bitpay.com

What is Bitcoin & How Does It Work? A Beginner's Guide to BTC| BitPay

The BitPay Team

13–16 minutes

Bitcoin, initiated in 2009 by an entity known as Satoshi Nakamoto, is a digital currency that operates independently of traditional banking systems and governments, utilizing a decentralized network for transactions.

Distinctive for its finite supply limit of 21 million coins, Bitcoin's existence hinges on a process called mining. This procedure not only generates new Bitcoins but also fortifies the network's security and transaction integrity.

Bitcoin has garnered attention for facilitating swift global transactions without the need for intermediaries, such as banks, making it a favored option for international transfers. Additionally, its investment appeal lies in its scarcity and potential for value appreciation, contrasting with traditional financial assets.

The trajectory of Bitcoin reflects growing acceptance and technological enhancements, including layer-2 solutions like the Lightning Network, aimed at boosting transaction efficiency. Despite its promise, regulatory concerns remain significant discussion points in its ongoing evolution.

On October 31, 2008, a white paper describing a new “peer-to-peer electronic cash system” was sent to an email list of software developers. The paper promised to solve the double-spend problem that had plagued programmers for decades. Until then, it had seemed impossible to create a form of digital value that could be spent only once and not be replicable.

Then, on January 3, 2009, the genesis block of the Bitcoin blockchain was mined. In the 15 years since, Bitcoin and other

digital currencies have become a multi-trillion dollar asset class, with a growing share of financial transactions being made with this medium of exchange.

But what exactly is Bitcoin, and how does it work? This guide aims to shed light on the fundamentals of Bitcoin, its technological underpinnings, and its uses as a store of value and unit of exchange.

Bitcoin explained: What is Bitcoin?

At its simplest, Bitcoin (BTC) is a form of digital currency, independent of any government or institution. It was introduced in 2009 by a person or group using the pseudonym Satoshi Nakamoto. Unlike traditional currencies, Bitcoin operates on a decentralized network of computers and relies on blockchain technology to maintain its integrity and security.

National currencies like the US dollar, European euro, or Japanese yen are known as fiat currencies. Merriam-Webster defines the word fiat as meaning “by arbitrary order or decree.” In other words, fiat currencies are issued by governments and don’t have any tangible monetary value backing them. Before 1971, the US dollar was backed by gold, but that is no longer the case.

Bitcoin is not backed by a physical commodity, but instead by a tremendous amount of computing power that goes into securing the network. Unlike fiat currencies, which cost almost nothing to create and can be printed at will by governments, there will only ever be 21 million BTC in existence. A pre-programmed process known as “halving” cuts the rate at which new coins are created approximately every four years, ensuring the scarcity of Bitcoin.

Halvings slow the creation of new Bitcoins, keeping the supply low and preventing inflation of the currency. We'll touch on the mining aspect of Bitcoin further into this guide.

Bitcoin is based on blockchain, a public ledger that records all transactions across a network of computers. Blockchain is a type of distributed ledger technology (DLT). While all blockchains are distributed ledgers, not all distributed ledgers are blockchains.

The Bitcoin blockchain is the ledger that stores a record of every Bitcoin transaction ever sent. Each transaction is verified by network participants, called miners, who use powerful computers to solve complex mathematical puzzles. Successful miners are rewarded with newly minted coins.

Ownership of Bitcoin is established through digital keys, bitcoin addresses, and digital signatures. These elements ensure that only the owner of the coins can spend them. One of the most significant breakthroughs of Bitcoin is that it solved the "double-spend problem," creating a form of digital property that can only be sent one time and not be replicated, as other digital files can be.

To gain a better understanding of how Bitcoin works, it's helpful to look at what Bitcoin mining is and how individuals can use Bitcoin.

Bitcoin mining

Bitcoin mining is the backbone of the Bitcoin network. Miners provide security and confirm new blocks of Bitcoin transactions. Without miners, the network would be vulnerable and easy to attack.

Bitcoin mining involves using computer hardware to perform

complex mathematical calculations, known as proof-of-work (PoW). This process secures the network by verifying the legitimacy of Bitcoin transactions. Each transaction is added to a block, and once the block is full, miners compete to validate the transactions and add the block to the blockchain. When a miner solves the next block, they are rewarded with newly created coins, known as block rewards.

Bitcoin mining also presents several challenges. The difficulty of mining adjusts approximately every two weeks to ensure that blocks are added to the blockchain on a consistent basis, roughly every 10 minutes. As more miners join the network, the difficulty of mining also rises, requiring more computational power.

Mining is an in-depth, complex topic with a lot of intricacies. The simple ideas described here have only scratched the surface.

Acquiring and storing Bitcoin

There are two main ways to acquire Bitcoin: buying coins on an exchange or mining them yourself.

For most people, buying coins will be the preferred method. Mining requires more technical knowledge in addition to purchasing large mining machines that use a lot of energy while generating heat and noise.

Buying BTC has become as easy as making any other online purchase. Crypto exchanges serve as a medium for users to buy, sell, and trade Bitcoin and other cryptocurrencies.

Some well-known, reputable exchanges accessible for US-based users include Coinbase and Kraken. Creating an account is a straightforward process and involves providing identifying

information and linking a payment method like a credit card, bank account, or PayPal account.

After having acquired some Bitcoin, users can choose to store it in multiple ways. The simplest way involves leaving it on an exchange. This can be convenient but also means that your assets are in the custody of a third-party, similar to how a bank holds cash on behalf of its customers.

One of the unique attributes of Bitcoin is that it can be held in self-custody and kept secure. Rather than leaving your assets held on an exchange, an independently managed Bitcoin wallet is used to store your BTC and make transactions. When done correctly, this ensures that no one can take your coins or stop you from spending them as you choose. While this involves a level of personal responsibility, many users prefer this method of storage for its increased security and financial autonomy. Read more about managing your BTC with self-custody.

Bitcoin as a payment method

Satoshi Nakamoto, the inventor of Bitcoin, envisioned the cryptocurrency as a peer-to-peer form of digital cash. Bitcoin stands out in comparison to other historical currencies, gold and fiat, in a few key areas:

- **Finite supply:** Unlike fiat currencies, which central banks can print in unlimited quantities, Bitcoin has a capped supply of 21 million coins. This scarcity mirrors gold's value proposition but does in a digital context, protecting against inflation.
- **Digital nature:** Bitcoin’s digital form allows for instant global transactions, a stark contrast to the physical limitations of gold and

the intermediary hurdles of fiat currency transfers.

- **Divisibility:** Bitcoin can be divided into much smaller units than fiat currency or gold, facilitating micro-transactions and making it adaptable to a wide range of financial activities.
- **Fungibility:** Each BTC is equivalent to another, ensuring a consistent value across the network, unlike physical commodities which can vary in purity.
- **Portability:** Carrying large sums of gold or fiat can be impractical or unsafe. Bitcoin can be moved effortlessly across borders, stored on a digital wallet, and accessed with a private key.
- **Verifiability:** The blockchain technology underpinning Bitcoin provides a transparent, immutable ledger, making transactions easily verifiable and reducing the risk of fraud.

  Over a decade after Nakamoto released their whitepaper, thousands of businesses accept BTC payments for a whole range of goods and services. You can buy practically anything using Bitcoin - from luxury goods and cars, to plane tickets and clothes, plus everything in between.

  Using Bitcoin as a payment method is secure, fast, and low-cost - and functions all without any bank or financial institution. As with buying and storing BTC, there are a number of ways you can spend Bitcoin:

- Shop directly with merchants that accept crypto payments
- Make a peer-to-peer (P2P) payment from your wallet directly to another wallet
- Use a crypto debit card to convert crypto to cash

- Use a solution like BitPay Bill Pay to make bill payments with Bitcoin
- Buy gift cards with crypto to use at popular brands and retailers

Bitcoin as an investment asset

Bitcoin has gained popularity as an investment asset, with many attracted to its potential for high returns and non-correlation with other asset classes. The launch of US-based Bitcoin ETFs in 2024 has accelerated this trend. But there is more to the story than a simple “number go up” factor.

Bitcoin is unique among other assets for several reasons. A few of these include:

- A fixed supply cap of 21 million
- The highest hash rate of any proof-of-work blockchain, meaning it’s the most secure network
- A high number of nodes distributed around the globe
- Bitcoin can be bought and sold by anyone with an internet connection
- The asset can be bought, sold, and traded without a third party
- Bitcoin markets operate 24/7

Bitcoin can be very volatile at times. But when zooming out and looking at the overall trend of Bitcoin’s price as measured in US dollars, things have been going up and to the right over an extended period of time.

As of March 2024, the Bitcoin price sits near a record-high in US dollar terms, meaning that anyone who bought Bitcoin before this

time and held it is now in profit. On the other hand, those who try to trade the volatility often lose. As with traditional investments, utilizing a dollar-cost averaging (DCA) strategy allows investors to make smaller, regular investments and lower their cost basis.

As always, do your own research before making investment decisions, and only invest what you can afford to lose.

The future of Bitcoin

A lot is going on that could shape Bitcoin's future development, including technological advancements, regulatory landscapes, and overall mainstream adoption.

One prominent technological component is layer-2 technology, like the Lightning Network. Lightning allows for fast and affordable microtransactions to be sent off-chain, avoiding the long wait times and high fees of sending a standard Bitcoin transaction.

The regulatory landscape is always changing, but appears to be growing more favorable toward Bitcoin. With the approval of the first spot Bitcoin ETFs in the US on January 10, 2024, the Securities and Exchange Commission (SEC) has declared Bitcoin to be a commodity rather than a security.

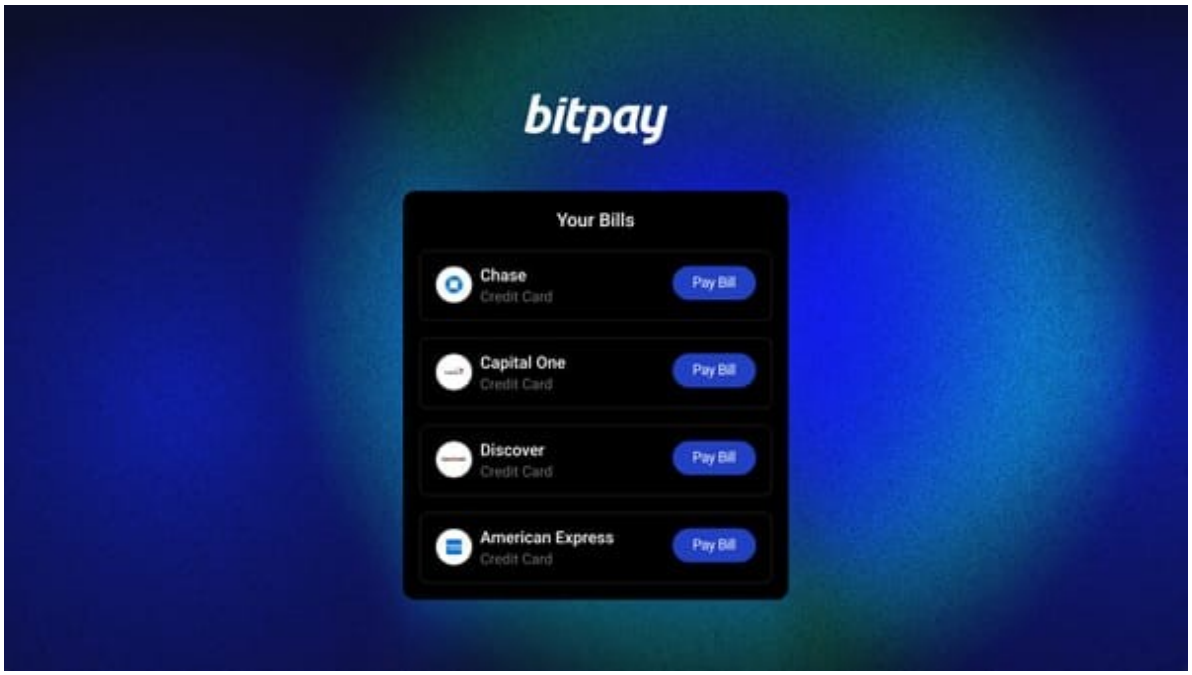
Despite Bitcoin accounting for a small portion of global monetary transactions, its usage and the number of transactions on its network, along with other blockchains, have seen consistent growth over the years. In January 2014, the Bitcoin blockchain processed fewer than two million transactions for the entire month. Fast forward to January 2024, and this volume of transactions now occurs within just a few days, with the monthly total approaching nearly 15 million transactions.

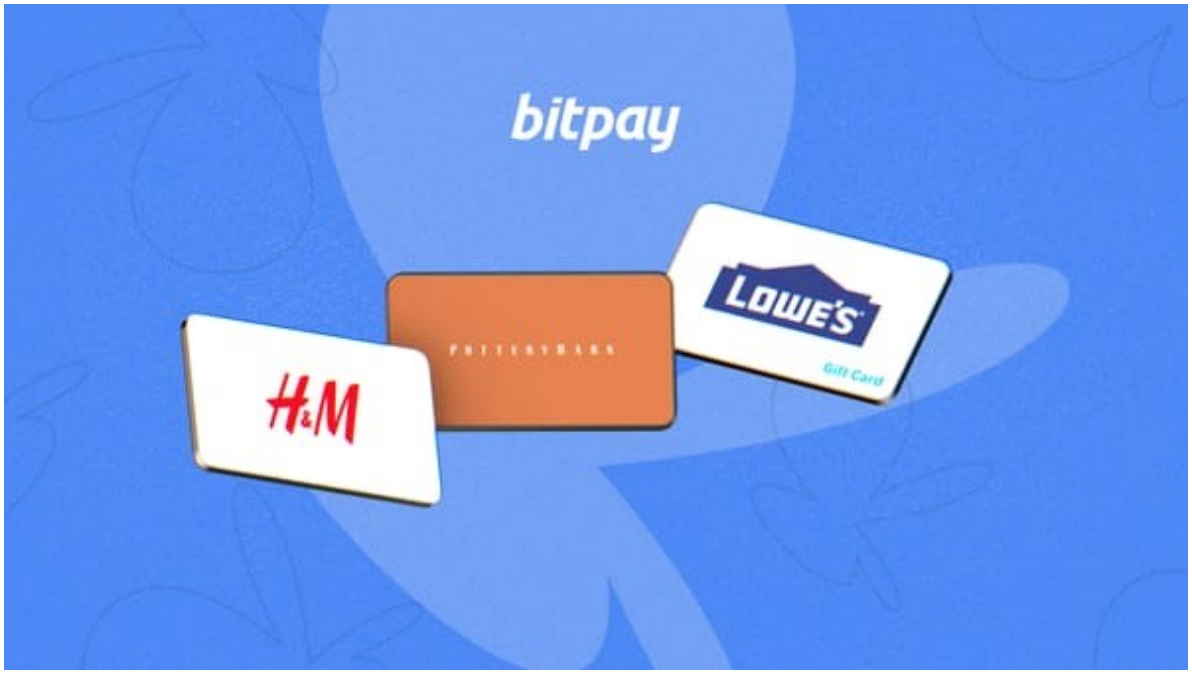
Recap and wrap up on Bitcoin

Bitcoin represents a censorship-resistant payment method, a digital form of money with a fixed supply cap, and the most secure computer network in the world. This remarkable innovation has spawned a new era in finance and technology, the repercussions of which have only just begun to be realized and understood.

Part of Bitcoin's significance lies in its ability to challenge traditional financial systems and offer an alternative form of hard money that is transparent, secure, divisible, portable, and accessible. As the digital economy continues to evolve, Bitcoin has already begun to play a crucial role in shaping the future of finance.

Note: *All information in this article is for educational purposes only, and shouldn't be interpreted as investment advice. BitPay is not liable for any errors, omissions or inaccuracies. The opinions expressed are solely those of the author, and do not reflect views of BitPay or its management. For investment or financial guidance, a professional should be consulted.*





Subscribe to BitPay Blog

Get the latest posts delivered right to your inbox

Subscribe