# Introduction to Bitcoin

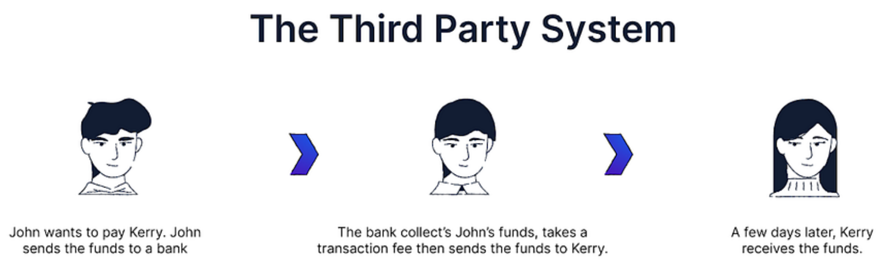
## Introduction

On October 28th 2008, the world was forever changed. And like other world-changing events, this event was not necessarily an action taken, but more an idea made known to the world. This idea was for an inflation-resistant, double-spend proof, fully trustless and digital form of currency. The theory of this currency, laid out in the “Bitcoin Whitepaper” opened people’s perceptions of currency to a reality where they could transfer money transparently and anonymously.

After gaining a first mover advantage and achieving a substantial network effect, bitcoin has become the most valuable crypto-asset in existence. Bitcoin also possesses the most decentralized and robust network out of any digital currency.

## What is Bitcoin?

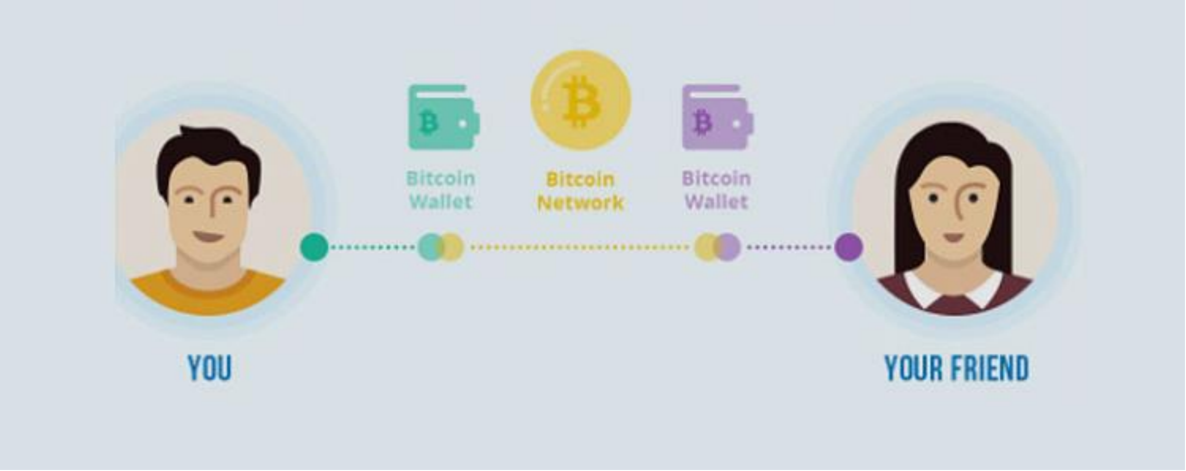
Bitcoin is digital money that can be used to make secure peer-to-peer transactions on the internet without the need for a third-party intermediary (like a bank) to facilitate transactions. It was created by an open-source community in part due to banks’ detrimental actions during the Great Financial Crisis of 2008, which involved governments printing money and bailing out the financial institutions responsible for the crash.


The Third Party System
John wants to pay Kerry. John sends the funds to a bank
The bank collect’s John’s funds, takes a transaction fee then sends the funds to Kerry.
A few days later, Kerry receives the funds.

At its core, Bitcoin allows the user to "be their own bank" eliminating the need to get permission from a company to complete a transaction. On the bitcoin network there are no restrictions on who a user can send money to and how much money can be sent, and operations run around the clock not just during business hours. Beyond enabling users to "be their own bank" bitcoin also "banks the unbanked", as financial services cost money to set up and maintain.

Bitcoin itself can be used as a store of value or medium of exchange that only exists in the digital domain. One cannot hold or see bitcoin. The Bitcoin network and the bitcoins that power the network were created to be used on the internet, it is not owned by anyone or company — it is a true open payment network that anyone with an internet connection can access.

***"Bitcoin is a peer-to-peer version of electronic cash that allows payments to be sent directly from one party to another without going through a financial institution. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work." – Satoshi Nakamoto***



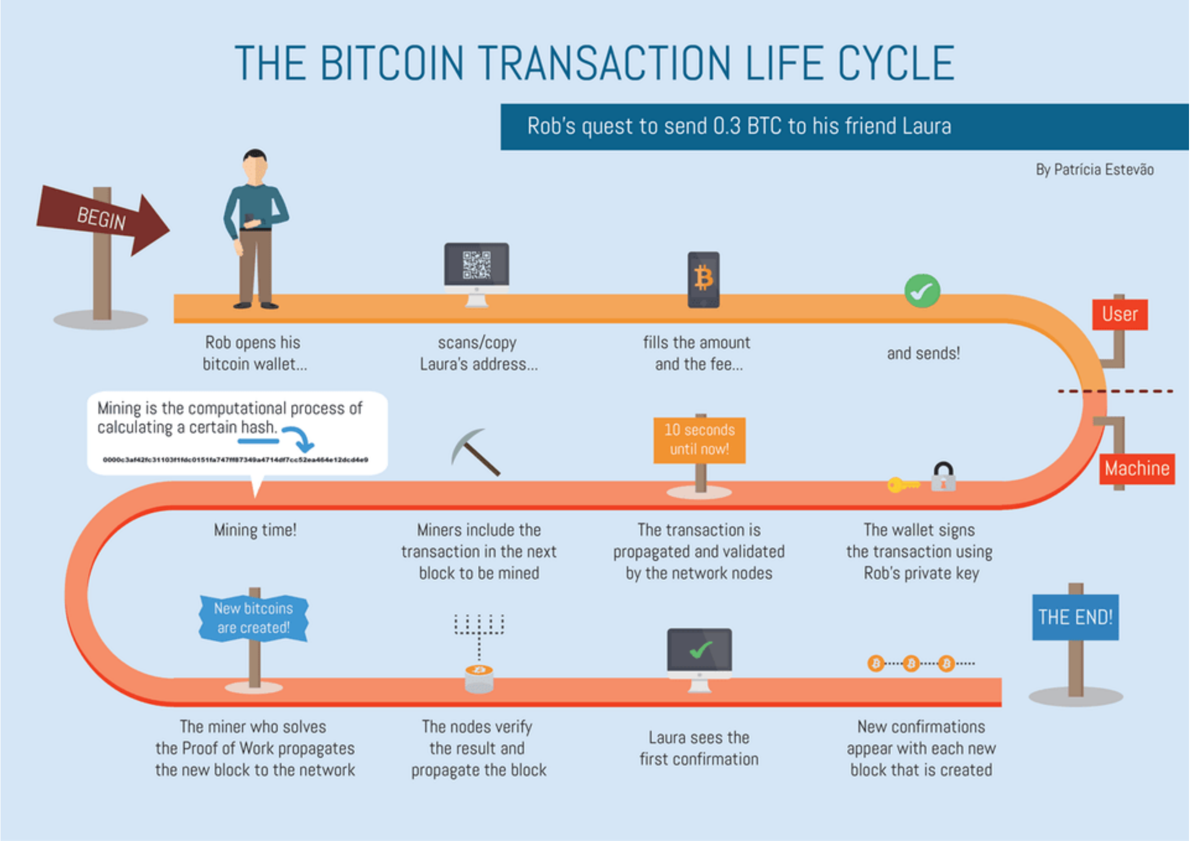
*Bitcoin Transfer Illustration Source: CryptoNinjas*

**What one can do with bitcoin?**

- **Use it like money**. Accepted by many companies including Starbucks and Virgin Galactic, Bitcoin can be used to make purchases.
- **Transfer funds more quickly and cheaply**. Funds can be transferred more efficiently (peer to peer) without high processing fees by the removal of a third party intermediary like a bank or payment processor.
- **Use it as a store of value**. A store of value should be worth the same or more over time. Bitcoin is often referred to as 'digital gold' — it's limited in supply with specific use-cases. Amidst its volatility — bitcoin has appreciated immensely since conception.

**How does it work?**

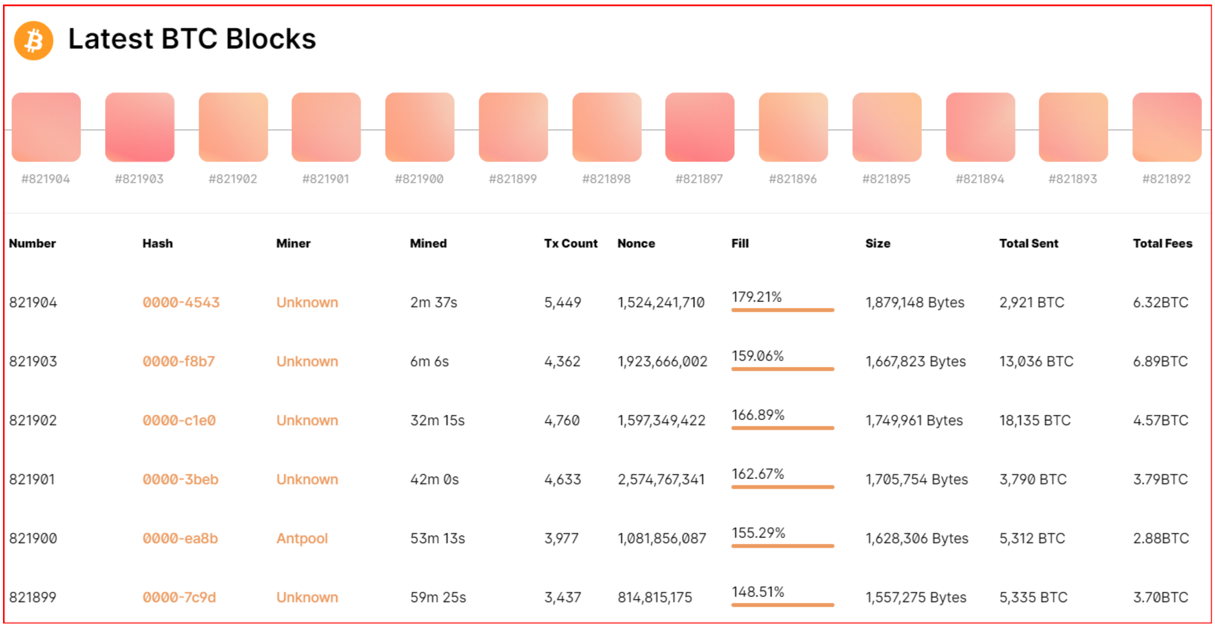
The Bitcoin blockchain can be accessed and managed by any computer, anywhere in the world. The computers that run on the bitcoin blockchain are embedded with a set of rules which makes the data (bitcoins) scarce and valuable. As a rule, only 21 million bitcoins can be produced, and this scarcity limit ultimately gives bitcoin its value.


THE BITCOIN TRANSACTION LIFE CYCLE
Rob's quest to send 0.3 BTC to his friend Laura
By Patrícia Estevão
BEGIN
Rob opens his bitcoin wallet...
scans/copy Laura's address...
fills the amount and the fee...
and sends!
User
Machine
Mining is the computational process of calculating a certain hash.
10 seconds until now!
Mining time!
Miners include the transaction in the next block to be mined
The transaction is propagated and validated by the network nodes
The wallet signs the transaction using Rob's private key
New bitcoins are created!
THE END!
The miner who solves the Proof of Work propagates the new block to the network
The nodes verify the result and propagate the block
Laura sees the first confirmation
New confirmations appear with each new block that is created

Here is a simple breakdown of what happens when someone wants to send bitcoin using blockchain technology.

1. When someone joins the bitcoin network they are given a public key, which one can think of like an email address and a private key which one can think of like a password.
2. Every bitcoin transaction made, along with the sender's public key, is recorded in a public list called the blockchain.
3. The main mechanism by which bitcoin transactions are confirmed and validated is called "mining"
4. The public full list is then distributed to every computer that is connected to the Bitcoin network.
5. As this public list is in chronological order of transactions, it's possible to trace the history of all bitcoin activity that's ever occurred. The bitcoin ledger is resistant to both tampering and censorship.

This "open" nature prevents and discourages people or "bad actors" from spending coins that aren't theirs, making copies of coins or even reversing transactions.One can check all transactions on the Bitcoin network on the Blockchain.com Explorer.



Latest BTC Blocks

| Number | Hash | Miner | Mined | Tx Count | Nonce | Fill | Size | Total Sent | Total Fees |
|---|---|---|---|---|---|---|---|---|---|
| 821904 | 0000-4543 | Unknown | 2m 37s | 5,449 | 1,524,241,710 | 179.21% | 1,879,148 Bytes | 2,921 BTC | 6.32BTC |
| 821903 | 0000-f8b7 | Unknown | 6m 6s | 4,362 | 1,923,666,002 | 159.06% | 1,667,823 Bytes | 13,036 BTC | 6.89BTC |
| 821902 | 0000-c1e0 | Unknown | 32m 15s | 4,760 | 1,597,349,422 | 166.89% | 1,749,961 Bytes | 18,135 BTC | 4.57BTC |
| 821901 | 0000-3beb | Unknown | 42m 0s | 4,633 | 2,574,767,341 | 162.67% | 1,705,754 Bytes | 3,790 BTC | 3.79BTC |
| 821900 | 0000-ea8b | Antpool | 53m 13s | 3,977 | 1,081,856,087 | 155.29% | 1,628,306 Bytes | 5,312 BTC | 2.88BTC |
| 821899 | 0000-7c9d | Unknown | 59m 25s | 3,437 | 814,815,175 | 148.51% | 1,557,275 Bytes | 5,335 BTC | 3.70BTC |

*Bitcoin Blockchain Illustration Source: Blockchain.com*

### Bitcoin, bitcoin, or BTC?

- Bitcoin (B): Bitcoin with an uppercase B is referring to the Bitcoin network and protocol. This is the system that the bitcoin currency runs on.
- Bitcoin (b): The lowercase spelling of bitcoin refers only to the cryptocurrency, not the payment network or blockchain protocol.
- **BTC**: BTC is the abbreviated version of bitcoin, and again refers to the cryptocurrency. The use of BTC is similar to a stock ticker symbol and is what one will usually see on price charts.

### Characteristics of Bitcoin

- Bitcoin is a fairly new technology. There are some of the characteristics of bitcoin, which makes it different from the traditional currency:
- **Decentralization:** The first and most crucial characteristic of bitcoin is its decentralization. There is no central power in bitcoin as there are in traditional currencies, which are issued and managed by a central authority, which can be the country's government or any other organization. Bitcoin decentralization provides many advantages over traditional currency like no vulnerability to seizure, tax, thievery, etc.
- **Transparency:** It is well known to us that how much bitcoin does a person owns can't be known, but at the same time, it is visible to everyone on the ledger board that how much transaction has been made by which user and who is/ are the receiver/receivers of the bitcoins. So, its transaction is crystal clear to everyone in the ecosystem of bitcoin. And from this mentioned history on the ledger board, on a proper analysis, the asset owned by any person can be easily known if one wants to. But many things can be done to prevent this too.
- **Opaqueness:** Now, we do not need to tell repeatedly that the user of bitcoin remains anonymous, and there is no chance of tracking back to the user. No requirement of any

legal paper helps in the identification of the person. And this is also the reason that no government can even know who is behind a particular account. At the same time, when someone make an account in the bank or make transactions through the bank, they will demand address, phone number, legal papers, and on transactions, they will have a good history of date, time, amount, receiver and every other single detail.

- **Fast:** As compared to other banks or any other method of transaction, bitcoin is faster. Sending money from one side of the world to another side of the world is a matter of just a few minutes if sent in the form of bitcoin. Simultaneously, if the same amount is sent through any other bank or method, it will take approximately a week or more.
- **Non-repudiable:** What comes under this characteristic is if bitcoin is transacted once, there is no getting back unless the receiver is willing to do so. It means there is no going back; the receiver can't claim that he never received any bitcoin.
- **Digital Currency:** Bitcoins are not physically present in the form of notes or coins, unlike traditional money. And in this way, it is easy to carry in the phone. It is tough to be stolen by thieves in the market or from the house.
- **Simple to set up:** Generally, banks take long documentation and procedures for in opening an account and managing it, including dealer records, credit checks, even they need many legal papers for identification of the user, but at the same time, one can make an address in bitcoin in a few seconds, without any need of any legal documents, one need to set a strong password and must not forget that password because once that password is gone. There is no getting it back.
- **Value is determined by demand:** There is no fixed value or price of bitcoin. For its value and price, it entirely depends on its demand. The members of the ecosystem of bitcoin determine the cost and value of bitcoin in the market.
- **Commission of own choice:** Whether someone want to give some transaction fee or not is entirely according to their choice. The only difference is that if one pays transaction fees, they will be provided with some additional facility whose absence won't harm non-fees paying users in any way. It is entirely voluntary.

Other than these characteristics, some other characteristics are similar to money, which makes bitcoin function as money. Such characteristics are durability, portability, divisibility, fungibility, Scarcity, acceptability.

- **Durability:** Bitcoin cannot be destroyed. So long as the blockchain is maintained on even a single computer, Bitcoin exists. Since its inception, the network's uptime has been a remarkable 99.99%, and it has gone more than 3,200 days without an outage. For a point of comparison, the Federal Reserve's money transfer system went offline for several hours in February 2021.
- **Portability:** Bitcoin can be sent anywhere there's an internet connection in seconds with probabilistic final settlement within an hour. A bitcoin user who has memorized their private key literally carries their bitcoin with them wherever they go.
- **Divisibility:** A single bitcoin consists of 100 million smaller units known as satoshis.
- **Fungibility:** Bitcoins are all the same. No coin is any more valuable than the next one. Unlike with gold or paper currency, counterfeiting is impossible.
- **Scarcity:** Bitcoin is the first provably scarce object. There will only ever be 21 million bitcoins. Anyone can check the protocol's code to confirm this limit. A vast majority of

nodes, the enforcers of Bitcoin's rules, would have to act against their own economic self-interest for the limit to be altered.

- **Acceptability:** While estimates for the number of bitcoin holders vary, some peg adoption as high as over 100 million active users. This number grows each day as knowledge of the protocol spreads and bitcoin becomes easier to buy, spend, and store.

**Who created Bitcoin & its history?**

Satoshi Nakamoto, the mysterious creator of Bitcoin (BTC), synthesized existing ideas and technologies, successfully putting the pieces of the puzzle together to solve the Byzantine Generals problem sometime around 2007.

**Bitcoin History**

An interactive timeline of events from the past that shaped Bitcoin, and current events and technologies paving the way to the future of Web3, and beyond.

**November 1, 1976: Diffi-Hellman Day**

Whitfeld Diffie and Martin E. Hellman release their proposal for a cryptographic protocol used for secure communication over an insecure channel. Their paper, titled "New Directions in Cryptography," provided a revolutionary method for secure key exchange without relying on a pre-shared secret. Most notably, it presented an implementation of public and private key pairs for secure communication over public channels. The Diffie-Hellman key exchange would become a foundational component of modern cryptography and serve to raise awareness for the importance of secure communication in the digital age. It would also serve as the foundation for the eventual implementation of public and private key pairs in crypto transactions.

**1989: DigiCash is founded**

David Chaum, a cryptographer, founded DigiCash and subsequently created one of the first electronic money corporations. It was one of the first attempts to create a completely anonymous, secure digital payment system. DigiCash was based on Blind Signature Technology, an invention of Chaum's that built upon technological developments for public and private keys. The idea of "binding" involved encrypting a message so that the recipient could not see the contents, but they could still confirm that the message came from the sender. This technique would effectively allow for secure and private transactions without needing a trusted third party (in other words, it would be trustless by nature). Initially, DigiCash was used for small-scale transactions, such as payments between individuals and purchases from online vendors. Unfortunately, it failed to gain widespread adoption due to a number of factors, including the lack of a clear business model and the emergence of other digital payment systems, such as PayPal.

**August 18, 2008: Registration of Bitcoin.Org Domain Name**

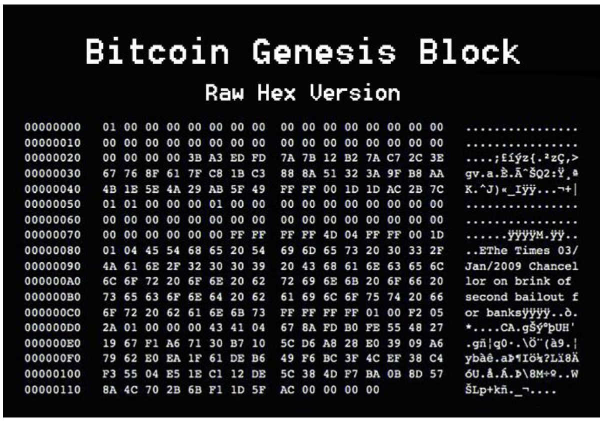
The domain name "bitcoin.org" was registered by an unknown individual using a privacy protection service to hide their identity. The identity of the individual is still unknown, but many believe it to be Satoshi Nakamoto, the pseudonymous creator(s) of Bitcoin. The domain is currently maintained by an open-source community of developers and volunteers who work on the Bitcoin Core software and related projects. The website serves as a central hub for information about Bitcoin, including guides for beginners, technical documentation, and news and updates about the Bitcoin ecosystem. It also includes information to introduce people to the Bitcoin economy, including a launchpad for them to buy Bitcoin, and resources on how to run Bitcoin nodes.

### October 31, 2008: Bitcoin Whitepaper Released

The Bitcoin whitepaper is released by an unknown individual or group of individuals going by the pseudonym “Satoshi Nakamoto.” The whitepaper, titled “Bitcoin: A Peer-to-Peer Electronic Cash System” was also published on the Cryptography Mailing List. The whitepaper described a decentralized digital currency system that would allow for peer-to-peer transactions without needing a trusted third party, like a bank. It proposed the use of a blockchain, a public ledger that would record all transactions in a secure and transparent manner. The Bitcoin network would rely on a network of computers to validate transactions and maintain the integrity of the blockchain. The whitepaper also described the use of proof-of-work (PoW), a mechanism used to deter fraudulent activity by requiring users to solve complex mathematical problems in order to add new blocks to the blockchain. This mechanism was meant to incentivize users to participate in the network by rewarding them with newly minted bitcoins.

### January 3, 2009: The Genesis Block: Bitcoin’s Birthday

The anonymous creator of Bitcoin, known as Satoshi Nakamoto, mines the first block of the Bitcoin blockchain. This genesis block is referred to as Block 0 or the Block 1. Bitcoin’s genesis block contains a message in the coinbase parameter, which is the input of the first transaction in the block. The message reads: “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.” This message is believed to be a reference to a headline from The Times newspaper on the same day the block was mined, reporting on the UK government’s plan to bail out failing banks. The message is significant because it highlights one of the key motivations behind the creation of Bitcoin: the creation of an alternative to traditional financial institutions and their centralized control over the economy. The genesis block also contains the first 50 bitcoins ever mined. Their creation and the genesis block represent the beginning of a new era in decentralized, peer-to-peer transactions.



Bitcoin Genesis Block

Raw Hex Version

```
00000000   01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of 
000000B0   73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00            ŠLp+kñ._¬....
```

### January 12, 2009: First BTC Genesis Transaction

The first ever Bitcoin transaction between two people occurs just days after the launch of the Bitcoin network. Satoshi Nakamoto sends 10 bitcoins to Hal Finney’s Bitcoin address, a sign of Finney’s early involvement in the Bitcoin project. The transaction is notable for a number of reasons. Firstly, it demonstrates the early adoption of Bitcoin by a small group of enthusiasts who were involved in the development of the cryptocurrency. Secondly, it highlights the use of Bitcoin as a means of exchange, even in its early stages when the value of the cryptocurrency was extremely low. It also highlights Finney's relationship with Nakamoto that continued throughout the early development of Bitcoin. Finney was an early contributor to the project, and was one of the first people to promote Bitcoin and share his experiences using the cryptocurrency with the broader public.

### February 2009: First Bitcoin Wallet

The first Bitcoin wallet was the result of a years-long collective effort by a mysterious individual or group of individuals operating under the pseudonym Satoshi Nakamoto. Nakamoto's whitepaper, published in late 2008, laid out the conceptual framework for Bitcoin and blockchain — a decentralized, immutable ledger and cryptocurrency's foundation. While the first Bitcoin wallet was rudimentary by today's standards, it later lead to the widespread adoption of blockchain technology. Known as Bitcoin-Qt, the Bitcoin wallet made Nakamoto's vision come to life. Its user-friendly interface that allowed early Bitcoin adopters to create and manage their digital wallets to send and receive Bitcoin. Bitcoin-Qt also held cryptographic keys — public keys for receiving funds and private keys for authorizing transactions, and gave users an address book and enabled them to digitally sign transactions. In the years that have followed, Bitcoin wallets have evolved significantly to include various types, such as software wallets, hardware wallets, and paper wallets, catering to different security preferences. Many Bitcoin wallets (particularly extension wallets) also allow users to connect to decentralized applications (dApps) in the wider cryptocurrency and Web3 space.

### May 22, 2010: Bitcoin Pizza Day Transaction Takes Place

The first known commercial transaction takes place using Bitcoin when Laszlo Hanyecz paid 10,000 bitcoins for two large Papa John's pizzas, which were delivered to him in Jacksonville, Florida. At the time of the transaction, the value of the 10,000 bitcoins was only a few dollars. However, the transaction has become infamous as an example of just how much the cryptocurrency has appreciated in value. Today, Bitcoin Pizza Day is celebrated by Bitcoin enthusiasts around the world as a reminder of the early days of Bitcoin and the community's roots in experimentation, innovation, and risk-taking. In many ways, Bitcoin Pizza Day represents the beginning of the mainstream adoption of Bitcoin and the broader cryptocurrency ecosystem.

### July 18, 2010: Mt. Gox Founded

On July 18, 2010, Mt. Gox was founded by programmer Jed McCaleb. Initially, it got its unlikely start as a platform for trading virtual cards in the game Magic: The Gathering, then evolved into a pioneer Bitcoin exchange. Its history was marred by chaos, hacks, and scandals, ultimately culminating in its downfall and the ongoing legal proceedings involving its ex-owner, Mark Karpelès. Mt. Gox, originally mtgox.com, was a platform that exchanged fiat currency for Bitcoin. It was one of the first Bitcoin exchanges, signaling the growing interest in cryptocurrencies as a form of digital value. McCaleb's involvement in Mt. Gox as a Bitcoin exchange was relatively short-lived. Within a year of its inception, he sold the platform to Mark Karpelès, a French-born developer. Under Karpelès' leadership, Mt. Gox would experience both remarkable success and catastrophic failures.

### November 1, 2010: Current Bitcoin Logo Released

Satoshi Nakamoto, the anonymous creator of Bitcoin, initially offered two earlier versions of the Bitcoin logo – the first at Bitcoin's inception, and then an updated version the next year. However, the infamous Bitcoin logo that we have come to associate with the cryptocurrency was created by an unknown artist using the handle "Bitboy." The new logo effectively took Satoshi's earlier creations and improved upon them to create a distinct look for the Bitcoin blockchain. "Bitboy" rendered a white and slanted "B" on top of a bright orange background in a design.

### March 17, 2010: First-Ever Recorded Price of Bitcoin

March 17, 2010 was the first-ever recorded price of bitcoin at a value of $0.003 on the now-defunct bitcoinmarket.com. This event's implications – while seemingly minor at the time – would contribute to the gradual emergence of bitcoin as a recognized and valued asset. In the years that followed, Bitcoin's price experienced considerable volatility and fluctuation. As it rose, it garnered attention from the growing community of early adopters, technologists, and investors. Bitcoin's price was characterized by sharp increases and dramatic declines, a pattern that continues to this day.

### February 2011: Silk Road Marketplace Goes Live

The Silk Road online black market launches and begins its two-year run. Before being shut down by federal authorities in 2013, it would also become significant to the Bitcoin community as it was one of the first real-world applications of Bitcoin as a medium of exchange. Prior to the Silk Road, Bitcoin was primarily used as a speculative investment and peer-to-peer money exchange. However, Silk Road allowed users to buy and sell goods and services anonymously as an alternative to traditional financial systems. It is important to note that due to its association with illicit activities, the Silk Road did, unfortunately, contribute heavily to a narrative that linked Bitcoin with criminal activity. However, the widespread adoption of Bitcoin and other cryptocurrencies over the years – as well as education about crypto and blockchain – has reversed much of that narrative as more people become familiar with Bitcoin and the digital asset world.

### June 2011: First Bitcoin Bubble

The Bitcoin Bubble of 2011 becomes a major event in the history of Bitcoin. While Bitcoin was created in 2008, it wasn't until 2011 that its price really began to skyrocket. Leading up to June 2011, Bitcoin had been trading at less than a dollar per coin earlier in the year. But by June 2011, it had risen to over $31 per coin. This rapid rise in value was fueled by a number of factors, including increased media coverage, growing interest among investors, and the fact that Bitcoin was still a relatively unknown, untested technology that garnered the interest of many. Shortly after hitting its peak, Bitcoin quickly fell down to just a few dollars per coin. A large-scale hacking incident involving the Mt. Gox exchange saw 25,000 bitcoins stolen, which garnered its fair share of media attention and negative sentiment towards Bitcoin, as a result. By November 2011, the price of Bitcoin had fallen to $2. Bitcoin was able to recover in the months ahead, however, though the First Bitcoin Bubble was among the first examples of market volatility.

### June 13, 2011: First Individual Bitcoin Hack Occurs

In June 2011, the world was just beginning to comprehend the transformative potential of Bitcoin, a digital currency that had evolved from a tight-knit community of hobbyists into something more significant. This newfound attention also brought forth the dark side of the cryptocurrency world, as it witnessed its first major hack. This event, known as the first Bitcoin hack, saw a user named allinvain lose a staggering $500,000 worth of bitcoins to malicious hackers, impacting the perception of Bitcoin at the time. In the early days of Bitcoin, the community was relatively small, and mining the cryptocurrency was largely a hobbyist's pursuit. Unlike the sophisticated mining operations of today, one could generate thousands of bitcoins using a conventional home PC. This was precisely what allinvain claimed to have done, accumulating a substantial fortune of 25,000 bitcoins. At the time, the value of bitcoins had risen significantly, reaching around $20 per coin in June 2011, which meant that allinvain's holdings were worth approximately $500,000. The hack that targeted allinvain demonstrated the urgent need for enhanced security practices within the Bitcoin community.

### June 20, 2011: Mt. Gox Hacked

On June 20, 2011, the cryptocurrency world faced a significant milestone when Mt. Gox, the world's largest Bitcoin exchange at the time, experienced its first major hack, when hackers targeted the exchange, exploiting a vulnerability to make the price of Bitcoin on the platform plummet from $17 to mere cents in a matter of minutes. This sharp price crash was exclusive to Mt. Gox and did not affect the underlying Bitcoin protocol. The hack resulted in the disappearance of approximately $8.75 million worth of bitcoins at the time. Despite the severity of the breach, reports indicate that Mark Karpeles and the Mt. Gox team were strangely nonchalant about the situation. However, they ultimately took steps to address the crisis and rectify the damage. This incident marked the beginning of a series of security-related challenges that would continue to plague the exchange. Over the following years, Mt. Gox faced a string of breaches, hacks, lawsuits, and scandals. While it initially maintained its reputation as an honest player in the Bitcoin community, the exchange's challenges began to mount. A leaked Mt. Gox document revealed that hackers had been siphoning off bitcoins from the exchange for years, leading to the disappearance of over 850,000 bitcoins, valued at over $460 million at the time.

### April 18, 2011: Namecoin Mines its Genesis Block

The first altcoin, Namecoin, mines its first genesis block. It is a cryptocurrency and decentralized domain name system (DNS) that was created in 2011 as a fork of the Bitcoin protocol, boasting some similarities to Bitcoin (including the use of a proof-of-work mechanism). It is designed to provide a decentralized, censorship-resistant system for registering and managing domain names, as well as for storing and transferring arbitrary data. In the Namecoin system, domain names are registered as transactions on the Namecoin blockchain. This allows for a decentralized system where no central authority has control over domain names, and censorship or domain seizure is much more difficult. While Namecoin still has not gained widespread adoption, it does offer a unique approach to managing online identities and information.

### November 28, 2012: First BTC Halving Event

The first Bitcoin halving event occurs and sets the stage for subsequent halving events. Bitcoin halving events occur every four years or so and cut the reward for Bitcoin miners in half, reducing the rate of new Bitcoin issuance. During this first halving, the block reward was reduced from 50 bitcoins to 25 bitcoins. The purpose of halving events is to ensure that the total number of Bitcoins in circulation does not exceed 21 million, the maximum supply set by the Bitcoin protocol.

**May 2, 2013: First Bitcoin ATM**

The first Bitcoin ATM is installed in Vancouver, Canada. Since this event in October 2013, Bitcoin ATMs have become more common, with thousands of machines installed worldwide. Bitcoin ATMs allow users to conduct Bitcoin-related transactions – most notably between Bitcoin and cash – making it easier for people to enter and exit the Bitcoin market. They are normally automated machines connected to the Internet that allow users to buy or sell Bitcoin using cash, their debit card, or a cryptocurrency wallet.

**March 28, 2013: Bitcoin Market Capitalization Exceeds $1 Billion for the First Time**

The market cap of the entire Bitcoin network surpasses $1 billion for the first time.

**July 3, 2013: First Utility Coin ICO**

The Mastercoin Initial Coin Offering (ICO) stands as a pioneering event took place in July 2013 when the crypto landscape was still in its infancy. Mastercoin, later rebranded as Omni, aimed to push the boundaries of the Bitcoin blockchain by introducing innovative features that laid the groundwork for many subsequent blockchain projects. At its core, the Mastercoin ICO was a groundbreaking fundraising mechanism. It was one of the earliest instances of a project raising capital by issuing tokens on top of an existing blockchain, in this case, Bitcoin. Participants in the ICO sent Bitcoin to a designated address and, in return, received newly created Mastercoin tokens (MSC). This approach showcased the potential of token sales as a means to fund blockchain development, setting a precedent for the countless ICOs that would follow in its wake. Mastercoin's vision was ambitious. It sought to enhance the functionality of the Bitcoin network, enabling the creation of a diverse array of digital assets, smart contracts, and decentralized exchange capabilities. This vision laid the foundation for future projects, contributing to the evolution of decentralized finance (DeFi) and the broader blockchain ecosystem.

**December 18, 2013: HODL Day**

HODL Day is born after a user on the bitcointalk.org forums made a post titled “I AM HODLING” to explain why, despite falling prices, they still intended to hold onto their Bitcoin. This misspelling of “hold” has since become a popular term that refers to the act of holding onto cryptocurrencies rather than selling them in response to short-term price fluctuations. On HODL Day, people in the cryptocurrency community frequently express their commitment to holding onto their digital assets and encourage others to do the same in a way to show support for the crypto space and their belief in its long-term potential.

**February 25, 2014: Mt. Gox Files for Bankruptcy Protection**

Mt. Gox – a Bitcoin exchange based in Tokyo, Japan, that was one of the largest crypto exchanges in the world – files for bankruptcy. The exchange claims that it lost 850,000 bitcoins – worth approximately $450 million at the time, due to a hacking attack.The bankruptcy filing was the result of the company's inability to recover the lost assets and repay its creditors. The process lasted for several years, during which creditors tried to recover their lost assets.

### October 12, 2015: Liquid Launches

On October 12, 2015, the cryptocurrency landscape witnessed a significant development with the launch of Liquid. Liquid, often referred to as a Bitcoin sidechain and layer, introduced a novel approach to enhancing the functionality and versatility of Bitcoin, addressing some of the limitations inherent in the Bitcoin blockchain. Liquid was designed to operate as a separate blockchain, running in parallel to the Bitcoin network. It was developed by Blockstream, a blockchain technology company, and aimed to provide faster and more confidential transactions compared to the main Bitcoin blockchain. One of its primary objectives was to allow for the efficient transfer of assets, such as Bitcoin and other digital tokens, between exchanges and financial institutions. One of the key innovations of Liquid was its use of the concept of "federated pegs." These federated pegs allowed for the movement of assets between the Bitcoin blockchain and the Liquid sidechain in a way that maintained a level of decentralization and security. This innovation enabled users to lock Bitcoin on the main chain and issue Liquid Bitcoins (L-BTC) on the Liquid sidechain, which could then be quickly and confidentially transferred to other users or platforms within the Liquid network.

### January 14, 2016: Official Release of the Lightning Network Whitepaper

Joseph Poon and Thaddeus Dryja publish the Lightning Network whitepaper to present a protocol for conducting off-chain transactions on top of the Bitcoin blockchain in a fast and scalable manner. The Lightning Network was intended to speed up transaction times and present a scaling solution to Bitcoin's L1. As such, it introduced the concept of off-chain transactions to ease congestion on the Bitcoin blockchain, as well as multisignature payment channels. The Lightning Network whitepaper presented a compelling case for the use of off-chain transactions to improve the scalability and speed of the Bitcoin network while maintaining the L1's high level of security and decentralization.

### May 10, 2017: First Lightning Payment on LTC

The first Lightning payment occurs when developer ACINQ successfully completes a test transaction on the Lightning Network. The transaction is for 0.0001 LTC (Litecoin) and is sent from Zurich, Switzerland to San Francisco, California. The successful completion of the Lightning payment was a significant milestone for the Lightning Network and marked the beginning of a new era for blockchain-based payments. Since then, the Lightning Network has also grown in popularity and usage, with many developers and businesses building on top of it to create more efficient and scalable payment systems.

### August 1, 2017: Bitcoin Cash Hard Fork

The Bitcoin Cash hard fork occurs as a result of a disagreement among the Bitcoin community over the future direction of the cryptocurrency. While many members of the Bitcoin community welcomed the soft fork that created Segregated Witness (SegWit), a group of miners and developers decided on a hard fork of Bitcoin that created a new cryptocurrency. This new cryptocurrency was called Bitcoin Cash (BCH), and was designed to offer faster transaction times fees than the original BTC. Since this date, Bitcoin Cash has undergone several additional forks and upgrades, with most of these upgrades happening primarily on May 15 or November

15 of any given year. While the network continues to evolve and grow, there is still much debate over the merits and drawbacks of Bitcoin Cash versus Bitcoin, making it a contentious point of discussion within the cryptocurrency community. The main difference between BTC and BCH is their block size limit. Bitcoin technically has a 1MB block size limit (4MB thanks to SegWit upgrade), while Bitcoin Cash has an 32MB block size limit. This larger block size allows for more transactions to be processed per block, which avoids congestion to lead to faster transaction times and lower fees.

**August 23, 2017: SegWit Activation Day**

SegWit is activated on August 24, 2017 at 1:57 UTC at block height 481,824, marking the launch of one of the most significant developments to the Bitcoin network aimed at addressing several long-standing issues, such as transaction malleability and scalability. For many in the Bitcoin ecosystem, SegWit's activation marked the end of the block size wars that divided the Bitcoin community, thereby cementing August 1 as Bitcoin Independence Day. Segregated Witness, often abbreviated as SegWit, was proposed as a solution to increase the capacity of the Bitcoin blockchain by separating transaction data from the digital signatures. This innovation aimed to reduce the size of transactions, allowing more of them to fit within a single block and thereby increasing the network's throughput. Additionally, SegWit brought on several security improvements, making Bitcoin transactions more resilient to certain types of attacks.

**January 1, 2018: RSK Launched Its Full-Featured Mainnet Network (IOVlabs)**

On January 1, 2018, the launch of IOVlabs brought Bitcoin and smart contracts closer to each other. IOVlabs was created to bring smart contract capabilities to the Bitcoin network through the Rootstock platform. Rootstock, often referred to as "Smart Bitcoin" or "RSK," is a Turing-complete smart contract platform that is merge-mined with Bitcoin. This means that Bitcoin miners can secure both networks simultaneously, enhancing security while enabling smart contract execution on Bitcoin's blockchain. IOVlabs served as the development and operational arm of Rootstock, driving its growth and adoption. IOVlabs' purpose was to enable smart contracts with Bitcoin, a feature previously unavailable on its blockchain. Smart contracts have numerous applications, including decentralized finance (DeFi), tokenization of assets, supply chain management, and more. By launching IOVlabs and Rootstock, the goal was to tap into the vast potential of smart contracts while leveraging Bitcoin's security and network effects. IOVlabs' launch was significant because it allowed Bitcoin to compete with other smart contract platforms like Ethereum

**May 2020: Bitcoin Halving Event 2020**

The third Bitcoin halving event occurs on (Block 630,000). Mining rewards were cut from 12.5 bitcoins to 6.25 bitcoins per block.

**January 2021: Stacks Bitcoin Layer Launched**

The Stacks Bitcoin layer launches to enable smart contracts, DeFi, NFTs, and other additional use cases for Bitcoin. The Stacks project was originally known as Blockstack and co-created by Trust Machines CEO Muneeb Ali and Ryan Shea. The layer features its own programming language, Clarity, and consensus mechanism known as Proof-of-Transfer (PoX). Together, they allow for the execution of smart contracts on the Bitcoin blockchain.

### February 19, 2021: Bitcoin Hits $1 Trillion Market Capitalization

The price of Bitcoin hits $54,000, effectively taking the cryptocurrency to a $1 trillion market cap 13 years after its inception.

### SEPTEMBER 7, 2021: Bitcoin Becomes Legal Tender in El Salvador

On September 7, 2021, El Salvador made history by becoming the first nation in the world to pass a groundbreaking Bitcoin law, officially recognizing the cryptocurrency as legal tender alongside the U.S. dollar. Spearheaded by President Nayib Bukele, this landmark decision promised to transform the country's financial landscape. In the wake of this development, signs have emerged that Bitcoin is gaining traction within the nation, with restaurants, shops, and even hotels now accepting Bitcoin payments. El Salvador's Bitcoin law notes that the use of the cryptocurrency is optional. Citizens are not compelled to use Bitcoin for transactions if they do not wish to. President Bukele emphasized that individuals receiving payments in Bitcoin can opt to automatically convert them into U.S. dollars, providing flexibility and choice. El Salvador's decision has sparked global interest in the intersection of cryptocurrencies and traditional finance. It has also raised questions about the potential consequences and benefits of such a move for other countries.

### October 19, 2021: First Bitcoin ETF, Bitcoin Strategy Fund (BITO) Begins Trading

The first Bitcoin exchange-traded fund (ETF) starts trading on the New York Stock Exchange (NYSE) eight years after the Winklevoss brothers filed an application. The ProShares Bitcoin Strategy ETF (BITO) tracked bitcoin prices through futures contracts that were traded on the Chicago Mercantile Exchange (CME) and inspired future institutional adoption of Bitcoin.

### November 14, 2021: Taproot Upgrade Largest Bitcoin Advance Since 2017

The Taproot upgrade activation is successfully achieved, marking the largest advancement to the Bitcoin core following 2017’s SegWit activation. It was designed to enhance the privacy, security, and flexibility of Bitcoin transactions by introducing several important features. The most notable of these features was the ability to combine multiple transaction scripts into one, enhancing privacy and efficiency for bitcoin transactions. Additionally, Shnorr signatures and smart contract functionality improvements were also introduced.

### January 21, 2023: Ordinals Protocol Launched

Developer Casey Rodarmor launches the Ordinals protocol on Bitcoin, ushering in a new wave of interest in Bitcoin. Rodarmor’s protocol effectively allowed unique numbers to be assigned to each satoshi – the smallest unit in a single bitcoin – which enabled anyone to track individual sats. However, it was the invention of inscriptions using Ordinals that really allowed the protocol to take off. Not only could Bitcoin users assign numbers to each sat, they could also create digital artifacts by ascribing content and data to each satoshi as well. What’s more, all of this content was inscribed directly to the Bitcoin blockchain as the process to inscribe content on to sats took the form of a Bitcoin transaction. In short, users could essentially create their own NFTs (though there are key differences between digital artifacts and NFTs) directly on the Bitcoin blockchain itself.

### Is Bitcoin safe?

The cryptography behind bitcoin is based on the SHA-256 algorithm designed by the US National Security Agency. Cracking this is, for all intents and purposes, impossible as there are more possible private keys that would have to be tested (2256) than there are atoms in the universe (estimated to be somewhere between 1078 to 1082). There have been several high-profile cases of bitcoin exchanges being hacked and funds being stolen, but these services invariably stored the digital currency on behalf of customers. What was hacked in these cases was the website and not the bitcoin network. In theory if an attacker could control more than half of all the bitcoin nodes in existence then they could create a consensus that they owned all bitcoin, and embed that into the blockchain. But as the number of nodes grows this becomes less practical.

Of course, the eventual arrival of practical quantum computing could break it all. Much cryptography relies on mathematical calculations that are extremely hard for current computers to do, but quantum computers work very differently and may be able to execute them in a fraction of a second.

So, Bitcoin does not come without risks, here are some one should be aware of:

- **Loss of crypto keys:** As with all crypto self-custody, if someone lose their keys, they can lose access to their crypto funds.
- **A "51% attack":** In theory, this could occur when a single miner or mining group takes majority control of the bitcoin blockchain and essentially "hacks" the network.
- **Actions are irreversible:** The user is ultimately responsible for what they do. When someone click send on a cryptocurrency transaction, it can't be undone.
- **Unclear regulation:** Although crypto and bitcoin are regulated in parts of the world such as the US, crypto assets could be subject to stricter regulations in the future.

**Disadvantages associated with Bitcoin**

Like any currency, there are disadvantages associated with using Bitcoin:

**Bitcoins Are Not Widely Accepted:** Bitcoins are still only accepted by a very small group of online merchants. This makes it unfeasible to completely rely on Bitcoins as a currency. There is also a possibility that governments might force merchants to not use Bitcoins to ensure that users' transactions can be tracked.

**Wallets Can Be Lost:** If a hard drive crashes, or a virus corrupts data , and the wallet file is corrupted, Bitcoins have essentially been "lost". There is nothing that can done to recover it. These coins will be forever orphaned in the system. This can bankrupt a wealthy Bitcoin investor within seconds with no way form of recovery. The coins the investor owned will also be permanently orphaned.

**Bitcoin Valuation Fluctuates:** The value of Bitcoins is constantly fluctuating according to demand. As of June 2nd 2011, one Bitcoins was valued at $9.9 on a popular bitcoin exchange site. It was valued to be less than $1 just 6 months ago. This constant fluctuation will cause Bitcoin accepting sites to continually change prices. It will also cause a lot of confusion if a refund for a product is being made. For example, if a t shirt was initially bought for 1.5 BTC, and returned a week later, should 1.5 BTC be returned, even though the valuation has gone up, or should the new amount (calculated according to current valuation) be sent? Which currency should BTC tied to when comparing valuation? These are still important questions that the Bitcoin community still has no consensus over.

**No Buyer Protection:** When goods are bought using Bitcoins, and the seller doesn't send the promised goods, nothing can be done to reverse the transaction. This problem can be solved using a third party escrow service like ClearCoin, but then, escrow services would assume the role of banks, which would cause Bitcoins to be similar to a more traditional currency.

**Risk of Unknown Technical Flaws:** The Bitcoin system could contain unexploited flaws. As this is a fairly new system, if Bitcoins were adopted widely, and a flaw was found, it could give tremendous wealth to the exploiter at the expense of destroying the Bitcoin economy.

**Built in Deflation:** Since the total number of bitcoins is capped at 21 million, it will cause deflation. Each bitcoin will be worth more and more as the total number of Bitcoins maxes out. This system is designed to reward early adopters. Since each bitcoin will be valued higher with each passing day, the question of when to spend becomes important. This might cause spending surges which will cause the Bitcoin economy to fluctuate very rapidly, and unpredictably.

**No Physical Form:** Since Bitcoins do not have a physical form, it cannot be used in physical stores. It would always have to be converted to other currencies. Cards with Bitcoin wallet information stored in them have been proposed, but there is no consensus on a particular system. Since there would be multiple competing systems, merchants would find it unfeasible to support all Bitcoin cards, and therefore users would be forced to convert Bitcoins anyway, unless a universal system is proposed and implemented.

**No Valuation Guarantee:** Since there is no central authority governing Bitcoins, no one can guarantee its minimum valuation. If a large group of merchants decide to "dump" Bitcoins and leave the system, its valuation will decrease greatly which will immensely hurt users who have a large amount of wealth invested in Bitcoins. The decentralized nature of bitcoin is both a curse and blessing.

### Uses of Bitcoin

Among the major companies that accept Bitcoin as of 2023 include Tesla, PayPal, Microsoft, KFC, Subway, Shopify and Home Depot. Furthermore, there has been an increase in the number of institutional investors and crypto whales getting into Bitcoin. It's also increasingly being viewed as a store of value, with many big-time investors joining the action in early 2021. This unprecedented buying pressure has caused Bitcoin's price to rise. Cointelegraph said in March 2021 that "Institutions are buying more Bitcoin per month than what's being mined, and there just isn't enough for everyone." As this number grows, the amount of Bitcoin available is becoming scarcer, especially with another Bitcoin halving expected in April 2024.

### Summing up

Bitcoin entered the game in 2009 being a very innovative digital currency. In the past years Bitcoin became the most popular and accepted virtual currency on the market. Bitcoin has several benefits such as the ability of making anonymous transaction with any user in the world without making use of a third party. However, it also has some disadvantages, like the risk of hacking or being collapsed due to competition, also the volatility of this virtual currency and the deflationary nature which makes it difficult to become a unit of account.

References:

https://medium.com/blockchain/bitcoin-explained-91a868c65b27

https://startup.info/characteristics-of-bitcoin/

https://medium.com/poloniex/what-is-bitcoin-f831371f99f5

https://trustmachines.co/bitcoin-history/

https://medium.com/interdax/a-beginners-guide-to-understanding-bitcoin-d7bcf250d652