know. I'm not a Bitcoin expert, and this book will not make you a Bitcoin expert either. There are so many layers to Bitcoin that it would take a book much denser than this one to explain everything.

As a disclaimer, I might not have gotten everything correct. Please do your own due diligence. In fact, a lot of the contents of this book are my opinion, and others may disagree with me.

I wrote and edited this book myself. It is an original work. I wanted to put it into my words so that I would learn as I went. It should have a fresh feel to it since many of the topics were learned as I wrote it.

If you find anything that is not accurate, please email me at durrettdon@hotmail.com

Don Durrett 8/16/2019

Table of Contents

Where did Bitcoin come from and who created it?

On October 31st, 2008, the Bitcoin whitepaper was posted on the Internet. It was titled, *Bitcoin: A Peer-to-Peer Electronic Cash System*. The author's name was Satoshi Nakamoto.

On January 3rd, 2009, Satoshi Nakamoto created the first block, called the genesis block. In that block, he put the comment, "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks." Which was an article from the *London Times* newspaper on that date.

On January 9th, 2009, the Bitcoin open-source software was posted on the Internet. Then, on January 12th, Satoshi sent the first Bitcoin transaction to Hal Finney in California. Finney was one of the first adopters of Bitcoin and contributed to enhancing the code.

From 2009 until late 2010, Satoshi emailed people who were working on enhancing the Bitcoin software. His emails have the same grammar and writing style as the Bitcoin whitepaper. He was very precise and eloquent in his writing style. He also used the British English spelling of words. These emails offer proof that he did indeed write the whitepaper.

In late 2010, Satoshi handed over the code depository to Gavin Andresen and vanished. He disappeared and has never corresponded with anyone since that time. His real identity has never been determined, but it is recognized that Satoshi Nakamoto was an alias.

The very first Bitcoin exchange (BitcoinMarket.com) listed Bitcoin at 1 cent in March 2010. A year later it was up to $1 in February 2011. Two years after that it was over $1,000 in 2013. It did crash in 2014, but Bitcoin has been on a steady rise in popularity ever since it was released in 2009. Today that popularity is reflected by more than 1 million computers mining Bitcoin

and more than 30 million accounts on Coinbase.com. It is estimated that at least 25 million people own Bitcoin worldwide.

The Bitcoin price has always been volatile, often with sharp rises followed by crashes. Here is a history of that volatility, which seems to be the norm for Bitcoin.

May 2010: 1 Cent
October 2010: 12.5 Cents
February 2011: $1
June 2011: $31
December 2011: $2
December 2012: $13
April 2013: $266
June 2013: $100
November 2013: $1,242
March 2015: $200
January 2017: $1,150
December 2017: $19,783
February 2019: $3,178
June 2019: $13,829
July 2019: $9,220 (current month)

What is Bitcoin?

- It is an Internet-based virtual currency that is stored on a blockchain.
- Bitcoin has eight decimal places, with the smallest amount (.00000001) called a satoshi. A single Bitcoin is comprised of 100,000,000 satoshis.
- Currently, there are about 18 million Bitcoins on the blockchain, and the maximum will reach 21 million in the year 2140.

- Only about 3% of Bitcoin owners have at least 1 Bitcoin.
- The Bitcoin blockchain can be thought of as an electronic ledger of Bitcoin transactions that are secured through encryption.
- Each transaction transfers ownership of Bitcoin from the current owner to a new owner.
- Bitcoin balances are displayed on electronic wallets, which can read the blockchain.
- Ownership of Bitcoin is proven by owning the private keys to a public address.
- Every Bitcoin that has ever been created currently belongs to a specific public address as recorded by a Bitcoin transaction.
- The blockchain is a history of all Bitcoin transactions that have ever occurred.
- This blockchain can be viewed and searched by anyone with an Internet connection using a Blockchain Explorer.
- The blockchain is open to the public (via an Internet connection) and is not owned or controlled by anyone.

Satoshi called Bitcoin a peer-to-peer electronic cash system in his whitepaper. That's true to a certain extent, but there is a middleman, which is the Bitcoin network (connected via the Internet). Also, cash isn't involved, but virtual digital currency.

Bitcoin does not transfer directly from person to person. Instead, Bitcoin remains on the blockchain, and ownership of Bitcoin transfers from person to person.

Bitcoin does use a peer-to-peer network. It has a flat network topology with no hierarchy. This means there is no centralized server. Without a centralized server, all that is required to keep the Bitcoin network up and running is a small number of peers (also called Bitcoin network nodes). As

long as the Internet is up, then Bitcoin should be running. And without any peer having more influence than another, it creates a trustless, decentralized, permissionless system.

It is trustless because each peer operates independently using a decentralized blockchain. Also, the blockchain is secured using encryption, creating a high degree of trust. It is permissionless because anyone can join the network. All you need is an Internet connection and a computer with the required hardware specifications.

Bitcoin exists as a decentralized network that is anti-fragile (i.e., hard to break). It was designed to be self-correcting with very few points of failure. In fact, it is very difficult to bring down the Bitcoin network. Since 2009, it has been up and running 99.98% of the time. It has been referred to as the Honey Badger because of its toughness.

A better title for the whitepaper would have been, Bitcoin: A decentralized Internet-based virtual currency system. That's what it really is. What makes Bitcoin so powerful is that it is completely decentralized. There is no Bitcoin organization, other than those who deploy changes to the software.

The team that updates the software is called Bitcoin Core, and I don't think they even have an office. Updating the software was the role that Satoshi Nakamoto originally performed and has now been passed to the Bitcoin Core open-source developer team. Only a few individuals have the ability to update the software. These updates are done using consensus (explained later).

Bitcoin Strengths

1) Decentralized and Permissionless.

It is decentralized because there is no Bitcoin organization. It is permissionless because anyone can install and run the current version of Bitcoin.

There is a group of developers who decide which upgrade will be added, but they do this through consensus.

Because of decentralization, it is practically impossible to kill Bitcoin. All you would need is one country to keep it legal, plus the Internet.

2) Store of Value.

Because nearly all of the Bitcoins that will ever be created already exist (about 18 million out of 21 million), it places upward pressure on the price. Very few Bitcoins are created on a daily basis (currently only 1800). And every four years, the number that is mined drops by half. In 2020, only 900 Bitcoins will be created daily. In 2024, only 450 Bitcoin will be mined daily, and so on until 2140.

If Bitcoin survives, then they become rarer and rarer over time. It will be almost impossible for an average citizen to own a single Bitcoin. This should make Bitcoin one of the best stores of value of any asset on the planet. Why? Because the rarity of Bitcoin will make it difficult for them to drop in value.

That said, this store of value is not guaranteed and is only in theory. The key will be Bitcoin demand and usage. But if Bitcoin is widely used, then the odds favor higher prices and a strong store of value.

3) A Bank in Your Pocket.

When you have a Bitcoin hard wallet in your pocket, you hold your money without any counter-party risk. This means you have a bank in your pocket. The power of this feature of Bitcoin is revolutionary. This has the potential to change banking and finance as we know it.

4) Peer-to-Peer Money Transactions without Borders.

   With your Bitcoin wallet, you can send or receive Bitcoin from any other Bitcoin wallet in the world. This occurs without any counter-parties other than the Bitcoin network. There is no permission required for these transactions, and they can occur 24/7. All that is needed is for the transaction to be confirmed by the Bitcoin Network, thereby updating the blockchain.

5) First Mover.

   Bitcoin was the first cryptocurrency. The Bitcoin network has been up and running since 2009 and has an uptime of 99.98%. It has proven itself to be reliable. By being first, Bitcoin has become entrenched. It will be very difficult for another cryptocurrency to unseat Bitcoin as the leader.

6) Large Developer Network.

   The Bitcoin developer network is the largest cryptocurrency group of developers. There are thousands of people working on improving the Bitcoin software, especially second-layer solutions. This brainpower ensures Bitcoins future.

7) Secure, Reliable, Immutable.

   Bitcoin has never been hacked and likely won't. The only hacks that have occurred is when someone acquired access to Bitcoin private keys. These types of hacks will continue, but as long as your private keys are secured, then your Bitcoin should also be secured.

   What makes Bitcoin secure and reliable is cryptography. The heart of Bitcoin's security is cryptography that was designed by the NSA (National Security Agency).

The blockchain cannot be modified. Once a block is created, that block is immutable. This is one of the reasons for Bitcoins reliability.

8) Anti-Fragile and Trustless.

   Bitcoin is considered anti-fragile software. What this means is that it is self-correcting and very difficult to bring down. For instance, forks automatically resolve through consensus, and the mining difficulty automatically adjusts every two weeks. This is the reason it has such a high up-time of 99.98% over ten years.

   Many antagonists have tried to disrupt the Bitcoin network, and some have succeeded at filling up the transaction pool, thereby increasing transaction fees. However, Bitcoin was designed to adapt to attacks.

   All you need to do is read how Bitcoin has overcome attacks in the past to see how resilient it is and why it has earned the distinction of being called anti-fragile.

   Because Bitcoin is decentralized and anti-fragile, it can be considered trustless. You don’t have to rely on anyone to use it. As long as the Internet is up and consensus works, then there is no one to trust.

9) Consensus Driven.

   Both the creation of new blocks and software upgrades are handled through consensus (explained later). Software upgrades can get messy at times and require longer timeframes to implement changes, but the end result is usually positive for Bitcoin.

   One strength of consensus is that it prevents a powerful interest group from modifying Bitcoin. Without the consensus of nodes and miners, it is nearly impossible to implement changes. Instead, you end up with a hard fork and an altcoin (explained later).

Another benefit of Bitcoin is that it does not need to be encrypted when being transmitted over the Internet. Because Bitcoin is a public ledger, there is nothing that needs to remain private. This means that the blockchain and transactions can travel around the Internet without being encrypted. This many seem like a minor benefit, but we are talking about transferring money. Most money transactions are highly encrypted and protected. Because Bitcoin is already encrypted, it can travel around the Internet as text. Any hacker can grab it, but there isn't anything they can do with it.

Bitcoin Weaknesses

1) Spam Attacks.

   DDOS (Denial of Service) attacks. These are when Bitcoin nodes (computers on the Bitcoin network) act in a nefarious manner to undermine the Bitcoin network. They are basically enemies of Bitcoin who are trying to create havoc.

   One type of DDOS attack is simply to make non-stop requests to a Bitcoin node and force it to respond. For instance, one way to do this is to create fake transactions that will fail to be validated. However, Bitcoin has gotten better at fighting off these types of attacks.

   Another type of DDOS attack is called Dust attacks. They are called dust because they are very small transactions. When you send thousands of individual transactions with very low fees, they can flood the Bitcoin network and the transaction pool.

   > Note: To get a transaction into the transaction pool, it requires the sender to pay a fee. Thus, these types of DDOS attacks are usually short-lived because they cost money. Also, because these types of DDOS attacks have failed in the past, we have begun to see fewer of them.

2) Sybil Attacks.

   This is when Bitcoin nodes pretend to be a legitimate node on the Bitcoin network, but in fact is a nefarious enemy. These fake (a.k.a. Sybil) nodes try to cause havoc by not confirming transactions or not relaying transactions.

   Like spam, Sybil attacks cost money (someone has to buy the hardware and pay for the electricity). For this reason, Sybil attacks tend to come in spurts and usually do not last for an extended period of time. Also, Bitcoin has created many counter-measures. There are currently around 25 counter-measures in place to prevent spam and Sybil attacks.

3) Double-Spend.

   This can occur if a single miner (or group of miners) obtains 51% of the network hash power. This is unlikely to occur with Bitcoin's large number of miners.

   Without 51% of the network hash power, double-spending is prevented by using irreversible transactions and by the Bitcoin transaction and block verification process. Each new block confirms that the same Bitcoin is not double-spent.

   Let's use an example. Let's say you have $10 in a Bitcoin wallet and try to spend $6 in one transaction and $5 in another transaction. In this example, both transactions will try to use the same inputs. During the network node verification process, a transaction is only verified if there are enough inputs to transfer to outputs (refer to Appendix). This prevents double-spending. So, in this example, only the first transaction would get verified and added to the transaction pool.

4) 51% Attack.

If an attacker (one miner or a group of miners) controls 51% of the Bitcoin network hash power, they can effectively undermine the security of the blockchain. They can double-spend, reverse transactions, and even shut down the network by preventing confirmations.

The chances of a single miner controlling 51% of the Bitcoin hash power is unlikely. First, someone would have to invest billions to acquire that much hash power. Second, why would someone invest that much money only to undermine Bitcoin and destroy its value? A government perhaps, or maybe a competitor, but it is not likely to occur.

> Note: Actually, a 51% attack can be successful with as little as 30% of the Bitcoin hash power. A 51% attack will always be successful, but a 30% (or more) attack has the potential to cause harm and is a threat to Bitcoin's security.

5) Legality.

   This is perhaps the biggest risk for holders of Bitcoin. What happens if you hold Bitcoin and your country makes Bitcoin illegal? Or worse yet, not only makes it illegal, but demands that you give it to them! This is a very real possibility. In the 1930s, the U.S. government demanded that everyone turn in their gold bullion for a set price, and then made it illegal to possess. Any government could do the same thing for Bitcoin. It would be a mess, and they would turn many of their law-abiding citizens into criminals, but it's possible.

6) Software Virus.

This has never occurred to Bitcoin, but no software is immune from virus attacks. At some point, Bitcoin will have to fend off a virus attack of some kind.

7) Competition.

   Many people have made the argument that Bitcoin is not the best cryptocurrency. I personally think the Bitcoin code is elegant and built to last, but that might not be true. It is always possible that a better cryptocurrency emerges to overtake Bitcoin.

8) Bad Decisions.

   I've always said that the biggest threat to Bitcoin is Bitcoin. What I mean is that if consensus for software improvements leads to bad decisions, then Bitcoin will undermine itself. Conversely, as long as consensus leads to good decisions, then Bitcoin should thrive.

9) Reliance on the Internet

   Unless the Internet is running, Bitcoin cannot function. Currently, there is a backup Bitcoin satellite network that can be used to insure that the Bitcoin network does not go down. However, how many people will have access to this network if their local Internet is down?

   If Bitcoin becomes more entrenched, I would expect the Bitcoin satellite network to expand and become a better backup system. However, how Bitcoin could function without the current land-based Internet seems problematic.

Bitcoin Open-Source Software

The Bitcoin software can be downloaded by anyone with access to the Internet. It is written in the C++ programming language. Amazingly, the

original Bitcoin release had only 70,000 lines of code. As a comparison, most software applications, such as MS Word, have millions of lines of code.

The Bitcoin software upgrades are called a BIP (Bitcoin Improvement Proposal). These are public documents that propose changes to the Bitcoin software. Since Bitcoin went live, there have been about 100 BIPs added to Bitcoin. That is an average of about ten enhancements per year.

A BIP gets approved when it has 95% support from the miners who have mined the last 2,016 blocks. Why Satoshi choose 2,016 is anyone's guess. However, we do know that 2,016 is approximately two weeks. On average, a new block is mined every ten minutes, with 144 new blocks created each day. So, 2,016 = 14 days x 144 blocks.

Usually, if the miners approve a BIP, then the BIP gets added to the Bitcoin software, and the nodes and miners upgrade their software to the new version. However, that's not always what happens. Why? Because the nodes running on the Bitcoin network do not get to vote, but they do get to decide which Bitcoin version to install. Over the years, there have been a few rebellions on installing a new version, and it will likely happen again.

BIP software upgrades can create soft forks and hard forks. This will be explained later.

Who Modifies the Bitcoin Software?

There are essentially two types of Bitcoin software programmers (also called developers or contributors), those who are paid and those who volunteer. Because there is a large amount of money to be made in Bitcoin mining or Bitcoin commerce, there are companies who will pay people to code improvements for Bitcoin. In fact, there are many well-paid Bitcoin

developers, and I expect this to continue. Originally, all of the Bitcoin developers were volunteers.

Because Bitcoin is open-source software, anyone can propose a BIP and get it approved. That's the power of Bitcoin. The Bitcoin developer network is very large, with thousands of people working on Bitcoin improvements.

What is the blockchain?

The blockchain is perhaps the most important part of Bitcoin to understand, because that is where Bitcoin is stored. The blockchain is currently comprised of over 550,000 blocks. It grows by adding new block approximately every ten minutes. Every day there are approximately 144 (6 per hour x 24) new blocks added. I say approximately, because block creation is determined by mining, which can have variability.

The first block was created in January 2009, and because the Bitcoin network has practically never been down, there has been one new block created, on average, every ten minutes for the last ten years.

Here are some characteristics of the blockchain:

1) Each block contains a group of transactions, which are validated by the network nodes and miners (explained later).
2) The number of transactions in each block varies, but it generally contains about 1,000 to 3,000 transactions.
3) Once a block is created, the transactions in that block cannot be reversed or modified (immutability). In fact, no part of the block information can ever be changed.
4) Each block contains a pointer to the previous block. This is why it is called a blockchain. Essentially, the blocks are linked together into one

long chain, with the genesis block at the beginning and the most recently mined block at the end.

5) The Bitcoin blockchain is a public ledger which consists of all Bitcoin transactions that have ever occurred.
6) The entire blockchain is currently about 220 GB in size, but is constantly growing in size.
7) A new block is creating through mining approximately every ten minutes. This means approximately 144 blocks are created each day.
8) The blockchain can be searched by a Blockchain Explorer. These are available for free on my websites.
9) The blockchain is decentralized and does not exist in a single location, but in multiple locations all at once. In fact, every full node has a copy of the blockchain. What makes a blockchain valid is if it is the longest chain. This is called proof-of-work because the longest chain has had the most work performed to make it the longest chain. Thus, the number of blocks is the proof-of-work.

What makes Bitcoin secure?

Bitcoins are secured by encryption. This is why Bitcoin is called a cryptocurrency. The main encryption used by Bitcoin is called SHA-256. This is a function that converts an input value into a 64 character hexadecimal value. Hexa means six. This means the output value is comprised of digits 0-9 and the first six letters of the alphabet (a-e). This 64 character hexadecimal value is also called the hash value, hash key, or hash.

The word hash means to chop up, which is essentially what an encryption function does. It takes an input and chops it up and produces an output, whereby no one can determine the input from the output. The input value

becomes the key that produces the output value, and anyone who has the input value can re-create the output value. That is essentially how Bitcoin encryption works.

Bitcoin also uses the term hashing to describe how Bitcoins are created. To create new Bitcoins a computer has to solve a math problem, and the process for solving this problem is called hashing. This is just another term for guessing. Basically, Bitcoin miners make trillions of guesses until they find the answer using the SHA-256 function.

The SHA-256 function is secure because no one has ever been able to reverse engineer the input value from the hash output value. Also, it is practically impossible to guess a hash value. It's a 64 character password. The number of guesses required is a number with 78 digits. It would take the fastest computer thousands of years to guess using brute force.

These hash values are the foundation of Bitcoin, because it is how new blocks are added and how transactions are encrypted. Every block has its own hash value (block ID), every transaction has its own hash value (transaction ID), and every public address in a wallet has its own private key hash value.

These hash values are essentially really long passwords, but they are also encrypted. The encryption key is the input that created the hash value.

What is a Bitcoin block?

A block contains a single header and many transactions (usually 1,500 to 3,000). If there were six blocks created in the last hour, then approximately 12,000 transactions were added to the blockchain. However, this can be misleading when the Lightning Network is used (explained later).

The header contains the following six values:

1) **Version Number**: The current Bitcoin software version.
2) **Previous Block**: The previous block's identifier, which is also called a hash key or hash. The block's hash key is a 64 character hexadecimal value.
3) **Merkle Root**: Also called Merkle root hash key. This is the aggregate hash of all transaction hash keys in the block. This is used to validate the transactions in a block and by the miners to guess the next block's hash key.
4) **Timestamp**: The UTC timestamp when the block was created.
5) **Difficulty**: This number is the difficulty for creating the next block versus the difficulty of mining the first block in 2009. It is currently about 7 trillion times more difficult today to mine a block versus mining the first block.

   The difficulty is used to determine how many calculations will be needed to create the next block in ten minutes. It is based on the hash rate of the Bitcoin mining network, which is currently about 65 million terahashes (1 trillion) per second. The difficulty automatically adjusts every two weeks.

   The difficulty is increased by adding another leading zero to the target (discussed later), which effectively doubles the difficulty. The next block's 64 character hexadecimal number (block ID) has to begin with a string of leading zeros, which is extremely difficult to obtain when using the SHA-256 function.

   The difficulty is a number that is used to calculate the target (also referred to as Bits in Bitcoin lingo) for solving the hash problem to create the next block.

6) **Nonce**: This is the nonce that was used to create the block. The nonce is an integer, but it can be very large (32 bits, or a maximum of 4.3 billion). To understand the nonce, you have to understand how Bitcoins are mined (explained later).

Below is a screenshot of information from an example block. It was created by BlockChain.com and includes information from the header and transactions. Those items highlighted in blue are from the header.

Where to find the current block:

https://www.blockchain.com/btc/blocks

Number Of Transactions	2281
Output Total	7,651.74102929 BTC
Estimated Transaction Volume	1,971.34556572 BTC
Transaction Fees	0.57879256 BTC
Height	582276 (Main Chain)
Timestamp	2019-06-24 20:33:36
Received Time	2019-06-24 20:33:36
Relayed By	ViaBTC
Difficulty	7,409,399,249,090.25
Bits	388365571
Size	1280.391 kB
Weight	3879.366 kWU
Version	0x20000000
Nonce	2180842596
Block Reward	12.5 BTC

Hash	00000000000000000007c548068532827ed09eb0cb1f5caf9c495b7191bebb92
Previous Block	00000000000000000000e7c426bb2310c633eda2054299474ff70f221fcec87f3
Next Block(s)	
Merkle Root	878a6d5b2d3c5d9ad684d369af3043a239a82a4ebbe97cd94cbb5642b5c89081

Below are descriptions of the non-header fields that are provided by Blockchain.com.

Number of Transaction: Total number of transaction in the block.

Output Total: Total amount of Bitcoin that was transferred for all of the transactions in the block.

Estimated Transaction Volume: Total amount of Bitcoin that was transferred for all of the transactions excluding any change (explained later).

Transaction Fees: This is the amount of BTC that the miner who created the block received in addition to the current mining reward.

Height: The number of blocks in the blockchain, or the number of a specific block.

Relayed By: The miner who created the block.

Bits: This is the difficulty used for creating the block. The target represents that difficulty as a hexadecimal number. The miner who gets to create the next block is whoever can find a value equal to or less than the target (explained later). Note that the target changes every two weeks when the difficulty is adjusted.

Size: The size of the block in kilobytes.

Weight: This is used with SegWit addresses for determining transaction fees. Transactions receive discounts if they use SegWit (explained later). When using SegWit, the transaction size can be as large as 4MB (megabytes) versus the standard 1MB transaction size limitation. The discounts can be significant, so everyone should be using SegWit addresses as much as possible. (Note that kWU mean thousands of weighted units).

Block Reward: How much Bitcoin the miner receives for successfully mining a block. The reward started at 50 Bitcoins per block in 2009. Today it is 12.5 and will go to 6.25 in May 2020. This decrease is due to halving, which occurs every four years (explained later). The reward for mining a block is currently about $125,000 (12.5 x $10,000).

> Note: Why are blocks created on average every 10 minutes? It was selected to avoid forks, yet confirm transactions in a timely manner. It was decided that 20 minutes would be too long to confirm transactions, and 5 minutes would result in too many forks. So, 10 minutes was considered the ideal length of time.

How Bitcoin works

There are several parts of Bitcoin that allow it to work. Here is a list of some of those parts:

1) The creation of Bitcoin, which is done through mining (explained later).
2) Transactions that allow people to purchase and spend Bitcoin (explained later).
3) Transactions are validated through Bitcoin network nodes. Currently, there are about 10,000 nodes located throughout the world. The majority of them are in Europe, with the second-most in the U.S., and Asia third.
4) Independent companies create Internet-based cryptocurrency exchanges that allow people to buy, sell, and trade Bitcoin.
5) Independent companies create electronic wallets to store Bitcoin.
6) Independent companies allow products and services to be purchased using Bitcoin, such as local businesses or Internet websites.

7) Countries, states, and cities create regulations for Bitcoin. These regulations apply to the independent companies that use Bitcoin and to those who purchase and sell Bitcoin, such as tax laws.
8) Bitcoin's open-source software is updated through a consensus process using BIPs.
9) Bitcoin's open-source software is supported by a large network of developers throughout the world.

Mining: How Bitcoins are Created

Each Bitcoin mining computer (currently more than 1 million located throughout the world) runs the Bitcoin mining software. The software reads the blockchain and the transaction pool (also called the memory pool or mempool) to create new blocks. If a miner solves the math problem first, then it creates the next block and sends it out to the network for confirmation. This occurs approximately every ten minutes.

Here are the steps that a miner takes to create a new block:

1) Verify unconfirmed transactions in the transaction pool that can be used in new blocks.
2) Bundle a group of verified but unconfirmed transactions into a block (usually 1,000 to 3,000 transactions).
3) Insert the hash key from the previous block into the new block (thus, a new block cannot be mined until the previous block exists).
4) Insert a payment transaction for the reward (currently 12.5 Bitcoin), plus the transaction fees in the block being created. This is how miners get paid and how new Bitcoin gets created.

Note: The newly created Bitcoin, plus the transaction fees go into the miner's wallet. There is a 24-hour delay until it can be transferred to another wallet to ensure the integrity of the blockchain. This delay is needed for potential forks (explained later).

5) Solve the hash problem. Only one miner (one computer) can solve the block's hash problem first. The hash problem is solved by using the SHA-256 function that accepts an input string and returns a hexadecimal value.

   The SHA-256 function is passed the concatenated values of the block header, plus a nonce (an integer less than 4.3 billion). If the result is not equal to or lower than the target, then the nonce is incremented. This is repeated until a miner finds the solution.

   If the hash problem is not solved in 4.3 billion tries (the maximum size of the nonce), then the coinbase transaction is modified, which generates a new Merkle root. With a new Merkle root in the header, another 4.3 billion tries can be made to find a solution. This is repeated until a solution is found.

   Note that today a fast miner can do 4.3 billion calculations in a few seconds, so the Merkle root is constantly modified to find the next block's hash value.

6) Add the hash value from the previous step to the new block. This is a 64 character hexadecimal value with several leading zeros. This becomes the block's hash identifier or block ID.

   Note: This step and the next two steps only occur if the miner solves the hash problem first.

7) Add the new block to the blockchain.

8) Propagate it to the Bitcoin network for validation.

9) Begin mining the next block.

Those nine steps are what is occurring right now and never stops. It continues 24/7. This will continue until about the year 2140 when the last Bitcoin is mined.

Currently, there are about 17.7 million Bitcoins on the blockchain with 1,800 added daily (12.5 every ten minutes).

Mining is this reason why Bitcoin is considered a proof-of-work cryptocurrency. The proof of work is obtained by solving the hash problem, which allows a miner to create a new block and pay themselves a reward.

It should be noted that miners use a special transaction to pay themselves, which is called a coinbase transaction. These are the transactions used to generate new Bitcoin. This is always the first transaction in a block, and it is the transaction that is modified to solve the math problem.

Mining is how Bitcoin is created, but many people believe that mining is a waste of electricity. However, others argue that using electricity to provide proof-of-work is the only way to make Bitcoin inflation proof. Currently, it is impossible to counterfeit Bitcoin or generate more than is planned (21 million). This is what makes Bitcoin so alluring and popular with investors.

Until someone can come up with a better way to make a cryptocurrency trustworthy and inflation-proof, then the Bitcoin proof-of-work model may remain dominant.

> Note: Mining profitability generally comes down to two numbers, which are the average cost of per kilowatt-hour, and the average amount of Bitcoin rewards and fees obtained. Because of different electricity costs

globally, the breakeven costs are different throughout the world. It is currently estimated, that Bitcoin could crash to $1,000 and there would be plenty of miners still making a profit.

Note: After each halving, the rewards are cut in half. This has the potential impact of reducing the number of miners, whereby the less profitable miners go out of business. Thus, over time, there will be fewer and fewer miners. Likewise, the electrical consumption needed for mining will also drop.

Mining Pools

Practically all Bitcoins are mined by mining pools. These are groups of computers that mine together and then share the Bitcoin reward. Because only one computer can guess the answer correctly for a new block, the pools have to determine how much of the reward each member of the pool will receive. There are several methods they use for splitting up the reward, but the most common way is the percentage of the hash rate (a miner's contribution).

There are only approximately 144 blocks mined each day, so if you do not belong to a large pool, the odds are low that you will get a reward on a daily basis. If you have solar power with low energy costs and want to setup a miner (or several miners) at your house, then you would join one of these large pools. If you tried to mine on your own, the chances are almost impossible that you would ever mine a block and be first to answer the hash problem.

There are currently about 1 million Bitcoin miners (individual computers) that are configured around the world. One large pool that is used by individuals is called Slushpool and has about 200,000 miners. It holds about 12% of the total network hash rate, so it has a 12% likelihood of mining the next block.

If you only have one miner on Slushpool, your share of a reward would be tiny, because you would have to share it with 200,000 machines. Even with free electricity, it would take a while to pay-off the hardware costs of purchasing a miner.

If you owned 5% of the machines on Slushpool and had very low electricity costs, then it would probably be a very profitable business. With the huge number of computers mining Bitcoin, the only way to make money is to have very low electricity costs and a large number of mining computers.

Most pools work together by splitting up the work. One way this is done is by giving each miner a different 608-bit work string, which is the potential header of the next block. Each miner then provides their own nonce, which they increment 4.3 billion times. Once they are done working the 608-bit string, they either request a new one or are given a list of them to work on.

The number of potential 608-bit work strings is nearly infinite. The 1 million miners are using trillions of different work strings trying to find a number smaller than the target. The number of guesses per block is astronomical.

The 608-bit work string constantly changes by modifying the coinbase transaction in the block, which results in a new Merkle root value. This means that there are only three changing values to create a possible 64 character hexadecimal value smaller than the target. They are the coinbase transaction, the Merkle root, and the nonce. Note that the miners are only

guessing the solution. The only advantage one pool has over another is a larger hash rate, which allows them to make more guesses.

Decentralized Mining Pools

Decentralized mining pools use a peer-to-peer network of miners. The reason these came into existence is to make large mining pools less of a threat to Bitcoin using a 51% Attack. For instance, a single large miner (or a group of miners) could cause havoc to the Bitcoin network with as little as 30% of the hash power. However, if a mining pool uses its own peer-to-peer network, then this threat is alleviated.

Bitcoin Halving

One of the features of Bitcoin that makes it so valuable is something called halving. This is the process that reduces the reward by half every 210,000 blocks. On average, Bitcoin mines a block every ten minutes, or 144 daily, or 52,560 per year. So, the reward is cut in half every four years. The next halving will occur approximately in May 2020. We do not know the exact date because Bitcoin blocks are randomly created with a ten-minute variable target.

> Note: Currently, Bitcoin mining is stable with a consistent network hash rate. As long as that consistency remains, then the halving will occur on schedule. This schedule will only change if there is a large amount of variability in the number of active miners.

After the next halving occurs in 2020, the number of newly created Bitcoins will drop to 900 per day. Then, in 2024 it drops to 450, then in 2028, it drops to 225, and on and on until 2140. As you can imagine, with fewer

Bitcoins created every four years, it should put upward pressure on the value of Bitcoins.

Bitcoin Transactions

The blockchain is populated with Bitcoin transactions. Each time that you purchase, transfer, or sell Bitcoin, it becomes a transaction that is stored in a block on the blockchain.

A transaction is a transfer of Bitcoin from one public address to another public address. Or, in some cases, from multiple public addresses to multiple public addresses. It is a transfer of ownership, with a third party or third parties (miner, exchange, ATM, Lightning Network, payment provider, etc.) taking a fee.

Most transactions occur between two wallets. One is the sender of Bitcoin, and the other is the receiver. The technical terms that Bitcoin uses are inputs (the source of Bitcoin to be sent) and outputs (the destination of Bitcoin to be received). In a transaction, for every Bitcoin received, it has to have a correlating input (unless you are a miner creating new Bitcoin).

Inputs and outputs are always associated with a public address. The public address of the input is where you receive Bitcoin. The public address of the output is where you send Bitcoin. Note that each wallet can have an unlimited number of public addresses.

So, each input points to a public address, and each output points to a public address. This makes sense because Bitcoin has to transfer from one public address to another. Every Bitcoin at all times has to be associated with a public address, and the owner of the private keys (explained later) to that public address owns that Bitcoin. As I mentioned previously, Bitcoin never

leaves the blockchain; all it does is change ownership to a new public address.

For most transactions, there is only one input and one output. However, it is possible to have multiple inputs (sources of Bitcoin) and multiple outputs (receivers of Bitcoin). You can think of a source of Bitcoin as a public address and the receiver of Bitcoin to also be a public address. There are no names or descriptions associated with these addresses. They are only long alphanumeric values (explained later).

How Bitcoin transactions occur is confusing and took me some time to understand. I'll try to make it as simple as I can, but this is probably the most confusing part of Bitcoin because this is how encryption is put to work.

I'm only going to explain a simple transaction between two wallets (a sender and receiver), but the same concepts apply with transactions sending to multiple wallets.

First of all, the transaction is created by the wallet that wants to send Bitcoin to another wallet. You can think of sending as the same thing as spending, although the only thing that is occurring is a transfer of Bitcoin ownership from one public address to another (plus a fee to the miner who creates the block, and perhaps another third party helping you to make a transaction).

So, let's say that I want to send 1 Bitcoin from my wallet to another wallet's public address. Here are the steps that occur from a high-level understanding:

Someone has to build a GUI (graphical user interface), such as a wallet that allows me to enter a public address and the amount to be sent. After I enter these two values and press OK, my wallet will generate a transaction. The transaction will include the following:

1) A list of inputs (or a single input) that identify the Bitcoin that I own and plan to spend in this transaction.

> Note: If I use the terms spend or spent, that could also mean transfer. Quite often, we transfer Bitcoin from one wallet that we own to another that we own. For these types of transactions, we aren't really spending Bitcoin. Instead, we are transferring ownership to another wallet that we own.

Each time a wallet receives or spends Bitcoin, it occurs in a transaction. The wallet keeps track of these transactions to know the current balance. In Bitcoin lingo, the wallet's current balance is the sum of unspent transaction outputs or UTXOs. The wallet keeps track of how many outputs have been received and have not been spent, and then uses those as transaction inputs that can be spent.

The UTXOs are all of the unspent Bitcoin on the blockchain. Each time a new block is created, the UTXO database is updated and stored with the new block. Thus, the UTXO database has the current balance for all public addresses on the blockchain.

> Note: The UTXO, or the blockchain, does not know about wallets. Thus, there are no wallet identifiers stored on the blockchain. The UTXO only knows about public addresses. Only wallets know which public addresses are its own.

If a transaction tries to spend more Bitcoin than it has available in the UTXO database, it will not get validated. Each time that you spend Bitcoin, a transaction will "lock" the UTXO that you are trying to spend while it sits in the transaction pool. This way, it can't be double-spent.

For a transaction, outputs are Bitcoin that you plan to send to a public address(s), and inputs are Bitcoin that is available in your wallet (your current UTXO). Every transaction has at least 1 input and 1 output.

The source of every output is an input from the UTXO (the one exception is a coinbase transaction used by miners to get paid). For this reason, all outputs correlate back to a public address that received Bitcoin. Note that there can be multiple inputs for a single output, and multiple outputs.

Each UTXO is from a previous transaction with an associated public address. Each UTXO also has a unique transaction ID. These are the IDs that are used to validate transactions and are the IDs that go into the blocks.

One thing that is odd about Bitcoin transactions is that you cannot spend part of an input. For instance, if you have 1 Bitcoin in your wallet that was received from a single output, you can’t spend part of it. If you only want to spend .5 Bitcoin, the entire 1 Bitcoin is spent in the transaction. What happens is that the receiver will receive .5 minus the transaction fee and you will receive .5 Bitcoin as change (usually into a new public address).

This concept of change is often not understood. Sometimes people receive back change from a transaction, and they do not realize that it is their Bitcoin. Always remember that every transaction could return change if you do not spend all of an input.

For many wallets, the concept of change is hidden, and all you see is your current balance. For these wallets, all of the UTXOs are aggregated for simplicity. However, depending on your wallet type, this could be an issue if you have a lot of change addresses (explained later).

2) Digital signatures and public keys that prove you own the public addresses for the UTXO (unspent Bitcoin) being spent.

   Each transaction includes the transaction IDs for the inputs that are going to be spent. This allows Bitcoin to lookup those transactions and get the public addresses for the inputs.

   To verify the transaction, three important things are needed to prove that whoever is spending Bitcoin, actually owns it. First, the inputs need to have been sent to a public address that you own. This is easily proven. All that is needed is for the transaction to include the transaction IDs that are the source of the Bitcoin (also called an input list). These previous transactions can be looked up to return your public addresses that hold the Bitcoin.

   Now that the node verifier has the public addresses from the previous transactions, the verifier can then use the digital signatures and public keys included in the transaction to verify that you are the owner. First, the public keys are compared to the public addresses, and through math, they will show that they are the same. Then the public keys will be compared to the digital signatures. Again, through math, they will show that both were created from the same private keys.

   To clarify, each public address has its own private key/public key pair. A wallet can have many public addresses, so it can also have many private key/public key pairs. Also, there is a separate digital signature for each public address.

   The digital signature is generated by combining a private key, public key, and transaction data. This signature can be used as the private key's stand-in on the blockchain for a transaction. This allows private keys to remain off the blockchain. This signature can be used to prove

that a public address was created by the same private key/public key pair.

3) A recipient public address(s).

   This is the public address(s) that the Bitcoin is sent to.

   The public address (also called a wallet address) is the hashed public key (explained later). Only the owner of the private key that generated this public address will be able to spend the Bitcoin that is received.

   > Note: When a transaction is validated, the public addresses that are validated strenuously are those of the *inputs*. The recipient's public addresses (the outputs) generally have very little impact on the validation of the transaction.
   >
   > Note: The only validation that occurs to validate a recipient's public address is the length (26 to 35 characters) and the 58 characters that are allowed. There is no validation to see if the recipient's public address exists.
   >
   > Note: If you send Bitcoin to public address without an owner, then the Bitcoin is lost and cannot be recovered (although refer to RBF, explained later).

4) The amount to be sent.

   Bitcoin has eight decimal places, or 100,000,000 satoshis. Because of mining fees, there is a minimum amount that can be sent, which is currently about 500 satoshis. This minimum is constantly changing based on the value of Bitcoin and the average transaction fee. If you

try to send a very small amount, it might not get validated if the mining fees exceed the amount to be sent.

Each transaction is encrypted, which secures ownership of Bitcoin. Each transaction is encrypted using private keys for the public addresses. Whereas the private keys remain off the blockchain, the public addresses, public keys, and digital signatures do go on the blockchain. For transactions, the public addresses are used in conjunction with a public key and a digital signature that is created for each public address. The wallet keeps track of all of the addresses and keys that it owns. You can have an unlimited number of private keys, public keys, and public addresses for each wallet.

To clarify, each time that you create a public address, the wallet automatically creates a corresponding public key and private key. Then a digital signature is created if you try to spend Bitcoin from one of your public addresses that have received Bitcoin.

Bitcoin transactions are created (one at a time) by following a set of rules (refer to the Appendix) and then submitting the transaction to the Bitcoin network for validation by the network nodes. After a transaction is validated by the network nodes (who compare the transaction with the rules), it goes into the transaction pool (also called memory pool or mempool). This is the pool of transactions that the miners use to create the next block.

A transaction is confirmed when it is added to a new block by a miner. Each new block creates a single confirmation for the transaction. So, when you spend or receive Bitcoin, it takes about ten minutes for the first confirmation (the time it takes to create a block), and about an hour for six confirmations. Note that for Lightning Network transactions, confirmations can be nearly instantaneous (explained later).

Before a miner adds transactions to a new block, they also verify that the transactions follow the rules in the same way that network nodes validate transactions. You can think of it has double-checking. The biggest difference is that thousands of nodes validate the transactions before the miners do a single final verification. This is why it is called verification when the miners validate the transactions.

Creating blocks has multiple purposes. Here is a list.

1) Creates new Bitcoin.

   When a new block is created, the miners add a special transaction called the coinbase transaction. This is how they pay themselves the reward and fees for the block creation.

   There is a 24-hour delay between when they pay themselves and when they can transfer the Bitcoin (spend it). This delay is in the event of any possible forks (explained later).

2) Prevents double-spending.

   Because only one block is created at a time, the miners verify that the UTXOs are only spent once in a block. This is how the double-spend problem was solved and one of the reasons for the proof-of-work model.

   Bitcoin is smart enough to allow multiple transactions that use the same input in the same block. The only limitation is that the transactions have to be ordered correctly. For instance, if A sends to B, and then B sends the same Bitcoin to C, the transaction order has to be the same. If they are not ordered correctly, then B will not have any Bitcoin unless the first transaction occurs.

   Bitcoin is quite complex to prevent double-spending. Think of all of the potential ways to transfer Bitcoin between addresses. Bitcoin is adept

at making sure that during a single block, all outputs do not exceed matching inputs. Any transaction that does not have an input to satisfy an output, then the transaction is invalid.

The key to preventing double-spending is the current amount of UTXOs that a wallet owns. If a wallet tries to spend more than it owns, the transaction will not be validated.

If there are multiple transactions trying to spend Bitcoin from the same wallet, then it is possible for some of these transactions to be validated if there is adequate UTXOs.

3) Confirms transactions.

   About 1,500 to 3,000 transactions are included in each block. Once a transaction is confirmed, it falls out of the transaction pool.

4) Secures the blockchain.

   The entire chain is connected sequentially from the original genesis block to the current block. After a block is created, it cannot be modified. This creates an unchangeable public ledger that is secure.

5) Resolves consensus.

   The longest chain wins. There are forks that constantly occur (about 1 per day), but usually these are resolved within one or two new blocks. The reason for most forks is the large size of the Bitcoin network. There are so many miners that we often get two blocks that are created at nearly the same time.

   The Bitcoin blockchain is self-correcting by consensus. While it may appear that Bitcoin has two branches, it is rare for a fork not to resolve itself after about thirty minutes. All forks eventually resolve on their own because it costs money to mine them. At some point, mining an unprofitable fork becomes untenable.

> To clarify, it costs money to create a new block because of the electricity cost. If you are a miner and you are adding blocks to a branch that is likely to become orphaned, then you are wasting money. The blocks on that orphaned branch will not get validated, and they will not have a reward. If you remember, it takes about 24 hours (100 blocks) until miners get paid.
>
> The orphaned branch returns its transactions to the memory pool. Most of them are likely already on the other fork. Because of this potential for forks, it is good practice to wait for at least three confirmations (about 30 minutes) before you spend Bitcoin that you have received.

A small payment can be confirmed with one confirmation in the next block, but most exchanges required three confirmations for a deposit (about 30 minutes). Many merchants require six confirmations (6 blocks or about 1 hour). For most transactions, three confirmations are usually sufficient. For large transactions, it is better to wait for six confirmations to be sure.

The reason to wait for three confirmation is the potential for forks. Usually, about once a week, there is a fork. These forks are usually resolved within three blocks. The losing branch dies (becomes an orphan), so if your transaction was in a branch that died, it might need to get re-confirmed on the next block.

Each transaction does not have the name of who transferred or received Bitcoin. Instead, it has a 64 character transaction ID, which is a hash result of the transaction inputs and outputs. The transactions are associated with public addresses, with at least one public address input and one public address output. Because Bitcoin is supposed to last forever, each transaction is simply a transfer of ownership between public addresses.

There is no cost of owning Bitcoin in a wallet, other than the transaction fees to do a transaction. In other words, it is free to leave Bitcoin on the blockchain. There are no annual fees to let it sit there.

How to Cancel a Transaction

It is possible to cancel a transaction, but only if it has not yet been confirmed, and it is not a Lightning Network transaction. Also, your wallet has to support something called RBF (Replace by Fee). In practice, the transaction isn't actually canceled, instead it is replaced.

> Note: Some wallets default all transactions to RBF, others require that you check a box to opt-in, and others do not support it.

RBF is very powerful, and I'm surprised it is even allowed. For instance, if you make a transaction to send Bitcoin and that transaction allows RBF, then you can replace it before it gets confirmed. We generally think of Bitcoin as having immutability, but that is only after it is added to the blockchain. When a transaction is in the mempool, it can be replaced – if the transaction supports RBF.

RBF can be used to scam a business that accepts a transaction before it is confirmed. These are called zero-confirmation transactions. RBF has made the practice of accepting zero-confirmations very risky.

The new RBF transaction used to replace the old one will have the same transaction ID. However, because it is marked as RBF, it will be accepted as a replacement. The original transaction will get canceled.

Normally, RBF is used for transactions that are stuck in the mempool because they have low fees. All that is required to unstick them is to replace

it with an identical transaction with a higher fee. However, it can also have a new recipient address of where the Bitcoin goes. Thus, you can send the Bitcoin back to yourself. That seems problematic and can potentially be used by scammers. But it can only be exploited if a business accepts a zero-confirmation transaction.

Wallet software makers seem to agree that it could be problematic. Currently, I do not know of any wallets that allow you to change the receiver's address for an RBF transaction. However, this functionality does exist, and I would not be surprised if a wallet supports it in the future.

One feature of RBF is that you can use it to get low fees. For instance, you can put in a fee of 1 satoshi per byte for your transaction. Then if it does not get confirmed, you can increase it to 2 satoshis per byte and so one. These low fee transactions will confirm if the mempool empties.

A transaction will automatically get canceled after it sits in the mempool for a certain period of time. The default is 14 days, but this can be set by each node. However, when you send Bitcoin, it can get stuck in the mempool and you can't double-spend it. To get it back, you could use RBF. I think that was the rationale behind why it was added.

You could accidentally put a low fee for a transaction and then it would get stuck for several days until it was automatically canceled. Also, you could send a transaction to the wrong address. Once you realized your mistake, you could use RBF to replace the transaction. Considering the need to rectify these problems, I can understand why RBF was added. I personally would like to have a wallet that allows me to use RBF and change the recipient's address if I made a mistake. After all, anyone can make a mistake.

> Note: Because of RBF, businesses should not accept unconfirmed transactions. Ironically, some businesses

> still accept them, expecting them to be confirmed. In Bitcoin lingo, this is called zero-confirmation transactions or zero-conf. There is a lot of different opinions about the risks of accepting zero-confirmation transactions. However, it is now recognized that because of RBF, accepting unconfirmed transactions is risky.

Child Pays For Parent (CPFP)

Instead of canceling (replacing) a transaction that is stuck in the mempool using RBF, there is another way. If a transaction gets stuck in the mempool because of a low fee, you can unstick it by using CPFP (as long as your wallet supports it).

To use CPFP, all you need to do is send one of the outputs (it must be your address) in the stuck transaction to a new address while using a higher fee. This will not only move the output to the new address, but it will also unstick the transaction that was stuck.

This can also be used for change that you are expecting. So, if you send Bitcoin to someone and it gets stuck, as long as there is some change in that transaction, you can use CPFP (as long as your wallet support it).

> Note: Because of the power of RBF and CPFP, make sure that your wallet supports both of these features.

Change

If you spend Bitcoin from a wallet and do not spend all of an input, then you will generate change. This Bitcoin change will normally go into a new address (also called a change address), but it could go back to the original address depending on how the wallet is configured.

Bitcoin uses an all-or-nothing rule for spending Bitcoin that you have received (inputs). If you want to spend Bitcoin, your wallet will check your inputs (available Bitcoin). Unless you have inputs with the exact amount that you want to spend, then you will get change back. Over time, you could end up with many of these change addresses.

> Note: You can aggregate these change addresses by transferring (spending) them into a new address. This is called sweeping. Often this is done by moving Bitcoin into a new wallet.

> Note: When you move your Bitcoin into a new wallet, all of the private keys/public keys will have changed. If you do this with a VPN, it is a good way to add privacy to your Bitcoin. It's like moving to a new city, and no one knows your address.

More Information about Transactions

To review, the blockchain is composed of transactions, whereby each transaction is between two or more wallets. The source can be one or more wallets, and the recipient can be one or more wallets. Each recipient provides a public address where the Bitcoin will be sent. By sending Bitcoin to a public address, you are effectively locking (using encryption) that Bitcoin in a transaction, whereby only the owner of that public address can unlock it (using decryption).

The owner of a public address can unlock a transaction sent to them because they own the public key and private key associated with that public address. That is how Bitcoin works.

Transactions are confusing because they always look at previous transactions to see if the sender (transaction creator) owns the Bitcoin they want to spend.

Bitcoin doesn't care very much about who is receiving the Bitcoin. The software only does rudimentary validation on the destination public address. What Bitcoin cares about is if the sender owns the Bitcoin it wants to spend.

When you send Bitcoin to a public address, you are essentially transferring your rights of ownership to that public address. It is then up to the owner of that public address to unlock the transaction (using their associated public and private keys) if they want to spend the Bitcoin.

A public address identifies where the Bitcoin is sent. Then once it is sent, the receiver proves that it is their address by using their associated public and private keys to unlock it. It is locked by the sender by including a public address and then it is unlocked by the receiver using their associated public and private keys.

Private keys are not on the blockchain. These keys are long alphanumeric values that usually reside in the wallet, or in a location where the wallet can access them. Each private key can be used to unlock the Bitcoin associated with a public address. Protecting your private keys is your responsibility.

Many choose to leave their private keys on an exchange and let the exchange to protect them. This is similar to leaving your money in a bank and trusting the bank with your money. Other people prefer to take their private keys off the Internet completely, which are called cold wallets.

Private keys are used to produce a digital signature that is generated for each public key used in a transaction. The private key/public key pair, along with the transaction data, are combined to create a digital signature. The

digital signature can then be used to prove that the recipient's public address was created by the same private key/public key pair. This allows the private keys to remain off the blockchain.

When a transaction is validated, the spender (who is creating the transaction) has to prove that they own the public address(s) that has the UTXO (unspent transaction output) that they want to spend. So, the spender's wallet creates a transaction that includes the public address(s) of the UTXO to be spent in the transaction, along with their associated public key(s) and digital signature(s). The transaction is validated if all three came from the same private/public key pair.

Batch Transaction

A batch transaction is when you combine multiple payments into a single transaction. For every additional output (Bitcoin recipient), it only adds about 34 bytes. If you make a separate transaction to pay each recipient, then you are wasting fees. So, if you know you need to pay multiple people, you can do it all at once and save a lot on fees. Also, you can make the mempool more efficient because it has to handle fewer transactions.

CoinJoin Transaction

A CoinJoin transaction is when Bitcoin is spent from multiple inputs into multiple outputs. A transaction can have as many public address inputs and public address outputs as long as it fits in a block (1 to 4MB). When this is done with a lot of addresses, it is difficult to know which input is paying which output. These types of transaction add privacy, but also draw scrutiny from regulators who prefer transparency.

How Bitcoin is Lost (Forever)

1) A wallet is lost (or cannot be accessed) and there is no backup.
2) Someone sends Bitcoin to a legitimate Bitcoin address (verified using rudimentary validation) that does not have an owner on the blockchain.
3) Someone restores a wallet using an old backup, and the backup is missing new addresses that contain Bitcoin that was received after the backup.

In theory, every Bitcoin that is created should exist as a UTXO (unspent transaction output). However, if any of the scenarios listed above occur, then those Bitcoins are lost and likely will never be found.

> Note: It is estimated that Satoshi Nakamoto mined 1.8 million Bitcoin and did not spend 1.1 million Bitcoin. This could mean that at least 1 million Bitcoins have been lost. However, if you try to find the public addresses that hold these 1.1 million Bitcoin, you likely won't find them, or at least I couldn't. Until someone posts the public addresses of this hoard of Bitcoin, I think we have to assume it is an urban myth.

Public Addresses

Public addresses (also called wallet addresses) are derived from a private key/public key pair. Every public address has one of these pairs. This is how ownership of each Bitcoin is proven. Each public address is correlated back to a private key/public key pair. If a wallet contains all three values, then that wallet can prove ownership.

Often public addresses are synonymously called public keys. This is somewhat misleading because public keys are not public addresses. Public

keys are included in transactions, and we never see them. What we see are the public addresses, which are hashed public keys.

People will often tell others to send them their public key. They do this because they have no idea that they are not the same thing. They are referring to their public address.

Bitcoin is secured by using very long alphanumeric values as keys. Moreover, the creation of these keys and addresses only goes in one direction. A public address comes from a public key; a public key comes from a private key. However, you can't go in the other direction. If you have a public address, you can't determine the public key, and if you have the public key, you can't determine the private key.

A public address is an alphanumeric value (26 to 35 characters) or QR code that you provide someone to send you Bitcoin. In other words, public addresses are only used to receive Bitcoin. You can create as many public addresses for a single wallet as you need. If you use the same public address over and over, then someone who knows your public address can look up your transactions and see how much Bitcoin that address has received. It is recommended to use a new public address each time that you receive Bitcoin.

A public address is created using three steps:

1) The public key is hashed using SHA-256, whereby the public key is the input.
2) The result from step one is hashed using RIPEMD-160. This shortens the length of the address without losing security.

3) The result from step 2, along with the version and checksum, is converted using Base58. This removes letters and numbers that can cause confusion.

These three steps can be combined as follows:

Public Address = Base58(Version + RIPEMD160(SHA256(Public Key)) + CheckSum)

Version: This is the digital version of Bitcoin.

CheckSum: This the first eight digits that are returned from SHA256 function.

SHA-256: This is a function that converts an input value into a 64 character hexadecimal value (256 bits). Hexa means six. This means the value is comprised of digits 0-9 and the first six letters of the alphabet (a-e). This 64 character hexadecimal value is also called the hash value, hash key, or hash.

RIPEMD-160: This is the same as SHA-256, only it returns a 160-bit hexadecimal value. This second hash function is used to reduce the length of public addresses without degrading security.

The results of this double hash (SHA-256 and RIPEMD-160) is a variable-length output, depending on the size of the binary number. This is why public addresses are not all the same length (26 to 35 characters).

Base58: Converts a binary number into an alphanumeric value. It only includes these 58 characters. If you look closely, you will see that zero, upper case o, upper case i, and lower case l are missing. This was to remove confusion:

123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz

Public Address Rules (Rudimentary Validation)

1) 26 to 35 characters in length.
2) Begin with a 1, 3, or BC1.
3) Alphanumeric characters that do not include a zero, upper case o, upper case i, or lower case l.

Public Address Types

1) P2PKH (Pay To Public Key). Begins with a 1. These were the original Bitcoin public addresses.
2) P2SH (Pay To Script Hash). Begins with a 3. These are used for SegWit and multisig transactions. SegWit was introduced in 2017 to fix a malleability bug, and to allow blocks to hold more transactions, and to provide second-layer solutions. Multisig transactions can require multiple signatures for more security (explained later).

> Note: These addresses transfer responsibility from the sender to the receiver for paying extra fees for large transactions, such as multi-sig. The sender only has to include a single hash script key instead of multiple public addresses. Then the receivers have to prove that they own that hash script key.
>
> When the receivers go to spend the Bitcoin that they received, they have to include the script information which becomes bytes in the transaction. There is the saying that time is money, well, in Bitcoin, bytes become fees. P2SH addresses (being with 3) keep the bytes small for the sender.

3) BECH32. Begins with BC1. These are the most recent type of addresses and are still uncommon. They are considered native SegWit addresses and are more efficient than P2SH addresses. They allow more transactions to be squeezed into a single block and have the potential to have lower fees than non-native three addresses. I would expect these to be the most used addresses in the near future.

> Note: Many wallets now support both sending and receiving BC1 addresses. However, it is not yet fully supported. SegWit addresses that begin with 3 are close to being fully supported. I would expect most exchanges to support BC1 addresses in the near future. Also, some Blockchain Explorers (explained later) do not yet support BC1 addresses.

Private Keys / Public Keys

As mentioned previously, every public address comes from a pair of private/public keys.

Private keys are 256-bit numbers (78 digits) and are either randomly generated, or deterministically created using a master private key (explained later). Once a private key is created, the public key is deterministically created from the private key.

A private key is not something that you share with the public. It is used to encrypt your transactions with a digital fingerprint. Each wallet is essentially protected by its private keys. This is how you retain ownership of your Bitcoin. If someone obtains your private keys, they can spend your Bitcoin.

A private key is often hidden and doesn’t need to be displayed. If you do want to see a private key, it is usually displayed as a Base58 value, with

about 50 to 60 characters. It can also be displayed as a 64 character hexadecimal value.

A public key is created using something called the Elliptic Curve Digital Signature Algorithm (ECDSA), which generates a 256-bit integer from the private key. Each private key can only generate a single public key. Thus, it is deterministic.

One way to understand how private and public keys are generated is looking at how Hierarchical Deterministic (HD) wallets work with master seeds (explained next).

> Note: Sometimes private keys are encrypted for added security. This was common practice when paper wallets were widely used. If a private key is encrypted, then it cannot be spent until a passphrase is provided. With today's wallets, there isn't any reason to encrypt private keys, because the wallet itself has a passphrase.

Master Seed / Seed Phrase / Root Seed / Recovery Seed

Hierarchical Deterministic (HD) wallets provide a master seed (also called root seed, recovery seed) to recover your wallet. The master seed/root seed is a single number, although it is very long. The master seed/root seed is then represented by a series of short words, which are generated from the master seed/root seed.

These words are also called mnemonic words, because they are used to make it possible to memorize your recovery words. Memorizing a long number is practically impossible.

Collectively, these words are called seed phrases. The seed phrase is usually 12 or 24 words, although sometimes people use eight words as a brain wallet (remembered in their head). A 12-word master seed is 128 bits. A 24-word master seed is 256 bits, which doubles the encryption.

For HD wallets, these seed words (8, 12, or 24) are hashed into a 512-bit master private key. This is done by passing in the words as a string, along with an optional password, to a SHA-512 hash function. The master private key is deterministic because it can be reproduced if you know the master seed.

Once you have the master private key, you can then create an unlimited number of private keys from the master private key. These private keys are also deterministic. Meaning that if you have the master private key, you can re-create the private keys.

As mentioned previously, public keys are derived from private keys using the ECDSA algorithm, so public keys are also deterministic. Also mentioned previously, public addresses are derived from public keys. So, these are also deterministic.

To re-generate an HD wallet, all you need is the master seed (list of words, plus the optional password), and then the wallet will automatically re-generate private keys, public keys, and public addresses. It will re-create them in the same order that they would have originally been created. It will then search the blockchain using the re-generated public addresses for any transactions that the wallet could own. Normally, the wallet will stop searching the blockchain after 20 public address have not been found.

If you forget your wallet's password or lose your wallet, you can restore the wallet using the master seed. You can even use the master seed to create a duplicate wallet (as long as the wallet is compatible with the original wallet).

If you create a duplicate, then you can spend your BTC from either wallet. These wallets will essentially be duplicates and will show the same balance.

If you have a good memory, then you can store your recovery seeds in your head. Perhaps 24 words are too hard to remember, but 12 is possible for some people, and eight is possible for most people. Some people call these brain wallets. Think of the possibilities. At any time, in any country, you can generate a Bitcoin HD wallet simply by entering the seed. All you need is Internet access to do the re-generation.

Perhaps it’s not wise to use a brain wallet with an eight-word phrase for all of your Bitcoin, but it might not be a bad idea for some of your Bitcoin. Also, it is not easy to hack an eight-word phrase, plus a password.

If you go on a trip and want to spend Bitcoin, you could put a wallet on your phone, and then remember the master seed in your head as a backup. Or, you could put hints for each seed on your phone as a backup. Have you ever used the notes section for one of your contacts on your phone? That's a great place to put your hints.

Can someone guess your master seed and re-create your wallet? In theory, the answer is yes. But in practice, it's nearly impossible. To guess all possible master seeds for HD wallets by brute force, the probability for 12 words is 2048^{12}. This is a huge number with about 40 digits. It would take all of the computers in existence more than a million years to guess all of the combinations. However, the possibility of guessing a single random wallet has a higher probability. A hacker could start with 12 words and try all of the combinations, and then try 12 more. They might get lucky and find a wallet, but the chances are infinitesimal, and the chances of it being your wallet is even more unlikely.

Many experts say that 12 words are more than enough to secure a wallet. I prefer 24, plus a password. This might be overkill, but you probably will never use this master seed anyway, so why not be extra careful?

One thing should be obvious to you after reading about HD wallets, and that is how useful they are for restoring a wallet that is lost. If you don't have an HD wallet, then you are neglecting this useful feature of Bitcoin.

Transaction Verification

After a transaction is created, the following occurs:

1) It is broadcast to the Bitcoin network.
2) Bitcoin nodes receive the transaction and verify if it follows the required rules (refer to the appendix).
3) Re-broadcast it out to the Bitcoin network.
4) Add it to their local transaction pool (also called the memory pool or mempool).

Steps 3 and 4 are only used if the transaction is verified. The transaction pool consists of verified but unconfirmed transactions that have not yet been added to the blockchain.

Usually, after a node verifies a transaction, it will re-broadcast it to the network so that other nodes can verify it as well. This verification process ensures that miners have transactions that can be used for the next block.

> Note: If a transaction fails the verification test, the node will send back a message informing the sender that it failed. Some wallets will display that the transaction failed.

Each node has its own transaction pool. This means that there is no global transaction pool that the miners share. This also means that many transaction pools do not match, but that is not a problem. Eventually, all transactions will get verified and confirmed if they abide by the rules.

The Bitcoin network normally can pass each transaction to all of the nodes in only a few seconds. A miner can reasonably assume that their transaction pool is quite similar to what the other miners are using. The hard part for a transaction is getting from the transaction pool onto the blockchain. This means that has to be included in the next block, which requires at least ten minutes, and sometimes days, depending on how much you are willing to pay in fees.

There is no minimum number of nodes that need to verify a transaction. The only requirement for a transaction to be included in a block is that it follows the rules. For this reason, it is possible for a miner to create its own transactions and then add them to a new block without any other nodes seeing those transactions until the block is verified.

How transactions leave the transaction pool:

1) The transaction was included in a new block.
2) The transaction or one of its unconfirmed ancestors (parent transactions) conflicts with a transaction that was included in a new block.
3) The transaction was replaced by a newer version.
4) The transaction expired (by default, 14 days after entering the transaction pool).

5) The transaction pool became full (every transaction pool can have a different memory size) and lower-fee transactions were replaced with higher-fee transactions.

Transaction Fees

Transaction fees are very confusing. Here is a list of reasons why:

1) There is currently no such thing as a flat fee for a Bitcoin transaction.
2) Fees are calculated using two different methods based on the address type. Addresses that begin with 1 are calculated using satoshis per byte. SegWit addresses that begin with a 3 or BC1 also use satoshis per byte, although the weight is converted into virtual bytes.
3) You can pay whatever fee you want for a transaction, and it is based on bidding. Most wallets default to a calculated fee (satoshis per byte) that is close to the current average transaction fee. Some wallets allow you to set your own fee in satoshis per byte.
4) Fees are based on demand and can change from minute to minute, although they are usually fairly consistent on an average day.
5) The miners determine the fees because they decide which transactions will get confirmed. However, they compete against each other, so it is a free market. If they are offered transactions with high fees, then they will confirm those first.
6) Transaction fees are paid in addition to the block reward. The block reward is currently much more attractive to miners than transaction fees. This gives miners incentive to confirm low fee transactions if that is all that exists in the transaction pool.

There is currently no minimum fee for a transaction. If the transaction pool is empty (or close to empty), then bids can be very low (1 to 10 satoshis per

byte), and transactions can still get confirmed. At $10,000 Bitcoin, the average on-chain transaction fee at 1 satoshi per byte would be about 3 cents.

The average transaction size is about 250 bytes. If you bid 50 satoshis per byte, the cost is based on the current price of Bitcoin. At $10,000 Bitcoin, that is about $1. That would be too high for a cup of coffee, which is why the Lightning Network was created (explained later).

The higher you bid, the faster your transaction will be confirmed. Often, there are estimated fees for estimated times. Let's say you want to have a transaction confirmed in 1 hour or 1 day. You can get the current fee estimate for those times. You can either use an Internet website, a phone App, or a wallet that provides this feature to get estimates.

> Note: When you get an estimate for your fees, you will likely see a choice for SegWit. Often you will see bytes displayed as vbytes (virtual bytes). What they are doing is converting weight into bytes. You will also notice that the discount is significant if you use SegWit addresses.

In the past, when the mempool has filled up, transaction fees went as high as 400 satoshis per byte. That would require an average transaction fee today of around $8.

Many wallets now allow you to set your own bid of satoshis per byte. If you don't mind waiting a day or several days for confirmation, then you can put very low bids. The risk is that the transaction will get stuck in the mempool and eventually canceled (usually after 14 days). Thus, you will have to re-submit it with a higher fee. This is what RBF will help you with.

Many businesses want their transactions to be confirmed quickly and can charge high fees to consumers. You pay these fees, and they don't, so be careful when making transactions. You could be paying high fees and not realize it.

Now that second layer solutions have been introduced (such as the Lightning Network), fees can be much lower. The miners are only paid for on-chain transactions, and Lightning Network transactions are off-chain.

> Note: Transaction fees are not included separately in the transaction (refer to the appendix). Instead, fees are the difference between the inputs and outputs. The miners get what is left over. They create a transaction to pay themselves for transaction fees using the leftover inputs. So, the leftover inputs in a transaction are the transaction fees.

SegWit

I've mentioned SegWit many times, so perhaps I should explain what it is. SegWit stands for Segregated Witness. It was a brilliant idea from a Bitcoin developer.

Initially, it was designed to fix a malleability error. This error allowed attackers to alter digital signatures without invalidating transactions in the mempool. Basically, they found a way to replace existing transactions in a nefarious manner. The SegWit solution to this problem removed the witness data (digital signatures) from the transaction inputs and placed the witness data in another part of the transaction. It is called segregated witness because it segregates the witness data from the inputs and places the witness data somewhere else in the transaction (the witness list).

By fixing the malleability error using SegWit, it created three additional benefits.

1) Larger Blocks.

   Bitcoin is now able to have blocks larger than the current 1MB limit if SegWit addresses are used in a transaction. The maximum size is currently around 4MB if SegWit is used. The current average-sized Bitcoin block is about 1.2MB, with some larger than 2MB blocks. With SegWit increasing in usage, I would expect the average block size to increase.

2) Lower Fees.

   If you use SegWit addresses, you can get discounts for your transactions. The reason why is because more transactions can be included in a block. This means that miners are willing to pay less per transaction if the block contains SegWit transactions.

3) Secondary Layers.

   The third benefit was that secondary layers could now be used. This led to the adoption of the Lightning Network (explained later), and more secondary layers are currently being tested.

> Note: If you transfer Bitcoin between two wallets that you own, there is still a transaction fee. For this reason, always use a SegWit address when sending Bitcoin to yourself to save on fees. The savings can be significant. There is no benefit for using traditional addresses that begin with a 1.

Blockchain Explorers

It is possible to search and display the details for transactions. Also, because transactions are linked to the previous transaction and the next transaction, you can track all of the transactions linked to a known public address. This is done using a Blockchain Explorer. Most of these are free and are useful for several reasons:

1) Finding out if a transaction was validated (added to the transaction pool).
2) Finding out if a transaction was confirmed (added to a block).
3) Tracking the history of a public address.
4) Viewing the details of a block.
5) Viewing the details of all transactions in a block.
6) Viewing unconfirmed transactions in the mempool.

It can be useful to find out if your transaction is sitting in the transaction pool and what fees you will pay. This will give you peace of mind that the transaction should be confirmed soon, based on the current average fee.

Another nice feature is the ability to monitor how many confirmations your transaction has at this time. Most people take it for granted that their transaction will be confirmed, but you can watch in the background if you want.

One of the features of Bitcoin is that you can have many public addresses. Monitoring them manually using a Blockchain Explorer can be tedious. It would be nice to have a wallet ID where you could enter all of your addresses. Unfortunately, the blockchain does not use wallet IDs. In theory, a wallet should be able to do this, but I have not heard of a Blockchain Explorer at the wallet level yet.

> Note: If you use BlockExplorer.com as a Blockchain Explorer it will include all of the inputs (public addresses) for a transaction and consider that a wallet. But it does not have the ability to include all public addresses for a wallet.

Not only can you view all of the transactions for your public address, but all of the connected transactions. This can create a vast tree of transactions. For instance, if you send Bitcoin to a public address, that address becomes connected to your public address, and any transactions that it does also become connected.

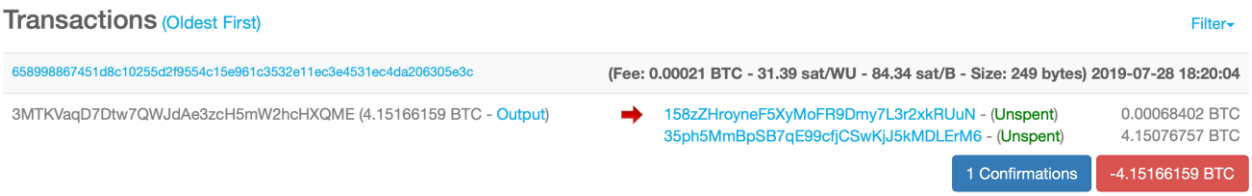
As you can imagine, it is possible to follow the trail because of this connectivity. This reduces Bitcoin's privacy and anonymity. If you purchase or sell Bitcoin on an exchange, then that exchange can associate your identity to a public address. If a government agency has access to the exchange's data, then they can follow the trail for purchase and sells. So, it is recommended that you pay your crypto capital gains taxes!

This lack of anonymity with Bitcoin is the reason why altcoins such as Monero, Zcash, and Dash came into existence. They make it much more difficult to track the buyers and sellers of Bitcoin, or to follow the trail of transactions.

Here are the more popular Blockchain Explorers:

1) Blockchain.info
2) BlockExplorer.com
3) Blocktrail.com

Here are some screenshots from Blockchain.info.



The screenshot above shows the high-level information for a transaction.

The top line shows the transaction ID (blue link) on the left. Then on the right, it shows the fees, size in bytes, and date/time. The fees are listed in both satoshis by weighted unit and satoshis per byte. Two of the addresses begin with a 3, which are SegWit addresses. These use weighted unit fees.

Below the top line, are inputs on the left (amount of Bitcoin that is being spent from a public address) and the outputs on the right (amount of Bitcoin being received into a public address). Everything in blue is a link to display more details.

The output will be marked as either Spent or Unspent. If it is Spent, then you can click on the Spent link to see where it was subsequently spent. If it is Unspent, then this Bitcoin is still in the UTXO and available to be spent.

Summary	
Size	2394 (bytes)
Weight	9576
Received Time	2019-07-25 04:32:55
Included In Blocks	586908 (2019-07-25 04:33:53 + 1 minutes)
Confirmations	571
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	0.3984916 BTC
Total Output	0.3949006 BTC
Fees	0.003591 BTC
Fee per byte	150 sat/B
Fee per weight unit	37.5 sat/WU
Estimated BTC Transacted	0.3949006 BTC
Scripts	Show scripts & coinbase

The last line shows how many confirmations have been made for the transaction. It also shows how much Bitcoin was spent for this transaction, not including fees. If you look carefully, you will see that the total in the red box matches the input (although marked output to make everyone confused).

The screenshot above displays some of the details for a transaction. Most of this is displayed on the previous screenshot showing high-level information. The one option on that is useful is View Tree Chart, which will show all connected transactions.

There are some companies that are adding functionality to Block Explorers, such as a 3D view of the connections. In the future, we can expect to see very powerful tools that allow tracking of transactions.

Bitcoin Wallets

You can think of a Bitcoin wallet as a holder of Bitcoin in the same way that a regular wallet is a holder of your money. The main difference is that Bitcoin is an electronic wallet.

A Bitcoin wallet can only receive Bitcoin if another wallet sends Bitcoin to one of your public wallet addresses. Your wallet will keep track of your

current balance, and it will keep track all of your incoming (Bitcoin received) and outgoing (Bitcoin spent) transactions.

Ideally, you want to use a new public address each time that you receive Bitcoin. If you use the same public address, then anyone who knows that address can check how much Bitcoin you have received and spent on that address. This can be done using Block Explorers (explained previously) which can track transactions and search public addresses.

Exchange Wallets

These are the most common. If you join an exchange, they give you a wallet. You can access this wallet from the exchange's website, or a phone app if they support one. There are a few negatives keeping your Bitcoin in an exchange wallet. First, you will not have access to the private keys, so you cannot re-create the wallet using a master seed. Second, if the exchange gets hacked, your Bitcoin is at risk. Third, the exchange could commit fraud and close down. Fourth, you could get locked out of your account.

Exchanges will tell you that your Bitcoin is insured while it is on their website. However, it is not insured if your account gets hacked by someone who knows your password. They only insure it if the exchange itself gets hacked.

Because of these risks, most people recommend keeping your Bitcoin off of exchanges. That said, exchanges do offer a place to store your Bitcoin. They may seem risky, but once you remove your Bitcoin from an exchange, it is now your responsibility to secure your Bitcoin.

For some people, letting Coinbase or Gemini or another exchange hold their Bitcoin may make sense. All they need to know is their password to log in. Yes, it has more risk, but it also offers ease of use.

Smartphone Wallets

These are wallets that can be installed as apps on a smartphone. These are very common. Most exchanges have an app that provides direct access to an exchange wallet. There are also private smartphone wallets that act as your personal wallet. These wallets can hold dozens of different cryptocurrencies, but likely not all of them. Often people own multiple wallets because they can't find one that holds them all.

I have read that smart phones are more secure than laptops or desktops. They are much more difficult to hack. So, from a security standpoint, the smartphone wallet is probably more secure than a laptop/desktop wallet.

Laptop/Desktop Wallets

These are software wallets that exist on a laptop/desktop. These wallets are essentially the same as a smartphone wallet but run on your laptop/desktop. Some analysts recommend against keeping your wallet on a laptop/desktop if it is connected to the Internet. Laptop/desktops are notorious for getting hacked. If you prefer these wallets, then consider getting a VPN (virtual private network).

Hardware Wallets

These are personal wallets with a high degree of security. Hardware wallets allow you to hold your private keys in the wallet itself, off of the Internet. Plus, you can re-create the wallet using a master seed if you forget the password or lose the wallet. All hardware wallets are also HD wallets.

Currently, the two most popular hardware wallets are Trezor and Ledger Nano.

Cold Wallets

Any wallet that is offline is considered a cold wallet. The first cold wallets were paper wallets. People would print out their private keys and public addresses onto paper. Very few people use paper wallets anymore now that we have hardware wallets, although people do write down their master seeds.

Any wallet that if offline is considered to be in cold storage. Often people will back-up a software wallet onto a USB drive and then take it off their computer. Perhaps the best cold wallets are hardware wallets. They are only online when you make transactions.

Multi-signature Wallets (also called multisig)

These wallets add extra security by requiring extra digital signatures. Multisig wallets can be used by organizations, families, or individuals who want extra security and want to use two or more digital signatures per transaction.

Typically, these wallets work by using a graphical interface that allows someone to setup a shared wallet and then invite others to share it. If it was only for themselves, then they would share it with themselves. The transactions are created in the same manner as a normal transaction, thereby sending an amount to a public address. The only difference is that the same transaction is repeated by the number of people required to finish creating the transaction.

It is somewhat similar to two-step authentication, although you can have as many people as you want to approve the transaction. Multisig wallets are configurable and can require everyone who shares the wallet to approve the transactions, or only a few people. For instance, 1 of 2, 2 of 2, 3 of 5, etc.

A typical multisig transaction would occur with someone starting the transaction and then sending an email to the other people who share the wallet. These people would log-in and send the same transaction to finish creating the transaction.

Multisig wallets are common with institutions, where the person doing the transaction does not own the funds. However, they can also be used by individuals for added security.

Multiuser Wallets (also called shared wallets)

Some wallets can be shared using multiple accounts. In other words, there is one Bitcoin balance, and multiple people can spend it using their own account. Thus, it would have one source of funds, and then multiple users could spend it. Then the wallet could track who spent it and how. This could be useful for a family.

Lightning Wallets

A lightning wallet is used on the Lightning Network (explained later). It is funded from an on-chain wallet. Once an LN payment channel is closed, the Bitcoin transfers from the Lightning wallet to the on-chain wallet. These wallets are only used by vendors/merchants or LN nodes. They are not used by consumers.

Wallet Transaction Descriptions

Some wallets allow you to include a description or label for a transaction. This information is not included with the transaction. Instead, these descriptions remain in the wallet. This is a wallet feature that helps you to remember how you spent your Bitcoin. If your wallet does not have this feature, you can find a wallet that does.

Full Nodes

A computer running Bitcoin software and connected to the Bitcoin network is called a node. If the node is configured to be in compliance with the Bitcoin rules and has downloaded the blockchain, then it is considered a full node. It can then begin verifying blocks and transactions.

Anyone can run a full node if they have a computer with sufficient software and hardware capabilities, such as the ability to download the blockchain, which is currently about 220 GB. There is no Bitcoin organization that gives authorization to run a full node. The software is free to download and install.

Because full nodes hold then entire blockchain, only a few nodes are needed to ensure the integrity of the blockchain. Thus, the blockchain is not stored in a single location but in many locations all at once.

There are four main functions that a full node performs:

1) Mining.

   A mining pool needs to have its own full node in order to create new blocks.

2) Routing.

   Full nodes do not have to mine. They can be used for validating transactions and blocks, and routing this information to other nodes.

3) Validation/Verification (synonymous words).

One of the most important functions of a full node is to ensure that transactions and blocks are created following the Bitcoin rules. Without validation, the blockchain would lose its integrity.

4) Wallet Support

A full node can have its own wallet and create transactions. It can also provide wallet functions for private/personal wallets.

Currently, there are about 10,000 full nodes, with the majority of them in Europe. The second most are in the U.S., with Asia third. The rest are spread out through the world.

> Note: When a new node is added to the Bitcoin network, it only connects to a few nodes in its proximity. These are the only nodes that it talks to and listens to. The network is smart enough to have enough nodes talk to each other to propagate a transaction to nearly all of the nodes in a few seconds.

Lightweight Node

A lightweight node (also called light node) installs the Bitcoin software, but does not download the entire blockchain. These nodes only download the blockchain headers, which is a fraction of the size of the entire blockchain. The purpose of these nodes is not to verify transactions, but to confirm that a transaction is on the blockchain. This confirmation is mostly done for wallets to display if a transaction has been confirmed. This is done using SPV (simplified payment verification) (explained later).

The main purpose of a lightweight node is that it can be used by companies that support wallets. Many of the popular wallets utilize SPV to verify that transactions were confirmed. Many of these are called thin wallets or thin

clients because they rely on SPV. Many of the smartphone wallets rely on SPV.

If you have a wallet, you can check if it is an SPV or API wallet type. An API wallet is the traditional wallet that relies on a centralized server that supports an API, such as Blockchain.info. An SPV wallet goes out and finds the information from a random lightweight node or perhaps from its own lightweight node.

The idea behind SPV is that you can determine if your own transactions have been confirmed without needing to ask someone else or having the full blockchain. Thus, a wallet software maker can do this for their wallets instead of relying on someone else.

Forks

Often (about once a week) there are two blocks created at nearly the identical date/time. This creates a fork that is resolved by the branch with the longest overall chain. On most occasions when this occurs, the shorter chain (also called a branch) dies within the next 2 blocks. Once a branch dies, its transactions go back into the mempool, if they are not already on the blockchain.

On most occasions, when there is a fork, it is handled nearly seamlessly. Most of the transactions on the branch that died are likely already on the blockchain on the other branch. Any transaction missing from the blockchain that was added back to the mempool will be included in subsequent blocks.

A fork can occur because each block can only have one parent. Here is an example comparing two miners that create a fork. Let’s say that both miners have a blockchain with three blocks A, B, and C. Then, when block D is

mined, the two miners receive different D blocks. Let's call these D1 and D2. These D blocks were mined at the same time and are both valid.

In this situation, both D1 and D2 would both have the same C parent. So, one miner's chain is A, B, C, D1. The other miner's chain is A, B, C, D2. When the E block is mined, it can only have a parent of D1 or D2. This means that the E block cannot be added to both chains. It can only be added to its parent, which will either be D1 or D2.

As long as there is not another duplicate E block (E1 and E2), then the longest chain will be apparent fairly quickly. Either D1 or D2 will be the orphan branch that dies.

One thing to be aware of is that when these duplicate valid blocks are created, they go into an orphan block pool if the parent is not found. Then if the parent arrives, the full node adds the parent and child (or children) blocks to the chain. In other words, all of the valid blocks that are mined are propagated to the Bitcoin network; then they are stored either on the blockchain or in the orphan block pool.

The blockchain can consist of three things: the main chain, branches, and orphans. Most of the time, the only thing that exists is the main chain, which is a single chain of blocks that are made up of parents and children. However, on occasion, the branches and orphans can make their presence known until the singular chain reasserts itself.

> Note: Blocks contain their parent block ID, but not their own block ID. So, when a new block is mined and propagated to the network, what is received by the full nodes is a new block with its parent block ID. The full node will calculate the block ID (hashing the header and the nonce) of the last block on the chain and see if it

matches the parent block ID. If they match, then the block is added to the chain. If they don't, then it becomes an orphan block.

Soft Fork

A soft fork is when there is a Bitcoin software upgrade, and it is backward compatible. This means that any changes made will only take effect on those nodes (and miners) that upgrade. The nodes that remain on the old software can continue verifying and mining, but they will not have the new changes.

A soft fork is the preferred method for doing an upgrade because it allows a steady, seamless transition to a new version. However, it can create situations where nodes are running different versions of the Bitcoin software. Even if these versions are compatible, some nodes will have different functionality.

Most soft forks are non-contentious. These are forks that are approved by miners during the BIP process, and then everyone slowly upgrades. However, because voting for BIP's is only done by miners and not the nodes, you can get contentious soft forks.

What usually happens for BIP's, is that the miners agree to a BIP and then the Core Developer Team releases a new version. Then both the miners and nodes slowly upgrade to the new software release. In this type of upgrade, the nodes are kind of taken for granted. The expectation is that the nodes will follow the miners.

If some of the nodes do not like the new changes, they do not have to upgrade. They can be intransigent and remain on the old version. This results in a contentious soft fork, with multiple versions of Bitcoin being used.

A user-activated soft fork is usually a rebellion against the miners. This happened in 2017, with the adoption of SegWit. This type of soft fork is when the nodes, and Core Development Team, try to enforce new rules by adopting a BIP that the miners have not yet approved. The nodes go first and upgrade to a new software release, which then puts pressure on the miners to upgrade as well.

Hard Fork

A hard fork is a Bitcoin software upgrade that is not backward compatible. This means that a new blockchain will be created once the software is installed. Usually, a pre-determined date/time is decided for the software release. A hard fork requires a software upgrade by both the miners and the nodes.

After the hard fork software is deployed, normally the previous blockchain is abandoned. However, if there are enough miners and nodes to support both blockchains, then you end up with two competing blockchains. This has occurred several times in the past, leading to the creation of a new altcoin, such as Bitcoin Cash and Bitcoin Gold.

The Bitcoin Cash hard fork was the most contentious in Bitcoin's history. In fact, to this day, supporters of Bitcoin Cash call it the "real" Bitcoin. What happened is that a group within Bitcoin disagreed over how to scale Bitcoin to handle more transactions. This dissident faction created a hard fork to create a new altcoin with their preferred scaling solution. When they did this, they kept the existing blockchain, but all new blocks were created with a new version of the Bitcoin software.

After the Bitcoin Cash hard fork, there was a duplicate blockchain. This meant that if you owned any private keys on the Bitcoin blockchain, you also

owned the private keys in Bitcoin Cash. Essentially, this meant that anyone who owned Bitcoin at the time of the hard fork could receive Bitcoin Cash for free (plus a capital gains tax). For example, if you owned 1 Bitcoin, then you also owned 1 Bitcoin Cash.

When these hard forks occur, and a new altcoin is created from Bitcoin, you have to find out how to claim your free cryptocurrency (plus a capital gains tax). Some exchanges and some wallets support the ability to claim your cryptocurrency. Do your own DD (due diligence).

Hard forks do not have to be contentious as along as everyone agrees to upgrade. The problem is that Bitcoin has gotten so big that it is very difficult to get everyone to agree to make a major change to the software. For this reason, soft forks are the preferred method of making changes.

Even if a contentious hard fork occurs, it is very difficult to maintain a new altcoin, especially a proof-of-work altcoin, such as Bitcoin. If a group wants to create a new altcoin, then they will need significant support to make that happen. Many of these altcoins are likely to have a short lifespan unless they can maintain enough support from miners, users, and investors.

Many of these hard forks are not contentious, but they still lead to new altcoins. What happens is that someone decides to create a new altcoin and uses Bitcoin as their starting point, then they modify the software and create a new version. Since it is open-source software, no one can stop them. This is how Bitcoin Gold and many other altcoins came into existence.

> Note: If there is a contentious hard fork that lasts for an extended period, then you could have two long branches. The way that the proof-of-work is calculated for each branch is not the number of blocks. Instead, it

the sum of difficulty in each block. The difficulty is an integer, so it is easy to add up.

Consensus

The first type of Bitcoin consensus is proof of work. This basically means that the longest chain wins. When there is a fork, the longest branch becomes the blockchain, and the shorter branch dies. This is a type of economic consensus, whereby the majority of miners decide which blockchain to mine (add new blocks).

The second type of consensus is how the Bitcoin software is upgraded. The software upgrades are called a BIP (Bitcoin Improvement Proposal). These are documents that propose changes to the Bitcoin software. Since Bitcoin was deployed in 2009, there have been about 100 BIPs added to Bitcoin. That is quite a few, and an average of about 10 per year.

A BIP gets approved when it has 95% support from the miners who have mined the last 2,016 blocks (14 days x 144 blocks = 2,016). Usually, it's that simple. If the miners approve it, then the BIP gets added. However, that's not always what happens. Why? Because the nodes running on the Bitcoin network do not get to vote, but they do get to decide which Bitcoin version to install. Over the years, there have been a few rebellions on installing a new version, and it will likely happen again.

Ultimately, all types of Bitcoin consensus are economic. For instance, miners choose which blockchain to mine based on their economic interest. Nodes and miners run the Bitcoin software that they believe has the best economic outcome. What is unique about Bitcoin is that consensus is built into how it evolves. No single person, group, or organization can determine the outcome, unless they can garner enough support to create consensus.

Anonymous / Privacy

Bitcoin is not completely anonymous because the blockchain can be searched by anyone who has access to the Internet. What is anonymous are the private keys, which are not exposed to the public. What is exposed are the public addresses and the transactions to those public addresses. If someone can find out who owns a public address, then they can know that person's transactions for that address.

One of the ways to limit exposure of a public address is to use a new public address for each transaction. Another way is to use two wallets and transfer Bitcoin between them. However, this method is not ideal, because the IP addresses can be traced. If you are going to transfer Bitcoin between wallets, then use a VPN to hide your IP address.

Perhaps the ideal way to protect your identity is to use a mixer (also called tumbler) service. How it works is that you send your Bitcoin out into the Bitcoin network, but on its journey, it gets split up and sent to various addresses numerous times. To use a mixer service, it's probably better to have two wallets. One to send and one to receive. Ideally, use these in conjunction with a VPN.

Buying and Selling Bitcoin

Coinbase is the largest U.S. exchange and is based in San Francisco. It is perhaps the easiest to use, and they have phone support. Most people consider it the best exchange for newbies.

Coinbase Fees

- Buy Bitcoin using ACH (linked bank account) or a funded Coinbase dollar account: 1.49% of the total purchase.

- Buy Bitcoin using a Credit Card: 3.99% of the total purchase.
- Sell Bitcoin: 1.49% of the total sale.

I use Coinbase and consider it easy to use. They do have high fees compared to some of the other exchanges. For instance, Robinhood (also based in the United States) does not charge any fees to purchase Bitcoin. You can setup a link to your bank account using Robinhood and purchase Bitcoin with no fees, and then transfer the Bitcoin to your personal wallet.

Robinhood currently does not have a feature to sell Bitcoin for dollars. Once they offer that feature, there won't be a reason to use Coinbase for buying and selling Bitcoin – unless Coinbase lowers their fees.

> Note: You do not have to sell your Bitcoin on Coinbase if you purchase them there. You can transfer your Bitcoin to your personal wallet (with no Coinbase fees) and then sell them somewhere else. In the future, there will likely be exchanges that sell Bitcoin for much less than 1.49% of the total sale (the current Coinbase fee for selling).

Exchanges

There are dozens of cryptocurrency exchanges all over the world. Some of these exchanges only use cryptocurrency, and others allow you to buy with fiat currencies and sell your cryptocurrency for fiat.

The exchanges that only use cryptocurrency are only for trading. Thus, you transfer your cryptocurrency to the exchange, do your trading, and then transfer it back off the exchange. Most of these exchanges have low fees for trading, but also charge fees for moving your cryptocurrency off of the exchange.

There have been many exchanges that have been hacked over the years. If you Google for Cryptocurrency Exchange Hacked List, you will see the long list. There have been eight exchanges hacked in 2019, so this problem has not gone away. For this reason, it is recommended not to leave your Bitcoin on exchanges when you are not trading.

Some exchanges have suddenly went offline, such as QuadrigaCX (based in Canada) in 2019. The founder was found dead, and $190 million in cryptocurrency was missing and owed to 115,000 customers. They estimate the company only has about $20 million in assets. It's unlikely the customers will receive a settlement.

Because these exchanges are all over the world, most investors stick close to home. Those who use foreign-based exchanges face more risk. For instance, Binance, which is based in Taiwan and Japan, has said they are no longer going to allow USA customers on their exchange.

Also, some countries are still deciding if they will allow cryptocurrencies or cryptocurrency exchanges. Countries such as China, India, and South Korea are still deciding what to do.

Currently, Japan, Australia, Western Europe, Canada, and the USA seem to be backing cryptocurrencies. However, it is still early, and countries could still change their mind. I think Japan is the most important country because of their government's strong support for Bitcoin. If Japan continues to support Bitcoin, then the rest of the world will have a hard time making Bitcoin illegal. I doubt that the rest of the world is going to give Bitcoin to Japan. Also, Switzerland seems to be supporting Bitcoin. All it really takes is for one significant country to get behind Bitcoin to keep it alive.

Bitcoin versus Litecoin

Litecoin was created by Charlie Lee in 2011. Litecoin is basically a copy of Bitcoin, and was created using a hard fork of Bitcoin. There are not very many significant differences between Bitcoin and Litecoin, although there are some.

1) Faster Blocks.

   Litecoin creates a block every 2.5 minutes. This means that Litecoin creates four times as many coins each day. Whereas Bitcoin has about 17 million Bitcoins in circulation, Litecoin has about four times as many.

2) Faster On-Chain Confirmations.

   Because Litecoin creates a block every 2.5 minutes, an on-chain transaction can have its first confirmation in 2.5 minutes. Thus, confirmations on-chain are four times as fast as Bitcoin.

3) Different Mining Algorithm.

   Litecoin uses a different hash algorithm for mining. This was Charlie's idea to create a separate mining network for Litecoin. He didn't want to disrupt the Bitcoin mining network. His intention was to supplement Bitcoin and not to replace it, or impact it in a negative way.

4) Marketing.

   Because of the Litecoin Foundation, Litecoin reaches out to merchants and businesses to use the Litecoin software. It also advertises and promotes the brand.

5) Easier to Modify.

   Because of the Litecoin Foundation, Litecoin has shown the ability to avoid contentious consensus feuds for software upgrades. Changes to Litecoin software have been much easier and faster than Bitcoin.

Other than those significant differences, currently Bitcoin and Litecoin share most of the same software.

When Litecoin was created, the idea was to create faster transaction confirmations and to have lower fees, especially for micro-payments. Charlie Lee, who created Litecoin, always said that his vision was to compliment Bitcoin and not compete against it. However, while that might be good in theory, they are both transactional currencies and do compete with one another.

They both use their own Lightning Network, so they compete directly for fast transactions, low fees, and micro-payments. In many respects, the use-case for Litecoin has been diminished by LN.

Litecoin is likely to survive because it has been around since 2012 and has a strong brand name. Although it will have a difficult time competing against Bitcoin. Currently, it is only valued at .093% (less than 1%) of Bitcoin. In theory, it should be valued much higher if it were a true equal to Bitcoin.

Litecoin does have one strength that Bitcoin does not, which is the Litecoin Foundation. This foundation has a board of directors, and Charlie Lee is the managing director. This foundation is the de-facto leadership of Litecoin.

I say this is a strength because it allows Litecoin to adopt changes much easier than Bitcoin. For instance, it adopted SegWit and LN before Bitcoin. Some people consider Litecoin as the "Test Bed" for Bitcoin. New technologies tend to be introduced on Litecoin first before they make it to Bitcoin.

If Bitcoin survives, then Litecoin should have some popularity because of its strong correlation to Bitcoin, along with its strong brand name. The Litecoin Foundation has always said that it does not want to compete with Bitcoin

and that it wants to supplement Bitcoin. Charlie believes that there is room for both, and he might be right.

In many respects, Litecoin acts like Bitcoin's little brother and there in case Bitcoin stumbles. It's like a backup plan for low fee micro-payments. Also, it will likely test new technologies to ensure that low fee micro-payments are possible for consumers.

Bitcoin versus Bitcoin Cash

Bitcoin Cash was created from a fork in Bitcoin in 2017. This was the first significant Bitcoin consensus battle between competing factions. On one side of the feud were those who believed bigger blocks were the answer to scalability. On the other, were those who believed bigger blocks were not the answer.

The summer of 2017 will go down in history as when SegWit was adopted, which allowed secondary layers to be added to Bitcoin. There was a faction who disagree with this approach. The result of which was a fork that spawned Bitcoin Cash.

Currently, Bitcoin Cash has a maximum block size of 8MB, whereas Bitcoin has a maximum block size of 1MB, unless SegWit is used.

Bitcoin Cash got its wish of increasing the block size; however, it has not adopted SegWit or secondary layers. This means that it might not be able to provide micro-payments at the tiny fees that the Lightning Network allows.

It is my opinion that Bitcoin Cash appeared because the miners wanted it. Why? Because secondary layers limit their profitability. Any transactions that occur off the blockchain do not require fees to the miners. The secondary

layers lock out the miners from receiving fees, other than the opening and closing transactions.

I've always been a fan of secondary layer solutions because large blocks are not a good solution to the scalability problem. All that happens is that larger and larger blocks are needed. Thus, it is not a solution but a Band-Aid. Also, larger blocks make hardware more expensive, which centralizes the network, and prices out any average Joe who wants to support the Bitcoin network. Plus, larger blocks create spam issues. It is much easier for Bitcoin to fight against spam with smaller blocks.

In short, large blocks and no secondary layers seems like a silly idea to me. So far, the market has agreed, although Bitcoin Cash is still around. The irony is that even with their large 8MB blocks, the average size Bitcoin Cash block is less than 1MB. Their strategy seems to be, build it, and they will come. However, they may never need 8MBs.

One thing that Bitcoin Cash has going for it is that their fees have been very low. Currently, the average transaction fee is only about 1 cent. But those tiny fees are from small blocks. The average-sized block is about 200K. If their blocks jump in size, so will their fees. The result would likely be fees much higher than the Lightning Network.

Alt Coins

The definition of an altcoin is any cryptocurrency that is not Bitcoin. There are currently more than 2,000 altcoins that trade on cryptocurrency exchanges.

I like to break altcoins into categories. Here are some categories to consider:

1) Transactional Currencies.

Litecoin, Bitcoin Cash, Monero, Dash, Zcash, DigiByte, ByteCoin.

2) Development Platforms and Smart Contracts.

   Ethereum, EOS, NEO, Stellar, Cardano, Chainlink, NEM, Iota, QTUM, TRON, Aion, Corda, Waves, Stratis, Tezos, Nxt, Ontology, ICON, Lisk.

3) Special Use-Cases.

   Most of the altcoins have special use-cases. For instance, anything that you can think of that you could monetize could be used with virtual money. Here are a few examples.

   Ripple: Used to transfer cryptocurrency across borders. Ripple is currently used by banks and financial institutions, but could spread to individuals and other businesses. Note that Ripple does not use a blockchain.

   Populous: Attempts to solve the problem of accounts payable. Let's say you're a business and your customers pay you on-average every 90 days. You could sell part of that income stream to investors on the blockchain and get paid much quicker than 90 days.

   Ravencoin: Used to transfer assets from one owner to another. It is similar to Bitcoin and was a fork of Bitcoin. However, the use-case is not to be a transactional currency. Instead, it aims to designate ownership of assets. Practically anything you could define as an asset could be held on the Ravencoin blockchain, such as deeds or stocks.

Some people think that altcoins are rubbish and are all going to be worthless in a few years, but that's not my opinion. Many of these altcoins offer news ways to conduct finance and new products and new technology that is going to be popular. I will be surprised if many of these altcoins are not highly successful.

Here is something to ponder for transactional cryptocurrencies. Currently, there are only 6 million Bitcoin wallets with more than $180. That means practically no one owns Bitcoin. Even if there are an estimated 32 million people with a Bitcoin wallet, most of these wallets are empty or have a very little amount of Bitcoin in them. Also, there are only about 600,000 wallets with more than 1 Bitcoin.

What that information tells me is that once cryptocurrency becomes popular for making money transactions, Bitcoin will likely to be very expensive and very few people will own more than one. In my opinion, this opens the door to altcoins that are less expensive. How many people are going to want to buy .0001 Bitcoin? That’s depressing. Many would rather buy 1 Litecoin or 1 Monero, or 1 whatever. I will be surprised if these lower-valued cryptocurrencies do not find demand just because of the high valuation of Bitcoin.

Lightning Network (LN)

This technology attempts to solve the scalability problem with Bitcoin. It overcomes the current seven transactions per second limit. In theory, LN should be able to perform thousands of transactions per second. It does this by performing off-chain transactions using a secondary layer.

This secondary layer sits on top of the Bitcoin network. It works by setting up payment channels between LN peers. It's a secondary peer-to-peer network with potentially millions of interconnected LN nodes. It works by allowing payments to hop through these LN nodes and eventually into the seller’s Bitcoin wallet. I say eventually because LN uses a delayed payment settlement system in order to reduce fees.

The idea behind LN is that not all transactions need to be on the blockchain. Instead, a series of LN transactions can be grouped together into a single blockchain transaction. Then that single transaction can have a single on-chain transaction fee. This final settlement transaction moves Bitcoin from the LN wallet into a blockchain wallet. Note that until the final settlement is made, the Bitcoin in the LN wallet is locked and not yet on the blockchain.

The main purpose for LN is to scale Bitcoin to be able to do thousands of transactions per second, but it also has the effect of lowering fees. Initially, it will be used by merchants to accept small payments, but it is not inconceivable that it could evolve to include larger purchases.

The benefits of LN are substantial:

1) Scales Bitcoin to handle more transactions per second.
2) Lowers fees.
3) Creates nearly instantaneous confirmations for buyers.
4) Lowers the requirements of the Bitcoin transaction pool, thereby making the Bitcoin network more efficient.
5) Creates the potential for Bitcoin to be a widely used transactional currency.

Unfortunately, there are also several weaknesses with LN:

1) Payment channels have to be pre-funded before they can be opened.
2) Payment channels are vulnerable to hacking because the private keys for the LN wallets (hot wallets) exist on LN nodes.
3) It is based on trust, and any threat to that trust could impact its usage.

4) It requires a settlement transaction to transfer Bitcoin from an off-chain LN wallet to an on-chain wallet. This delays payment until the settlement transaction is completed and confirmed.
5) It is still in its infancy and issues are still being worked out, such as effective routing.

From my perspective, the key to the success of LN is trust. As long as the merchants trust that they will get paid, then it should be a success. Without this trust, then it will fail.

One potential flaw with LN is that it requires on-chain Bitcoin transactions to open and close payment channels. If there are high fees on the Bitcoin blockchain, then this could impact the trust of LN. The reason why is that it is possible for fees to be too high in relation to the capacity of the channel.

For instance, let's say the transaction pool fills up and fees jump to an average of $5 per transaction. In this scenario, a channel might have a capacity of $30 and opening/closing fees of $10. If they open and close the payment channel daily, they would be paying $10 a day to maintain the payment channel. Some merchants might turn off the LN nodes under this scenario.

In my example above, high Bitcoin transaction fees could impact trust in LN. If a merchant cannot trust that transaction fees will remain low and stable, then they might not want to use LN.

Another potential flaw with LN is that nefarious nodes can try to cheat their peer counterparts. This can be done if one of the peers goes offline. When a peer is offline, the other peer can try to do a settlement transaction that is not accurate and attempt to steal Bitcoin from the other peer. We will likely hear more about this potential flaw when this situation occurs.

Stealing from a counterpart requires that the counterpart remains offline for an extended period. Also, there is something called a watchtower that is planned to prevent this occurrence. The watchtower will monitor LN settlement transactions to close them accurately.

Another potential flaw is data corruption. If an LN node is corrupted and it does not have the latest backup, then it could lose the Bitcoin in the LN wallet. The reason why is that there is no master seed for an LN wallet.

The good news is that these issues are not necessarily deterrents to LN usage. LN is meant for small transactions, so the risk can be limited. I am confident that LN will continue to expand. There are already three compatible implementations (C-Lightning, Eclair, and Lightning Labs), and thousands of LN nodes are appearing. These companies are providing software that can be used to create LN nodes. Today the LN is up and running and likely will continue to expand.

What makes LN so powerful is that once a channel is open (with capacity in both directions), it can make hundreds or thousands of low fee transactions off-chain, and then use a single on-chain transaction to close the channel. The closing transaction settles the payment and moves the Bitcoin to a blockchain wallet.

There are two types of LN nodes. The first type is a routing node (also called hopping node) that simply transfers payments to the next node. Routing nodes are used to hop through the LN. To make an LN payment, it usually takes more than one hop.

For each hop from the sender to the merchant, an LN node collects a small fee. This fee is usually less than a penny. When a routing node does a closing transaction, they move the Bitcoin they used to open the payment channel, plus any fees they received for doing transfers, to the blockchain.

When payments hop between nodes from the sender to the merchant, LN uses something called onion routing. What this means is that each LN node only knows the previous node's address and the next node's address. Thus, an LN node cannot send the transaction anywhere else except forward a single node or backward a single node. They only have enough information for a single hop in both directions.

For a routing node, one of the factors that impacts their profit is how much it costs them to open and close the channel. Both of which are done on-chain and require Bitcoin transaction fees. If Bitcoin on-chain transaction fees are high, then the breakeven cost can be significant since fees received to route LN transactions are very low.

The LN nodes that receive the final payment that hops through the LN are called merchant nodes. They are called merchant nodes because it is merchants who receive payment for products or services that they sell.

> Note: It's possible for a business to use LN to move money between their organization. So, while they are called merchant nodes, they are really receiving nodes. They are the end of the line for LN transactions.

When a merchant closes their payment channel, it includes all of the Bitcoin received while the payment channel was open. This Bitcoin sits in their LN wallet until the payment channel is closed. This delay in moving Bitcoin from their LN wallet to their blockchain wallet is done so that fees can be reduced for their customers.

To review, the way that LN works is that when you buy something, such as a cup of coffee, your wallet shows that you spent some Bitcoin (because a transaction was made). The transaction is instantly confirmed because it was an LN transaction. However, the Bitcoin that you spent is now sitting in an

LN wallet and is not yet on the blockchain (available to be spent by the receiver). It will sit in that LN wallet until there is a settlement transaction that closes the payment channel and moves the Bitcoin to a blockchain wallet.

If a merchant wants to sell you coffee with a low fee, they can currently do that by using LN and making their transactions through an LN node. These all occur off-chain. All they need to do is trust that they will eventually get paid with a settlement transaction. Instead of getting paid on-chain using hundreds (or thousands) of daily on-chain transactions, instead, they will get paid with one on-chain transaction at the end of the day.

The merchant using LN does take a risk that the Bitcoin in their LN wallet will not be transferred to the blockchain at the end of the day (there are several reasons why this could occur). However, as long as LN is dependable, they should be willing to use it.

What happens during the day is that LN wallets hold Bitcoin that has not been transferred to the blockchain. Thus, there is a delay before the Bitcoin is moved to the blockchain. This length of this delay can be determined by either peer in the payment channel. Every payment channel is between two peers, with each peer sharing an LN multisig address.

At any time, a peer can attempt to close the payment channel and move their Bitcoin to the blockchain. If both payment channels are on-line, then closing the channel should be straightforward. However, if one of the channels is off-line, then there is a delay until both peers can confirm the settlement. However, once this delay period expires, the peer who started the settlement transaction can proceed to move their Bitcoin to the blockchain without approval from the other peer.

This problem with both peers needing to be online to close the payment channels is the reason for the watchtower. They are currently under development. In theory, the watchtower should be able to act as an intermediary and approve or deny closing the channel.

Most merchant accounts do not have this online issue of closing payment channels because they use a payment provider. In fact, when using a payment provider, merchants can use LN and not even have an LN wallet. It is all seamless to them, and they get paid in dollars.

If you were a merchant and wanted to provide your customers a Bitcoin payment option, why not open a low-fee LN payment channel? You could open it in the morning and then close it at the end of the day. Why force your customers to pay high fees when LN is available?

> Note: There are payment providers, such as Coingate and Paytomat, that allow merchants to use LN. From the merchant's perspective, they do not need to know anything about Bitcoin or LN, because they are paid in cash by the payment provider. These LN payment options allow consumers to purchase items using Bitcoin. The LN is hidden from the customer. As far as the customer is concerned, all they are doing is making a Bitcoin payment.

LN works using multisig addresses, where two LN peer nodes share an address. The multisig address is essentially a payment channel. The peer that opens the channel creates the payment channel address and requests another peer to share the address. This address becomes a virtual invoice with multiple transactions. Then the invoice is paid using an on-chain settlement transaction.

To share a payment channel address, both peers need enough Bitcoin in their LN wallets to fund a transaction. This is called the payment channel capacity. Each payment channel has a maximum capacity for a single transaction, such as .001 Bitcoin. It also has a defined transfer fee in satoshis, which is usually very low, such as 1 satoshi. This is the cost to hop through the LN node.

As mentioned earlier, the capacity is the combined inbound capacity (also called remote balance) and outbound capacity (also called local balance). If this capacity is not balanced, then it can create routing problems. For example, if the combined capacity was .002 Bitcoins, but the inbound capacity was much lower than .002, it could restrict routing on that LN node. Ideally, you want the inbound and outbound capacity to be balanced.

Most LN nodes are hopping nodes. All they do is forward a transaction to the next node. To perform this forwarding service, they take a small fee each time they forward a transaction, usually less than 1 cent.

LN is a peer-to-peer network with each pair creating a payment channel with a specific capacity and a transfer fee. A transaction can take several hops through the LN before reaching its destination, which is usually a merchant. A single satoshi is less than a penny, so these fees can be very low.

LN uses a mesh network, whereby a payment can be routed from peer to peer as long as those peers have shared open payment channel with sufficient capacity. However, it looks more like a hub and spoke network because it is more economical to open channels to large hubs that have more traffic.

When an LN transaction is created, the LN attempts to find the cheapest route from start to finish using all available connected channels. Some say that this type of mesh network routing is flawed and will create problems.

Others say that LN routing will improve over time. What everyone does agree on is that routing is still a work in progress, and no one knows how it will evolve. In fact, each of the LN implantations (which have compatible nodes) all use different routing methodologies.

One of the current routing flaws is that the sender, who must determine the route before it sends a payment, cannot see the local and remote balances of each LN node. They can see the capacity, but not the distribution of that capacity. Unless an LN node has enough inbound and outbound capacity, it cannot route a payment. The inbound and outbound capacity is not exposed, because capacity is the combined inbound and outbound capacity. So, routing is determined using capacity, when it's possible that the inbound or outbound capacity is much less than the overall capacity. That is a flaw that needs to be fixed.

One way the flaw mentioned above is fixed is using balancing. This means that the inbound capacity (the remote balance) and outbound capacity (the local balance) of a node is balanced, with equal amounts of Bitcoin in each. However, that is easier said than done and requires vigilance to maintain.

When a payment channel is opened, it only creates outbound capacity (the local balance). This is fine if you are an end-user and only spend Bitcoin to the channel you opened. However, in most cases, you will want to also receive Bitcoin on your LN node.

There are several options for creating inbound capacity (the remote balance):

1) The easiest way is to open a few channels to large hubs and then simply wait for others to join your channel. This will work but will require some time. However, this does not guarantee balancing.

2) Ask channels to join yours.
3) Spend Bitcoin of the amount of your desired inbound capacity.
4) Purchase inbound capacity (there are several companies that offer inbound capacity for sale).

The whole capacity issue is confusing. In some ways, this is good because only people who know what they are doing are going to run LN nodes. The bar to understanding LN is much higher than running a Bitcoin full node.

Whereas, running a Bitcoin full node is permissionless, running an LN node requires that peers accept your invitation (it takes two to tango). This has the potential to root any bad actors. Because LN is not permissionless, it is inevitable that LN turns into some type of self-policing network. Eventually, we will see tools that show which are the most trusted routing hubs.

Because hubs are likely to have more trust and more traffic, it creates the potential for the mesh network to turn into a somewhat centralized hub and spoke network. Some analysts say that it is inevitable that some type of centralized hub and spoke network will appear. However, this type of centralization will not necessarily be bad if costs remain low, and stability is the outcome.

The way that LN routing currently works is that senders of LN transactions determine the cheapest route by checking all of the alternative routes. There is a map of all the LN nodes that are stored on the blockchain. The client making the LN transaction checks the map and looks for the cheapest route to the destination. Often routing fails. When it does fail, the sender's application will automatically try again using another route. This should be seamless to the person making the payment. Note that routing usually fails because of an LN node being offline or a lack of capacity (usually inbound capacity).

Glossary (As Defined for Bitcoin)

Anti-Fragile: Self-correcting software with very few points of failure.

Ancestors: Previous Bitcoin transactions related to the most recent transaction for a public address.

BASE58: Converts a binary number into an alphanumeric value. It only includes these 58 characters (see below). If you look closely, you will see that zero, upper case o, upper case i, and lower case l are missing. This was done to remove confusion:
123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz

Batch Transaction: A batch transaction is when you combine multiple payments into a single transaction. For every additional output (Bitcoin recipient), it only adds about 34 bytes. If you make a separate transaction to pay each recipient, then you are wasting fees. So, if you know you need to pay multiple people, you can do it all at once and save a lot on fees. Also, you can make the mempool more efficient because it has to handle fewer transactions.

BIP: Bitcoin software upgrades occur using something called a BIP (Bitcoin Improvement Proposal). These are documents that propose changes to the Bitcoin software. Since Bitcoin went live, there have been about 100 BIPs added to Bitcoin. That is an average of about ten enhancements per year.

A BIP gets approved when it has 95% support from the miners who have mined the last 2,016 blocks (14 days x 144 blocks = 2,016). Usually, it's that simple. If the miners approve it, then the BIP gets added. However, that's not always what happens. Why? Because the nodes running on the Bitcoin network do not get to vote, but they do get to decide which Bitcoin

version to install. Over the years, there have been a few rebellions on installing a new version, and it will likely happen again.

Bitcoin: An Internet-based virtual digital currency that is stored on a blockchain.

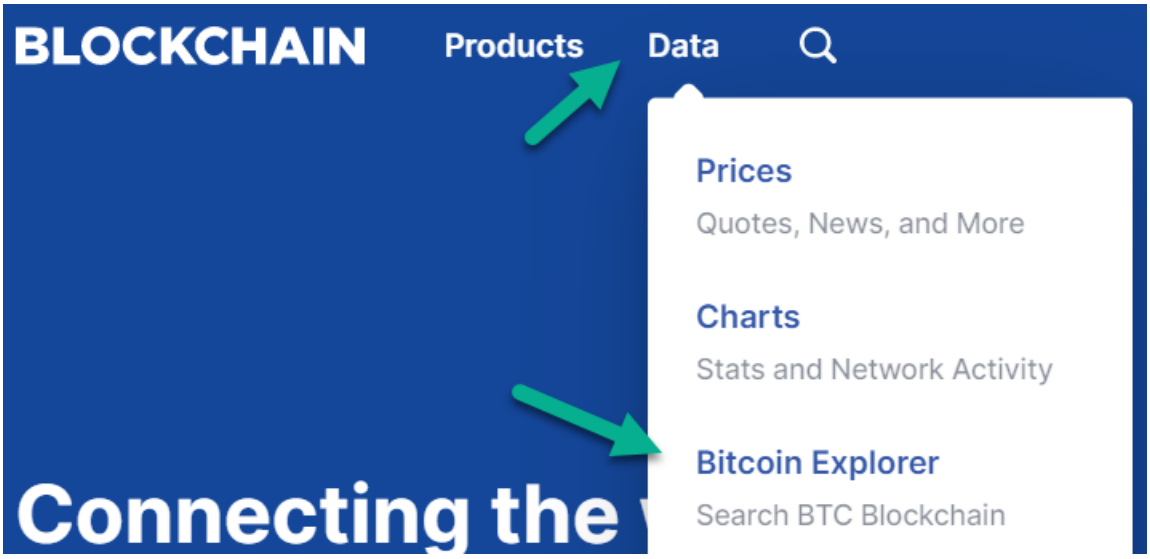
Bitcoin Mining: The process used to create new blocks. The first miner to find the next block's hash key gets to create the next block. This miner also receives a block reward, which is the generation of Bitcoin. This is how new Bitcoin is created.

Block: Approximately every ten minutes, a new block is created (144 per day). These blocks contain a block header and Bitcoin transaction data. The current average block size is about 1.2MB with about 2,000 transactions.

Block Header: This is the header data stored in each block. The header is comprised of six values: version number, previous block identifier, Merkle root, timestamp, difficulty, and nonce.

Blockchain: A chain of blocks with each block linked to the previous block. When a new block is created, it gets added to the end of the chain. At the beginning of the chain is the genesis block, which was mined in 2009.

Blockchain Explorer: Also called Blockchain Browser. They are usually Internet websites that allow you to search and display details about the blockchain. Most of them are free, although there are some that charge. The most well-known is www.blockchain.info (see screenshot below).



Blockchain Height: The number of blocks in the blockchain, or the number of a specific block. The Bitcoin blockchain currently has about 550,000 blocks.

Block Reward: The Bitcoin received by a miner for creating the next block. This reward is received approximately 24 hours after the block is validated. To create a new block, you must be the first miner to solve the hash problem. The current Bitcoin reward is 12.5 Bitcoins, dropping to 6.25 in May 2020.

Bloom Filter: This is a search method used by Bitcoin SPV wallets to prevent hackers from finding out which addresses they own. Bitcoin SPV wallets often do a lookup (search) on the Internet to find out if a transaction occurred or was confirmed. These searches use bloom filters to find the address but not include the entire address in the search.

Change: If you spend Bitcoin from a wallet, and you do not spend all of a previous input, then you will generate change. This change will normally go into a new address (also called a change address), but it could go back to the original address depending on how the wallet is configured.

Bitcoin uses an all-or-nothing rule for spending Bitcoin that you have received (inputs). If you want to spend Bitcoin, your wallet will check your inputs (available Bitcoin). Unless you have inputs with the exact amount that you want to spend, then you will get back change. Over time, you could end up with many of these change addresses. Note that you can aggregate these change addresses by transferring them into a new address.

Child Pays For Parent (CPFP): Instead of canceling (replacing) a transaction that is stuck in the mempool using RBF, there is another way. If a transaction gets stuck in the mempool because of a low fee, you can unstick it by using CPFP (as long as your wallet supports it).

To use CPFP, all you need to do is send one of the outputs (it must be your address) in the stuck transaction to a new address while using a higher fee. This will not only move the output to the new address, but it will also unstick the transaction that was stuck.

This can also be used for change that you are expecting. So, if you send Bitcoin to someone and it gets stuck, as long as there is some change in that transaction, you can use CPFP (as long as your wallet support it).

> Note: Because of the power of RBF and CPFP, make sure that your wallet supports both of these features.

Coinbase Transaction: When a new block is created, the miners add a special transaction called the coinbase transaction. This is how they pay themselves the reward and transaction fees for the block. This is the first transaction in the block.

CoinJoin Transaction: A CoinJoin transaction is when Bitcoin is spent from multiple inputs into multiple outputs. A transaction can have as many public address inputs and public address outputs as long as it fits in a block (1 to

4MB). When this is done with a lot of addresses, it is difficult to know which input is paying which output. These types of transaction add privacy, but also draw scrutiny from regulators who prefer transparency.

Cold Storage: Anytime that a wallet is off the Internet, it is considered to be in cold storage. Conversely, when a wallet is on the Internet, or on a device with access to the Internet, that wallet is considered to be a hot wallet. Cold storage is considered to be the safest location for a wallet.

Cold Wallet: Any wallet that is offline is considered a cold wallet. The first cold wallets were paper wallets. People would print out their private keys and public addresses onto paper. Very few people use paper wallets anymore now that we have hardware wallets, although people do write down their master seeds.

Consensus: The first type of consensus is proof of work. This basically means that the longest chain wins. When there is a fork, the longest branch becomes the blockchain, and the losing branch dies (the transactions for the losing branch go back into the transaction pool). The consensus is done automatically by the majority of miners mining the longest chain.

The second type of consensus is how the Bitcoin software is upgraded. The software upgrades are called BIP (Bitcoin Improvement Proposal). These are documents that propose changes to the Bitcoin software. Since Bitcoin went live, there have been about 100 BIPs added to Bitcoin. That is quite a few, and an average of about 10 per year.

A BIP gets approved when it has 95% support from the miners who have mined the last 2,016 blocks (14 days x 144 blocks = 2,016). Usually, it's that simple. If the miners approve it, then the BIP gets added. However, that's not always what happens. Why? Because the nodes running on the Bitcoin network do not get to vote, but they do get to decide which Bitcoin

version to install. Over the years, there have been a few rebellions on installing a new version, and it will likely happen again.

Cryptocurrency: Any form of virtual digital money can be considered cryptocurrency. Bitcoin was the original form of virtual digital money, and it is based on cryptography to remain secure. This is where the term cryptocurrency came from.

Cryptography: This is the science if encoding letters, numbers, and symbols to make them hidden and secret. Encryption is used to encrypt (encode), and decryption is used to decrypt (decode). When something is encrypted/decrypted, it is done using the science of cryptography.

Decentralized Mining Pools: Decentralized mining pools use a peer-to-peer network of miners. The reason these came into existence is to make large mining pools less of a threat to Bitcoin using a 51% Attack. For instance, a single large miner (or a group of miners) could cause havoc to the Bitcoin network with as little as 30% of the hash power. However, if a mining pool uses its own peer-to-peer network, then this threat is alleviated.

Difficulty: This is how much more difficult it is to mine a block versus how difficult it was to mine the genesis block. The difficulty is currently about 7.4 trillion. The difficulty is used to calculate the target, which the miners use to mine the next block in approximately ten minutes.

Digital Ledger: Bitcoin uses a public digital ledger, which is stored on a blockchain. The ledger contains all of the historical transactions of Bitcoin. The ledger can be queried using a Blockchain Explorer to display transaction information. Each transaction only includes amounts and digital IDs, and does not include names or descriptions.

This ledger only has one purpose, which is to identify who owns Bitcoin. If you have a wallet that has received Bitcoin, then the public ledger guarantees your ownership — as long as you can provide the private keys to that Bitcoin.

Double-Spend: This is the possibility for an input to a public address (Bitcoin received) to be spent twice, or multiple times. Bitcoin prevents this from occurring by using immutability and UTXOs (unspent transaction outputs). Because the blockchain cannot be edited and only one block is created at a time, the miners can verify that the UTXOs are only spent once in a block.

ECDSA: A public key is created using something called the Elliptic Curve Digital Signature Algorithm (ECDSA), which generates a 256-bit integer from the private key. Each private key can only generate a single public key.

Exchange Wallet: These are the most common wallets. If you join an exchange, they give you a wallet. You can access this wallet from the exchange's website, or a phone app, if they support one. There are a few negatives keeping your Bitcoin in an exchange wallet. First, you will not have access to the private keys, so you cannot re-create the wallet using a master seed. Second, if the exchange gets hacked, your Bitcoin is at risk. Third, the exchange could commit fraud and close down. Fourth, you could get locked out of your account.

Full Node: A computer running Bitcoin software and connected to the Bitcoin network is called a node. If the node is configured to be in compliance with the Bitcoin rules and has downloaded the blockchain, then it is considered a full node. It can then begin verifying blocks and transactions.

Anyone can run a full node if they have a computer with sufficient storage space to download the blockchain, which is currently about 220 GB. There is

no Bitcoin organization that gives authorization to run a full node. The software is free to download and install.

Genesis Block: This was the first block that was mined on January 3rd, 2009. That is when Bitcoin mining began.

Halving: One of the features of Bitcoin that makes it so valuable is something called halving. This is the process that reduces the reward by half every 210,000 blocks (approximately four years). On average Bitcoin mines a block every ten minutes, or 144 daily, or 52,560 per year. The next halving will occur approximately in May 2020. We do not know the exact date, because the Bitcoin blocks are randomly created with a ten-minute target.

After the next halving occurs in 2020, the number of newly created Bitcoins will drop to 900 per day. Then, in 2024 it drops to 450, then in 2028, it drops to 225, and on and on until 2140.

Hard Fork: A hard fork is a blockchain software upgrade that is not backward compatible. This means that a new blockchain will be created. To use this new blockchain requires a software upgrade by both the miners and the nodes. Normally, the previous blockchain is abandoned. However, if enough miners and nodes support both blockchains, then you end up with two competing blockchains.

Hardware Wallet: These are personal wallets with a high degree of security. These wallets allow you to hold your private keys in the wallet itself, off of the Internet. Plus, you can re-create the wallet using a master seed if you forget the password or lose the wallet. All hardware wallets are also HD (Hierarchical Deterministic) wallets.

Hash: In Bitcoin terminology, the word hash can mean two different things. First, it can refer to a single attempt by a miner at identifying the next block's hash key. Miners will attempt trillions of guesses, and each guess is a single hash. The process of identifying these keys is called hashing, because they guess over and over until someone guesses correctly.

Second, the result of encrypting is considered a hash. In other words, a hashed value is an encrypted value. Often a hashed value is called a hash.

Hash Problem: This is the target value that miners are trying to find. The target value is a 64 character hexadecimal number with several leading zeros. Currently, the number of leading zeros is about 18. The number of leading zeros is determined by the current difficulty level. It is very difficult to randomly guess a number with 18 leading zeros. In fact, it currently takes 1 million Bitcoin miners about ten minutes. Bitcoin automatically adjusts the difficulty every two weeks to ensure that it takes ten minutes to solve the problem.

Hierarchical Deterministic (HD) Wallet: These wallets provide a master seed (also called root seed, recovery seed, or seed phrase) to recover your wallet. These seeds are short words that are randomly generated. Collectively, they are called seed phrases. Normally, the seed phrase is 12 or 24 words, although sometimes people use eight words as a brain wallet.

To generate an HD wallet, all you need is the master seed (list of words, plus the optional password), and then the new wallet will automatically re-generate private keys, public keys, and public addresses. It will re-create them in the same order that they would have originally been created. It will then search the blockchain using the re-generated public addresses for any transactions that the wallet could own. Normally, the wallet will stop searching the blockchain after 20 public address have not been found.

Hot Wallet: When a wallet is on the Internet or on a device with access to the Internet, that wallet is considered to be a hot wallet. This means that the wallet is at risk because its private keys are vulnerable to being hacked.

HODL: This term was created years ago when someone posted on a blog that they were not selling their Bitcoin and planned to hodl. They typed hodl on accident instead of hold. It caught on, and everyone started using the term.

HODLR: Also referred to as Hodler. This is the term for someone who plans to HODL.

Inbound Capacity: This is the amount of Bitcoin that a Lightning Network channel can have in a transaction that is received. This is the maximum amount that can be sent to an LN node (open channel).

Input: An input is Bitcoin that has been received by a wallet from a Bitcoin transaction. It can also be thought of as outputs from a previous Bitcoin transaction. All inputs originate as outputs (except for miners).

KYC: The acronym for "know your customer." This is the proof of identity that most crypto exchanges require because of government regulations. This came from the banking system that requires banks to collect sufficient information on customers to know their identity.

Laptop/Desktop Wallet: These are software wallets that exist on a laptop/desktop. These wallets are essentially the same as a smartphone wallet, but run on your laptop/desktop. Some analysts recommend against keeping your wallet on a laptop/desktop if it is connected to the Internet. Laptop/desktops are notorious for getting hacked. If you prefer these wallets, then consider getting a VPN (virtual private network).

Lightning Network (LN): This technology attempts to solve the scalability problem with Bitcoin. It overcomes the current seven transactions per second limit. In theory, LN should be able to perform thousands of transactions per second. It does this by performing off-chain transactions using a secondary layer.

This secondary layer sits on top of the Bitcoin network. It works by setting up payment channels between LN peers. It's a secondary peer-to-peer network with potentially millions of interconnected LN nodes. It works by allowing payments to hop through these LN nodes and eventually into the seller's Bitcoin wallet. I say eventually because LN uses a delayed payment settlement system in order to reduce fees.

Lightweight Node: A lightweight node (also called Lightweight Client) installs the Bitcoin software, but only downloads the blockchain headers and not the transactions. Its purpose is not to verify transactions, but to confirm that a transaction is on the blockchain. This is mostly done for SPV wallets to identify if a transaction has been confirmed. This is done using something called SPV (simplified payment verification).

Lightweight nodes are mostly used by companies that support wallets. Many of the popular wallets utilize SPV to verify transactions. Many of these are called thin wallets or thin clients because they rely on SPV. Many of the smartphone wallets rely on SPV.

If you have a wallet, you can check if it is an SPV or API wallet type. An API wallet is the traditional wallet that relies on a centralized server that supports an API, such as Blockchain.info. An SPV wallet goes out and finds the information from a random node or perhaps from its own server.

Lightning Wallet: A wallet that is used on the Lightning Network. It is funded from an on-chain wallet. Once an LN payment channel is closed, the Bitcoin transfers from the Lightning wallet to the on-chain wallet.

Master Private Key: Also called Master Key. This is a 512-bit key that is created from the master seed. Once you have a master private key, you can then create an unlimited number of private keys from the master private key. These private keys are also deterministic. Meaning that if you have the master private key, you can re-create the private keys.

Master Public Key: Public keys are derived from private keys using the ECDSA algorithm, so public keys are deterministic. The master public key is derived from the master private key. If someone has the master public key to a wallet, then they can look at its current balance.

Master Seed: Hierarchical Deterministic (HD) wallets provide a master seed (also called root seed, recovery seed, or seed phrase) to recover your wallet. These seeds are short words that are randomly generated. Collectively, they are called seed phrases. Normally, the seed phrase is 12 or 24 words, although sometimes people use eight words as a brain wallet.

Most HD wallets use the BIP 39 standard, which uses the same 2048 word list. Each of the 2048 seed words is at least three letters long. If a word is four letters or longer, then the first four letters are unique.

Maximalist: This is someone who thinks Bitcoin is the only cryptocurrency worth owning, and all of the altcoins will eventually become worthless. They believe that Bitcoin can or will provide all of the features that other altcoins can provide. Thus, the only cryptocurrency to own is Bitcoin.

Merkle Root: Also called the Merkle Root Hash Key. This is the aggregate hash of all transaction hash keys in a block. This is used by miners to find

the next block's hash key and to validate that the transactions in the block are correct.

Mining Pool: Practically all Bitcoins are mined by mining pools. These are groups of computers that mine together and then share the Bitcoin reward. Because only one computer can guess the answer correctly for a new block, the pools have to determine how much of the reward each member of the pool will receive. There are several methods they use for splitting up the reward, but the most common way is the percentage of the hash rate (a miner's contribution).

There are only 144 blocks mined each day, so if you do not belong to a large pool, the odds are low that you will get a reward on a daily basis. If you have low energy costs and want to setup a miner (or several miners) at your house, then you would join one of these pools. If you tried to mine on your own, the odds are terrible that you would mine a block and be the first to answer the hash problem.

There are currently about 1 million Bitcoin miners (individual computers) that are configured around the world. One large pool that is used by individuals is called Slushpool and has about 200,000 miners. It holds about 12% of the total network hash rate, so it has a 12% likelihood of mining the next block.

If you only have one miner on Slushpool, your share of a reward would be tiny, because you would have to share it with 200,000 machines. Even with free electricity, it would take a while to pay-off the hardware costs of purchasing a miner.

Multisig Address: This is a Bitcoin address that allows for multiple digital signatures. This feature adds security. Wallets that support these addresses can be flexible in how they are implemented. You can have several digital

signatures for a wallet, and then decide how many of these signatures are required to spend Bitcoin from that wallet.

Multisig addresses can be used by organizations to ensure that money is spent correctly. However, it can also be used by individuals to add security to their Bitcoin.

Multisig Wallet: These wallets add extra security by requiring extra digital signatures. Multisig wallets can be used by organizations, families, or individuals who want extra security and want to use two or more digital signatures per transaction.

Multiuser Wallet: Also called shared wallets. Some wallets have the ability to be shared using multiple accounts. In other words, there is one Bitcoin balance, and multiple people can spend it using their own account. Thus, it would have one source of funds, and then multiple users could spend it. Then the wallet could track who spent it and how. This could be useful for a family.

Nonce: The nonce is an integer, but it can be very large (32 bits, or a maximum value of 4.3 billion). A nonce is used to determine the next block ID. When miners search for the next block ID, they constantly increment the nonce. Once they increment it 4.3 billion times, they start over with a new Merkle root value. They will try trillions of combinations until the target is found. The nonce that is used to solve the math problem (find the target) is saved in the block's header.

Outbound Capacity: This is the amount of Bitcoin that a Lightning Network channel can have in a transaction. This is the maximum amount that can be sent from an LN node (open channel).

Output: This is the amount of Bitcoin that is transferred or spent in a Bitcoin transaction. The destination can be a single public address or several. Most transactions go to a single public address.

Private Key: Private keys are 256 bits and are either randomly generated, or deterministically created using a master private key. Once a private key is created, the public key is deterministically created from the private key.

A private key is not something that you share with the public. It is used to encrypt your transactions with a digital fingerprint. Each wallet is essentially protected by its private keys. This is how you retain ownership of your Bitcoin. If someone obtains your private keys, they can spend your Bitcoin.

Private keys are normally stored in wallets because they are needed to create transactions. However, they are not stored on the blockchain.

A private key is often hidden and doesn't need to be displayed. If you do want to see a private key, it is usually displayed as a Base58 value, with about 50 to 60 characters. It can also be displayed as a 64 character hexadecimal value.

Pruning: Bitcoin nodes can turn on pruning to delete older blocks that are not needed for validating transactions. Only the last 550 blocks are needed to validate transactions. That is a fraction of the size of the entire blockchain, which has over 550,000 blocks.

Public Address: Also called Wallet Address. These are the addresses that a wallet uses to receive Bitcoin. Public addresses are derived from a private key/public key pair. Every public address has one of these pairs. This is how ownership of each Bitcoin is proven. Each public address is correlated back to a private key/public key pair. If a wallet contains all three values, then that wallet can prove ownership.

Public address = Base58(Version + RIPEMD160(SHA256(Public Key)) + CheckSum).

> Note: Often, people refer to their public addresses as public keys. This doesn't create confusion because public keys are generally never seen. In the formula above, you will see where the public key is used to generate the public address.

Public Key: A public key is created using something called the Elliptic Curve Digital Signature Algorithm (ECDSA), which generates a 256-bit integer from the private key. Each private key can only generate a single public key. Thus, it is deterministic.

RIPEMD-160: This is the same as SHA-256, only it returns a 160-bit hexadecimal value. This second hash function is used to reduce the length of public addresses without degrading security.

RBF (Replace By Fee): It is possible to cancel a transaction, but only if it has not yet been confirmed. Also, your wallet has to support something called RBF (Replace by Fee). In practice, the transaction isn't actually canceled, instead it is replaced.

> Note: Some wallets default all transactions to RBF, others require that you check a box to opt-in, and others do not support it. Also, RBF does not work with Lightning Network transactions.

RBF is very powerful, and I'm surprised it is even allowed. For instance, if you send Bitcoin to an address and the transaction gets stuck in the mempool (usually because of a low fee), you can replace that transaction.

SegWit: SegWit stands for Segregated Witness. Initially, it was designed to fix a malleability error. This error allowed attackers to alter digital signatures without invalidating transactions in the mempool. Basically, they found a way to replace existing transactions in a nefarious manner. The SegWit solution to this problem removed the witness data (digital signatures) from the transaction inputs and placed the witness data in another part of the transaction. It is called segregated witness because it segregates the witness data from the inputs and places the witness data somewhere else in the transaction (the witness list).

By fixing the malleability error using SegWit, it created three additional benefits: larger blocks, lower fees, and secondary layers. SegWit public addresses begin with a 3, whereas standard public addresses begin with a 1. Native SegWit addresses begin with BC1, which are more efficient, and were created specifically for SegWit.

SHA-256: This is a function that converts an input value into a 64 character hexadecimal value (256 bits). Hexa means six. This means the value is comprised of digits 0-9 and the first six letters of the alphabet (a-e). This 64 character hexadecimal value is also called the hash value, hash key, or hash.

The SHA-256 input value always returns the same output value. For instance, if you enter your name as the input value, it will always return the same 64 character hexadecimal value. It works for encryption because no one has ever been able to covert the output into the input. Thus, the input value becomes the key to knowing the output.

Smartphone Wallet: These are wallets that can be installed as apps on a smartphone. These are very common. Most exchanges have an app that provides direct access to an exchange wallet. There are also private smartphone wallets that act as your personal wallet. These wallets can hold

dozens of different cryptocurrencies, but likely not all of them. Often people own multiple wallets because they can't find one that holds them all.

Soft Fork: A soft fork is when there is a Bitcoin software upgrade, and it is backward compatible. This means that any changes made will only take effect on those nodes (and miners) that upgrade. The nodes that remain on the old software can continue verifying and mining, but they will not have the new changes.

A soft fork is the preferred method for doing an upgrade because it does not impact the blockchain. However, it can create situations where the nodes are running different versions of the Bitcoin software. This means that some nodes will have different functionality.

Sweep: This is done by moving all of your Bitcoin into a new wallet. When you move your Bitcoin into a new wallet, all of the private keys/public keys will have changed. People often do this for security and privacy concerns. For added security, you can do this with a VPN.

SPV (Simplified Payment Verification): This is the process that lightweight nodes (also called lightweight clients) use to verify that transactions are on the blockchain. They do not verify transactions, but instead ensure that transactions have been added to the blockchain. Thus, they check if a transaction has been confirmed. This is mostly used for SPV wallets.

Target: This is a 64-bit hexadecimal value that miners have to find in order to create a new block. It currently begins with about 18 leading zeros. The miner who gets to create the next block is whoever can find a value equal to or less than the target. The target changes every two weeks when the difficulty is adjusted.

Transaction: A Bitcoin transaction occurs between two or more wallets. It can be very simple with one input and one output, or it can be very complex with many inputs and outputs.

Each transaction consists of a list of inputs and a list of outputs. The inputs are UTXO that you have available to spend, and the outputs are what you will be spending. Bitcoin is smart enough to ensure that you can only spend what you have available and will invalidate a transaction if you try to spend more than your UTXO.

Transaction Fees: Each transaction has its own fee and is determined by the wallet that creates the transaction. Some wallets use a default value that is calculated, such as the current average fee. Other wallets allow users to select how much they want to pay.

Fees are paid in satoshis per byte. Each transaction includes this amount. In effect, these fees are bids. Miners look at the fees in each transaction and then decide if they will put them in the next block. If the bid is too low, then it may never get added to a block. If it is high, then it likely will be included in the next block.

Because of Bitcoin's decentralized design, it was inevitable that fees would be confusing and volatile. It's a true free market, with the miners deciding which transactions they want to confirm. If you only want to pay 1 penny, then your transaction may never confirm. If you want to pay the current average transaction fee, then your transaction will likely confirm within an hour or perhaps minutes.

You may be thinking if miners decide which transactions to confirm, can't they force fees higher? In theory, yes, but the free market tends to put downward pricing pressure on miners. However, if the transaction pool becomes full, then transaction fees tend to increase.

Many wallets allow you to state how much you want to pay for a transaction. This is stated in satoshis per byte. What's confusing is that the value of a satoshi is based on the current value of Bitcoin. So, what you pay today could change significantly in a short period of time. Plus, you can only estimate what you think you will be paying, which is only a guess. You will likely be very close, but unlikely spot-on.

To make it even more confusing, SegWit addresses provide discounts and make it more difficult to estimate the transaction fees. Eventually, a third-party will provide somewhat accurate real-time estimates for fees.

Also, the Lightning Network is currently difficult to estimate accurate fees, although they are very low. It's unlikely that Bitcoin will every have some type of flat fee per transaction, but it might happen.

> Note: Fees are not included in the transaction structure (refer to the appendix). Instead, fees are the difference between the inputs and outputs. The miners get what is left over. They create a fee transaction to pay themselves when they create a block.

Vanity Address: You can create a public address with your name or initials in it. These are not free, but if you are a business, it could be good for marketing. I expect these to become more popular.

UTXO (Unused Transaction Output): When a wallet receives Bitcoin, it comes from a transaction output. Your wallet then keeps track of all of the outputs that your wallet has received. This is Bitcoin that you can spend.

If you have never spent any of your received Bitcoin, then your UTXO will be equal to what you have received. As you spend some of your received outputs, your UTXO will decrease. This is the balance in your wallet.

Your wallet knows how much UTXO you currently have because it keeps track of how much Bitcoin you receive and how much you spend. The balance is your UTXO.

Generally, the UTXO is hidden from you, and all you see is your balance. However, some wallets allow you to display your UTXO. It will appear as transactions that received Bitcoin and have not yet been spent.

Appendix

I will include the Transaction Structure, Transaction Validation Rules, and some of the Block Validation Rules. However, I will not attempt to explain them since that would become too technical. You can do further research if you are interested. I'm including it because I found them useful to understand how Bitcoin works.

Bitcoin Transaction Structure

1) Version
2) Flag
3) Number of Inputs
4) Input List (Previous Trx ID, Index, Script Length, ScriptSig, Sequence)
5) Number of Outputs
6) Output List (Amount, Script Length, ScriptPubKey)
7) Witness List
8) Lock time

> Note: Notice that fees are not included in the transaction structure. Well, actually they are, but in a stealth manner. Fees are the difference between the inputs and outputs. The miners get what is left over. They create a fee transaction to pay themselves when they create a block using the leftover inputs.

Bitcoin Transaction Validation Rules

1) Check syntactic correctness.
2) Make sure neither input or output lists are empty.
3) Size in bytes <= MAX_BLOCK_SIZE.
4) Each output value, as well as the total, must be in legal money range.
5) Make sure none of the inputs have hash=0, n=-1 (coinbase transactions).
6) Check that nLockTime <= INT_MAX, size in bytes >= 100, and sig opcount <= 2.
7) Reject "nonstandard" transactions: scriptSig doing anything other than pushing numbers on the stack, or scriptPubkey not matching the two usual forms.
8) Reject if we already have matching tx in the pool, or in a block in the main branch.
9) For each input, if the referenced output exists in any other tx in the pool, reject this transaction.
10) For each input, look in the main branch and the transaction pool to find the referenced output transaction. If the output transaction is missing for any input, this will be an orphan transaction. Add to the orphan transactions, if a matching transaction is not in there already.
11) For each input, if the referenced output transaction is coinbase (i.e. only 1 input, with hash=0, n=-1), it must have at least COINBASE_MATURITY (100) confirmations; else reject this transaction.

12) For each input, if the referenced output does not exist (e.g. never existed or has already been spent), reject this transaction.
13) Using the referenced output transactions to get input values, check that each input value, as well as the sum, are in legal money range.
14) Reject if the sum of input values < sum of output values.
15) Reject if transaction fee (defined as sum of input values minus sum of output values) would be too low to get into an empty block.
16) Verify the scriptPubKey accepts for each input; reject if any are bad.

Bitcoin Block Validation Rules (First 15 rules)

1) Check syntactic correctness.
2) Reject if duplicate of block we have in any of the three categories.
3) Transaction list must be non-empty.
4) Block hash must satisfy claimed nBits proof of work.
5) Block timestamp must not be more than two hours in the future.
6) First transaction must be coinbase (i.e. only 1 input, with hash=0, n=-1), the rest must not be.
7) For each transaction, apply "tx" checks 2-4.
8) For the coinbase (first) transaction, scriptSig length must be 2-100.
9) Reject if sum of transaction sig opcounts > MAX_BLOCK_SIGOPS.
10) Verify Merkle hash.
11) Check if prev block (matching prev hash) is in main branch or side branches. If not, add this to orphan blocks, then query peer we got this from for 1st missing orphan block in prev chain; done with block.

12) Check that nBits value matches the difficulty rules.

13) Reject if timestamp is the median time of the last 11 blocks or before.

14) For certain old blocks (i.e. on initial block download) check that hash matches known values.

15) Add block into the tree. There are three cases: 1. block further extends the main branch; 2. block extends a side branch but does not add enough difficulty to make it become the new main branch; 3. block extends a side branch and makes it the new main branch.