Free Bitcoin Guide

The history, advantages, and uses of Bitcoin.

About

The purpose of this guide is to provide a resource to understand Bitcoin and how to safely use it. Bitcoin is an innovation that enables individuals to exert their monetary sovereignty through self-custody and disintermediated payments. However, there exists a high degree of security risk when bitcoins are not safely stored or managed. This guide aims to provide the user with the background, tools and resources to be able to manage bitcoin wallets and private keys and to transact in bitcoin. Additionally, the guide provides historical context around the innovation of bitcoin and how it evolved to its current state.

The world is in an increasingly precarious position due to the abandonment of sound money. Bitcoin provides a sound money tool for preserving wealth that cannot be inflated by any central government or entity. In order to take advantage of this unique innovation, we must learn how to use it and protect it. The fight for Bitcoin is a fight for freedom and a fight against centralization, corruption and censorship.

As Bitcoin is continually evolving, so too will this guide. The goal is to enable and empower more people to run their own full nodes, self-custody bitcoin, and invest for the long-term. Monetary sovereignty is a team sport and we all need to play our part in order to see the bitcoin vision come to fruition.

Table of Contents

History of Bitcoin

In 2008, the world experienced a global banking crisis, spurred by fractional reserve banking, predatory mortgage lending practices, enormous bilateral swap risk, and housing price collapses. As real estate prices fell and defaults began to take hold, the fragility of the entire financial system was exposed and the largest banks in the country needed multibillion dollar bailouts that were funded by taxpayers.

The 2008 crisis exposed a system that was built upon layers of risk-taking that served to benefit the large banks and their stakeholders, while leveraging the assets of the individual. Instead of safely holding customer deposits, banks were lending them out to riskier and riskier counterparties in an effort to earn higher and higher returns. At the same time, banks were also getting involved in large financial derivatives transactions with other banks, attempting to securitize mortgage loans to customers and trade them as financial assets. When the risk became too much and the trades collapsed, the banks did not have the capital to stay in business and safekeep customer deposits – they were bailed out by the public, at great direct and indirect cost to the average citizen.

Direct bailouts were done through the Troubled Asset Relief Program, in which up to $700B of taxpayer funds was authorized to purchase distressed assets off of bank balance sheets. In addition to that, the Federal Reserve instituted a policy of Quantitative Easing. Quantitative Easing was a euphemism for increasing the money supply and inflating the value of fiat currency, effectively decreasing the wealth of users holding their savings in fiat. More information on fiat currency will be discussed in the “Economics” section.

Amidst a backdrop of failing banks, customer deposits at risk, and the prospect of unchecked money printing, the bitcoin whitepaper was

produced. Bitcoin (with an upper case “B”, denoting the protocol) offered a truly decentralized form of money, in which there was no reliance on a third party to store funds or effect transfers. Bitcoin (with a lowercase “b”, denoting the asset) was capped in the total amount available, so it could never be inflated and any ownership would never be diluted. It solved many problems of 2008, but it went even further in its promise of monetary sovereignty as a seizure- and censorship-resistant asset with a finite amount of supply and no central party that owned or controlled it.

Economics

Fiat Currencies

To understand bitcoin, we need to briefly understand fiat currencies, which currently dominate the world in which we live. Fiat money is issued by a central government and is not backed by any physical asset such as gold. It’s supported solely by the full faith and credit of the government issuing it.

Because fiat currency is created by central banks and on behalf of central governments, there is no limit to how much currency can be produced. The central banks can decide to increase the supply at any time, creating more money out of thin air and inflating the currency – thus decreasing the purchasing power for any individual holding that currency. Transacting in fiat currencies means bearing the counterparty credit risk of the government for every payment that is received; this is a risk that does not exist when dealing in hard currencies such as gold or bitcoin.

Fiat currency gives the government control over the money supply, allowing it to adjust the money supply to suit its agenda and desired spending. For example, governments can simply print money in order to fund wars that

they desire to engage in. Fiat currency also lends itself to fractional reserve banking, in which banks can create money IOUs in order to lend to customers multiples of the amount of currency they actually hold.

A fiat system is more fragile and susceptible to corruption than a system that is backed by hard money such as bitcoin. Fiat currencies also serve as particularly poor stores of value since the value can, and does, decrease dramatically as governments decide to print more money.

Federal Reserve & Central Banking

In the US, the Federal Reserve (Fed) is the Central Bank with responsibility for monetary operations for the dollar. The Federal Reserve Open Markets Committee (FOMC) is the group that meets periodically to determine the target federal funds rate which is used to control the supply of money through government bond purchases and sales. The FOMC is a small, centralized set of appointed officials that have control and power over the monetary system and the value of the US dollar.

The Fed also oversees the US banking system, which is intricately tied into the broader monetary system. Banks can operate on fractional reserves, meaning they can lend more than they have. If they ever face a bank run, the Fed can step in to bail them out. The Fed has enormous power to allow and disallow banking operations that suit their needs, and to print more money (at the expense of fiat holders) to bail out those banks when it goes south.

Digital Scarcity

Bitcoin stands in contrast to fiat currency first in its limited, scarce supply.

Bitcoin's supply is fixed at 21 million bitcoin, the total amount of bitcoin that will ever exist. It is impossible to increase this supply, which makes bitcoin a form of 'hard money'. In a way bitcoin is like 'digital gold', though it has advantages to gold in its transferability and interchangeability.

In order to maintain its fixed supply, bitcoin new emission – how many bitcoin are added to the network – is halved approximately every four years until the year 2140. At this point, no further new bitcoins are produced. This distribution of new supply ensures that there will only ever be 21 million bitcoin.

For users who wish to hold their assets in a store of value that cannot be inflated and is not owned or controlled by a single entity, bitcoin provides the solution. Any bitcoin holder can rest assured that their stake in bitcoin will not become diluted by central bankers or by governments who need to print money for various reasons.

Stock-to-Flow

Stock-to-Flow is a way of measuring how rare different commodities are. The 'stock' refers to the amount of the underlying commodity in circulation, and the 'flow' refers to the amount of the commodity that is produced every year. The stock-to-flow ratio is thus a measure of the new production relative to existing supply, and it reflects the level of scarcity of the underlying asset.

As an example, the US Dollar has experienced drastic 'production' (in the form of money printing) relative to the circulating supply, making it an asset with low scarcity. Gold is much better, where its annual mining production flow is 1.7% of total stock. Bitcoin (BTC) is even better than gold; currently, there are 3.125 new BTC per block relative to circulating supply of 19.72 million. This means that on an annual basis bitcoin's production is 0.8% of its total supply, and the amount will only decrease over time as the new emission is halved every four years, while the total maximum supply remains fixed at 21 million.

The stock-to-flow ratio can be described as how many years it would take to replace the existing supply. For gold, this value is around 59 years. For bitcoin, following the halving in April 2024, the value is now 125 years. Bitcoin is the most scarce, hard money around.

Impossible Trinity

Many philosophies exist in the study and practice of economics. One of them is the impossible trinity, which states that it is possible to have two, but it is impossible to have all three of these:

- A stable foreign exchange rate
- Free capital movement
- Independent monetary policy

In fiat currencies, there are plenty of historical examples of this dynamic at play as sovereign nations aim to direct monetary policy. Bitcoin, however, starts to upend this traditional thinking. It revolutionizes the way we store and transfer value by providing highly mobile capital that is independent of centralized monetary policy.

Network Effects

Bitcoin's growth has been driven by seven major network effects, each of which makes up a fundamental part of bitcoin's ecosystem and contributes to its global adoption. The existence of network effects leads the strongest cryptocurrency to dominate all capital investment and transaction flow; as such, bitcoin is proving to be the winner in a winner-takes-all market.

1. Speculation

Bitcoin as a protocol is a piece of open-source software, but bitcoin is also an asset that can be transferred seamlessly from one user to another without any centralized entity or government controlling or effecting the transfer. This asset fluctuates in price relative to other assets, and can be bought and sold for other assets. The most common denomination for bitcoin is relative to the USD and Bitcoin/USD is frequently traded as market participants speculate on its short- and long-term value. Speculation drives liquidity and price

discovery and is the first of the network effects that has led to broad, mainstream adoption.

2. Merchant Adoption

Any user can receive bitcoin if they have access to the internet to set up a bitcoin address. This means that anyone who provides a good or a service to someone else can accept payment for that good or service without the need for a third party, such as a bank or payment processor. Merchants may seek to use bitcoin to avoid credit card fees and chargebacks, as well as having full autonomy and control over collecting payments. The more merchants that accept bitcoin, the more avenues there are for using bitcoin for payments.

3. Consumer Adoption

As merchants are incentivized to accept bitcoin because of reduced credit card fees and chargebacks, they are in a position to pass along those savings to consumers in the form of price discounts. Consumers will desire to purchase things using bitcoin when the cost savings are preferable, or if they wish to avoid their transaction being subject to a bank or payment processor. As consumers adopt bitcoin for spending, they create a use case that necessitates the purchase of bitcoin and keeps it within the system.

4. Security / Miners

As bitcoin price increases from speculation and adoption, the incentive to mine bitcoin increases. Miners earn bitcoin from the block reward and from transaction fees. As Bitcoin/USD price rises, this revenue is worth more to them. The more miners that join the bitcoin network to mine, the more competitive it becomes and the more it increases bitcoin's security. The increased security strengthens the network and bitcoin's immutability. More about mining is discussed later.

5. Developers (including Lawyers, Regulators, Accountants, etc.)

Bitcoin is a permissionless, open-source financial application programming interface (API) that anyone can build upon. In the financial sector, there is no other API like this. Most financial services APIs are controlled by gatekeepers that block access from outside parties. Because of this aspect, bitcoin attracts developer talent and allows innovation from all over. The developer community continues to grow as developers are rewarded for building upon bitcoin, and the open-source protocol continues to attract developers who want to be a part of financial innovation and monetary sovereignty.

In addition to software developers, bitcoin relies on growth from other types of professionals who build upon bitcoin. Lawyers and regulators help craft the legal and regulatory framework for this new asset class. Accountants help craft the financial and tax treatment. All professionals who are building upon bitcoin in some way, whether through software or other means, are part of bitcoin adoption and growing its network effects.

6. Financialization

The sixth network effect is financialization as bitcoin grows to be a dominant asset and source of wealth transfer from the traditional financial system. We have seen this play out with the growth of financial products such as options, futures, and Exchange-Traded Funds (ETFs). Traditional players are actively trading all sorts of products built upon bitcoin. Asset managers are allocating substantial funds to bitcoin ETFs, and custodians are working to hold bitcoin on behalf of customers. These financial pieces are driving adoption across a range of customers who are integrated with the traditional financial system and still prefer the value proposition of a scarce digital asset like bitcoin.

7. World Reserve Currency

The final network effect is the adoption of bitcoin as the world reserve currency, where individuals, corporations, and governments will hold bitcoin

as their primary store of value and use it as their primary unit of account. Bitcoin is poised to become the ultimate source of collateral, supporting all financial transactions. When this network effect is reached, the adoption curve will level out and the market cap will be much, much higher

Sound Money

What is Sound Money?

Sound Money describes the quality of money, or the capacity of money to fulfill its functions as a medium of exchange, store of wealth, and unit of account. The higher the quality of money, or the more sound it is, the greater the demand for that money.

Sound money is not subject to arbitrary inflation and reduction in purchasing power; as such, it can be relied upon by users for storing wealth over long periods of time.

Characteristics of Sound Money

1. Recognizability

The first quality of sound money is that it must be recognizable. This means that it must be easy to recognize and to verify its authenticity. For example, one can note that a USD bill is a form of US currency, but it's challenging to confirm the validity. Similarly, one can easily identify gold on the periodic table and by eyeballing it, while fully recognizing it requires melting down the gold and confirming its chemical properties.

Bitcoin is recognizable not just in name, but also in its authenticity as bitcoin. The recognition merely requires running a full node (described later), syncing to the network, and confirming transactions on the blockchain.

2. Scarcity (High Stock-to-Flow)

The next quality of sound money is scarcity, which can also be described as having a high stock-to-flow ratio. For most assets, as the asset gains in value, the issuer or producer will increase the supply of that asset so that they can profit from the price appreciation. This dilutes the value of money for all the holders, as the flow of new emission is increased relative to the existing stock.

The difference between the cost to produce a commodity and the current market value of the commodity accrues as a gain to producers and an expense to consumers. By maintaining a high stock-to-flow ratio, the expense for consumers holding the commodity is reduced as there is less supply issued at the higher market value.

Gold is a commodity that has a high degree of scarcity, and a high stock-to-flow, given how difficult it is to produce more of it. On the other hand, fiat currencies are incredibly easy to produce more of. Financial and political elites make the determination behind closed doors and single-handedly increase the money supply, benefiting themselves and hurting consumers.

Bitcoin maintains its scarcity and high stock-to-flow through proof-of-work mining, which is described later in this guide. Proof-of-work makes it extremely costly and difficult to produce new emission of bitcoin and requires that miners incur the cost in order to create new coins. This behavior solidifies the scarcity of bitcoin and protects the value for holders.

3. Censorship-Resistance

Quality money must be censorship-resistant, meaning that it is not restricted, tracked, or controlled. Many forms of money have been exposed to censorship through taxation, asset seizure, legal tender laws, and through oversight of centralized systems that facilitate commerce and payments. Through these mechanisms, governments can exert control over money and how it's used. They can use this control to impede and censor the flow of money when it suits them.

Bitcoin subverts those mechanisms by existing as a truly decentralized currency that operates off of a network of nodes (described later in Section VII). There is no single point through which a government can exert force or control over bitcoin. The government cannot seize your bitcoin private key, it cannot prevent a bitcoin transaction from being sent to the bitcoin network, nor can it change the emission schedule or alter historical data. The monetary properties are upheld through the source code, running on decentralized nodes and maintaining a distributed ledger of transactions.

Additionally, bitcoin has been freely chosen by the market as a form of currency. No central government or entity has forced or mandated that people use bitcoin. Instead, the free market has decided that bitcoin has characteristics that render it suitable for adoption. Bitcoin is censorship-resistant because the market has freely chosen to adopt it.

4. Durability & Indestructibility

Quality, sound money needs to be durable and indestructible. Gold is a form of money that is extremely durable and indestructible; it can withstand all forces of nature and remain in its elemental form for millenia. It can tolerate harsh environments without ever being eroded.

Bitcoin offers similar durability in its own way. Bitcoin is maintained by code running on nodes throughout the world. The amount of computational

power backing bitcoin far exceeds the amount of computing power controlled by any single company or entity. The Bitcoin network is incredibly resilient due to the accumulation of network power that has backed it since its inception. With the network being indestructible, the currency (bitcoin) is also highly durable.

5. Extensibility

Quality money is extensible, which means it provides for future growth. To use the gold comparison again, gold has very low extensibility – its atomic structure is fixed and it has no way to be modified or improved. Fiat currencies, on the other hand, are highly extensible. Governments can allow products and services to be built upon the fiat rails to enable better banking and payments; they can also do the opposite. For example, they can introduce legislation to hinder the value and flexibility of the currency.

Bitcoin as a protocol is an open-access API. Anyone can build upon it and innovate new functionality and use cases. Bitcoin is unique in this way – it functions both as a form of money and as open-source software. In this vein, bitcoin is highly adaptable. There have already been many upgrades and improvements that have been introduced, and there will continue to be changes and upgrades going forward.

6. Salability

Next, quality money needs to be salable. This means that when someone wants to sell the currency, they can do it quickly, in size, for minimal transaction costs or slippage. Fiat currencies are some of the most liquid assets in the world; they trade trillions of dollars a day within fractions of a penny. Fiat currencies are highly salable.

People attach a monetary premium to liquidity. When a good or product is highly liquid, demand for that good increases, thus increasing the liquidity

and driving even more demand. This price reflexivity has been evident in bitcoin's growth to date.

Compared to the early days of when bitcoin's market cap was in the single-digit millions, it's now more than 1,000,000x that size. As it's grown in market cap, it's grown in volume as well, with billions of dollars trading each day. Bitcoin is quite salable for most market participants and the ability to trade it for other currencies will only grow as its market cap and liquidity continue to increase.

7. Portability

Quality money must be portable, or easy to transfer through space. While gold meets some of the criteria for quality money so far, it is not very portable. It's costly to move, especially when transferring across oceans or large land distances. Fiat currencies might be better when they move electronically through the banking system, but they are mired in governmental controls and regulations that drastically impede the ability to freely move them.

Bitcoin is merely information, represented in bits. It can be transferred 24/7/365 around the world nearly instantaneously, all through an internet connection. It isn't subject to banking holidays, local governmental regulations, freight trains, or cargo ships. Bitcoin is the most portable form of money that exists.

8. Fungibility

A good form of sound money must be fungible, which means all forms of the money are interchangeable and identical to each other. Fungibility increases the liquidity and desirability of money.

At a fundamental level, gold is fungible since it's the same atomic structure no matter what. However, at a higher level there are different types of gold

that exist and it's difficult to verify its fungibility. One would need to melt it down to its base layer in order to have it in its fungible form.

The US Dollar is less fungible because it is tied to a serial number, as well as held in a bank account that is linked to an account owner. The identical nature that exists with gold is missing with this currency, even though these dollars are largely interchangeable in practice.

Bitcoin's fungibility comes from the fact that every bitcoin that is ever produced is the same in its properties. Over time, bitcoin has become less fungible due to the ability to track movements on the blockchain so each bitcoin has distinct provenance, but the bitcoin that is created by the protocol is identical in nature.

9. Privacy

Next, sound money must be private. A user should be able to store funds or transact in currency without others knowing the amount, nature, or location of the transaction, or other transactions that it was associated with. Gold and cash have these properties to some degree, but they are not always practical for large transactions.

Bitcoin is private in that there is no identifying information that is revealed with transactions that are broadcast to the blockchain. However, the bitcoin blockchain is a public ledger and anyone can access any transaction to see its sender addresses, recipient addresses and amounts. One can also use those addresses to view other linked transactions. In this regard, bitcoin offers some privacy but not full privacy.

10. Divisibility

Finally, sound money must be divisible. Divisibility is important for utility as a method of payment, so people can easily make transfers of different amounts.

It's also important for salability and liquidity, as not every participant would want to transact in the same amount at the same time.

Bitcoin is highly divisible – down to the Satoshi, which is 1/100,000,000th of a bitcoin – enabling convenience and microtransactions.

Bitcoin as Sound Money

As we can see, bitcoin contains all the properties of sound money, though in various degrees.

- Bitcoin is easily recognizable, as anyone can run a node and verify its authenticity.
- With its high scarcity, bitcoin has the highest stock-to-flow of any asset.
- It's durable and extensible by virtue of having an extremely powerful, open-access network that ensures its integrity and allows anyone to develop on it.
- Bitcoin is highly portable, as any participant can seamlessly transfer bitcoin to any other participant with solely an internet connection.
- Lastly, it is highly divisible out to eight decimal places.

Where bitcoin has the properties of sound money to a lesser extent are with censorship-resistance, salability, fungibility and privacy. Salability has increased with time, but bitcoin is still only approximately $2T in market capitalization. In addition, the current market is limited in supporting its liquidity. The other properties – censorship-resistance, fungibility and privacy – all relate to the same core issue: bitcoin is on a public ledger where all movements can be linked and tracked. As such, bitcoin doesn't necessarily offer the best guarantees in these areas, even though it exhibits the properties to some degree.

Bitcoin as Superior Money

Once an asset like bitcoin exhibits traits as a superior form of money, it is subject to economic forces that drive its dominance over existing money (in this case fiat). Gresham's law tells us that bitcoin will become the predominant store of value while users deplete their fiat. This change in balance is explained by the desire to hold the more valuable currency as a store of value, driving it out of circulation, while the less valuable currency remains the tool for spending.

As the Fed continues to increase the money supply by injecting fiat into the economy, they are benefiting the elites who are closest to the money printing at the expense of the individuals who face higher prices from inflation (see Cantillon effect). This serves to drive bitcoin adoption starting at the individual level, for these people are most hurt by inflation and most desperate for a scarce store of value.

Bitcoin will reach a Schelling Point as more people adopt bitcoin and assume that others will adopt it for the same reason. Participants need not coordinate or communicate directly in order to correctly assume that other market participants will choose bitcoin as the preferred form of money. This behavior has a compounding effect as the network effects continue to grow due to the belief that others will participate in the network. Bitcoin has exhibited characteristics of a social choice that has already reached a Schelling Point.

Bitcoin Components / Building Blocks

Bitcoin was built upon several different cryptography innovations, many of them decades older than bitcoin itself. This section describes some of those building blocks and how they are used in bitcoin.

Hashing

Hashing is a fundamental part of how bitcoin proof-of-work and addresses work, as it provides security and privacy. Hashing functions have several properties that make them particularly convenient.

First, hashes are one-way and irreversible. This means that you can compute the hash of any value (e.g., a number or string), but you can never reverse the hash to derive the initial value from the hash.

Here are examples of the SHA256 hashing function being used to hash text:

“this is a sha256 hash” →

```
Unset
62ec965a6c2506b3378703186b64317867013912385dbfb3e4870a1aa45d6c4b
```

“it is irreversible and will return the same fixed-length hash every time” →

```
Unset
fdd1bd060637853fbc6688eda5ad9ee51dc3a46c4439c200a0abf51f5b12ee3e
```

Next, hashes are unique and deterministic. This means that, given a particular input, the same hashing function will produce the same output in every case. No two inputs will produce the same hashed output.

Finally, hashes are fixed-length. No matter the size of the input, the hash of the output will always be the same length. This makes it impossible to glean any insight into the size of the input based on the hash.

The hashing functions used in bitcoin are RIPEMD-160 and SHA256.

Public/Private Key Cryptography (ECC)

Public/private key cryptography enables encryption where a message is encrypted with a public key and decrypted with a private key. This means that two people can share encrypted messages with each other without having to reveal their private keys.

Public/private key cryptography, or asymmetric encryption, is distinct from symmetric encryption. In the case of symmetric encryption, the same key is used to encrypt and decrypt the input.

The public/private key scheme that is used in bitcoin is Elliptic Curve Cryptography (ECC). For an ECC overview, check out this primer.

Digital Signatures (ECDSA)

Public/private key cryptography underlies digital signature algorithms that enable one to authenticate a message and ensure its integrity and inability to be tampered with. The algorithm similarly allows a receiver of a message to know that the message was authentic and in its original form.

The algorithm that is used for signing bitcoin transactions is based on ECC and is the Elliptic Curve Digital Signature Algorithm (ECDSA).

Proof-of-Work / Hash Cash

Bitcoin's proof-of-work is based on prior innovations, particularly Hash Cash, which was developed by Adam Back in 2002 as an anti-spam and anti-DDOS mechanism. Hash Cash required a Central Processing Unit (CPU) processing

power to be devoted to solving an arbitrary math problem every time an email was sent. This arbitrary use of energy and resources was known as proof-of-work and served as an anti-spamming mechanism.

As we'll see when we discuss mining, the proof-of-work mechanism that requires energy and computation power is a critical component of bitcoin's security and decentralization.

Merkle Trees

Bitcoin is a global currency that anyone can use. When it reaches its seventh network effect and becomes a world reserve currency, bitcoin usage is going to be enormous.

Bitcoin uses Merkle Trees as a way to store hash and transactions so node operators do not need to keep the full transaction data, but they can still verify that a transaction had been previously accepted by other nodes. This is done by discarding old transaction data while keeping the Merkle Root of the tree stored in the block header. This consolidation allows a lightweight node to verify that a transaction had previously been accepted by other nodes, without needing to store all transaction data. Instead, it can rely just on the block header and the Merkle branch of the relevant transaction.

How Bitcoin Works

Private Keys

A private key is a very large number that is used to secure bitcoins. It acts as a password; with access to the private key, one can gain access to the bitcoin and send it to any destination.

More specifically, the private key is used to digitally sign a bitcoin transaction in order to send that bitcoin to someone else. The signature scheme that bitcoin uses is ECDSA.

The private key must be held securely at all times. If the private key is revealed, whomever it was revealed to can now have access to all the bitcoin. The private key must also be safely backed up; if the private key is lost and there are no backups, then all access to the bitcoin is lost.

When generating the private key, it must be generated with sufficient randomness (entropy) so that the probability of a bad actor being able to randomly pick the private key is exceptionally low. A bitcoin private key is 256 bits, which means that the bad actor would have to guess the random number that is anywhere from 1 to 2^256. This is nearly impossible. There are approximately 10^77 possibilities; as reference, the universe is estimated to contain 10^80 atoms.

Bitcoin private keys may be displayed in multiple formats including Hex and WIF. The Hex format takes a 256-bit number and displays it in a set of 64 alphanumeric hexadecimal characters (16 characters). The WIF format is a base58 encoding with a checksum and is often used in the QR code representation of keys.

An example of a Hex bitcoin private key is:

8f8cc518a51a7e61788536022f65d872ec57fc02dd9715e8c4c13b5101ac9324

Private keys are primarily used to sign bitcoin transactions; however, one could use the bitcoin private key to also sign other arbitrary data. For example, if you wanted to prove that you controlled the private key to a bitcoin address without signing a transaction, you could sign a message with that private key. Another user could then verify using the same encryption scheme.

Public Keys

A public key is a very large number that is derived from the private key. The public key is derived using Elliptic Curve Cryptography (ECC). This derivation is one-way; it is impossible to find the private key from the public key.

The public key is used for signature verification in bitcoin. With the public key, one can confirm that a bitcoin transaction signed by the private key is valid without ever having access to the private key.

Unlike the private key, the public key does not need to be kept secret. An example of a bitcoin public key is:

```
038a0bd7bc9222e2897376590df6b203910a2e0cb050018bf7cca02eaedfe377cc
```

This is the public key associated with the bitcoin private key in the section above.

Addresses

An address is derived from the public key using a one-way hash. It is first hashed using SHA256 and then hashed using RIPEMD-160. These hashing functions are irreversible, and one cannot derive the public key from the address.

An address serves as an account in bitcoin. A user shares their address with other people in order to receive bitcoins to an account that is controlled by the user's own private key.

Bitcoin addresses are encoded in base58 (or bech32 in the case of Segwit addresses, explained later) with alphanumeric characters and include a checksum to detect errors like typos. An example of a bitcoin address is:

19Wqa3Z2DtTfzDGYHk3EJBUitYYcahmaNi

This is the bitcoin address associated with the bitcoin public and private keys in the section above.

All addresses and their associated balances and transaction history are visible on the public bitcoin blockchain and are monitored extensively by chain analytics services. While some users choose to reuse addresses for convenience, many privacy-focused individuals choose to never reuse bitcoin addresses.

There are a number of different address types in bitcoin, outlined here. More details about multisig, the Segwit, and Taproot upgrades are covered later in this guide.

Address Type	Name	Encoding	Prefix
P2PKH	Pay-to-Pubkey-Hash	base58	1
P2SH	Pay-to-Script-Hash	base58	3
P2WPKH	Pay-to-Witness-Pubkey-Hash	bech32	bc1q
P2WSH	Pay-to-Witness-Script-Hash	bech32	bc1q
P2TR	Pay-to-Taproot	bech32m	bc1p

Wallets

Cold vs. Hot Wallets

A wallet stores the keys associated with a bitcoin address or a collection of bitcoin addresses. A wallet is considered “cold” if it is not connected to the internet. A wallet is “hot” if it is connected to the internet.

It is generally recommended that bitcoin is stored in cold wallets to reduce the attack surface and the risk of theft. Hot wallets are used for bitcoin that needs to be sent, as they must be connected to the internet in order to broadcast transactions. Best practice is to keep minimal amounts of bitcoin in hot wallets, and not more than what is necessary for transacting.

Custodial vs. Non-custodial

Custodial wallets store the keys to bitcoin on a user’s behalf. The user does not actually own or control the keys to their coins. Instead, the user is entrusting a third party to safely store their bitcoin.

While custodial services may be suitable for a subset of users, it is generally recommended that bitcoiners use non-custodial wallets to store their coins. In a non-custodial setup, the user owns and controls their own private keys. The only way to truly have claim to one’s bitcoin – and to take advantage of the self-sovereignty and censorship-resistance that bitcoin offers – is to hold one’s own keys.

Mobile Wallets

Mobile wallets allow users to generate and store keys on their mobile device. Mobile wallets are hot wallets as phones are typically connected to the internet, but they provide convenience for transacting in bitcoin.

Hardware Wallets (HSMs)

Hardware wallets generate and store keys on a secure hardware device known as a Hardware Security Module ("HSM"). The keys are stored in a secure environment on the hardware device, and cannot be extracted or transferred out of the device in plaintext. The hardware devices are very specialized in the functions that they run; as such, they are not vulnerable to computer viruses that run on standard computer operating systems.

Hardware wallets are interacted with in a secure manner – they are not exposed to vulnerable systems. This allows a user to sign transactions while the private key stays within the HSM and never leaves the device.

While hardware wallets provide a secure environment for generating private keys and signing with private keys, they still expose the user to some attack vectors. The user must trust the wallet manufacturer and is exposed to any compromise in the production process, such as the introduction of a backdoor. Additionally, some hardware wallets are based on closed-source software, so they are not subject to the rigorous external testing and validation that open-source software receives.

Hardware devices are considered cold wallets, although they are sometimes connected to computers that are connected to the internet for purposes of setup or broadcasting transactions. However, even in those cases, the private key remains in the secure environment of the hardware device and the transaction signing takes place on that device. A hardware wallet should never be connected to an online computer any more than is necessary.

Examples of hardware wallets are those made by Trezor and Ledger.

Desktop Wallets

A user may set up their own cold wallet on a computer or laptop – a desktop wallet – that is never connected to the internet. The software needs to be

loaded onto the computer via USB or another device that ensures the computer remains disconnected from the internet. Signing transactions takes place on that computer, and signed transactions may be transferred back to an online computer via USB or QR code. The advantage of using QR codes is that it ensures the cold wallet computer remains air-gapped and protects it from any vulnerabilities that may stem from the USB device.

Examples of desktop wallets are Armory and Electrum. While Bitcoin Core also has wallet software that may be used, it is not recommended in this context due to the lack of support for mnemonic seed recovery.

Single Key vs. Multisig

As described so far, addresses are derived from a single private/public key pair. As such, they need just a single key and single digital signature in order to spend the bitcoin.

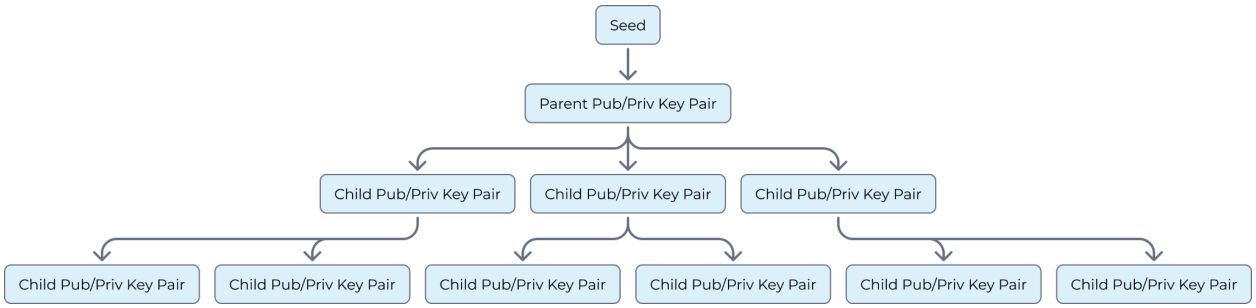
Bitcoin wallets also support multisignature, or multisig, schemes as well. This feature allows the user to set spending conditions for the bitcoin where multiple signatures are needed to complete the transaction. If the requirements are not met, the bitcoin cannot be spent.

Multisig wallets provide certain redundancy and security benefits to users. They allow for backups of keys, meaning that loss of a single key does not result in loss of the bitcoin. For example, in a 2-of-3 signature scheme, one key may be lost but the user can access bitcoin with the other two keys.

Multisig also enables key access to be spread across multiple users so that different people or entities can each hold a key to a given address. While splitting control across users can also be accomplished with sharing of a single key using Shamir's Secret Sharing, multisig addresses potentially offer greater protection because they don't face the single-point-of-failure risk of a single key being compromised at key generation or otherwise.

HD Wallets

Hierarchical Deterministic (HD) wallets leverage deterministic functions along with the nature of hashing functions in order to allow a user to generate many different 'child' public/private key pairs using a single 'parent' seed. One can take a value such as a large random number and append a nonce to it (e.g., add the digit "1", "2", "3", etc.) and have it return a fixed-length hash that bears no relation to the initial random number. Crucially, the result from the hashing function will be the same each time the same nonce is appended.



Once the child keys are generated, they are indistinguishable from any other private/public key pair. The child private keys can be used to sign transactions from the addresses generated from the child public keys, and they appear the same as any other bitcoin address. Given solely a public/private key pair that belongs to a child, there is no way to infer the parent keys, any siblings, or derive any children for that child.

This deterministic behavior allows a user to use a single parent seed and generate as many bitcoin addresses as they want, without creating a secure private key each time. It also enables wallet recovery for all addresses derived from a single seed, reducing the risk of loss.

Wallet Recovery / Seed

Wallets can be recovered through seed phrases. Seed phrases are a series of 12-24 words that are derived from the private key. The private key is encoded and split into 11-bit segments; each 11-bit segment is mapped to a word from a

predefined dictionary of 2,048 words. An example of a seed recovery phrase is (24 words):

spot mammal session broom giraffe own

sense obscure foster limit multiply hello

hero point scissors lobster normal satisfy

table foam diamond chef chimney fox

The seed recovery phrase has all the keys to the kingdom. It is critical that you store it safely and never share it with anyone. Best practices for storing your seed include keeping multiple copies in separate, safe physical locations. Do not store your seed anywhere online, including email, cloud storage, or password managers.

Getting Started with a Wallet

To get started with setting up a wallet, it's recommended to start with a cold storage setup and with small amounts of bitcoin. For a cold storage setup, an example would be something like Armory HD wallets that could be set up on an offline device.

1. Set up an offline computer

Set up a computer, laptop, or other device that is disconnected from the internet. Ensure that wifi is turned off and remains off for this device.

2. Load Armory onto offline computer

Using a different online computer, download Armory software onto a USB device. Then, use the USB device to load the software onto the offline computer.

3. Create a new wallet on offline computer

Create a new wallet on the offline computer. Armory will give you the option to symmetrically encrypt this wallet with a password; you can decide if you want to encrypt the wallet. This is an additional level of encryption beyond what is done at the bitcoin protocol level.

4. Make a paper backup of new wallet

Make a paper backup of the wallet by printing or copying the backup details by hand. It is recommended to store multiple copies of the backup in safe, secure physical locations.

5. Load watching-only copy wallet onto online computer

On the offline computer, create a watching-only copy of the wallet (detailed below). Save this file to the USB and insert the USB to the online computer. On the online computer, load Armory and import the watching-only copy of the wallet. In the wallet-properties dialog, click on “Belongs To” and select “This wallet is mine”.

This watching-only copy of the wallet will allow you to perform the same functions as the full wallet, except for sending bitcoins. This setup allows you to keep bitcoins safely in cold storage, but use the watching-only wallet for generating bitcoin addresses, monitoring addresses on the blockchain, and broadcasting bitcoin transactions.

6. Generate addresses to receive bitcoin

Now that you have a watching-only wallet on the online computer, you can click “Receive Bitcoins” to generate addresses for receiving bitcoin. When you’re sent bitcoin, you’ll see the transactions show up in your watching-only wallet.

Glacier Protocol

Glacier Protocol is a protocol that outlines best practices for individuals and institutions looking to set up a cold-storage custody solution. For more details on Glacier Protocol, click here.

Transactions

Transaction Components

A bitcoin transaction can be composed of multiple inputs and multiple outputs. This aspect is unique to bitcoin as compared to traditional financial transactions where there is a single source (“from”) account and a single destination (“to”) account. In the case of bitcoin, a single transaction can send many inputs across many different input addresses to many outputs across many different output addresses.

The inputs in bitcoin are Unspent Transaction Outputs (UTXOs). UTXOs can only be spent once per transaction. Any remaining balance must be sent to the sender's change address, which is controlled by the sender. If the balance is not sent to a change address, it becomes a transaction fee paid to miners.

In addition to the inputs and outputs, a transaction contains the sender's public key, the recipient's address, and a digital signature created using the sender's private key.

Transaction Types

Bitcoin has two main transaction types for sending and receiving bitcoin. The first is Pay-to-PubkeyHash (P2PH). As we know, addresses are simply a hash of the bitcoin public key. The P2PH transaction sends UTXOs from an address. Once the sender produces a valid signature associated with that address, the transaction is validated and the funds are sent to the recipient.

The other transaction type is Pay-to-ScriptHash (P2SH). In this case, the sender must satisfy a redeem script associated with the address from which the UTXOs are being sent. An example of a redeem script is a multisignature address that must contain m-of-n valid digital signatures. If the conditions are met, then the transaction is valid and the funds are sent to the recipient.

There is an additional transaction type which is the Coinbase transaction (not to be confused with the company). This transaction contains the block reward for each mined block; the transaction has no inputs, and the sole output is to the miner that won the block (discussed in more detail later).

Transaction Fees

A bitcoin transaction that is sent to the blockchain is accompanied by a transaction fee that is set and paid for by the sender. The transaction fee is a bid and the amount paid determines how long it will take for miners to confirm the transaction, or accept it into a block. Unconfirmed transactions remain in the memory pool. Transactions wait in the memory pool before they are mined into a block, and a miner has accepted the transaction into a valid block.

Users may pay different amounts for different transactions depending on the desired immediacy of confirmation. For example, if a user has a long time preference and can afford to be more patient, they may pay a lower fee and allow the transaction to sit unconfirmed in the memory pool for a longer time. On the other hand, if they need a quick confirmation, say to settle an OTC trade (defined later), they can pay a higher fee. This incentivizes the miners to include the transaction in the next block.

Bitcoin transaction fees are determined by the fee rate, which is expressed as a fee per unit of size. For the same fee rate, transactions of larger size will pay higher fees.

Transaction Confirmations

A bitcoin confirmation is when a bitcoin transaction is included in a valid block. The number of bitcoin confirmations refers to the number of valid blocks that have been mined since, and including, the initial block containing the transaction.

The higher the number of confirmations, or the higher the number of blocks since the transaction was accepted, the less likely that the transaction will be affected by a chain reorganization. A chain reorganization (reorg) means that a previously-valid block is no longer on the longest chain; as such, transactions inside that block are no longer valid bitcoin transactions. If you accept a deposit and there is a reorg, the deposit transaction is invalid on the main chain and bitcoins in that transaction no longer belong to your address.

In order to mitigate this risk, people will wait for a certain number of confirmations, such that it is extremely improbable or difficult to have a reorg that goes that far back. A reorg one block deep is much more likely than a reorg 10 blocks deep.

It takes about 10 minutes for a given block to be mined, so one could expect one confirmation every 10 minutes. The general rule of thumb is that waiting

for six confirmations, or roughly 60 minutes, is a safe amount to wait. Six confirmations provides a 99.99% chance that the transaction will not be reorged and is safe to be accepted as a deposit.

TXIDs

A transaction ID (TXID) , is a unique identifier for a bitcoin transaction. The TXID is created by first hashing the transaction data (some or all of the data, depending on whether it's a Segwit transaction), then hashing it again, and finally reversing the bytes to produce 64 hexadecimal characters. The hashing function used to create TXIDs is SHA256. An example of a TXID is:

```
99f92ef644897dc0e49a56878954f84681480b34d7813ccd818c5e101c0af585
```

TXIDs can be entered into any block explorer, a tool that allows one the ability to pull up real-time and historical information about a blockchain (transactions, inputs, outputs, fees, etc.). TXIDs are useful when conducting transactions with another party – they are the main reference identifier for the transaction. They can also be useful to see evidence of funds being sent, the number of confirmations for the transaction, and any other publicly-available information.

How to Send/Receive Bitcoin

1. Receive bitcoin into your Armory wallet

Following the setup instructions in the previous section, create a bitcoin address and share that address with the sender. Once the sender has sent the transaction to the bitcoin network, you'll see it reflected in your wallet.

2. Sending bitcoin

To send bitcoin, you will:

- Create the bitcoin transaction on your online wallet
- Sign the transaction on your offline wallet
- Broadcast the transaction on your online wallet

A. Use online wallet to Create Offline Transaction

In your online watching-only wallet, Create New Offline Transaction. You will not have the option to “Send” since the watching-only wallet cannot sign transactions. Click the button to “Create Unsigned Transaction”.

B. Transfer unsigned transaction to offline wallet

When a window opens in your watching-only wallet with the unsigned transaction, click “Save” to save the file to your USB device. Eject the USB device from the online device and insert it into the offline device. Click “Offline Transactions” and select “Sign” or “Broadcast Transaction”.

C. Sign transaction on offline device

Load the file from the USB device and click “Sign”. Make sure to verify the details, including the amount and the destination address, before you sign the transaction.

D. Transfer signed transaction to online device

On the offline device, click “Save” to file to save the signed transaction to USB. Eject the USB from the offline device and insert it into the online device. If the original window is still open, you can click “Next Step” to get to the broadcast window. If you have closed Armory, click the “Offline Transactions" button and

select “Sign” or “Broadcast Transaction”. Once the signature is verified, the transaction will be ready to broadcast.

E. Broadcast transaction

Press the “Ready to Broadcast” button to broadcast your transaction to the bitcoin network. This step is irreversible, and now your bitcoins have been sent.

How to Acquire Bitcoin

Receiving BTC

One of the easiest ways to acquire bitcoin is to receive it from another user. This transaction can be in exchange for goods or services provided to that user, or it could be in consideration of something else.

In order to receive bitcoin, you need to set up a bitcoin wallet and generate an address. Once you share that address with the sender, they can send you bitcoin. This is described in more detail in the section above.

Purchasing on Exchanges

Bitcoin can be acquired through a fiat-for-BTC purchase done on exchanges such as Coinbase or Kraken. In order to onboard with the exchanges, any individual or entity will need to provide Know-Your-Customer (“KYC”) documents and complete ID verification. Once those steps are complete, you can fund your account via ACH or wire transfer, purchase bitcoin through the exchange order book, and withdraw the bitcoin to your wallet.

Purchasing OTC

An alternative to purchasing bitcoin through an exchange is engaging in an Over-the-Counter (OTC) transaction. In this case, the buyer and seller deal bilaterally. Both sides agree to a trade price and quantity, and settle directly with each other. The buyer sends USD funds to the seller, and the seller sends bitcoin to the buyer.

OTC transactions are more well-suited to larger players that want to transact in larger sizes without the impact or visibility of trading on an exchange. OTC deals come with larger counterparty risk, because you face the other party directly, rather than through an intermediary like an exchange that guarantees the trade. Additionally, with OTC settlement, one side settles the trade first – they face additional risk if the second side does not settle.

Purchasing an ETF

In 2024, bitcoin ETFs, or Exchange-Traded Funds, were approved for trading. ETFs are funds that hold bitcoin and issue shares in the fund; investors can buy a share in the fund which equates to some portion of the bitcoin that the fund is holding.

ETFs are accessible to many people through a traditional brokerage account such as IBKR or Fidelity, so they serve as an easy onramp without needing new accounts and integrations. However, it's important to note that as an investor in a bitcoin ETF you have no claim to actual bitcoin, you merely just hold shares of the fund.

Mining

A more difficult way to acquire bitcoin is through the process of mining. With every block mined, there is a block reward of 3.125 bitcoin, as well as transaction fees that are paid to the miner who won the block. Mining is an

expensive endeavor, but it provides the miner with a source of bitcoin. This is discussed in more detail below (Section X. Mining).

Bitcoin Nodes

1. Peer-to-Peer Network

Bitcoin is a peer-to-peer (P2P) network. This means that there is no centralized server or service operating the network; instead, it is maintained by a network of nodes that all function as peers. All nodes have the same permissions and status within the network. It is through this peer-to-peer network that bitcoin establishes and maintains its decentralization.

2. Full Nodes

Full nodes are bitcoin clients that run software to validate transactions and ensure that the network meets consensus rules. They guarantee the security and integrity of the public blockchain ledger, storing copies of all transactions and routing valid transactions to other nodes. While full nodes also contain wallet services such as private key generation and key storage, users may choose to run a full node but use a separate wallet solution.

Anyone can run a full node. The most common version of software that people use to run a full node is Bitcoin Core. Running a node requires downloading the blockchain history and a constant internet connection to stay updated. Running a full node ensures that you are in control of the information you receive from the network, and allows you to independently verify any transaction activity or blockchain balances. The fact that any user can run their own full node is a critical part of the bitcoin innovation in monetary sovereignty.

Because full nodes store a substantial amount of data and can be computationally intensive, it is recommended to run them on fast hardware

that has good storage capacity. Some suggested requirements for running a full node include:

- Desktop or laptop hardware running recent versions of Windows, Mac OS X, or Linux
- 400 GB free disk space and minimum read/write speed of 100 MB/s
- 2 GB of RAM
- Broadband internet connection with upload speeds of at least 50 KB/s
- An unmetered connection with high upload limits. Full nodes can use 200 GB upload a month. Downloads are around 20 GB/month and the initial block download can be upwards of 340 GB the first time you start your node
- Six hours a day that your node can be left running, though more is better

For a comprehensive guide on running a full node, see this Kraken blog article.

3. Lightweight Nodes

Lightweight nodes are bitcoin clients that contain only the block header from each block on the network. The purpose of lightweight clients is that they are less computationally intensive to run, since they do not store the data associated with each individual transaction. At the same time, they can still verify blocks.

4. Mining Nodes

A small portion of the nodes on the bitcoin network are also mining nodes. A mining node is the most computationally intensive node by far, and it requires specialized software and hardware. We discuss mining in more detail in the next section.

Mining

What is Bitcoin Mining?

Bitcoin mining is the process of creating new bitcoins, adding bitcoin transactions to blocks, and appending new blocks to the bitcoin blockchain. The mining process is done by solving a computationally-intensive math problem, known as proof of work. The process is intentionally demanding of computational resources, as it is this aspect of the design that ensures the integrity of the ledger.

Mining is a core component of bitcoin's decentralization. Because there is no central party or intermediary to validate transactions, bitcoin relies on a network of miners to achieve decentralized consensus.

When miners add new blocks to the chain, they receive two forms of compensation per block. The first is the block reward, which is the new bitcoin created for that block. The bitcoin block reward was initially set at 50 bitcoin per block, with a halving schedule to be cut in half every 210,000 blocks. The current block reward is 3.125 bitcoin and will remain at this level until the next halving, which is estimated to be in 2028.

The second form of compensation is transaction fees. Transaction fees are variable depending on network demand, and miners will choose to mine the transactions that have the highest fees associated with them. In 2140, the block reward will go to 0 which means that no new bitcoin will ever be created. At this point, transaction fees will be the sole form of payment made to miners.

Proof of Work

Proof of work refers to the difficult math problem that miners must solve in order to mine a valid block. Miners first assemble a group of transactions that

they intend to include in the next block. They then hash the transactions, which produces a numeric value. The hash of the transactions must be below a specific target in order for the block to be considered valid based on bitcoin consensus rules. If the hash is not below the target, the miner will append a nonce to the transaction list hash and calculate the new numeric value associated with the combined hash. The miner will continue to change the nonce until it results in a valid hash that has a number below the target.

Because of the way that hashing works, there is no way to solve for the nonce that results in a hash that is below the target. As a result, the only way for the miner to solve the problem is to continue to compute the value for every nonce until it finds one that works. This is called proof of work .

Proof of work ties bitcoin network security to energy consumption, since it requires energy to compute the hashes necessary to satisfy the proof of work requirements for mining bitcoin. This consensus mechanism provides an incentive to harness energy in the most efficient way possible; per Jevons Paradox, we would expect these efficiency gains to lead to increased bitcoin usage and adoption.

Proof of work is an innovation that is critical to bitcoin's security and integrity. If any bad actor attempted to edit a past transaction, say to double-spend bitcoin that they had already sent to someone, they would need to redo all the proof of work that miners had done since that transaction. This would require an enormous amount of computing power.

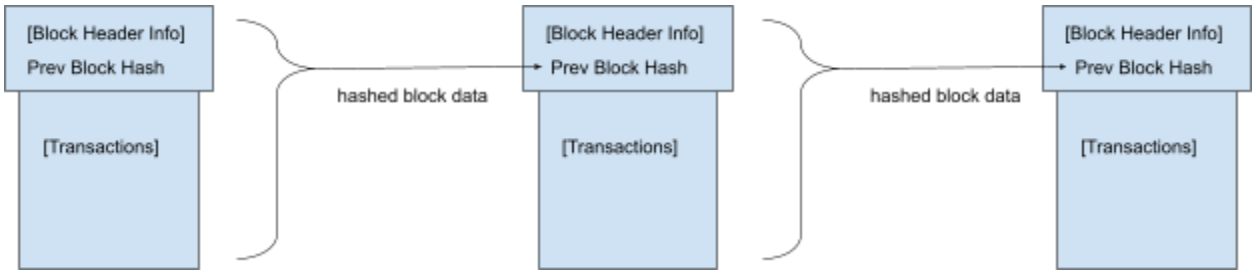
Difficulty

Bitcoin difficulty is a measure of how challenging it is to solve the proof-of-work math problem. A higher difficulty means that the target is lower; a lower target means that the miner has to try more solutions before finding a valid one that is below the target.

The bitcoin difficulty adjusts based on how quickly blocks are mined. The intention is for a new block to be found every 10 minutes. If blocks are mined faster, the difficulty adjusts higher so that it recalibrates back closer to the 10-minute timeframe. If blocks are mined slower, the difficulty adjusts lower to make it easier to mine. The difficulty adjustment is done every 2,016 blocks based on the average time it took to mine those blocks.

Creating the Blockchain

The blockchain consists of a series of valid blocks that have been mined. The "chaining" of blocks is done by reference to a hash of the prior block's block header, which is then included in the current block header. This means that if any data from a previous block were to be tampered with or amended, all the subsequent block headers would change and the chain would not be a valid blockchain.



Running a Miner

In order to run a miner, one needs specialized hardware and software. On the hardware side, miners today need Application-Specific Integrated Circuits (ASICs). These pieces of hardware allow miners to run the hashing algorithm used for proof of work (SHA256) extremely quickly, and in parallel, across multiple integrated circuits. This design gives the miner a better chance of finding a valid block faster than other pieces of generalized hardware that are not designed for this specific function.

In addition to having specialized hardware, a miner will run a mining node with specialized software, such as CG Miner. The mining node will communicate with the ASICs, sending the necessary blockchain data to the ASICs to solve the proof-of-work problem. Once a valid solution is found, the mining node transmits the block to its peers.

Mining Pools

In the early days of bitcoin, one could mine bitcoin on their laptop. Since then, the mining industry has become increasingly competitive, transitioning from Central Processing Units (CPUs) to Graphics Processing Unit (GPUs) to Field-Programmable Gate Array (FPGAs) and ultimately ASICs. It's anticipated that the mining industry will continue to grow in efficiency and competitiveness. As such, it is nearly impossible for any small miners to successfully mine a bitcoin block.

The growth of mining competitiveness has resulted in the introduction and adoption of mining pools. Mining pools allow miners to pool their hashing power and split the mining rewards. Rather than wait endlessly to mine a block with low hashing power, the combined pool has a greater chance of finding a block amongst them. They then split the rewards based on how much hashing power each miner contributed to the pool. While the rewards are lower, they are more frequent, drastically reducing the variance associated with individual mining and making it more compelling for small miners to devote their hash power to the network.

Mining pools are operated by pool operators who earn a percentage of the rewards as their fee for operating the pool. The pool operator runs specialized mining pool software, a mining pool server, and a bitcoin node, allowing them to validate blocks and transactions on behalf of the miners in the pool. Pool miners can connect to the mining pool server using a protocol such as Stratum.

Cloud Mining

Cloud mining is another option for individuals or entities who desire to mine but cannot afford to invest in the necessary infrastructure. In cloud mining, users do not need to own any hardware themselves. Instead, they can lease or rent hash power from companies that manage the infrastructure as well as the necessary aspects like electricity and cooling. The user then receives a portion of the rewards that are earned by the rented infrastructure.

This method allows people to participate in mining without directly purchasing and managing infrastructure. It can more easily be scaled up and down based on the user's desired investment, and it benefits from the economies of scale from the cloud company's entire operations.

51% Attacks

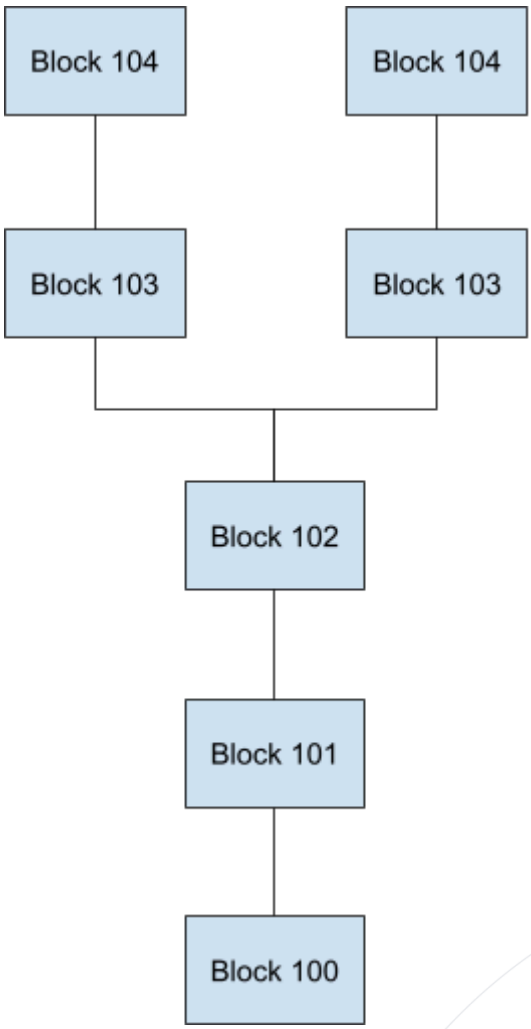
A 51% attack is when a miner or participant with majority hashing power leverages that hashing power to rewrite a portion of the chain, invalidating all transactions that were included in that portion. This enables the attacker to double-spend bitcoin, where they send bitcoin that was part of the invalidated transactions to another recipient. Now there are two recipients that think they have received bitcoin and had it confirmed on the chain, but one of those transactions is invalid.

The cost to do a 51% attack is enormous because it requires enough investment into mining equipment and electricity to control a majority of the bitcoin network's computing power. The reward of a 51% attack is also questionable. The attacker cannot rewrite historical blocks, so their attack is largely constrained to double-spending, which is more limited in upside. As such, 51% attacks do not seem to pose as much of a practical threat as they do a theoretical threat.

Bitcoin Forks

What is a Fork?

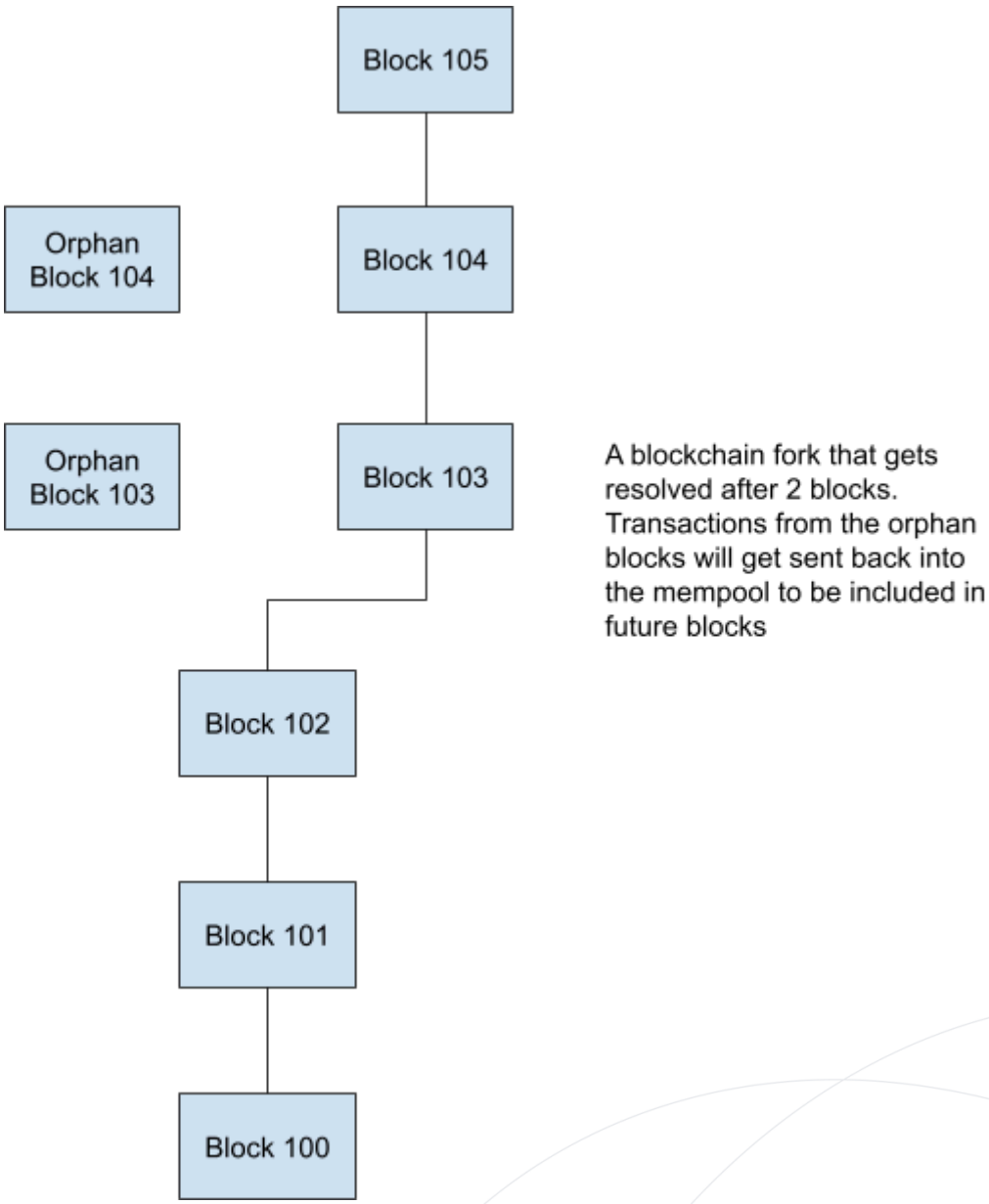
A fork in a blockchain is when two blocks of the same block height exist. This creates a fork in the chain where there are two resulting potential paths.



A blockchain fork at Block 102 resulting in two chains

Some forks happen in the normal course of mining, when two different miners simultaneously find valid blocks. These forks resolve fairly quickly as miners continue to mine and new blocks are added to one of the forks. The block from the other fork becomes an 'orphan' block and the transactions return to the mempool to likely be included in future blocks. The bitcoin

network is designed to handle these types of forks and they are largely harmless to the end user.



Some forks to the bitcoin protocol are intentional forks. These intentional forks could be designed to independently work on a new version of the protocol, such as in the case of Litecoin. Or they could be designed to upgrade the existing protocol, such as in the case of Segwit, which is explained later.

Chain Reorganizations

Blockchain reorganizations, or reorgs, are when an alternate version of the blockchain gains consensus and certain historical blocks are reorged. Essentially, they rewritten out of blockchain history.

In the example above, once the blockchain fork is resolved, both orphan blocks 103 and 104 are reorged – they are not valid on the main (longest) chain. As a result, the transactions in those blocks are also invalid.

While this sounds potentially dangerous, in practice reorgs are generally harmless. First, most reorgs are only one block deep as they occur due to normal variances as different miners compete to mine the next block. They are usually resolved within one block. Second, many of the same transactions appear in both the reorged block and the accepted block; this is due to the fact that miners are all mining transactions from the same mempool. Finally, in the event there is a reorg and a given transaction was not in the accepted chain, the transaction will be sent back to the mempool for inclusion in a subsequent block. With a normal transaction fee, this inclusion should happen in the same amount of time as normally expected for the transaction to be confirmed.

The risk with reorgs is if a nefarious actor, such as a miner with 51% hash power, is deliberately trying to take advantage of a reorg attack. In these cases, they could attempt to double-spend bitcoin; that is, to send the same bitcoin in two different transactions, one of which ends up on an orphan block. Only one of those transactions would end up being valid, and the recipient of the other transaction is out of luck.

Hard Forks

Hard forks are changes to the protocol that are not backwards compatible, meaning the rules changed or transactions are approved that were unsatisfactory. This requires all users to upgrade their nodes. In these cases,

the only way to use the protocol is to upgrade and entirely adopt the new ruleset. Other examples of changes that necessitate hard forks are changes to the difficulty rules and to the block structure / block hash.

Generally, hard forks are not preferred. The value of the bitcoin protocol is that its rules are not subject to change; users should be able to maintain valid nodes without needing to actively upgrade. And there should always be one main chain (outside of the incidental forks from mining). For those reasons, bitcoin never hard forks unless absolutely necessary.

Bitcoin hard forked once in 2013 as a result of a bug in a software upgrade. The fork was resolved by asking miners to switch back to the prior software version in order to maintain one consistent chain. Bitcoin hard forked accidentally again in 2018; this was fixed by a soft fork (described below) and there was no chain split.

Soft Forks

Soft forks are changes to the protocol that are backwards compatible, meaning older versions of Bitcoin software can still work with the updates. New blocks will continue to be valid with old nodes, while new nodes will be valid and/or mine according to the new rules.

New bitcoin transaction types may be introduced via soft fork; new miners and nodes recognize the new transaction type, while old nodes recognize the transaction as a valid ‘pay-to-anybody’ type transaction.

Upgrades, additions, and improvements to the bitcoin protocol are done via soft fork in order to reduce the risk of a chain split. While nodes do not need to upgrade for these changes to take hold, the network does require that the majority of miners upgrade. With a majority of miners upgraded, the majority of blocks on the network are being mined and validated according to the new rules.

Notable Bitcoin Forks

1. BitcoinXT and Bitcoin Classic

BitcoinXT and Bitcoin Classic were 2015 hard forks of bitcoin with certain changes made to the protocol. In particular, they called for block size increases, with Bitcoin Classic allowing the block size to double every two years until its size reached 8MB. While the hard forks garnered interest and attention, ultimately very little mining power moved over to mine the new chains and Bitcoin remained the dominant version.

2. Bitcoin Cash

Bitcoin Cash was a 2017 hard fork of Bitcoin that split the currency. This meant that it shared Bitcoin's transaction history up to a certain block height (478,558), after which the chain split into Bitcoin (BTC) and Bitcoin Cash (BCH). Holders of Bitcoin as of that chain height ended up getting 1 Bitcoin Cash for every Bitcoin owned; the Bitcoin Cash was valid on the BCH chain.

Bitcoin Cash was a fork that stemmed from debate about the size of blocks on the Bitcoin blockchain. Long discussions took place about potentially increasing the block size, dating back to 2015 and Bitcoin XT / Bitcoin Classic. However, the block size increase was a very controversial move due to the limitations it placed on running a node. Larger block sizes meant that average users would find it extremely difficult to run nodes; as a result, nodes would become more centralized among large institutions and miners who had the resources and capacity to handle the large blocks. This debate led to a contentious hard fork, with Bitcoin Cash being the fork that supported larger blocks.

Following the 2017 fork from Bitcoin, Bitcoin Cash later had another fork in 2018, splitting into Bitcoin ABC and Bitcoin SV, the latter of which would increase the block size even more to 128MB.

Bitcoin continues to remain the dominant source of hashing power, as miners have the most incentive to mine that chain due to its economic value. The other chains remain tiny in comparison.

3. Segwit

Segwit, or "Segregated Witness", was a soft fork upgrade to the format of Bitcoin transactions. It accomplished several things. First, it separated signature data from other transaction data, reducing the size of transactions and allowing more transactions per block. Second, it was updated to allow the UTXO's transaction hash to be changed without leaving the UTXO invalid. -By fixing transaction malleability and ensuring there is always a valid relationship between parent and child transactions, Segwit also enabled the Lightning Network, a network of payment channels built upon bitcoin.

Segwit would only be activated once 95% of miners signaled readiness for it. This threshold was reached in August 2017, at which point Segwit was 'locked in'. Two weeks later it was activated.

The timing of Segwit and the Bitcoin Cash fork were not coincidental. Miners who were unhappy with the Segwit solution and the lack of large blocks accompanying it proceeded to fork Bitcoin at that time, creating Bitcoin Cash.

4. Taproot

Taproot was a bitcoin soft fork in 2021 that enabled privacy and efficiency enhancements. Specifically, Taproot batched together signatures which condensed the size of multisig transactions and made it impossible to distinguish between single-signature and multi-signature transactions. The streamlined transactions paved the way for further smart contract usage on Bitcoin, as well as further Lightning Network adoption. As both rely upon the base layer, the faster transaction processing and smaller transaction sizes allow for increased activity that would otherwise be unattainable.

Taproot was activated in November 2021 following a 90% lock-in from miners.

Forks and Self-Custody

Most bitcoin forks to date have been hard forks that split the currency, such as Bitcoin Cash. In these cases, Bitcoin owners maintain their bitcoin holdings and also receive the forked coins, which are valid on the forked chain. However, this is only guaranteed if you hold your bitcoins in self-custody and control the private key to the addresses in which the bitcoin is held. If bitcoin is held with a third party, there is no guarantee that they will credit you the forked coins or the value of the forked coins.

This is an example of why “Not your Keys, Not your Coins” applies to bitcoin custody. In this case, “Not your Keys, Not your Forked Coins.”

Bitcoin Ecosystem

Miners

We discussed the role of miners in bitcoin and the function that they serve. Now we’ll dive more into the business of mining and how one could get exposure to mining companies.

How do Miners make money?

Mining as a business relies on producing bitcoins for the lowest amount relative to the market value of ~~the~~ bitcoins. For a bitcoin miner, the cost of producing bitcoin is a function of hardware, electricity, and operating costs. The revenue from bitcoin production is a function of their share of global hash rate, the block reward, transaction costs per block, and the price of bitcoin per USD.

On the hardware side, miners must purchase or design the most competitive ASICs that can compute as many hashes per second as possible. This is the primary driver behind how competitive a miner will be and their ability to win blocks. The more hashes per second that a miner has, the larger their share of global hash rate, and the better chance that they will find a solution to the mining math problem before any other miner.

In addition to acquiring hardware, miners must operate the hardware. This requires large-scale data centers with access to enough power to support all the miners, as well as cooling systems to ensure the hardware doesn't overheat and slow down. Many miners will choose opportunistic locations to set up their operations where either economic drivers or natural forces result in inexpensive electricity and cooling systems.

Miners make money if they are able to keep their costs of production low. The costs are within their control, as are some parts of production. The parts of production that are not within their control are:

- the global hash rate,
- the block reward,
- transaction fees, and
- BTC/USD price.

The global hash rate depends on how many other people and entities in the world decide to mine bitcoin. The higher the global hash rate, the lower the share that a miner has.

The block reward is baked into the protocol; when the block reward is halved every 210,000, miners earn half as many bitcoin per block. Transaction fees are subject to market demand and are out of the control of miners, as is the traded BTC/USD price.

All of these components together make up the interesting and complex business of mining. For people who might want exposure to bitcoin mining

but lack the resources or desire to build a mining operation, there exists another option: investing in publicly-traded miners.

Publicly-traded Miners

Many bitcoin miners have gone public as a way to tap into the liquidity of public markets. Prior to the bitcoin ETF, there were few ways for investors to gain access to bitcoin through publicly-traded stocks and other securities. Miners helped fill that gap with a business that was easy to understand and generally clear of significant regulatory oversight. Some publicly-traded miners today are:

Miner	Ticker	Last	Market Cap ($M)
Marathon Digital Holdings	MARA	$13.33	$4,691
Cleanspark	CLSK	$8.03	$2,255
Riot Platforms	RIOT	$7.84	$2,801
Iris Energy	IREN	$6.57	$1,475
Hut 8	HUT	$12.66	$1,578
Terawulf	WULF	$3.05	$1,170
Bitdeer Technologies Group	BTDR	$11.35	$2,233
Bitfarms	BITF	$1.02	$760
Cipher Mining	CIFR	$3.02	$1,121
Northern Data	NB2	$24.12	$1,540
Applied Digital	APLD	$5.25	$1,180
Hive Digital	HIVE	$1.73	$402
Bit Digital	BTBT	$2.01	$367
Prairie Operating Co	PROP	$4.45	$192

DMG Blockchain Solutions	DMGI	$0.23	$45
Soluna Holdings	SLNH	$0.70	$29
Greenidge Generation Holdings	GREE	$0.95	$14
Mawson Infrastructure Group	MIGI	$0.58	$11
Cathedra Bitcoin	CBIT	$0.04	$9
Sato Technologies	SATO	$0.14	$11

Spot Exchanges

We discussed the use of spot exchanges as a way to acquire bitcoin. A “spot” transaction is one where both sides are traded for immediate physical delivery. In the case of a spot FX transaction such as USD/JPY, one party immediately receives JPY and the other immediately receives USD. The most common spot transaction for bitcoin is BTC/USD where parties can buy or sell BTC for USD with immediate settlement.

How do Spot Exchanges Make Money?

Spot exchanges serve as unbiased platforms to match buyers and sellers. They typically make money by charging a fee on every transaction. Over time, fee structures have become very complex as exchanges aim to use fees to incentivize trading activity. Exchanges have a variety of fee schedules depending on how active a participant is on the exchange. Overall, all exchanges serve to both drive volume to the platform and drive revenue for the exchange.

In crypto, exchanges often serve other functions as well. They are a clearinghouse, guaranteeing and settling trades; they’re a custodian, storing bitcoin in custody for short or long periods of time; they’re a market data

provider, a broker, and a payment app. All these other functions serve as ancillary business lines, and exchanges will often charge for them as well.

List of Major Exchanges

Many spot exchanges have been developed for crypto. While in some sense exchanges have network effects and you would expect only a handful of them to "win", the crypto market is extremely fragmented due to its global nature. Different countries have different regulations, which require different licensing in order to operate a crypto exchange. As such, different exchanges have been developed that are particularly suited to certain markets and geographies.

The predominant bitcoin exchanges, along with their primary geographies, are:

Exchange	Geography
Coinbase	North America
Binance	Asia
Kraken	Europe
Bybit	Asia
LMAX Digital	Europe
Bitstamp	Europe
Huobi	Asia
Crypto.com	North America
OKX	Asia
Gemini	North America
BTSE	South America
Mercado Bitcoin	South America

Derivatives Exchanges

A derivatives exchange is a platform where people can trade contracts that allow them to bet on the future price of things like commodities, stocks, or cryptocurrencies without actually owning them. These exchanges help manage risks and also allow for speculation on price movements, in the hopes that the trade will result in a profit.

Types of Derivatives Products

1. **Futures**

Futures allow market participants to enter into a contract today to purchase bitcoin for settlement on a later date in the future. For example, a market participant can enter into a contract today to purchase bitcoin one month from now. In order to enter into that contract, the participant only needs to post a fraction of the margin upfront. Then, when the contract matures for settlement, the participant can post the remaining amount of capital in order to receive the bitcoin.

Many futures contracts are cash-settled to cash or crypto. In these cases, upon settlement the buyer needs to only post the difference between the purchase price and the price at settlement. This difference is posted in USD in the case of cash-settled futures and in BTC in the case of crypto-settled futures. Futures contracts can also be physically-settled, in which case they settle directly to bitcoin and the buyer receives bitcoin at the contract's expiration.

Futures contracts can be inverse contracts or linear contracts. If they're linear contracts, the contract is for a fixed amount of BTC and the settlement amount is the difference between the USD price of the contract (cash-settled contracts), or to the physical BTC (physically-settled contracts).

If they're inverse contracts, the contract is for a fixed amount of USD and the settlement is the difference between the BTC value of the contract at both levels of spot; these contracts are cash-settled to bitcoin.

In most cases, the purpose of buying futures on bitcoin is to be able to get levered exposure to the asset. Because of the way they are traded on margin – borrowing money to trade to increase the potential of profit – buyers and sellers can have price exposure to the asset without having to post the full USD or bitcoin amount. This leverage is attractive to speculators and entities that are balance-sheet constrained. Another reason why participants will trade futures, particularly inverse futures, is because they can post bitcoin as collateral in order to trade these contracts. This provides a unique opportunity to utilize bitcoin holdings for the purposes of trading and speculation.

2. **Perpetual Futures**

Perpetual futures are a type of future that have no expiration date. Instead, they settle on a daily basis forever. This allows participants to have constant exposure to bitcoin without worrying about a contract going away.

On a daily basis, the longs and shorts (define these terms) of perpetual futures contracts exchange cash flows based on (1) the difference in spot price day-over-day, and (2) the funding rate for the contract. The funding rate is based on market demand; if more buyers want to be long sellers than short, then the funding rate is positive and buyers pay the sellers. If more sellers want to be short, the rate is negative and sellers pay the buyers.

Perpetual futures can be inverse contracts or linear contracts. If they're linear contracts, the contract is for a fixed BTC and the daily settlement is the difference between the USD price at both levels of spot. If they're inverse contracts, the contract is for a fixed amount of USD and the daily settlement is the difference between the BTC value of the contract at both levels of spot.

Like futures with a specified expiration date, perpetual futures offer a way for participants to get levered bitcoin exposure. The difference with perpetual futures is that they don't expire; the economic mechanism that charges/compensates for this feature is the funding rate.

3. Options

Options are a type of derivative that provide two additional parameters in addition to price – expiration date and strike. This means that participants can bet not only on bitcoin being above/below a certain level, but also on it happening before a particular expiration date.

Two types of options exist – call and put. A call option gives the buyer the right to purchase bitcoin at a certain price on a certain date in the future. A put option gives the buyer the right to sell bitcoin at a certain price on a certain date in the future.

Options can also be linear or inverse contracts. In the case of a linear contract, the buyer receives a physical bitcoin or USD, such that the payout varies linearly with the BTC/USD spot price. In the case of an inverse contract, the buyer receives an amount in bitcoin that is equal to what the contract is worth at that spot price. In this case, the payout varies with the price of the inverse futures contract.

Participants will trade options for several reasons. First, options contracts have inherent leverage in them due to the asymmetric nature of the payoff; participants can hold positions that have substantial upside exposure with limited downside risk. Second, options allow participants to bet on different facets of price action, since every option has a strike price and expiration associated with it. This allows for more nuanced positions as well as more targeted exposure. Finally, options contracts contain a natural risk premium from bitcoin volatility. This risk premium can provide a source of earnings to market participants who sell options against their bitcoin holdings.

How do Derivatives Exchanges Make Money?

Derivatives exchanges make money in a similar manner to spot exchanges, which is on the transactional side. They typically charge a transaction fee associated with every trade and that fee makes up their revenue. The transaction fee per trade will vary based on the participant's fee tier, which is constructed based on their trading volume, the type of order (maker vs. taker), the underlying asset, and other similar factors.

Derivatives exchanges also function as clearinghouses and make revenue from this aspect of the business, particularly because derivatives trading activity tends to be highly levered. The leverage is provided by the exchange itself and they charge margin-related fees to participants who trade on leverage.

List of Major Derivatives Exchanges

Derivatives exchanges tend to be fragmented by their ability to serve US customers, as US regulators have proven to be most clear and direct with their jurisdiction over bitcoin derivatives. The types of underlying assets that can be pledged as collateral and the nature of the contracts are correlated with the ability to serve US customers. In particular, US derivatives exchanges tend to have more linear contracts, while international exchanges deal solely in crypto and offer inverse contracts.

Exchange	Geography	Products
Bybit	non-US	inverse perpetuals, futures, options
Deribit	non-US	inverse perpetuals, futures, options
CME	US	linear futures, options
Binance	non-US	inverse perpetuals, futures

Lenders

What is Bitcoin Lending?

Bitcoin lending is exactly what it sounds like. A holder of bitcoin can lend their bitcoin by sending it to an address controlled by the borrower, at which point the borrower is in possession of the bitcoin. The borrower will use the bitcoin for a certain period of time, perhaps for trading or as collateral, and then will return the bitcoin to the lender by sending it back to an address controlled by the lender.

It should be apparent that bitcoin lending has substantial risk associated with it, since the lender is no longer in control of the private keys associated with the bitcoin that they "own". This risk is typically mitigated by holding collateral, though some loans are uncollateralized.

How do Lenders Make Money?

In order to be compensated for the risk of lending, lenders will charge an interest rate to the borrower. This rate is usually paid in bitcoin and allows the lender to earn a rate of return on their bitcoin holdings.

Some companies engage in both sides of lending, where they will borrow bitcoin from some participants and lend it out to other participants. In these cases, they will aim to borrow for a lower rate than what they lend at, capturing the difference in interest rates. This style of lending is more risky than being a direct participant, as the lenders are highly levered in their exposure. In 2022, upon the collapse of FTX (add link), many lenders were unable to manage this risk and became insolvent and bankrupt very quickly.

Bitcoin Lenders

Following the collapse of FTX, many of the large bitcoin lenders went bankrupt. They lent out all the bitcoin that they had borrowed and ultimately

did not have enough bitcoin to pay back what they owed. Since then, bitcoin lending has very slowly picked up, but no large lenders have taken over the space. This is likely due to the fact that the bitcoin lending business was highly risky and leveraged, and the market has not returned to being comfortable with that level of risk.

OTC Desks / Prime Brokers

What is OTC Trading?

In typical trading that has been described so far, users trade on an exchange in a central limit order book. Every user puts their orders into that order book, which is managed by the exchange. User orders are then matched with other user orders based on the prices at the time orders are entered. This creates a single, liquid order book for trading and price discovery. While customer orders are matched with other customer orders, the exchange sits in the middle – as such, each customer faces the exchange for guaranteeing trade execution and settlement.

In over-the-counter (OTC) trading, customers face each other directly. Typically the two sides are the customer and an OTC trading desk, the latter being exclusively in the business of OTC trading. The customer and the OTC trading desk negotiate bilaterally on the terms of the trade, and they execute and settle the trade directly with each other. OTC trading is typically reserved for high net worth individuals and larger institutional clients.

Customers can use OTC trading to execute larger block trades that would otherwise move the market if done on an exchange. They also allow for more customized ~~and bespoke~~ trades, unlike an exchange where the contracts tend to be highly standardized and fungible in order to promote centralized liquidity. While many OTC trading desks are as large and established as top exchanges, OTC trades may still face higher counterparty risk due to trade settlement being done directly with the customer.

What is Prime Brokerage?

Prime brokerage refers to bundling services that facilitate trading for institutional clients. It can include lending, order routing and trade execution, cash and collateral management, risk management, and custody. This allows institutions to have a single touch point for ease of trading and efficiency of clearing, ultimately streamlining the process for them to access different pools of liquidity and trade with capital efficiency.

OTC Desks / Prime Brokers

Many OTC Desks also operate as Prime Brokers through offering ancillary services that cater to institutional clients. Similarly, many Prime Brokers also operate as OTC desks through offering direct bilateral trading capabilities.

Some of the OTC desks and Prime Brokers in the crypto space are:

Broker	Offerings
Coinbase Prime	spot trading, custody, lending
Cumberland	spot trading, options trading, lending
FalconX	spot trading, options trading, lending
NYDIG	spot trading, options trading, custody
Galaxy	spot trading, options trading, lending, structured products

Data Providers

Market data comes in many forms and is a backbone of trading and following markets. In crypto, the data provided can be fragmented across various exchanges around the world. Market data providers help to aggregate, clean, and provide this data to users for further analysis and visualization.

Some market data providers focus on providing raw data, while others focus on dashboards and tools to analyze the data. Both serve a purpose in the bitcoin ecosystem and can be suitable to investors large and small.

Some of the market data providers in the crypto space are:

Provider	Description
Coinmarketcap	market data aggregator
Coingecko	market data aggregator
Cryptoquant	market data aggregator and analytics provider
Kaiko	market data provider
Coinmetrics	market data and analytics provider
The Block	analytics provider

Corporations and Bitcoin

Why do Corporations hold Bitcoin?

In recent years, many public and private companies have taken to holding bitcoin on their balance sheet. Often, these companies are not bitcoin companies, so they have little need to hold bitcoin for any day-to-day operations. Instead, they decide to keep treasury assets in bitcoin purely for its promise as a store of value.

Companies that earn revenue and profit in USD accumulate it and hold it on their balance sheet. Some might be used to pay expenses, but any net earnings are saved in USD. Unfortunately, these savings are diminished in value as the money supply continues to be increased; the hard-earned profits are disintegrating on corporate balance sheets. For companies with this

exposure, converting some of those profits into bitcoin is a prudent way to manage this risk. Bitcoin doesn't have the same risk of being debased through increases in supply, so it can serve as a better store of value. Of course, bitcoin is more volatile than USD – but that volatility has historically been associated with large long-term price appreciation rather than the opposite.

Microstrategy: A Case Study

One of the earliest and most prominent companies holding bitcoin on their balance sheet is Microstrategy (ticker: MSTR). Microstrategy first started purchasing bitcoin in August 2020, when their former CEO and current Executive Chairman, Michael Saylor, announced that they had purchased $250 million dollars worth of bitcoin, or 21,454 bitcoin, at a price of $11,652.

Since 2020, MSTR has continued to purchase bitcoin on a consistent basis, accumulating more than 226,000 bitcoin to date. These purchases have often been funded by convertible debt; MSTR issues long-dated convertible notes through the debt market and uses the proceeds for purchasing bitcoin. The company pays the debt through revenue from its core business line, allowing it to continue to issue debt without having to sell bitcoin holdings.

The bitcoin strategy has led to a drastic appreciation in MSTR stock over the years and has led other companies accumulating bitcoin holdings to benefit from its price appreciation. MSTR may have been the first company to adopt bitcoin in such size, but they will not be the last.

Governments and Bitcoin

Why do Governments hold Bitcoin?

Many governments find themselves in possession of bitcoin. Sometimes this is due to explicitly purchasing bitcoin, but in many cases it's due to seizing bitcoin from illegal operations. Bitcoin that is seized typically sits on the balance sheet of the government until they decide to sell it.

Some governments may choose to hold the bitcoin for its long-term qualities as a value store, similarly to many governments that hold gold as part of their reserves. But bitcoin offers advantages over gold in that it's easily stored and transferred, should the government decide to sell it at a later date. In years prior, the US government has auctioned off bitcoin to market participants; that bitcoin would sometimes trade at a slight premium to bitcoin on exchanges. The reason for this dynamic is that bitcoin that comes directly from the US government is considered "cleaner" in some ways due to its source being the US government.

For non-US governments that typically hold USD reserves, bitcoin provides an alternative that can maintain its value but is less dependent on the US. This can be advantageous for countries seeking to increase their global standing and gain leverage in areas like trade and debt.

Overall, a variety of ways exist in which governments obtain bitcoin and different reasons that affect their desire to hold bitcoin. The trend worldwide has been towards more willingness and acceptance to hold onto this new asset that is a hedge against the US dollar.

El Salvador: A Case Study

In September 2021, El Salvador became the first country to make bitcoin legal tender, meaning that all businesses were required to accept it for payment. The country took further steps to increase adoption by rolling out its own app for people to be able to spend and use bitcoin. Half of the nation's households downloaded the app when it went live.

Since then, adoption and usage has waned a bit, though a set of users remain very active in using the app and in dealing in bitcoin day-to-day. Furthermore, El Salvador itself has accumulated more than 5,600 bitcoin that it holds in its treasury.

The move to adopt bitcoin as legal tender in El Salvador has led to growth for the country. In 2022, there were more lightning wallets than bank accounts, a testament to the promise of cryptocurrency in countries where a substantial portion of the population is unbanked. Additionally, bitcoin companies have been moving to El Salvador to have a permanent presence there. Further, people have been visiting El Salvador to experience the bitcoin ecosystem there. The increase of interest in El Salvador, regardless of the reason, has led to economic growth and tourism.

El Salvador has had much to gain from adopting bitcoin, as it was previously on the US dollar and in a state where many citizens lacked access to the banking system. Bitcoin's promise helps solidify the financial footing of the country and its citizens, driving their access to financial services and opportunity.

Custody Considerations for Corporates and Governments

Multisig / Sharding

Unlike in the case of individuals, corporations and governments have additional considerations that should drive the decisions around their monetary custody setup.

First, access to bitcoin needs to be spread across multiple people. This can be done through a multisig wallet in which the m-of-n scheme matches the exact permissioning desired by the entity. The advantage of this setup is that it doesn't require any third party and allows for storing coins in a wallet that is entirely controlled, managed, and accessed through the particular entity or government. However, this setup would require wallet rotation any time the permission set needs to change, either through the m-of-n scheme or through the particular individual's holding keys. Creating a new wallet with new keys and sufficient entropy every time permission change could be onerous for some entities. In those cases, it might be preferable to have the permissioning done at a different level.

This can be done by sharding, whereby Shamir's Secret Sharing Algorithm is used to split access to a single key across different individuals. A quorum of individuals is required where each individual successfully proves their access to the sharded key via a password. Once the quorum is reached, the bitcoin private key can be used to sign transactions.

Another alternative is Multi-Party Computation (MPC). Using MPC, multiple individuals can each hold a piece of private data and can combine it to run a function while never exposing the underlying data. This allows an entity to control how a key is accessed without sharing sensitive information across

users or outside of the secure environment where the key resides. It has a similar effect to sharding, though the mechanism is different.

Both sharding and MPC allow an entity or government to maintain the same wallet and modify access to it without reconstructing the wallet. It should be noted that the capacity to sharding or MPC permission schemes can be exploited to an attack vector, as that administrator user could simply override the permission set to be one within their control. But it allows for an additional set of user signing permissions that may be more practical for day-to-day usage.

Data Loss / Redundancy

While individuals need to worry about data loss and redundancy as much as entities and governments, their safekeeping and backup efforts might look different. In the case of an entity, it's important to identify physical spaces that can hold backups, support customized access controls, and be resilient against physical and environmental attacks. Each entity will need to decide on these physical locations and take care to choose backup sites that are of the highest level of security and reliability.

Additionally, entities may decide to set up their wallet in a way that factors in the risk of key loss or theft. In the case of a single key wallet, if any backup location is compromised, the wallet is compromised. A multisig wallet may allow different keys to be stored in different manners, so there is still control of the wallet even if a single key is compromised. It's important to note in this case that one still needs to be able to identify when key compromise has occurred, otherwise an attacker will simply hold the compromised key(s) for as long as possible until they gain access to the required m-of-n quorum.

Entities should also consider a backup strategy that minimizes the risk of data loss. Certain devices can become degraded over time, so it's important to have a number of backups and to potentially diversify how they are stored.

Cold vs. Hot Wallets

For most entities and governments, there is no need to hold any substantial funds in a hot wallet. Hot wallets are mainly used for on-chain transactions, and many businesses that are frequently transacting on-chain (such as exchanges) need to maintain hot wallets. But even in those cases, exchanges will maintain the minimum balances possible in the hot wallet since they are particularly vulnerable due to their connection to the internet.

Entities and governments can likely design a custody solution purely around cold storage, as they don't have the need to frequently send funds out of the wallet. They can always accumulate new holdings into that same wallet, and do so with privacy by using Hierarchical Deterministic wallets. Furthermore, a cold storage setup might be just what an entity needs to hold bitcoin for the long-term rather than trading it around based on the whims of the market.

Third-Party Custody

An entity may choose to hold bitcoin with a third-party custodian. Depending on the circumstances, it might be easiest and safest to allow a third party to hold private keys for a period of time. However, this relinquishes control to the third party and negates many of the benefits of holding bitcoin. Most entities that have the resources and appropriate permissions to self-custody bitcoin should choose to hold their own keys. Not your keys, not your coins.

One exception is to potentially use a third party to hold a subset of keys that would not constitute a controlling quorum. This third party could be used as a backup, holding keys that are held outside of the security setup that's used for the primary keys. In this case, it is still critical to vet any third parties appropriately and ensure that they have the system safeguards in place to custody private keys. It's also vital to have the right controls in place to prevent social engineering and other coordination attacks, especially if this third party is allowed to act as a co-signer.

Resources

Additional resources for corporations and governments looking to hold and custody bitcoin.

- Glacier Protocol
- Fireblocks MPC

Smart Contracts

What are Bitcoin Smart Contracts?

Smart contracts are pieces of code that enable automatic execution of logic on a blockchain, without the need for any third party or intermediary. Bitcoin smart contracts are written in its native language, Script , which provides for encoding more complex payment conditions in a trustless manner.

A bitcoin multisignature address is a basic smart contract example. It encodes logic that requires at least m valid signatures out of n total signatures in order for the bitcoin to be spent. This logic is slightly more complex than a simple bitcoin transaction from one address to another – though that is also done via smart contract – but it can be encoded in a permissionless, automated manner through Script.

There's no other place in the financial services industry where one can execute financial transfers using algorithmic logic in a permissionless manner. The banking system has APIs, but they are permissioned and often in walled gardens. Bitcoin was the first monetary innovation to enable a fully open-access API for payments and transfers.

HTLCs / Lightning Network

A Hashed Timelock Contract (HTLC) is a type of smart contract that has a time parameter. This time parameter can be used to create spending conditions that are only valid if they are met within a specified timeframe. For example, one could have an HTLC that returns assets back to the sender at a specified time if no further instructions were sent from that sender.

HTLCs can be used to set up bilateral payment channels, which form the basis of the Lightning Network. These payment channels – Lightning Channels – are smart contracts that sit on top of bitcoin and allow for faster and less expensive transactions. To open a payment channel, bitcoin is locked into the HTLC. Instructions can then be sent that allow payments to move back and forth between the bilateral users. These transactions take place off-chain, and they are recorded on the blockchain once they are finalized. The locking mechanism in the HTLC that allows for transaction guarantees. If one party were to violate their payment commitment, the other party can provide a proof that this commitment was violated and the bitcoin that is locked in the payment channel is sent to the party that delivered the proof.

Bitcoin Privacy: How to Use Bitcoin Privately

Background: Bitcoin Privacy

Bitcoin is a public ledger where every transaction, including its inputs and outputs, is recorded and published for anyone around the world to see and monitor. With crude analytics, anyone monitoring the bitcoin blockchain can begin to piece together the network of transactions and associated addresses. Ultimately, they can trace most bitcoin transactions across addresses.

Many exchanges and services require Know-Your-Customer (KYC) Personal Identifying Information (PII). With this information combined with transaction monitoring, it is becoming increasingly trivial to understand who exactly is behind certain bitcoin transactions. Even without that information, analytics can be run on a pseudonymous basis and still glean insights and hints as to who controls a given address.

Attaining full privacy on bitcoin is impossible at this point, and the privacy surface will only continue to shrink as financial institutions (e.g., ETF issuers) control more of the bitcoin supply and activity. However, there are still best practices and steps that can be taken to protect bitcoin privacy.

Bitcoin Privacy Tips

Don’t Reuse Addresses

Bitcoin addresses on the public blockchain act as accounts, where anyone can monitor and follow all flows into and out of a given address. As such, it’s considered best practice for privacy reasons to not reuse addresses – that way no related transaction history information is divulged. Using a Hierarchical Deterministic (HD) wallet, it’s trivial to generate a new address each time bitcoin needs to be received. As discussed in the wallet section, there’s no way to tie together two different child addresses that were generated from the same seed, so any sender to or recipient from one bitcoin address won’t know the transactions associated with other addresses.

Consider Masking Your IP Address

Anyone connected to the bitcoin network can monitor and log your IP address, associating it with addresses and transactions. For optimal privacy, you might consider hiding or masking your IP address. Many services can provide this, including Tor.) This makes it difficult for others to monitor the traffic that originates from your IP and provides a layer of protection when transacting in bitcoin.

Limit Use of Third Party KYC’d Services

Another way to reduce exposure is to limit the use of third party services that KYC your account. Most people will need to use these services – such as spot exchanges – at some point. However, these third parties collect identifying information that allow them, and anyone who requests from them (such as a government agency), to associate bitcoin addresses with specific identities. They also are privy to all off-chain activity. So the more the KYC’d service providers are used, the more they can construct a full profile of your on- and off-chain funds’ movements and activities.

Avoid Using Public Block Explorers

Public block explorers can associate your activity with your IP address. If you look up certain addresses, such as ones that you are sending to or receiving from, those will be associated with your IP. Avoiding public block explorers and~~/or~~ masking your IP address are ways to avoid this exposure.

Self-Custody & Run Your Own Node

Ultimately, the best privacy protection is to hold your own keys in custody and to run your own full node. While these won't fully protect your privacy – the base layer is public and all activity on the base layer is public – taking these steps will prevent divulging more information than is necessary. These security measures will enhance the privacy of your transactions by making it more difficult for parties to track your activity.

Bitcoin Protocol Privacy Upgrades

There have been various upgrades over the course of the years designed to increase bitcoin's privacy. As with steps that can be taken to protect one's privacy, these upgrades can't fix bitcoin's privacy, but they can greatly improve it.

Taproot

The Taproot fork consisted of several upgrades for bitcoin privacy. First was the adoption of Schnorr signatures, which consolidate multiple signatures into one and make it impossible to distinguish between single-signature and multi-signature transactions.

Second, the upgrade included Merkle Abstract Syntax Trees (MAST). MAST reveal only the parts of a transaction that are necessary for the transaction to be valid. For example, if multisig criteria were unnecessary or unsatisfied, that criteria will no longer be revealed as part of a given transaction. Previously, the

transaction would expose sensitive data, even if it were not directly relevant to the transaction's validity.

Lightning Network

Lightning Network is a layer that is one layer removed from the base bitcoin blockchain. Any two people can open a bilateral payment channel by locking up their bitcoin on the base layer. Bitcoin's security is maintained during these off-chain transfers between the two people, as the payment channel was locked when they opened it. Lightning Network increases the privacy of transactions that take place on Lightning, but the opening and closing of channels still takes place on the bitcoin blockchain and is subject to its transparency and traceability.

Atomic Swaps

What are Atomic Swaps?

In computer science, an "atomic" action is one that happens all at once. This same notion applies to atomic swaps.

Atomic swaps are a feature of decentralized, peer-to-peer protocols that allow users to directly exchange crypto assets with each other without requiring a third-party exchange or intermediary. Atomic swaps use smart contracts that encode logic to simultaneously transfer both assets, avoiding counterparty risk that results from doing the transfers one at a time.

Process for Trading via Atomic Swap

Atomic swaps can be used to exchange any two crypto assets that bear similar cryptographic properties. For example, one can use an atomic swap to swap Bitcoin into Monero. This can be achieved through various background mechanisms, one of which is explained here.

In an atomic swap that uses Hash Timelock Contracts (HTLCs), one party sends crypto to the smart contract on-chain address. That crypto remains locked in that address on its blockchain until the second party sends crypto; this locking is done via smart contract. The second party agrees to the transaction and sends crypto to the address on the other chain. Once this is done, both parties can redeem their respective cryptocurrency on the respective blockchain. This final step is instantaneous – there is no delay between when the first and second party settle, making this an atomic transaction.

The HTLCs underlying these contracts means that there is a timelock; the transaction must be confirmed by both sides within a certain amount of time. If that's not the case, the transaction is voided and any locked cryptocurrency is returned to the original owner.

Atomic swaps can also be done via multi-signature addresses with timelocks. Participants use Schnorr signatures to sign partial signatures that enable sending from the multisig address; the mechanics may differ slightly from the HTLCs, but the resulting atomic swap is the same.

Atomic Swaps Advantages

Because atomic swaps can be traded in a decentralized manner without the need for a centralized exchange, they can be done with much greater privacy protections. There is no need to provide KYC documents to a centralized entity, and the information related to the transaction is limited to the amounts and addresses that are on the public ledger. Atomic swaps don't provide full privacy guarantees due to the limitations of bitcoin privacy, but they are more private than traditional trading on a centralized exchange.

Additionally, atomic swaps can often be faster and cheaper than trading on a centralized exchange. There is no onboarding process, no need to go through exchange deposit/withdrawal processes, and fewer fees.

Key Bitcoin Events

Halvings

As mentioned earlier, the bitcoin block reward is cut in half every 210,000 blocks, or approximately every four years. These events are significant events for bitcoin because they drastically increase its stock-to-flow ratio, since less flow is produced each year, and they change the economics for miners, since there is bitcoin to be earned from the block reward. The halving events also potentially change the economics for consumers and users of the bitcoin blockchain who may need to pay higher transaction fees in order to pay the miners.

There have been four halvings of the block reward since bitcoin was launched in 2009:

1. November 28, 2012: from 50 BTC to 25 BTC
2. July 9, 2016: from 25 BTC to 12.5 BTC
3. May 11, 2020: from 12.5 BTC to 6.25 BTC
4. April 19, 2024: from 6.25 BTC to 3.125 BTC

The next halving is anticipated to take place in 2028.

Proof of Keys

Proof of Keys is a day held on the anniversary of the mining of the Genesis Block. Every January 3, Bitcoin users participate in an exercise to take their private keys off exchanges and hold them in their own self-custody with their own full node running.

The purpose of this day is to commemorate the idea of “Not your keys, not your coins”. Bitcoin’s value as a seizure-resistant, censorship-resistant tool for monetary sovereignty only applies when you are the owner and holder of your own private keys. Holding bitcoin in others’ custody is no better than the traditional financial system where banks can operate on fractional reserve and lend out your assets. Even worse, in the case of bitcoin, centralized custodians are exposed to the risk of theft and loss. If you don’t hold your keys, you don’t know that you actually own the bitcoin.

There are reasons to use centralized custodians, such as exchanges, but Proof of Keys day forces individuals to flex their monetary sovereignty muscles. Centralized counterparties must also prove that they have the bitcoin they claim to hold.

Historical Timeline of Events

Bitcoin Whitepaper

On August 18, 2008, the domain name bitcoin.org was registered. A few months later, on October 31, 2008, a link to a paper authored by a pseudonym of “Satoshi Nakamoto” was posted to a cryptography mailing list. The paper was titled “Bitcoin: A Peer-to-Peer Cash Electronic System.”

In just nine pages, including references, Satoshi outlined what would become the most important monetary innovation of the 21st century.

First Block Mined

The first bitcoin block was mined on January 3, 2009. This block is referred to as the ‘Genesis Block’. It was mined by Satoshi and the block reward was 50 BTC.

The block contained as output text that said:

> *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"*

This quote referred to a headline in the British newspaper *The Times*, referring to the banking crisis of 2008. Satoshi's bitcoin whitepaper offered an alternative to the fractional-reserve banking system that led to the financial crisis. In addition, it shifted power and control back to the end user and away from the financial intermediaries that had previously been relied upon to hold customer funds. This innovation is forever memorialized in the text in the Genesis Block.

First Exchange Rate

The first exchange rate for Bitcoin was established relative to USD by New Liberty Standard on October 5, 2009. The rate was 1,309 BTC per USD, or $0.0007639 per BTC.

First On-Chain Transaction

The first person to ever receive and use bitcoin was Hal Finney. Finney downloaded the bitcoin software the day it was released, and received 10,000 bitcoin from Satoshi Nakamoto on January 9, 2009 in block 170. All blocks prior to block 170 consisted solely of the mining reward transactions, but this transaction to Finney was the first in which bitcoin was actually sent from one user to another. A link to the transaction is below:

f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16

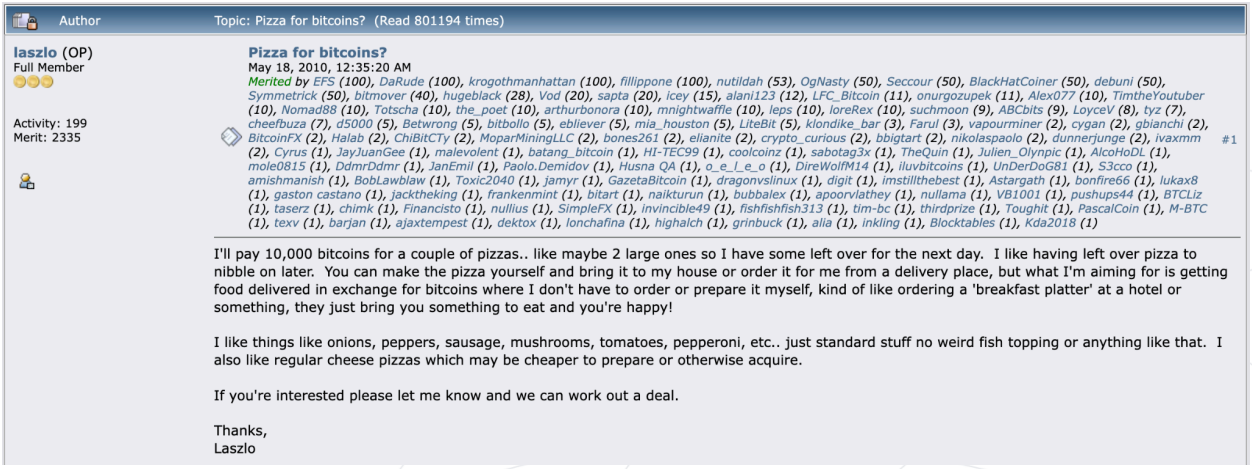
First Application

One of the first bitcoin applications was a Bitcoin Faucet developed by Gavin Andresen. The Bitcoin Faucet was a website launched in June 2010 that distributed bitcoin to visitors in an effort for bitcoin to grow and gain traction. The website gave away 5 bitcoins to users who simply had to solve a captcha and enter their bitcoin address. All in, the Bitcoin Faucet gave away 10,000 bitcoin – worth hundreds of millions of USD today.

First Retail Transaction

On May 18, 2010, Lazlo Hanyecz, one of the first bitcoin developers, posted on a forum that he would pay someone 10,000 bitcoin to buy him two pizzas. At the time, 10,000 bitcoin was worth around $40. A few days later, Jeremy Sturdivant, a bitcoin user, accepted Lazlo's offer and ordered two Papa John's pizzas delivered to his home.

In celebration of the first notable bitcoin retail transaction, May 22 became known as "Bitcoin Pizza Day."



Author | Topic: Pizza for bitcoins? (Read 801194 times)

laszlo (OP)
Full Member

Activity: 199
Merit: 2335

Pizza for bitcoins?
May 18, 2010, 12:35:20 AM
Merited by EFS (100), DaRude (100), krogothmanhattan (100), fillippone (100), nutildah (53), OgNasty (50), Seccour (50), BlackHatCoiner (50), debuni (50), Symmetrick (50), bitmover (40), hugeblack (28), Vod (20), sapta (20), icey (15), alani123 (12), LFC_Bitcoin (11), onurgozupek (11), Alex077 (10), TimtheYoutuber (10), Nomad88 (10), Totscha (10), the_poet (10), arthurbonora (10), mnightwaffle (10), leps (10), loreRex (10), suchmoon (9), ABCbits (9), LoyceV (8), tyz (7), cheefbuza (7), d5000 (5), Betwrong (5), bitbollo (5), ebliever (5), mia_houston (5), LiteBit (5), klondike_bar (3), Farul (3), vapourminer (2), cygan (2), gbianchi (2), BitcoinFX (2), Halab (2), ChiBitCTy (2), MoparMiningLLC (2), bones261 (2), elianite (2), crypto_curious (2), bbigtart (2), nikolaspaolo (2), dunnerjunge (2), ivaxmm (2), Cyrus (1), JayJuanGee (1), malevolent (1), batang_bitcoin (1), HI-TEC99 (1), coolcoinz (1), sabotag3x (1), TheQuin (1), Julien_Olynpic (1), AlcoHoDL (1), mole0815 (1), DdmrDdmr (1), JanEmil (1), Paolo.Demidov (1), Husna QA (1), o_e_l_e_o (1), DireWolfM14 (1), iluvbitcoins (1), UnDerDoG81 (1), S3cco (1), amishmanish (1), BobLawblaw (1), Toxic2040 (1), jamyr (1), GazetaBitcoin (1), dragonvslinux (1), digit (1), imstillthebest (1), Astargath (1), bonfire66 (1), lukax8 (1), gaston castano (1), jacktheking (1), frankenmint (1), bitart (1), naikturun (1), bubbalex (1), apoorvlathey (1), nullama (1), VB1001 (1), pushups44 (1), BTCLiz (1), taserz (1), chimk (1), Financisto (1), nullius (1), SimpleFX (1), invincible49 (1), fishfishfish313 (1), tim-bc (1), thirdprize (1), Toughit (1), PascalCoin (1), M-BTC (1), texv (1), barjan (1), ajaxtempest (1), dektox (1), lonchafina (1), highalch (1), grinbuck (1), alia (1), inkling (1), Blocktables (1), Kda2018 (1)

#1

I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy!

I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire.

If you're interested please let me know and we can work out a deal.

Thanks,
Laszlo

A link to the pizza transaction is below:

a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d

Satoshi's Disappearance

Satoshi's last message on the bitcoin forum was December 12, 2010, when he posted an updated software version. Satoshi went on to remove his name from Bitcoin's copyright statement and from the bitcoin.org website.

Author | Topic: Added some DoS limits, removed safe mode (0.3.19) (Read 25173 times)

satoshi (OP)
Founder
Sr. Member

Activity: 364
Merit: 6930

Added some DoS limits, removed safe mode (0.3.19)
December 12, 2010, 06:22:33 PM
Merited by EFS (100), fillippone (55), OgNasty (50), bumbacoin (50), cloverme (50), krogothmanhattan (47), sukamasoto (30), yahoo62278 (25), notaek (25), mindrust (20), Welsh (20), ABCbits (11), dragonvslinux (11), legendster (10), harrymmmm (10), aTriz (7), Betwrong (5), Mrpumperitis (5), Lauda (5), MicroGuy (5), TMAN (5), Steeley (5), minorman (5), FrueGreads (4), Danslip (3), finist4x (3), Ryu_Ar1 (3), BrianCryptoo (3), Yaunfitda (2), Bthd (2), casperBGD (2), Anon136 (2), cinnamon_carter (2), edgycorner (2), Syke (1), LFC_Bitcoin (1), ralle14 (1), hatshepsut93 (1), Searing (1), HI-TEC99 (1), bitcoinPsycho (1), DdmrDdmr (1), goldkingcoiner (1), famososMuertos (1), crypto_trader#43xzEXrP (1), bill gator (1), DaCryptoRaccoon (1), denzkillim (1), lx001 (1), akirasendo17 (1), Bardman (1), Woshib (1), ImHash (1), Scorpion (1), Rooster101 (1), domoy77 (1), dark08 (1), lesom (1), ryap12 (1), mx12.levins (1), CoolWave (1), glerant (1), 1Dq (1), nikolaspaolo (1), TheArchaeologist (1), ritaconscience (1), murrayrothbard (1), akopjpuge (1), sigri44 (1), OWZ1337 (1), livecoins (1), zantezu (1), Tech1k (1), EKAloji (1), Bohfin Legasof (1) #1

There's more work to do on DoS, but I'm doing a quick build of what I have so far in case it's needed, before venturing into more complex ideas. The build for this is version 0.3.19.

- Added some DoS controls
As Gavin and I have said clearly before, the software is not at all resistant to DoS attack. This is one improvement, but there are still more ways to attack than I can count.

I'm leaving the -limitfreerelay part as a switch for now and it's there if you need it.

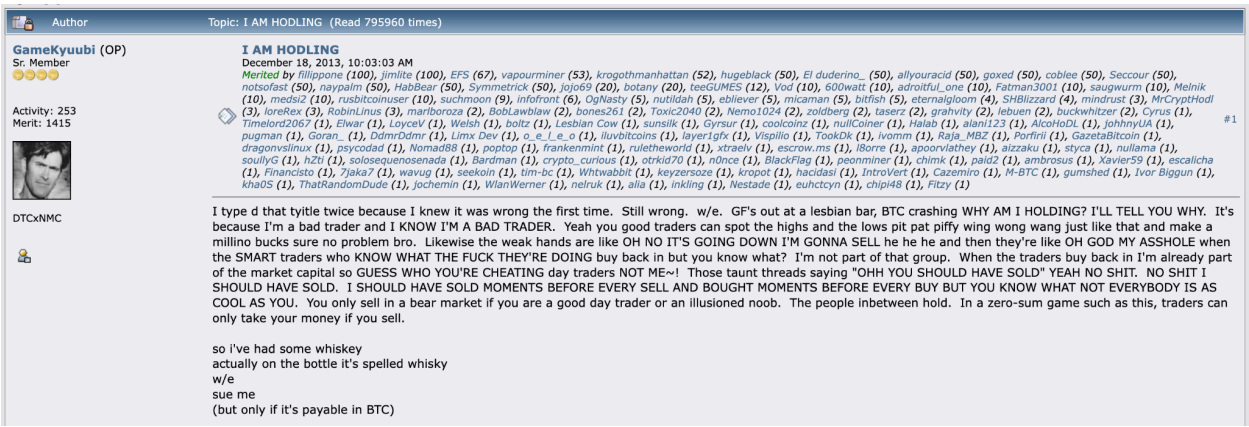
- Removed "safe mode" alerts
"safe mode" alerts was a temporary measure after the 0.3.9 overflow bug. We can say all we want that users can just run with "-disablesafemode", but it's better just not to have it for the sake of appearances. It was never intended as a long term feature. Safe mode can still be triggered by seeing a longer (greater total PoW) invalid block chain.

Builds:
http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.3.19/

There are some addresses that are known to be associated with Satoshi, such as the one that received the block reward for the Genesis Block. Nobody knows exactly how much bitcoin Satoshi has, but estimates range from 600,000 to 1.1 million – none of which has ever been touched or moved.

I AM HODLING

On December 18, 2013, amidst a bitcoin sell-off from recent all-time-highs of just above $1,000, user GameKyuubi posted on the Bitcointalk forum a post titled "I AM HODLING", which was a post about holding bitcoin and not selling it even during trying times.



Author | Topic: I AM HODLING (Read 795960 times)

GameKyuubi (OP)
Sr. Member

Activity: 253
Merit: 1415

DTCxNMC

I AM HODLING
December 18, 2013, 10:03:03 AM

Merited by filippone (100), jimlite (100), EFS (67), vapourminer (53), krogothmanhattan (52), hugeblack (50), El duderino_ (50), allyouracid (50), goxed (50), coblee (50), Seccour (50), notsofast (50), naypalm (50), HabBear (50), Symmetrick (50), jojo69 (20), botany (20), teeGUMES (12), Vod (10), 600watt (10), adroitful_one (10), Fatman3001 (10), saugwurm (10), Melnik (10), medsi2 (10), rusbitcoinuser (10), suchmoon (9), infofront (6), DgNasty (5), nutildah (5), ebliever (5), micaman (5), bitfish (5), eternalgloom (4), SHBlizzard (4), mindrust (3), MrCryptHodl (3), loreRex (3), RobinLinus (3), marlboroza (2), BobLawblaw (2), bones261 (2), Toxic2040 (2), Nemo1024 (2), zoldberg (2), taserz (2), grahvity (2), lebuen (2), buckwhitzer (2), Cyrus (1), Timelord2067 (1), Elwar (1), LoyceV (1), Welsh (1), boltz (1), Lesbian Cow (1), sunsilk (1), Gyrsur (1), coolcoinz (1), nullCoiner (1), Halab (1), alani123 (1), AlcoHoDL (1), johnnyUA (1), pugman (1), Goran_ (1), DdmrDdmr (1), Limx Dev (1), o_e_l_e_o (1), iluvbitcoins (1), layer1gfx (1), Vispilio (1), TookDk (1), ivomm (1), Raja_MBZ (1), Porfirii (1), GazetaBitcoin (1), dragonvslinux (1), psycodad (1), Nomad88 (1), poptop (1), frankenmint (1), ruletheworld (1), xtraelv (1), escrow.ms (1), l8orre (1), apoorvlathey (1), aizzaku (1), styca (1), nullama (1), soullyG (1), hZti (1), solosequenosenada (1), Bardman (1), crypto_curious (1), otrkid70 (1), n0nce (1), BlackFlag (1), peonminer (1), chimk (1), paid2 (1), ambrosus (1), Xavier59 (1), escalicha (1), Financisto (1), 7jaka7 (1), wavug (1), seekoin (1), tim-bc (1), Whtwabbit (1), keyzersoze (1), kropot (1), hacidasi (1), IntroVert (1), Cazemiro (1), M-BTC (1), gumshed (1), Ivor Biggun (1), khaOS (1), ThatRandomDude (1), jochemin (1), WlanWerner (1), nelruk (1), alla (1), inkling (1), Nestade (1), euhctcyn (1), chipi48 (1), Fitzy (1)

#1

I type d that tyitle twice because I knew it was wrong the first time. Still wrong. w/e. GF's out at a lesbian bar, BTC crashing WHY AM I HOLDING? I'LL TELL YOU WHY. It's because I'm a bad trader and I KNOW I'M A BAD TRADER. Yeah you good traders can spot the highs and the lows pit pat piffy wing wong wang just like that and make a millino bucks sure no problem bro. Likewise the weak hands are like OH NO IT'S GOING DOWN I'M GONNA SELL he he he and then they're like OH GOD MY ASSHOLE when the SMART traders who KNOW WHAT THE FUCK THEY'RE DOING buy back in but you know what? I'm not part of that group. When the traders buy back in I'm already part of the market capital so GUESS WHO YOU'RE CHEATING day traders NOT ME~! Those taunt threads saying "OHH YOU SHOULD HAVE SOLD" YEAH NO SHIT. NO SHIT I SHOULD HAVE SOLD. I SHOULD HAVE SOLD MOMENTS BEFORE EVERY SELL AND BOUGHT MOMENTS BEFORE EVERY BUY BUT YOU KNOW WHAT NOT EVERYBODY IS AS COOL AS YOU. You only sell in a bear market if you are a good day trader or an illusioned noob. The people inbetween hold. In a zero-sum game such as this, traders can only take your money if you sell.

so i've had some whiskey
actually on the bottle it's spelled whisky
w/e
sue me
(but only if it's payable in BTC)

This typo led to a meme within the bitcoin space and HODLing came to mean holding bitcoin no matter what. HODLers were people who were not going to sell amidst negative sentiment, fear, uncertainty, doubt, or even euphoria. To this day, HODLers are an important part of the bitcoin ecosystem.

Financial Milestones

Price Milestones

- **2009**: First block mined; first BTC/USD exchange rate: 1,309.03 bitcoins per USD
- **2011**: Bitcoin hits high of $30 and low of $2
- **2012**: First halving
- **2013**: Bitcoin reaches $1,000
- **2014**: Bitcoin falls to $100
- **2016**: Second halving
- **2017**: Bitcoin breaks $5,000 for the first time and later hits $20,000
- **2018**: Bitcoin drops to $6,000
- **2020**: Bitcoin crashes to $3,000; Third Halving
- **2021**: Bitcoin rises to all-time high of over $66,000
- **2022**: Bitcoin falls to $15,000
- **2024**: Bitcoin reaches all-time high of $100,000

Financialization Milestones

Throughout the years, various bitcoin financial products have been launched as bitcoin's seventh network effect – the adoption of bitcoin as the world reserve currency – has grown. These products have been regulatory and market milestones that open up bitcoin to a new set of investors, providing additional tools for a wide range of participants in the bitcoin ecosystem.

First U.S. Bitcoin Futures

The first U.S. Bitcoin Futures were launched December 18, 2017. They were listed and cleared by the Chicago Mercantile Exchange (CME), the predominant exchange for trading of currencies and commodities such as interest rates, gold, oil, and agricultural products.

The futures contracts were cash-settled and required USD collateral, setting the stage for institutional adoption and offering a bitcoin derivative that was within the confines of the U.S. regulatory and financial infrastructure.

The debate continues on whether the introduction of derivatives with no connection to the physical underlying asset has ultimately benefited the price, or whether they introduce more paper bitcoin into the ecosystem. Regardless, the CME futures launch was a pivotal moment for institutional and regulatory adoption in the U.S., and the product has remained dominant since its launch.

First Bitcoin Futures ETF

Once the U.S. had a viable, regulated futures market, it paved the way for a futures ETF. A futures ETF is a securities instrument that holds a rolling basket of bitcoin futures in order to simulate long bitcoin exposure, meaning to hold the bitcoin in anticipation of its value increasing. The instrument is a tradable security, making it easy for an average investor to have long bitcoin exposure in their traditional brokerage account in the same way they trade stocks.

The first bitcoin futures ETF was launched in October 2021, almost four years after the futures launch. These products had drawbacks due to the cost of rolling, particularly when bitcoin futures were trading with a steep term structure. They also were a degree away from actual bitcoin exposure, meaning that the end-user could not gain many of the benefits of holding bitcoin. But, they were still a critical milestone in the adoption of securitized products for bitcoin.

First Bitcoin Spot ETF

Bitcoin futures and the bitcoin futures ETF both paved the way for the ultimate investment vehicle, the bitcoin spot ETF . Bitcoin spot ETFs are tradeable securities that own outright bitcoin, allowing investors an easy way to get access directly to bitcoin. Bitcoin spot ETFs are suitable for retail and institutions alike. These ETFs are especially attractive to institutions that cannot directly hold bitcoin themselves due to regulatory or practical reasons.

The bitcoin spot ETFs faced a long trial through the SEC, but they were eventually approved by the SEC on January 10, 2024. Within the first 10 months, the ETFs saw inflows of more than $20B, largely contributing to bitcoin's price rise over that year. The ETFs will continue to play a big part in the financialization of bitcoin and the flow of fiat into the bitcoin ecosystem.

Summary

In summary, bitcoin is one of the greatest innovations in monetary sovereignty. It provides people with a scarce, transferable, fungible, divisible form of money – it can be transferred anywhere, anytime as long as there is a connection to the internet. No one party controls bitcoin but anyone can use it.

Get started with bitcoin today and flex your monetary sovereignty!

Glossary

51% Attack: vulnerability in the blockchain where an individual or a group gains control over >50% of the computational power, allowing them to manipulate the blockchain (transactions, fees, etc.). Also known as a majority attack.

Air-gapped: a system that is not connected to any public or external network (e.g., internet, connected devices); often used for high-security situations where data protection is vital.

Application Programming Interface (API): a set of rules that allows for communication between different software applications, allowing for data exchange and function utilization.

Application-Specific Integrated Circuits (ASICs): specialized computer chips designed to perform one specific task extremely efficiently; they are built for maximum performance, speed, and power efficiency in a single application.

Atomic Swaps: peer-to-peer trade of one type of cryptocurrency for a different type of cryptocurrency. It is an all-or-nothing trade, or indivisible.

Bitcoin Confirmation: the process of verifying a transaction within the Bitcoin network to ensure the transaction is valid and has been properly included in the blockchain.

Bitcoin Faucet: platform, usually a website or app, that gives away small amounts of Bitcoin in exchange for simple tasks.

Bitcoin Spot ETF: an ETF that is traded at Bitcoin's current price.

Bilateral Swap Risk: potential financial risks in a one-on-one swap agreement, particularly when one party defaults on the agreement terms.

Block Header: a small piece of data that contains key information about the block of transactions. A block header does not store the transaction data itself but serves as a summary of the block, as well as storing information used for security, validation, and linking blocks together.

Blockchain Fork: a split in the blockchain history. This can be caused by a change to the protocol.

Cantillon Effect: an economic concept that explains how newly-created money affects people unequally, depending on where it enters the economy. This has happened whenever a government prints more money without having any collateral (e.g., gold) to back the additional currency, and as a result the wealthy see the benefits the earliest.

Cold Wallet: a cryptocurrency wallet that is not connected to the internet or other network; provides higher level of security; ideal for long-term currency storage.

Convertible Debt: a loan that can be converted into stock (e.g., equity in a company).

Custodial Wallets: a wallet that holds someone's private keys; a custodian of the private keys.

Desktop Wallets: a wallet that is on a computer that never has and never will be connected to the internet. The software is loaded onto the computer via USB or other device that allows the computer to stay disconnected from the internet.

Elliptic Curve Cryptography (ECC): mathematics of elliptical curves used to keep cryptocurrency like Bitcoin – secure.

Elliptic Curved Digital Signature Algorithm (ECDSA): a secure and digital signature based on ECC.

Exchange-Traded Fund (ETF): a bundle of assets (e.g., stocks, commodities, etc.) that can be traded and purchased by investors on a stock exchange.

Fiat Currency: money that has value based on government backing, versus being backed by a physical asset like gold or silver.

Fork: a point in time when a blockchain's history splits, creating two or more new versions of the currency.

Fractional Reserve Banking: banks reserve a portion of their customer deposits, allowing them to loan out the rest.

Futures: contract agreements to buy or sell assets at a set price on a date in the future.

Futures ETF: a company or exchange that makes and holds a futures contract.

Genesis Block: first block in a block chain; typically referred to as Block 0 or Block 1.

Gresham's Law: an economic principle stating that "bad money drives out good money." When there are two forms of currency in circulation that have different values, they are perceived as bad. Bitcoin is perceived as "good" money in this context due to its digital and decentralized nature.

Hard Forks: a permanent change to a blockchain that results in two separate blockchains, each one then following a different set of rules. The old and new chains are unable to communicate or validate the blocks on the other chain.

Hardware Wallets: an offline device to store private keys; resembles a USB drive.

Hashed Timelock Contracts: a specific type of smart contract; if the user provides the secret keys (hash) before the time deadline (timelock), then the transaction can be completed.

Hierarchical Deterministic Wallet: a cryptocurrency wallet that organizes, backs up, and provides a way to use crypto wallets across multiple accounts or devices. It allows an individual to manage multiple addresses securely with one seed phrase or password.

HODLers: people who buy and hold Bitcoin for long periods of time; a misspelling of "holders"

Hot Wallet: a cryptocurrency wallet that is connected to the internet or other network.

Impossible Trinity: an economics concept that says a government cannot have all three of these simultaneously: free capital movement (money flowing in/out easily), fixed exchange rate (currency tied to something like gold), or independent monetary policy (control over interest rates and money supply). One of these three must be sacrificed as a trade-off to have two concepts.

Jevons Paradox: When technology makes things or a process more efficient, it drives the cost down. This results in increased demand and an overall growth of total usage.

Lightning Network: allows individuals to process transactions instantaneously and privately off-chain without paying high fees, and then settling them on the blockchain.

Litecoin: digital currency that has faster transaction times and lower fees, making it "lighter" than other digital currencies.

MAST (Merkle Abstract Syntax Trees): smart contracts, or scripts, that only reveal the relevant script when a transaction happens, keeping the remainder of the script hidden. This became possible during Bitcoin's Taproot soft fork.

Mempool: short for memory pool; it acts as a holding space for unconfirmed transactions before they're added to a block.

Mining Pools: a group of cryptocurrency miners who combine their computing power to increase the chances of successfully mining a block. They split the rewards based on how much each miner contributed.

Mnemonic Seed Recovery: the process of restoring access to a cryptocurrency wallet or secure system using a mnemonic seed phrase, which is a series of words generated when you first create your wallet.

Mobile Wallets: app on smartphone or smartwatch that stores private keys and allows you to use the device for crypto transactions.

Monetary Premium: the added value something has from being used as money, as it's treated as a store of wealth.

Monetary Sovereignty: a country's or monetary institution's ability to control and issue its currency, set interest rates, and manage monetary policy without relying on foreign currencies. This offers economic independence.

Monero: privacy-focused cryptocurrency, which enables users to send and receive transactions completely anonymously.

Multi-Party Computation (MPC): a group of people or miners (machines) that perform a secure task without either side knowing or having access to the other's private keys.

Network Effects: when a good or service becomes more valuable as more people use it.

Non-custodial Wallets: a digital wallet that you have full control over, including management of private keys.

Nonce: short for "number used once"; a number that miners adjust in order to find a valid hash for a new block of transactions.

Over-the-Counter (OTC): buying or selling assets directly between two parties, instead of going through a formal exchange, for large trades and to maintain privacy.

Perpetual Futures: a type of futures contract that has no expiration date.

Plaintext: data or text in its original, unencrypted form. It can be read and understood by anyone who has access to it.

Prime Brokerage: company that offers and bundles services in one place, such as trade handling, loans, custody, and risk management.

Proof of Work: a system where computers (miners) solve complex math problems to prove they've done computational "work."

Publicly-Traded Miners: companies or entities that offer customers to hold a share of the cryptocurrency and trade it, similarly to traditional stocks.

Scarcity: Bitcoin was designed to have a finite number of coins available – 21 million bitcoins. With a currency scarce in demand, it increases its value.

Schelling Point: a solution that people will naturally gravitate toward without needing to discuss anything, as it is obvious or natural. In terms of cryptocurrency, bitcoin is the Schelling Point.

Schnorr signatures: cryptographic signature algorithm that provides greater security, decreased signature sizes, and increased efficient verification; critical part of the Taproot fork and large improvement from ECDSA.

Script: a coding language that defines the rules on how cryptocurrency can be spent.

Seed Phrase: list of 12-24 words that serves as the password, or backup, to the full crypto wallet; it can regenerate all private keys, addresses, and funds.

Segwit: short for Segregated Witness; this separates the signature data ("witness") from the rest of the transaction, leading to smaller and faster transactions and lower fees.

Shamir's Secret Sharing: a cryptographic method used to split a secret (e.g., key or password) into multiple parts called shares, which are distributed among a group of participants. The secret can only be reconstructed if a minimum number of shares, or the threshold, are combined. *The threshold is often smaller than the total number of shares, ensuring that only the specified number of participants can rebuild the secret.*

Smart Contracts: code that runs on the blockchain to automatically carrying out actions when specific conditions are met.

Soft Forks: allows rules of the blockchain to update without breaking communication with previous nodes. It provides a smoother update than the hard fork.

Spot Exchange: buying and selling an asset at its present market value; an immediate transaction and settlement.

Stock-to-Flow (S2F): Stock = total supply available. Flow = amount added each year. In terms of bitcoin, the Stock is 21 million coins – this is the finite number that are available; the Flow is how many bitcoins are newly mined. To calculate the stock-to-flow ratio (S2F), divide the stock by the flow. As the S2F ratio increases, the commodity (bitcoin) becomes more valuable.

Taproot Fork: an optional Bitcoin network update that was added in November 2021, providing improved efficiency, privacy, and flexibility.

Time Preference: how someone values something – now or in the future. A higher time preference means someone wants to buy something now or earlier. A person has a lower time preference if they are willing to wait to buy something, as the value may increase. A good example of this: Would you rather have one donut today (high time preference), or two donuts tomorrow (low time preference)?

Transaction ID (TXID): a unique identifier for a bitcoin transaction.

Troubled Asset Relief Program: government program implemented in 2008 to stabilize the financial system following the housing crash.

Unit Bias: viewing a single unit of something as the "normal" or "right" amount, leading us to consume or buy that unit, even if it's more than we need.

Unspent Transaction Output (UTXO): the unspent part of a previous transaction that can be used in a new transaction.

Veblen Good: a type of product that increases in demand as its price increases, as consumers value the status associated with these products. This is seen in luxury items such as luxury cars, luxury watches, and designer clothing.

Wallets: digital program, device, or tool that gives the user the ability to store and manage their private keys.

Winner-Takes-All Markets: a type of market where the largest share is held by the leading competitor.