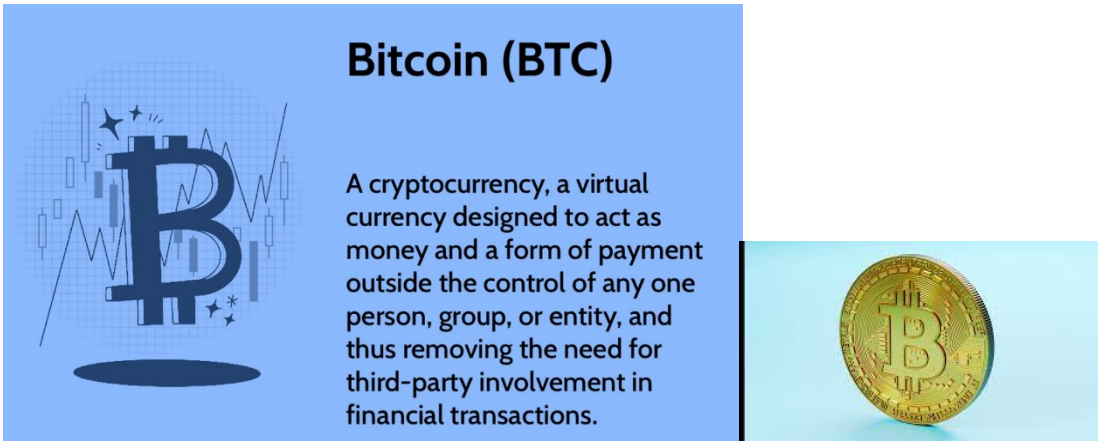
Bitcoin

- Bitcoin is a type of digital currency in which a record of transactions is maintained and new units of currency are generated by the computational solution of mathematical problems, and which operates independently of a central bank.
- Bitcoin is a protocol which implements a highly available, public, and decentralized ledger.
- In order to update the ledger, a user must prove they control an entry in the ledger.
- The protocol specifies that the entry indicates an amount of a token, bitcoin with a miniscule b.
- The user can update the ledger, assigning some of their bitcoin to another entry in the ledger.
- Because the token has characteristics of money it can be thought of as a digital currency.



History

- Bitcoin (BTC) was the first cryptocurrency ever created back in 2009, and it remains the most popular and valuable digital currency in the world today.
- Bitcoin is a blockchain-based decentralized digital currency powered by a network of users who verify and record transactions without relying on a central authority or intermediary.
- Bitcoin is an alternative to fiat currencies, such as the U.S. dollar, that are controlled by governments and central banks.
- Transactions are verified via a process known as a proof-of-work consensus mechanism.
- Bitcoin miners compete to verify transactions by solving complex mathematical functions using powerful computers.
- Some Bitcoin enthusiasts simply see the crypto as a fun asset for trading and speculation, while others believe it could ultimately become the universal currency of the digital world.

- There's no question Bitcoin has had a meteoric rise in popularity since its inception, but the first 13 years have also exposed several key flaws and shortcomings of the world's most popular digital asset.

When did Bitcoin Start?

- It's no coincidence that Bitcoin was born during one of the most chaotic financial environments in U.S. history.
- During the global financial crisis of 2007 to 2009, distrust of banks and central governments was at a peak.
- Bitcoin was created in 2009 by a person or group of people using the pseudonym Satoshi Nakamoto, the name which appeared on the original 2008 Bitcoin white paper that first described the blockchain system that would serve as the backbone of the entire cryptocurrency market.
- Over the years, several people have stepped forward claiming to be the real Satoshi Nakamoto, but none could provide sufficient evidence to support their claims.
- The Bitcoin blockchain was officially launched when the first Bitcoin block, the genesis block, was created on Jan. 3, 2009.
- In the first seven months following Bitcoin's launch, Satoshi reportedly mined up to 1.1 million Bitcoins.
- At August 2022 prices, those coins would now be worth about $22 billion.
- Joshua Peck, founder and chief investment officer of cryptocurrency hedge fund TrueCode Capital, says early Bitcoin enthusiasts were captivated with its design, even if they weren't exactly certain of what it was going to actually be.
- "It had some economic value, but I was looking at it more from an engineering perspective thinking that we could use it for secure message passing or getting strong cryptography into the hands of everyday users, so the financial value was somewhat secondary," Peck says.
- The first reported real-world financial transaction involving Bitcoin took place on May 22, 2010, when a Florida man negotiated to pay 10,000 BTC for two Papa John's pizzas priced at about $25.
- That transaction valued the price of one Bitcoin at roughly a fourth of a cent. To this day, the Bitcoin community celebrates Pizza Day on May 22.

Bitcoin Price History

- Bitcoin first became available to buy, sell and trade on online exchanges in 2010.
- In April 2011, the price of Bitcoin crossed the $1 threshold for the first time.
- Bitcoin also faced its first competition in the crypto space in 2011. Litecoin (LTC) was launched in October 2011.
- The Ethereum blockchain went live several years later in 2015.
- As Bitcoin's price continued to rise, so too did its visibility, popularity and volatility.
- By November 2013, Bitcoin prices reached $1,000. Bitcoin prices and trading

volumes really started to snowball in late 2017 – with prices hitting $10,000 per coin for the first time in November 2017 – and reached about $20,000 in December 2017.

- One of the driving forces behind the parabolic rise in Bitcoin prices was an announcement by CME Group Inc. that it would be launching Bitcoin futures contracts in December 2017. These contracts represented the first Bitcoin-related financial product offered by a regulated U.S. financial institution.
- JarekHirniak, founder and CEO of Generation Lambda, says Bitcoin followed a common innovation trajectory known as the Gartner Hype Cycle. According to the model, as a new technology such as Bitcoin gains visibility, expectations initially soar to an unreasonably high level.

Bitcoin usage

- Bitcoin was created as a way for people to send money over the internet.
- The digital currency was intended to provide an alternative payment system that would operate free of central control but otherwise be used just like traditional currencies.
- For example, if you use your credit card to pay, you will incur some fees from the credit card company. With Bitcoin, you have no such unnecessary costs.
- User can use Bitcoin to trade daily. Bitcoin is not just a digital currency for paying for your shopping.
- Among developed countries, cryptocurrency use was most widespread in English-speaking countries – first and foremost the United States, but also the UK, Canada, South Africa and Australia. Emerging economies India, China and Brazil also registered as heavy users.

Bitcoin storage

- User can store Bitcoin in up to four different types of wallets: mobile, desktop, web, and hardware. The types of wallets can be either internet-connected, "hot", or not internet-connected, "cold".
- However, no matter what kind of wallet you use, to access your currency, you'll need a set of private keys.
- If these keys are lost or stolen, you won't be able to access your Bitcoin, and that's true whether you store them physically or digitally.
- From losing physical items to digital devices malfunctioning and hacking, storing your Bitcoin safely requires thoughtful action.

Digital wallets

  - Digital wallets are either hardware or web-based wallets that can be used on a computer, phone, or even paper.
  - Again, it's best to only keep a small amount of Bitcoin in the digital wallet for spending, while the bulk of the Bitcoin should be stored in cold storage, a safer environment overall.
  - Of course, the digital wallet should be encrypted so no one can access your

private keys.
    - Pros: Digital wallets are accessible from anywhere in the world, making them a good choice for walking around money or traveling.
    - Cons: Like any digital service or product, digital wallets are vulnerable to hacking.

- Digital wallet based on your type of operating system, whether you want hardware, and other criteria and features such as:
- Control: This asks whether you want to have total control over your Bitcoin, meaning that you are fully responsible for securing and backing up your currency. Otherwise, you can work through a third-party provider, but that means giving up total control of your wallet.
- Validation: Relatedly, validation means having a third party verify transactions. In a full node digital wallet, no third party is needed.
- Transparency: Transparency measures whether the wallet is open-sourced and tamper-proof.
- Environment: If the wallet is stored on your computer, it should have a strong password, two-factor authentication, or multi-factor authentication. Learn more in our authentication guide.
- Privacy: Some wallets rotate addresses and don't disclose this information to peers on your network. Others allow for the use of Tor as a proxy server if you want to unlink your transactions from your IP address.
- Fees: While some wallets give users the option to control the fees before the transaction, others do not, leading them to sometimes pay more than necessary.
- Bech32: Bech32 is a special address format that not all wallets support; this format is also known as "bc1 addresses".
- Hardware wallet: If you want a physical wallet, check this box on the Bitcoin organization's digital wallet quiz.
- Legacy addresses: Rather than starting with bc1 like most modern Bitcoin addresses, legacy addresses start with the numbers one or three and are only available on older wallets or exchanges, typically.
- Lightning: For quicker transactions and lower fees, some users may want to try out the Lightning Network. It's a new and highly experimental network that lets users transfer Bitcoins without recording the transactions on the blockchain.
- Multisig: If you want to require multiple keys to authorize transactions, you can divide the required signatures into multiple parties.
- SegWit: SegWit reduces fees by using blockchain technology more efficiently, thus saving space.

Offline wallets

- Offline wallets are "cold storage" that isn't internet-accessible.
- However, that doesn't mean that they're necessarily physical objects; desktop

wallets, for example, are on a computer but are not connected to the internet.

- Rather, the keys are stored on the physical machine itself.
- Pros: Offline wallets are safer than digital wallets because they're at significantly less risk of being exposed online, creating the highest level of security possible.
- Cons: If they're stored on a computer, offline wallets can still be susceptible to Bitcoin-targeting malware, so it's best to use them with antivirus software that contains protection against malware (see below for more explanation on antivirus software).
- Users can choose between three types of offline wallets: hardware, paper, or coin.

Hardware wallets

- Hardware wallets mean that the cryptocurrency is stored on a piece of hardware like a USB stick.
- Pros: With hardware wallets, transactions are completely anonymous, as none of the user's personally identifiable information is on the hardware. And unlike desktop wallets, hardware wallets are resilient to malware. Finally, even if the user loses their key, they'll be able to recover their funds using a seed phrase, a 20-word phrase that the user will set up when they create the wallet itself.Ideally, the user stores the seed phrase on paper in a locked safe.
- Cons: If the user loses the hardware wallet, then they have no way of recovering the Bitcoin, even with the seed phrase.

Paper wallets

- Although paper wallets may seem like the most straightforward option, they actually require more knowledge of digital currencies than any other option and can be generated online or off.
- Pros: In a minimal amount of space, paper wallets allow for complete anonymity; essentially, they're a seed phrase written on a piece of paper.
- Cons: Paper can be lost, damaged, or smudged, and ink can fade.
- Plus, if the user is printing their paper wallet, they have to take into consideration any potential insecurities on their printer's network.
- Another issue is address re-usage; if you don't re-use the same address, then you'll need to create a new paper wallet for every transaction.
- But re-using the same address can make it easier to trace the private key signature, so the safest way, creating a new wallet for every transaction, is also the most cumbersome.

Bitcoin selling

- Selling Bitcoin (BTC) can be similar to buying Bitcoin, except in a somewhat reversed process.
- To sell BTC, you must first have BTC on hand in your wallet.
- Buying Bitcoin is possible via a number of routes.
- When you are ready to sell some or all of your Bitcoin, you can do so through a variety of avenues, including an online cryptocurrency exchange, direct peer-to-peer (P2P) transactions online or on-site, and through a Bitcoin ATM.
- Your two main options for selling bitcoin into local currency are:
- **Using an exchange service**
- An exchange service is a regulated business that interacts with the traditional banking system.
- An exchange service may take the form of a simple website with limited exchange functionality, a digital wallet with banking connections, or a full-service cryptocurrency exchange with order book, market makers, etc.
- **Pros and cons of selling bitcoin using an exchange service**
    - Exchange services can be divided into two groups:
        - 1) simple exchange&
        - 2) full-service exchange.
    - **Simple exchange services**
        - (eg. the Bitcoin.com Wallet, the Bitcoin.com Sell website).
    - **Advantages**
        - Fast, easy, and convenient
        - Guaranteed at or close-to market rates for sells
        - Can sell any amount
    - **Disadvantages**
        - Requires identity verification
        - Not available in all regions
        - Payments made to bank accounts only
    - **Full-service cryptocurrency exchanges**
    - **Advantages**
        - Can set 'limit' sells, thereby guaranteeing your specified rate
        - Can sell any amount
    - **Disadvantages**
        - Not available in all regions
        - Requires identity verification
        - Payments made to bank accounts only
        - Custodial (the exchange holds your bitcoin, not you)
        - Relatively difficult to use (for example, requires setting sell orders and understanding order books)
- **Selling peer-to-peer**
- When you sell peer-to-peer, you can bypass the traditional banking system to a certain extent by, for example, taking payment in cash, using a payment app like PayPal, or settling the transaction with goods or services.

- If you know someone who wants to sell bitcoin, you can buy directly from that person.
- Alternatively, there are a number of platforms that act as a matchmaking service, helping sellers find buyers and vice versa.
- Buyers and sellers then negotiate trades on a peer-to-peer basis.
- Pros and cons of selling bitcoin peer-to-peer
    - (eg. your friend or a match-making service like Hodlhodl)
    - Advantages
        - Identity verification is often not required
        - Any payment method is possible (including cash, payment app, barter, etc.)
    - Disadvantages
        - Less convenient (you must manually create and negotiate sell orders)
        - Higher risk of fraud
        - Generally only legal to sell small amounts

Bitcoin transactions

- A transaction is a transfer of Bitcoin value on the blockchain. In very simple terms, a transaction is when participant A gives a designated amount of Bitcoin they own to participant B.
- Transactions are created through mobile, desktop or hardware wallets.
- Bitcoin transactions are messages, like email, which are digitally signed using cryptography and sent to the entire Bitcoin network for verification.
- Transaction information is public and can be found on the digital ledger known as the 'blockchain.'
- The history of each and every Bitcoin transaction leads back to the point where the bitcoins were first produced or 'mined.'
- A Bitcoin transaction is a transfer of bitcoin from one address to another.
- The valid transaction must be signed by the sender.
- Bitcoin does not have accounts. Instead, pieces of Bitcoin of arbitrary size are all associated with an address, which is controlled by the owner of that bitcoin.
- A transfer of bitcoins from one Bitcoin user to another.
- Containing an embedded script, a Bitcoin transaction is created in a crypto wallet, residing in the user's computer, smartphone or tablet or in a cryptocurrency exchange.
- The transaction is published on the Bitcoin network where it is validated and added to the blockchain by a Bitcoin "miner."
- A Bitcoin transaction is a transfer of bitcoin from one address to another. The valid transaction must be signed by the sender.
- Bitcoin does not have accounts. Instead, pieces of Bitcoin of arbitrary size are all associated with an address, which is controlled by the owner of that bitcoin. These pieces of Bitcoin are called Unspent Transaction Outputs (UTXOs).

- All Bitcoin transactions are published to the mempool, where they are considered 'pending'.
- When a miner adds a transaction to a block, it is then considered confirmed.