UNIT II
BITCOIN AND CRYPTOCURRENCY

A BASIC CRYPTO CURRENCY

Cryptocurrency, sometimes called crypto-currency or crypto, is any form of currency that exists digitally or virtually and uses cryptography to secure transactions. Cryptocurrencies don't have a central issuing or regulating authority, instead using a decentralized system to record transactions and issue new units.

What is cryptocurrency?

Cryptocurrency is a digital payment system that doesn't rely on banks to verify transactions. It's a peer-to-peer system that can enable anyone anywhere to send and receive payments. Instead of being physical money carried around and exchanged in the real world, cryptocurrency payments exist purely as digital entries to an online database describing specific transactions. When you transfer cryptocurrency funds, the transactions are recorded in a public ledger. Cryptocurrency is stored in digital wallets.

Cryptocurrency received its name because it uses encryption to verify transactions. This means advanced coding is involved in storing and transmitting cryptocurrency data between wallets and to public ledgers. The aim of encryption is to provide security and safety.

The first cryptocurrency was Bitcoin, which was founded in 2009 and remains the best known today. Much of the interest in cryptocurrencies is to trade for profit, with speculators at times driving prices skyward.

How does cryptocurrency work?

Cryptocurrencies run on a distributed public ledger called blockchain, a record of all transactions updated and held by currency holders.

Units of cryptocurrency are created through a process called mining, which involves using computer power to solve complicated mathematical problems that generate coins. Users can also buy the currencies from brokers, then store and spend them using cryptographic wallets.

If you own cryptocurrency, you don't own anything tangible. What you own is a key that allows you to move a record or a unit of measure from one person to another without a trusted third party.

Although Bitcoin has been around since 2009, cryptocurrencies and applications of blockchain technology are still emerging in financial terms, and more uses are expected in the future. Transactions including bonds, stocks, and other financial assets could eventually be traded using the technology.

Cryptocurrency examples

There are thousands of cryptocurrencies. Some of the best known include:

Bitcoin:

Founded in 2009, Bitcoin was the first cryptocurrency and is still the most commonly traded. The currency was developed by Satoshi Nakamoto – widely believed to be a pseudonym for an individual or group of people whose precise identity remains unknown.

Ethereum:

Developed in 2015, Ethereum is a blockchain platform with its own cryptocurrency, called Ether (ETH) or Ethereum. It is the most popular cryptocurrency after Bitcoin.

Litecoin:

This currency is most similar to bitcoin but has moved more quickly to develop new innovations, including faster payments and processes to allow more transactions.

Ripple:

Ripple is a distributed ledger system that was founded in 2012. Ripple can be used to track different kinds of transactions, not just cryptocurrency. The company behind it has worked with various banks and financial institutions.

Non-Bitcoin cryptocurrencies are collectively known as “altcoins” to distinguish them from the original.

How to buy cryptocurrency

You may be wondering how to buy cryptocurrency safely. There are typically three steps involved. These are:

Step 1: Choosing a platform

The first step is deciding which platform to use. Generally, you can choose between a traditional broker or dedicated cryptocurrency exchange:

- **Traditional brokers.** These are online brokers who offer ways to buy and sell cryptocurrency, as well as other financial assets like stocks, bonds, and ETFs. These platforms tend to offer lower trading costs but fewer crypto features.
- **Cryptocurrency exchanges.** There are many cryptocurrency exchanges to choose from, each offering different cryptocurrencies, wallet storage, interest-bearing account options, and more. Many exchanges charge asset-based fees.

When comparing different platforms, consider which cryptocurrencies are on offer, what fees they charge, their security features, storage and withdrawal options, and any educational resources.

Step 2: Funding your account

Once you have chosen your platform, the next step is to fund your account so you can begin trading. Most crypto exchanges allow users to purchase crypto using fiat (i.e., government-issued) currencies such as the US Dollar, the British Pound, or the Euro using their debit or credit cards – although this varies by platform.

Crypto purchases with credit cards are considered risky, and some exchanges don't support them. Some credit card companies don't allow crypto transactions either. This is because cryptocurrencies are highly volatile, and it is not advisable to risk going into debt — or potentially paying high credit card transaction fees — for certain assets.

Some platforms will also accept ACH transfers and wire transfers. The accepted payment methods and time taken for deposits or withdrawals differ per platform. Equally, the time taken for deposits to clear varies by payment method.

An important factor to consider is fees. These include potential deposit and withdrawal transaction fees plus trading fees. Fees will vary by payment method and platform, which is something to research at the outset.

Step 3: Placing an order

You can place an order via your broker's or exchange's web or mobile platform. If you are planning to buy cryptocurrencies, you can do so by selecting "buy," choosing the order type, entering the amount of cryptocurrencies you want to purchase, and confirming the order. The same process applies to "sell" orders.

There are also other ways to invest in crypto. These include payment services like PayPal, Cash App, and Venmo, which allow users to buy, sell, or hold cryptocurrencies. In addition, there are the following investment vehicles:

- **Bitcoin trusts:** You can buy shares of Bitcoin trusts with a regular brokerage account. These vehicles give retail investors exposure to crypto through the stock market.

- **Bitcoin mutual funds:** There are Bitcoin ETFs and Bitcoin mutual funds to choose from.
- **Blockchain stocks or ETFs:** You can also indirectly invest in crypto through blockchain companies that specialize in the technology behind crypto and crypto transactions. Alternatively, you can buy stocks or ETFs of companies that use blockchain technology.

How to store cryptocurrency

Once you have purchased cryptocurrency, you need to store it safely to protect it from hacks or theft. Usually, cryptocurrency is stored in crypto wallets, which are physical devices or online software used to store the private keys to your cryptocurrencies securely. Some exchanges provide wallet services, making it easy for you to store directly through the platform. However, not all exchanges or brokers automatically provide wallet services for you.

There are different wallet providers to choose from. The terms “hot wallet” and “cold wallet” are used:

- **Hot wallet storage:** "hot wallets" refer to crypto storage that uses online software to protect the private keys to your assets.
- **Cold wallet storage:** Unlike hot wallets, cold wallets (also known as hardware wallets) rely on offline electronic devices to securely store your private keys.

Typically, cold wallets tend to charge fees, while hot wallets don't.

What can you buy with cryptocurrency?

When it was first launched, Bitcoin was intended to be a medium for daily transactions, making it possible to buy everything from a cup of coffee to a computer or even big-ticket items like real estate. That hasn’t quite materialized and, while the number of institutions accepting cryptocurrencies is growing, large transactions involving it are rare. Even so, it is possible to buy a wide variety of products from e-commerce websites using crypto. Here are some examples:

Technology and e-commerce sites:

Several companies that sell tech products accept crypto on their websites, such as newegg.com, AT&T, and Microsoft. Overstock, an e-commerce platform, was among the first sites to accept Bitcoin. Shopify, Rakuten, and Home Depot also accept it.

Luxury goods:

Some luxury retailers accept crypto as a form of payment. For example, online luxury retailer Bitdials offers Rolex, Patek Philippe, and other high-end watches in return for Bitcoin.

Cars:

Some car dealers – from mass-market brands to high-end luxury dealers – already accept cryptocurrency as payment.

Insurance:

In April 2021, Swiss insurer AXA announced that it had begun accepting Bitcoin as a mode of payment for all its lines of insurance except life insurance (due to regulatory issues). Premier Shield Insurance, which sells home and auto insurance policies in the US, also accepts Bitcoin for premium payments.

If you want to spend cryptocurrency at a retailer that doesn’t accept it directly, you can use a cryptocurrency debit card, such as BitPay in the US.

Cryptocurrency fraud and cryptocurrency scams

Unfortunately, cryptocurrency crime is on the rise. Cryptocurrency scams include:

Fake websites: Bogus sites which feature fake testimonials and crypto jargon promising massive, guaranteed returns, provided you keep investing.

Virtual Ponzi schemes: Cryptocurrency criminals promote non-existent opportunities to invest in digital currencies and create the illusion of huge returns by paying off old investors with new investors' money. One scam operation, BitClub Network, raised more than $700 million before its perpetrators were indicted in December 2019.

"Celebrity" endorsements: Scammers pose online as billionaires or well-known names who promise to multiply your investment in a virtual currency but instead steal what you send. They may also use messaging apps or chat rooms to start rumours that a famous businessperson is backing a specific cryptocurrency. Once they have encouraged investors to buy and driven up the price, the scammers sell their stake, and the currency reduces in value.

Romance scams: The FBI warns of a trend in online dating scams, where tricksters persuade people they meet on dating apps or social media to invest or trade in virtual currencies. The FBI's Internet Crime Complaint Centre fielded more than 1,800 reports of crypto-focused romance scams in the first seven months of 2021, with losses reaching $133 million.

Otherwise, fraudsters may pose as legitimate virtual currency traders or set up bogus exchanges to trick people into giving them money. Another crypto scam involves fraudulent sales pitches for individual retirement accounts in cryptocurrencies. Then there is straightforward cryptocurrency hacking, where criminals break into the digital wallets where people store their virtual currency to steal it.

Is cryptocurrency safe?

Cryptocurrencies are usually built using blockchain technology. Blockchain describes the way transactions are recorded into "blocks" and time stamped. It's a fairly complex, technical process, but the result is a digital ledger of cryptocurrency transactions that's hard for hackers to tamper with.

In addition, transactions require a two-factor authentication process. For instance, you might be asked to enter a username and password to start a transaction. Then, you might have to enter an authentication code sent via text to your personal cell phone.

While securities are in place, that does not mean cryptocurrencies are un-hackable. Several high-dollar hacks have cost cryptocurrency start-ups heavily. Hackers hit Coincheck to the tune of $534 million and BitGrail for $195 million, making them two of the biggest cryptocurrency hacks of 2018.

Unlike government-backed money, the value of virtual currencies is driven entirely by supply and demand. This can create wild swings that produce significant gains for investors or big losses. And cryptocurrency investments are subject to far less regulatory protection than traditional financial products like stocks, bonds, and mutual funds.

Four tips to invest in cryptocurrency safely

According to Consumer Reports, all investments carry risk, but some experts consider cryptocurrency to be one of the riskier investment choices out there. If you are planning to invest in cryptocurrencies, these tips can help you make educated choices.

Research exchanges:

Before you invest, learn about cryptocurrency exchanges. It's estimated that there are over 500 exchanges to choose from. Do your research, read reviews, and talk with more experienced investors before moving forward.

Know how to store your digital currency:

If you buy cryptocurrency, you have to store it. You can keep it on an exchange or in a digital wallet. While there are different kinds of wallets, each has its benefits, technical requirements, and security. As with exchanges, you should investigate your storage choices before investing.

Diversify your investments:

Diversification is key to any good investment strategy, and this holds true when you are investing in cryptocurrency. Don't put all your money in Bitcoin, for example, just because that's the name you know. There are thousands of options, and it's better to spread your investment across several currencies.

Prepare for volatility:

The cryptocurrency market is highly volatile, so be prepared for ups and downs. You will see dramatic swings in prices. If your investment portfolio or mental wellbeing can't handle that, cryptocurrency might not be a wise choice for you.

Cryptocurrency is all the rage right now, but remember, it is still in its relative infancy and is considered highly speculative. Investing in something new comes with challenges, so be prepared. If you plan to participate, do your research, and invest conservatively to start.

One of the best ways you can stay safe online is by using a comprehensive antivirus. Kaspersky Internet Security defends you from malware infections, spyware, data theft and protects your online payments using bank-grade encryption.

CREATION OF COINS

A cryptocurrency is a digital currency, which uses cryptography for secure transactions. It is designed to act as a medium of exchange on a computer network without relying on a central authority such as a government or a bank to manage it. Since cryptocurrencies have no central issuing or regulatory authority, they use a decentralized system to record transactions and issue new units. Cryptocurrency uses blockchain technology. Cryptocurrency units are created through a process called mining, which uses computer hardware to solve complex mathematical problems that produce coins. There are many cryptocurrencies in the market like Dogecoin, Bitcoin, and many more.

How is Cryptocurrency Created?

The units of cryptocurrency are created through a process called mining. Mining is the process of validating cryptocurrency transactions and creating new units of cryptocurrency. The mining process uses powerful computer hardware and software to solve complex mathematical problems that generate coins.

Cryptocurrencies use blockchain technology. Therefore, whenever a cryptocurrency transaction occurs, cryptocurrency miners (who also act as nodes on the blockchain network where these types of cryptocurrency transactions take place) try to decrypt the block containing the transaction information. The block not only verifies the transaction but also provides information about who sent how much cryptocurrency to whom, when and on what date. Once a block is decrypted and accepted as authentic by the majority of nodes in the blockchain network, the block is added to the blockchain. The verification process is very resource-intensive in terms of the required computing power. As a result, individual cryptocurrency miners often find the process too expensive, So because of this miners join mining pools to share computing power.

Coins and Tokens

Cryptocurrencies are broadly divided into two groups – **coins and tokens.** A coin is a cryptocurrency application that runs on its own blockchain, where all transactions take

place. Tokens, on the other hand, work on existing blockchain infrastructure and are typically used for physical objects like smart contracts. digital services, etc.

S No.	Coins	Tokens
1.	A new blockchain must be created for the coin.	Tokens can use an existing blockchain
2.	An in-depth understanding of how blockchain works and programming skills are required.	Tokens use open-source code and are relatively easier to create.
3.	Due to the creation of a new blockchain, the investment can be significant.	Creating tokens is faster and cheaper.

Create Coin and Token:

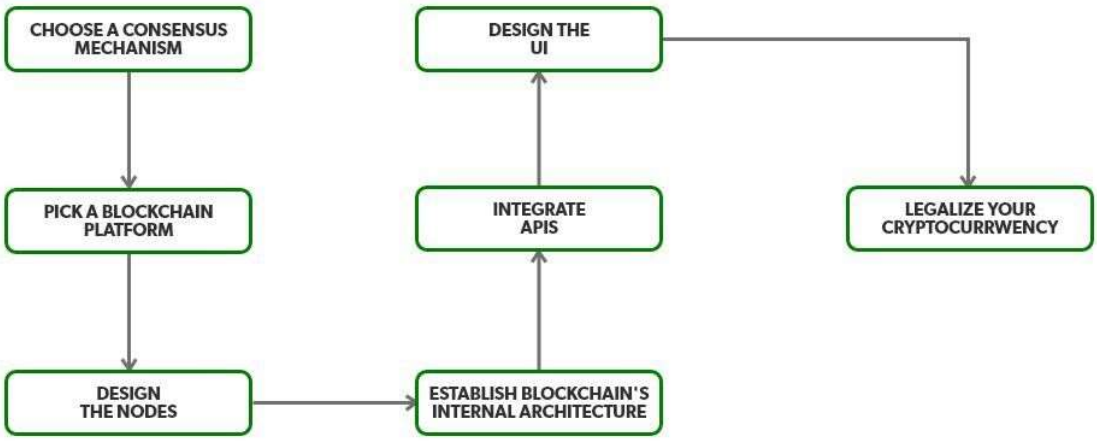
1. Creating a coin: The coin creation process is not that challenging. You can simply copy Bitcoin's code, add a new variable, or even change its value, and that's it – you have your blockchain and your coin. However, you must understand the code and know how to modify it, which requires extensive programming knowledge.

2. Creating a Token: As mentioned above, the token works with the existing blockchain infrastructure. Therefore, if you create a token on a high-performance blockchain such as Ethereum, your token should run on a highly secure network and also be secure from fraud attacks. Tokenization is less expensive in terms of money and time when you leverage your existing decentralized architecture and implement a consensus mechanism.

Popular solutions for making cryptocurrency

1. **Ethereum:** Ethereum is the first blockchain to offer a token creation service. It offers a superior level of trust due to its maturity and strong position in the cryptocurrency market. All tokens built on Ethereum use the **ERC-20 standard.** Tokens on Ethereum can only be written in Solidity (its own programming language).
2. **EOS:** EOS tokens use the **EOSIO.** Token standard and can be created with C++ or any other language like python, java, etc. that compiles to WebAssembly. With no transaction fees, blockchains offer excellent scalability, high transactions per second, and cost-effectiveness.
3. **NEO:** Neo is an open-source community-driven blockchain platform, Neo's vision is to be an open network for a smart economy. Neo uses the NEP-5 standard. Unlike Ethereum, you can create your own tokens on it using almost any high-level programming language like Java, Python, etc. HTTP API can be used to interact with the blockchain.

Steps to Create a Cryptocurrency



1. Choose a Consensus Mechanism: Consensus mechanisms are the protocols that consider a particular transaction legitimate and add to the block.
2. Pick a Blockchain Platform: Choosing the right blockchain platform for your business depends on the consensus mechanism you choose.
3. Design The Nodes: You need to determine how your blockchain will work and function, and design your nodes accordingly.
4. Establish Blockchain's Internal Architecture: Set up the internal architecture of the blockchain, Be sure about all the aspects before the launch as you won't be able to change several parameters of the blockchain after it's launched and running.
5. Integrate APIs: Some platforms don't offer pre-built APIs.Don't worry, there are several third-party blockchain API providers like ChromaWay, Gem, Colu, BlockCypher, etc.
6. Designing the UI: Building a top-notch cryptocurrency is useless if your UI is bad. You need to ensure that the web, FTP server, and external databases are up-to-date and that front-end and back-end programming is done with future upgrades in mind.
7. Legalize your cryptocurrency: Make sure your cryptocurrency is ready and compliant with upcoming international cryptocurrency regulations. That way, your work is preserved, and no sudden surprises can sabotage your efforts to create a new cryptocurrency.

Cryptocurrency mining reward

Cryptocurrency miners need money. They receive a small fraction of new units of cryptocurrency for completing "blocks" of verified transactions that are added to the blockchain.

- Miners are paid in the cryptocurrency they wish to mine.
- So when miners decide to decrypt a block of bitcoins, they get paid in bitcoins.
- By pooling resources, miners increase their chances of success and share the cost, but only receive a portion of the reward. This is known as a Cryptocurrency mining reward.

Pricing Cryptocurrencies

To understand cryptocurrency pricing, let's take the most famous example of Bitcoin.

- Like most other commodities in the market, the price of Bitcoin is determined by the interaction of supply and demand and expectations of future prices.
- For cryptocurrencies, pricing is entirely based on market dynamics.

- If the market believes that the price of Bitcoin will rise in the future, they will now be more people who are ready to pay more for it.
- On the other hand, if the market believes that the price will fall in the future, there will be more people selling cryptocurrencies now, and the price will be higher than at the future level.
- When selling, there are many people who accept lower prices than usual and expect lower prices in the future.
- Many Individual influencers can also significantly influence the price of cryptocurrencies.

Bitcoin Halving

The reward for mining, i.e. the amount of bitcoins a miner earns through successful authentication, is fixed. However, this reward is numerically halved every four years. So, when Bitcoin was introduced, miners could earn 50 BTC as a reward for successfully processing a block. This is called the Bitcoin halving. After the first halving, this number was reduced to 25, followed by 12.5, and the last halving as of 2020, which is currently 6.25. The next halving is planned for 2024.

Cryptocurrencies in the Market

Currently, According to Forbes in 2022 top Five best cryptocurrencies in the market are given below:

1. **Bitcoin (BTC):** Market cap of Bitcoin (BTC) is $880 billion.
2. **Ethereum (ETH):** Market cap of Ethereum (ETH) is $415 billion.
3. **Tether (USDT):** Market cap of Tether (USDT) is Over $79 billion.
4. **Binance Coin (BNB):** Market cap of Binance Coin (BNB) is Over $68 billion.
5. **U.S. Dollar Coin (USDC):** Market cap of the U.S. Dollar Coin (USDC) is Over $53 billion.

Advantages of Cryptocurrency

1. **Self-governed and managed:** Cryptocurrencies do not have a central issuing or regulatory authority, they use a decentralized system to record transactions. Records of cryptocurrency transactions are stored by miners on their hardware. Miners receive transaction fees as a reward. Therefore miners keep transaction records accurate and up-to-date.
2. **Secure and private:** Privacy and security have always been the main concerns of cryptocurrencies. Cryptocurrencies use blockchain technology, which uses encryption for secure transactions. This makes cryptocurrencies more secure than ordinary electronic transactions.
3. **Currency exchanges can be done easily:** Cryptocurrencies can be purchased in multiple currencies such as USD, EUR, GBP, INR, or JPY. With the help of various cryptocurrency wallets and exchanges, it is possible to convert one currency to another with minimal transaction fees by trading cryptocurrencies between different wallets.
4. **Transparency and anonymity:** Due to the distributed nature of the blockchain, every transaction is recorded and not changed. At the same time, if a crypto address is not publicly verified, no one knows who made the transaction and who received the cryptocurrency.
5. **A fast way to transfer funds:** Cryptocurrencies have always been the best solution for transactions. Cryptocurrency transactions, both international and domestic, are lightning-fast. This is because verification takes very little time.

6. **Low transaction fees:** Compare with Banks and other financial institutions, Cryptocurrencies charge relatively small amount transaction fees.

Disadvantages of Cryptocurrency

1. **Decentralized but still operated by some organizations:** Cryptocurrencies are known for their decentralized nature. However, the circulation and quantity of some currencies in the market are still controlled by their creators and some organizations.
2. **Can be used for illegal transactions:** Due to the high privacy and security of cryptocurrency transactions, it is difficult for governments to track users by wallet address or track their details. Bitcoin has historically been used as a currency exchange for many illegal businesses, such as buying drugs on the dark web.
3. **Data losses can cause financial losses:** Developers want to create virtually untraceable source code, strong protection from hackers, and authentication protocols that are hard to penetrate. This makes investing in cryptocurrencies safer than investing in physical cash or bank vaults. However, if the user loses the wallet's private key, it cannot be retrieved. The wallet remains locked along with the number of coins in it. This will bring financial losses to users.
4. **Cryptocurrencies are highly volatile:** Cryptocurrency markets are volatile and fluctuate frequently, even for famous cryptocurrencies like Bitcoin. Investing in cryptocurrencies is risky because you never know if it will be a profitable investment or not.
5. **Cryptocurrencies Transactions are irreversible:** If you enter an incorrect cryptocurrency address then there is no way to reverse a transaction.
6. **Cryptocurrency storage:-** If the user loses the wallet's private key, it cannot be retrieved. The wallet remains locked along with the number of coins inside. This will result in the financial loss of the user.

A cryptographic token is a digital unit that has a value and does not have its own native blockchain. Blockchain technology has huge potential to build a secure future internet system and also be able to solve big business problems. A blockchain is a digital, decentralized public ledger that has the special ability to record every data transaction exchange on its network. The blockchain network is able to track orders, payments, and more.

Purpose of Cryptographic Tokens

Cryptographic Tokens are tokens that do not have their own native blockchain. Hence, cryptographic tokens exist on the existing blockchain infrastructure. of another cryptocurrency. Therefore owners of cryptographic tokens can use them for purchasing products or they can also be used for trading for making a profit just like other securities. If one wants to create a high-performance token, then there is a need to develop the token on a high-performance blockchain like Ethereum, and then the token runs on a highly secure network and it is also secure from cyber attacks. Tokenization is less expensive in terms of money and time when leverage is existing on decentralized architecture and implementing a consensus mechanism.

Features of Cryptographic Tokens

Below are some of the features of crypto tokens:

- Cryptographic Tokens operate on existing blockchain infrastructure, therefore Cryptographic Tokens are secure.

- It makes payments easier and more secure.
- Cryptographic Tokens are used in a wide range of fields such as trading and investment.
- A cryptographic Token is a cryptocurrency that represents an asset.
- Tokenization is less expensive and time-consuming.

Types of Cryptographic tokens

Different types of cryptographic tokens are discussed below:

1. **Utility tokens:** Utility tokens are user tokens that grant access to users for specific services. For example, When an organization creates a utility token for their customers, it means they create a digital voucher that can be redeemed for discounts or for gaining special access to a service of that organization. There are many Utility tokens that exist in the market like Filecoin, Civic, and many more.
2. **Payment tokens:** Payment tokens are best known as coins. The main purpose of payment tokens is to serve as a medium of exchange of currency. Most cryptocurrencies like Bitcoin are payment tokens. Bitcoin is a digital currency that uses blockchain technology. It was created primarily to speed up cross-border transactions, reduce government control over trade, and simplify the entire process without the need for third-party intermediaries. The absence of intermediaries greatly reduces transaction costs. It uses cryptography to keep it secure. There are no physical bitcoins, bitcoin is a digital currency.
3. **Security tokens:** Security tokens work just like traditional securities. Security tokens are also known as equity tokens. As I said, security tokens are traditional assets that look like stocks and shares of a company or organization, security tokens are handed over to the buyer once the initial token supply ends. security tokens give the holder ownership rights along with sharing in the company stocks.
4. **Defi tokens:** Defi stands for Decentralized Finance. Defi token is a cryptographic token that uses a protocol designed to create a new financial system with the functions same as the old financial system such as lending, saving, trading, etc., by using blockchain technology with the use of smart contacts. For example, instead of borrowing money from a lender, you can borrow money in form of a Defi token from the Defi platform. Defi platforms have their own official currency in the form of tokens and they depend on investors who lend out their crypto funds for lending.
5. **Crypto rewards:** As discussed above, Defi platforms have their own official currency in the form of tokens, and they rely on investors to lend out their crypto funds to borrow. In return, investors gain (profit) crypto rewards. Crypto rewards are usually paid in the form of crypto tokens.
6. **Governance token:** A governance token is a cryptographic token and specialized defi token that gives its holders voting rights for the token's future. Governance token holders can propose and vote on proposals that will help determine the future of that particular cryptocurrency.
7. **Non-Fungible Tokens:** Non-Fungible Tokens (NFTs) are Cryptographic tokens that use blockchain technology. Non-fungible tokens (NFTs) are not a cryptocurrency because non-fungible tokens cannot be used for trading or exchange purposes, it is used as a cryptographic asset.NFTs are uniquely

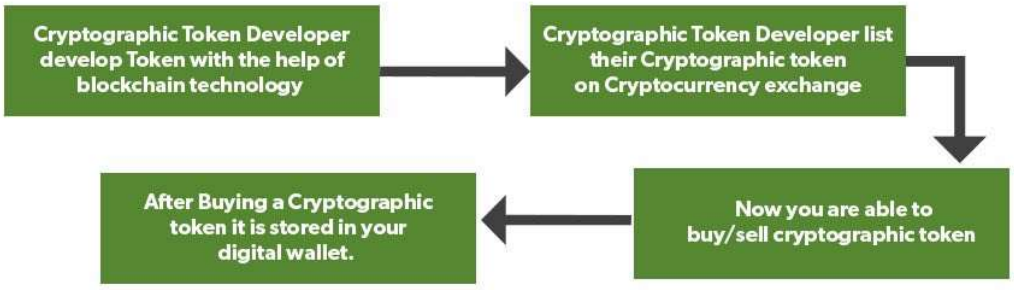
identifiable therefore they are different from most fungible cryptocurrencies such as Bitcoin. Non-Fungible Tokens (NFTs) are associated with digital things like photos, videos, arts, audio, etc.

How do Cryptographic Tokens Work?

Cryptographic tokens are the same as digital currency which is stored in a digital wallet. Below are steps to show how cryptographic tokens work:

1. **Develop Token:** Cryptographic Token Developer develops tokens with the help of blockchain technology.
2. **List Cryptographic Token:** Developers decide when to list their tokens on cryptocurrency exchanges.
3. **Token Available for Buy and Sell:** Any user can now buy a token from a cryptocurrency exchange.
4. **Token stored in Digital Wallet:** After buying a token it is stored in the user's digital wallet.

If one wants to transfer a token to someone else, it "leaves" the user's digital wallet and moves to another person's wallet. If one wants to sell it, the user will get money at the current price of that token in the market. Unlike Bitcoin or other coins, they use a system of public and private keys to facilitate transactions. The exchange with tokens uses a system called "smart contracts". Every blockchain as a token platform has a technical standard that defines smart contracts.



Cryptographic Tokens vs Cryptocurrencies vs Altcoins

To describe cryptocurrencies, the terms like Cryptographic Token, Cryptocurrencies, and Altcoins are used. Below are some points of these terms to help clarify the difference between each.

Cryptographic Tokens	**Cryptocurrencies**	**Altcoins**
Cryptographic Tokens are tokens	A **cryptocurrency** is a digital currency, which uses	**Altcoins** are a different type of cryptocurrency than

Cryptographic Tokens	Cryptocurrencies	Altcoins
that do not have their own native blockchain. Hence, cryptographic tokens exist on the existing blockchain infrastructure. of another cryptocurrency.	cryptography for secure transactions. It is designed to act as a medium of exchange on a computer network without relying on a central authority such as a government or a bank to manage it.	Bitcoin and have different functions. **Altcoins** are like stablecoins, they have the potential to solve problems the same as Bitcoin does in the everyday medium of exchange.
Cryptographic Tokens can be used for trading, storing as an asset, and using as a digital currency.	Since **cryptocurrencies** do not use third-party intermediaries, therefore the exchange of transactions is going to be easy, fast, and secure.	**Altcoin** gives high returns. A wide variety of altcoins exists in the market with their unique uses and for their competitive advantages.
Cryptographic Tokens have value and can be traded, but most important thing is that cryptographic tokens represent a physical asset.	**Cryptocurrencies** traded in the market are subject to price fluctuations.	Buying **altcoins** is not easy as they are only available on certain altcoin exchanges.

Top Cryptographic Token in the Market

Below are some top cryptographic tokens in the market with their market cap according to the year 2022:

- **Tether:** Market cap of Tether is $83,149,403,092
- **USD Coin:** Market cap of USD Coin is $49,044,062,431
- **Binance USD:** Market cap of Binance USD is $17,876,805,072
- **Shiba Inu:** Market cap of Shiba Inu is $11,533,509,510
- **Wrapped Bitcoin:** Market cap of Wrapped Bitcoin is $10,996,787,602 and More.

From where we can get Cryptographic Tokens?

The most common or easy way to get cryptographic tokens is through cryptocurrency exchanges. Cryptographic Tokens Developers decide when to list their tokens on cryptocurrency exchanges. The cryptocurrency exchange market on the Internet is huge. Many cryptographic tokens are often frozen by government regulation or by hacking attacks. One can buy tokens from any cryptocurrency exchange.

PAYMENTS AND DOUBLE SPENDING

Blockchain is a list of blocks. Each block comprises some information associated with some hash. Blockchain is used nowadays widely for transactions. It is an immutable, distributed, and decentralized ledger. The working of Blockchain is as follows. Suppose a user wants

to make a transaction. A block is created and sent to other users. Users validate the block and the transaction gets executed. The block is added and the users get incentives.

Understanding Double Spending

Although Blockchain is secured, still it has some loopholes. Hackers or malicious users take advantage of these loopholes to perform their activities.

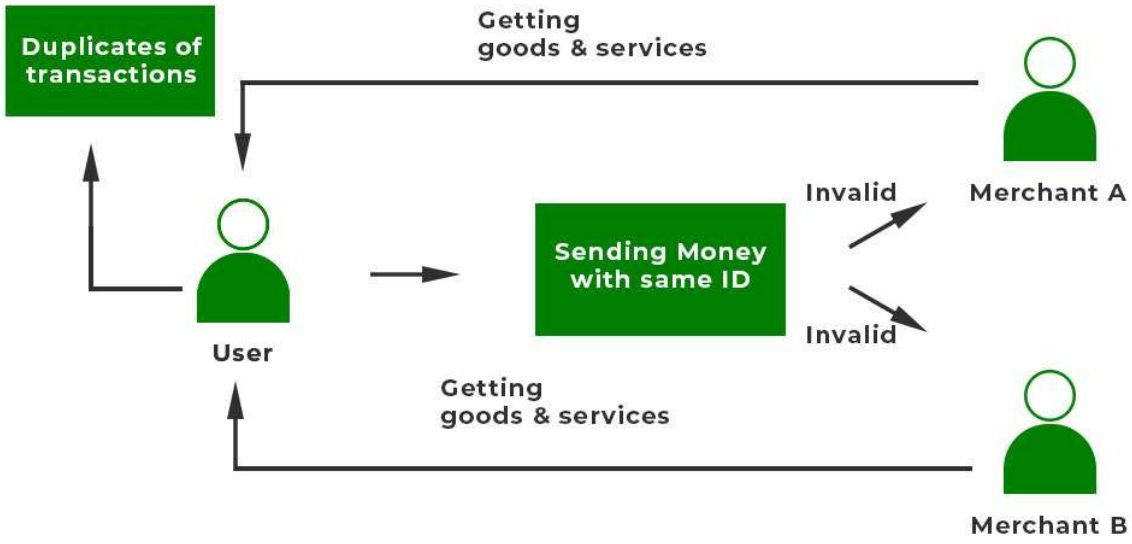
- Double spending means the expenditure of the same digital currency twice or more to avail the multiple services. It is a technical flaw that allows users to duplicate money.
- Since digital currencies are nothing but files, a malicious user can create multiple copies of the same currency file and can use it in multiple places.
- This issue can also occur if there is an alteration in the network or copies of the currency are only used and not the original one.
- There are also double spends that allow hackers to reverse transactions so that transaction happens two times.
- By doing this, the user loses money two times one for the fake block created by the hacker and for the original block as well.
- The hacker gets incentives as well for the fake blocks that have been mined and confirmed.

How Does Double Spending Happen?

Double spending can never arise physically. It can happen in online transactions. This mostly occurs when there is no authority to verify the transaction. It can also happen if the user's wallet is not secured. Suppose a user wants to avail of services from Merchant 'A' and Merchant 'B'.

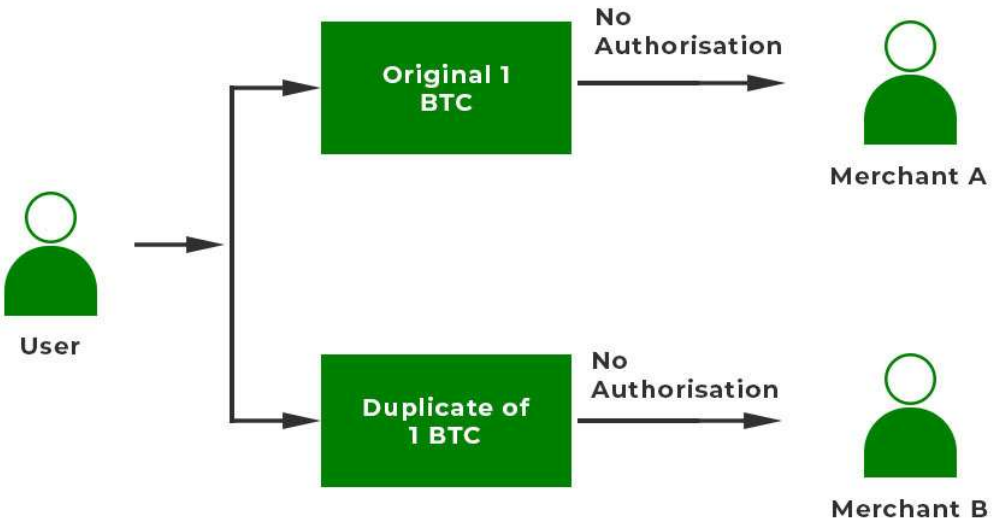
- The user first made a digital transaction with Merchant 'A'.
- The copy of the cryptocurrency is stored on the user's computer.
- So the user uses the same cryptocurrency to pay Merchant 'B'
- Now both the merchants have the illusion that the money has been credited since the transactions were not confirmed by the miners.

This is the case of double spending.



Example: Suppose a user has 1 BTC. He/She wants to avail of services from merchant A and merchant B. The user creates multiple copies of the same BTC and stores it. The user first sends the original BTC to Merchant A and gets the service. Simultaneously, the user

sends the copied version of 1 BTC to Merchant B. Since the second transaction was not confirmed by other miners, the merchant accepts the bitcoin and sends the service. But the cryptocurrency that was sent is invalid. This is the case of Double Spending.



Types Of Double Spending Attacks

There are different types of Double Spending attacks:

- **Finney Attack:** Finney Attack is a type of Double spending Attack. In this, a merchant accepts an unauthorized transaction. The original block is eclipsed by the hacker using an eclipse attack. The transaction is performed on an unauthorized one. After that, the real block shows up and again the transaction is done automatically for the real block. Thus the merchant loses money two times.
- **Race attack:** is an attack in which there is a 'race' between two transactions. The attacker sends the same money using different machines to two different merchants. The merchants send their goods but transactions get invalid.
- **51% Attack:** This type of attack is prevalent in small blockchains. Hackers usually take over 51% of the mining power of blockchain and therefore can do anything of their own will.

How Bitcoin Handles Double Spending?

Bitcoin is one of the most popular blockchains. To combat Double spending it uses some security measures. There are two types of examples of double spending in BTC.

1. The first case is making duplicates of the same bitcoin and sending it to multiple users.
2. The second case is performing the transaction and reversing the already sent transaction after getting the service.

To tackle these double-spending issues, some security measures are taken. They are:

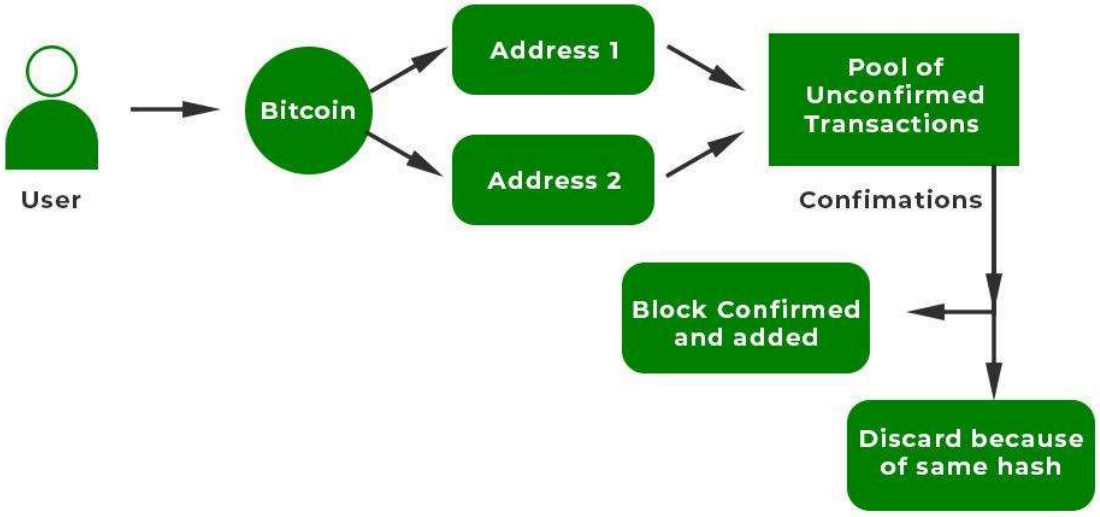
- **Validation:** Validation of transactions by a maximum number of nodes in the network. Once a block is created, it is added to a list of pending transactions. Users send validation for the block. If the verifications are done then only the block is added to the blockchain.
- **Timestamp:** The confirmed transactions are timestamped, therefore they are irreversible. If a transaction is involved with a bitcoin it is verified and done. But

in the future, if other transactions are made with the same bitcoin, the transactions will be canceled.

- **Block Confirmations:** Merchants get block confirmations so that they are assured that there was no case of double spending. In bitcoin, a minimum of 6 confirmations are done.
- **Saving copies:** A copy of each transaction is kept at each node so in case of network failure the whole network does not go down.

These security features have reduced double spending to a large extent. Let us discuss a detailed example of how bitcoin handles double-spending.

- A user wants to spend 2 BTC. He/She can create multiple copies of the same cryptocurrency.
- The user can send the same cryptocurrency to two different addresses say 'Bob' and 'Alice'.
- Both of these transactions are sent to the pool of unconfirmed transactions.
- The first transaction T1 would be approved via the confirmation mechanism.
- The confirmation mechanism states that a minimum of six confirmations by miners should be done for block validation. The block is added to the network.
- However, the second transaction T2 didn't get sufficient confirmation so it would be recognized as invalid by the confirmation process. The block with the highest number of confirmations is accepted and the other one is rejected. So transaction T1 is valid, and Alice received the bitcoin.



Solutions To Prevent Double Spending

Double Spending can be prevented using two approaches: Centralized and Decentralized

- **Centralized Approach:** In this case, a secured third party is employed to verify the transactions. The third-party can track each of the user's balances. Suppose a user makes a transaction. The third-party identifies the transaction with a unique identity. Then it verifies the transaction and allows the transaction. The problem is that suppose we want to make transactions with other countries where a third party is not required. So in such cases, decentralized systems come into play. another drawback is if the whole system fails, the users cannot have access.

- **Decentralized Approach:** This approach is used by Bitcoin. In this, there is no involvement of central authority. Each transaction is verified using powerful algorithms. The decentralized approach proved to be more secure than the centralized approach. Protocols are established and each protocol does its job at each step. Therefore this also promotes transparency.

How to Combat Double Spending?

Double spending has been minimized to a large extent as companies are using many security features. But we as users also have some responsibility so that such attacks don't happen.

- Any user should wait for a minimum of six confirmations of the transaction before performing another transaction. In the blockchain, more the confirmations by different users, lesser will be double spending attacks.
- Users should keep their hardware resources safe so that hackers do not misuse them for their own purposes. Often hackers target the hardware part because the hardware is costly. If they somehow steal the hardware, they can roll back any transaction or alter information.
- Users should delete spam mails and avoid phishing to avoid unnecessary malware attacks Phishing is a very common attack by hackers as hackers target login credentials.
- Software should be updated regularly with the latest antivirus installed. If the software is not up to date then the bugs present can cause major damage.

How Successful Double Spending is Administered?

With the increasing dependency on the blockchain, double spending attacks have also become a major problem. Many companies have adopted security features.

- Features like confirmation of the transaction by the nodes have been adopted. A minimum of six confirmations is required to approve the transaction.
- The blocks once created are immutable. They are made irreversible so that no transaction is reverted back.
- The network's distributed ledger of transactions autonomously records each transaction. Each node has a copy of all transactions that are being done in the network.
- Verification of each transaction's authenticity is done by Blockchain protocols to prevent double-spending. The concept of hashing is adopted. Here each block has a unique hash.

Disadvantages of Blockchain Concerning Double Spending

There are many disadvantages of blockchain concerning Double Spending:

- **Control of the blockchain:** The biggest disadvantage is if the hackers manage to take control of 51% computation power, they can do any transaction of their own will and can steal other users' money. Therefore there is a threat to security as millions and millions of money are involved in transactions.
- **Alteration of information:** Transaction information can also be altered by hackers. They can mine blocks and hide the original blocks using attacks like Eclipse attack, Finney Attack, etc.
- **No authority:** The third major problem is no central authority is present to verify the transactions. But these problems will be eliminated if companies take proper security measures and users are also aware of the measures.

THE PRECURSOR FOR BITCOIN SCRIPTING

Cryptocurrencies have revolutionized the way we think about money and transactions. At the heart of this transformation lies Bitcoin, the pioneer of decentralized digital currency. While many are familiar with Bitcoin as a form of currency, not everyone is well-acquainted with the underlying technology that makes it all possible.

In this article, we'll delve into the fascinating world of Bitcoin Script, a crucial component of the Bitcoin protocol. Whether you're a blockchain enthusiast, a developer, or simply curious about the inner workings of Bitcoin transactions, this guide aims to provide a comprehensive introduction to Bitcoin Script for beginners.

What Is Bitcoin Script?

Bitcoin Script serves as the scripting language behind Bitcoin transactions, allowing users to define the conditions under which funds can be spent. Unlike traditional financial transactions, Bitcoin transactions are not just about transferring value; they are also about executing specific conditions encoded in scripts.

It operates by manipulating items on a stack, with various opcodes representing operations that can be performed. This scripting language is deliberately limited and designed to be non-Turing complete for security reasons, preventing potentially malicious or infinite loops from being executed on the Bitcoin network.

Now, let’s cover some of the finer details about Bitcoin Script.

Evolution of Bitcoin Script

Over the years, Bitcoin Script has undergone evolution and refinement. Its initial design was intentionally kept minimalistic to ensure security and avoid potential vulnerabilities. As the Bitcoin ecosystem has grown, developers and the community have explored ways to enhance the functionality of Bitcoin Script without compromising the network's security and stability.

The evolution of Bitcoin Script reflects the ongoing efforts to strike a delicate balance between providing flexibility and maintaining the robustness of the Bitcoin protocol. Innovations in Bitcoin Script aim to enable more sophisticated transaction types and smart contracts while upholding the core principles of security and decentralization that define the Bitcoin network.

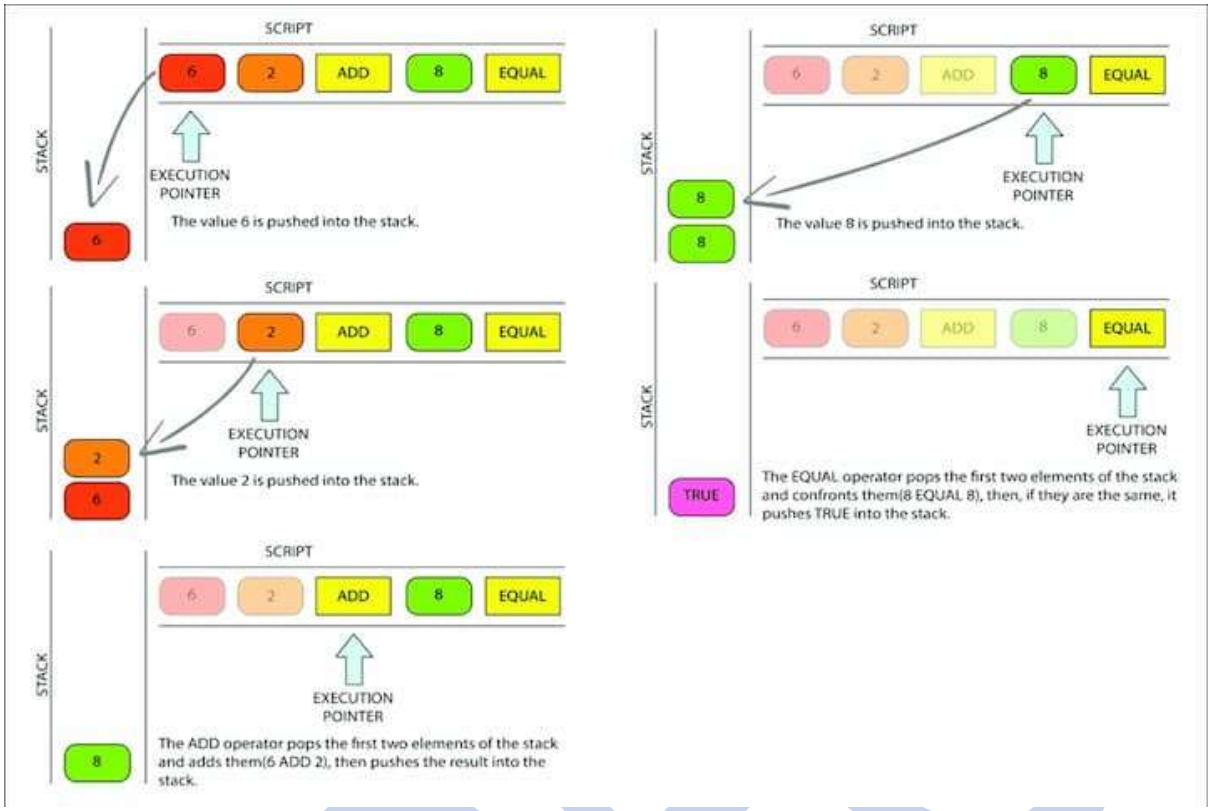
In the next sections, we'll delve deeper into the fundamental components of Bitcoin Script, exploring its stack-based architecture, Forth-like structure, and the intriguing concept of Reverse-Polish Notation (RPN). Join us as we unravel the intricacies of Bitcoin Script, bringing clarity to its role in shaping the world of decentralized finance.

The Fundamentals of Bitcoin Script

Bitcoin Script operates on a set of fundamental principles that shape its functionality. Understanding these fundamentals is key to grasping how scripts are constructed and executed within the Bitcoin network.

Stack-based Architecture

Bitcoin Script employs a stack-based architecture, where data is organized and processed using a Last-In-First-Out (LIFO) structure. The stack serves as a temporary storage mechanism for operands and results of operations, allowing the script to manipulate and operate on these values efficiently. As transactions unfold, the stack dynamically changes, reflecting the state of the script's execution.



Example of how Last In, First Out (LIFO) works with the Stack-based Bitcoin Script

This stack-based approach simplifies the scripting language, making it lightweight and efficient for the specific purpose of enabling conditional spending in Bitcoin transactions. The stack serves as a crucial element in executing various opcodes, each contributing to the overall functionality of the script.

Forth-Like Structure

Bitcoin Script draws inspiration from Forth, a stack-based programming language. This Forth-like structure is evident in the simplicity of Bitcoin Script's design, emphasizing minimalism and efficiency. The script is composed of a series of opcodes, each representing a specific operation that can be performed on the stack.

The Forth-like structure enhances the predictability and security of Bitcoin Script, as each opcode has a well-defined purpose and predictable behavior. This design choice aligns with the goal of creating a secure and robust scripting language for financial transactions on the Bitcoin network.

Reverse-Polish Notation (RPN)

One unique feature of Bitcoin Script is its use of Reverse-Polish Notation (RPN) to express operations. In RPN, operators are placed after their operands, eliminating the need for parentheses and order of operations rules. This notation simplifies the parsing and execution of scripts, contributing to the overall efficiency of Bitcoin Script.

The use of RPN in Bitcoin Script aligns with its commitment to simplicity and clarity. By adopting a notation that reduces ambiguity, Bitcoin Script enhances the readability of scripts and ensures that the execution of transactions follows a clear and predictable path.

Turing Incompleteness

Bitcoin Script is intentionally designed to be Turing incomplete. Turing completeness is a property of a system that can perform any computation that a Turing machine can. While Turing completeness allows for greater flexibility in programming languages, it also introduces potential security risks.

The decision to keep Bitcoin Script Turing incomplete is a deliberate choice to enhance the security and predictability of the Bitcoin network. By limiting the expressive power of scripts, the Bitcoin protocol minimizes the risk of unintended or malicious behavior that could compromise the stability of the entire network.

In the upcoming sections, we'll explore how these fundamental principles of Bitcoin Script come to life in the context of real-world transactions. Join us as we uncover the intricacies of BTC Script in the next installment of our journey into the world of cryptocurrency scripting.

Components of Bitcoin Script

Bitcoin Script is a simple yet powerful scripting language used within the Bitcoin protocol. It's designed to process and validate transactions, ensuring the correct transfer of Bitcoin between parties. The language consists of a series of opcodes that perform specific operations, two primary scripts that handle the locking and unlocking of funds, and a set of rules that govern their execution. These components work together to create a secure and decentralized system that can execute complex conditions for spending bitcoins. Understanding these elements is essential for anyone looking to grasp the functionality and potential of Bitcoin Script.

Now, let’s take a closer look at each of these components, starting with the fundamental operation codes, or OP_CODES, that act as the building blocks of every Bitcoin Script.

Understanding OP_CODE

At the heart of Bitcoin Script are operation codes, commonly known as OP_CODES. These are the basic building blocks of a script, instructing the network on how to process transactions. Each OP_CODE represents a specific operation, ranging from mathematical calculations to data manipulation and transaction validation. They are the equivalent of verbs in a programming language, defining actions that manipulate the stack during the execution of a script. Understanding OP_CODES is crucial because they define the conditions under which a transaction is considered valid and can be added to the blockchain.

scriptSig and scriptPubKey Components

Two fundamental components in the Bitcoin Script universe are scriptSig and scriptPubKey. These two scripts work in tandem across every Bitcoin transaction, ensuring the secure transfer of bitcoins from one party to another.

Role and Function of scriptSig

The scriptSig, or signature script, is used to provide evidence that the transaction initiator has the necessary permissions to spend the bitcoins. It typically contains a digital signature that matches the public key hashed in scriptPubKey of the output being spent. This signature serves as proof that the owner of the private key corresponding to the Bitcoin address in question has authorized the transaction. It's a critical part of the transaction verification process, as it unlocks the bitcoins held in a previous transaction, allowing them to be spent.

Purpose and Structure of scriptPubKey

Conversely, the scriptPubKey is the locking script. Placed within an output, this script specifies the conditions that must be met to spend the bitcoins in the future. It acts as a safeguard, ensuring that only the intended recipient can unlock and claim the bitcoins. This script can encode conditions such as requiring a correct digital signature or even more complex criteria like multisig requirements, time locks, or even the resolution of a cryptographic puzzle. The structure of scriptPubKey can vary depending on the type of

transaction, but its ultimate purpose is to ensure security and control over Bitcoin transactions.

Overview Of Common Opcodes in Bitcoin Script

The following section delves into common OP_CODES in Bitcoin Script, shedding light on their functions and significance in transaction processing.

OP_ADD: Pops two items off the stack, adds them together, and pushes the result back onto the stack.

OP_EQUAL: Pops two items from the stack and compares them to check if they are equal. if they are equal, then it pushes the result TRUE back onto the stack.

OP_RETURN: Can be used to store up to 80 bytes of arbitrary data on the Bitcoin blockchain and also to mark a transaction output as invalid. OP_RETURN transaction outputs are provably unspendable, making this opcode an efficient way to burn BTC. It also makes Komodo's delayed Proof of Work (dPoW) security mechanism possible.

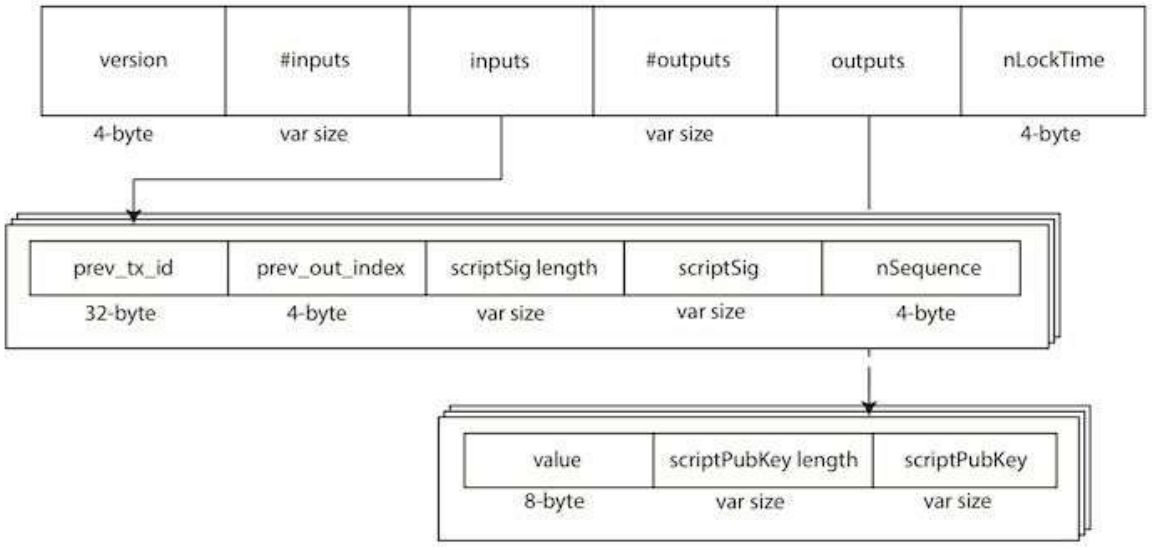
OP_CHECKSIG: Verifies that the signature for a transaction input is valid.

OP_CHECKMULTISIG: Commonly used in Pay To Script Hash (P2SH) transactions. **OP_CHECKMULTISIG** looks at 3 public keys and 2 signatures in the stack and compares them one-by-one. Funds become spendable only when the order of the signatures matches the order in which the public keys were provided.

A full list of opcodes can be found on Bitcoin Wiki.

Bitcoin Script in Transactions

Within each transaction, Bitcoin Script provides the flexibility to implement various types of payment conditions, from the most straightforward to the exceedingly complex. It's the foundation of trust in the Bitcoin network, as it allows for the creation of a decentralized system where trust is not placed in a central authority, but in the cryptographic proofs that the scripts provide. As we explore this section, we will unveil how Bitcoin Script operates within transactions, providing both security and versatility to the network.



Every Bitcoin transaction relies upon a series of inputs and ouputs.

How Bitcoin Script Operates in a BTC Transaction

Bitcoin Script plays a pivotal role in the execution and validation of transactions on the Bitcoin network. It's the underlying mechanism that enforces the rules for spending bitcoins. Every transaction comprises scripts that dictate both the spending conditions and the

fulfillment of those conditions. These scripts ensure that bitcoins can only be spent by the rightful owners and that the network reaches a consensus on the state of the blockchain.

Basics of a Bitcoin Transaction

A Bitcoin transaction is a digital exchange of bitcoins between parties. Each transaction consists of inputs and outputs. Inputs refer to where the bitcoins are coming from, typically referencing a previous transaction's output. Each input contains a scriptSig. Outputs designate where the bitcoins are going and contain a scriptPubKey. When you initiate a transaction, you effectively create a cryptographic puzzle that the recipient's scriptSig must solve in order to spend the bitcoins in the future.

Detailed Look at scriptSig and scriptPubKey in Action

The scriptSig and scriptPubKey are scripts that interact within a Bitcoin transaction to ensure secure transfers. The scriptPubKey lays out the conditions under which the funds can be claimed, and the scriptSig provides the solution to this cryptographic challenge. During the verification process, the scriptSig is executed first, followed by the scriptPubKey. If the final result is true, the transaction is valid, and the funds can be spent; otherwise, the transaction is rejected.

Interacting with Bitcoin Script via Command Line

For those with technical expertise, Bitcoin Script can be interacted with directly via the command line. This interaction involves the creation, analysis, and testing of Bitcoin Script transactions. Bitcoin Core, the reference implementation of Bitcoin, provides a set of RPC commands that allow users to construct transactions manually, inspect their scripts, and broadcast them to the network.

BITCOIN SCRIPT BITCOIN P2P NETWORK

Bitcoin works on top of peer-to-peer network architecture in a completely decentralized manner. It is an Adhoc network with a certain kind of random topology, and on top of that, it runs the bitcoin protocol using the well-known TCP port 8333. All nodes, the bitcoin network users, are treated equally, and new nodes can join the bitcoin network anytime. As it is a permissionless network, users need not authenticate or verify. These are the following activities need to perform for a new join node.

- Open wallet
- Wallet communicates to the seed nodes.
- Seed nodes provide a list of peer nodes addresses
- Ask for the most recent updated blockchain copy
- Accept the blockchain copy, which is received from most peers and the longest chain in the current blockchain.
- Start the transaction procedure.

Table of Contents hide

1 Node Management
2 Operations:
3 Summary
4 References:
5 Share this:
6 Like this:

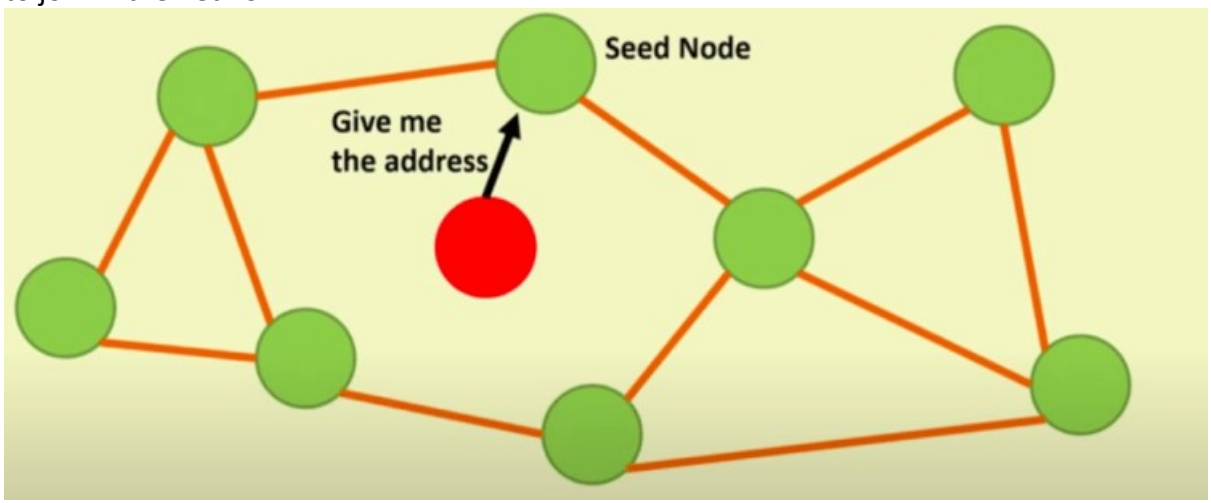
Node Management

Whenever a new node joins the network in such a kind of overlay network, they need to first communicate to the seed nodes. The seed nodes are the special kind of nodes that

keep a database of active peer nodes. As a response, seed nodes provide a list of peer nodes. Further, the new node will randomly select a certain number of peer nodes and peering relationships with those particular nodes.

If the old nodes are not responding for a certain duration in general, it is for three hours; then, seed nodes will remove them from their list. Later, whenever they open their wallet again, they will join the network and participate in some transaction;

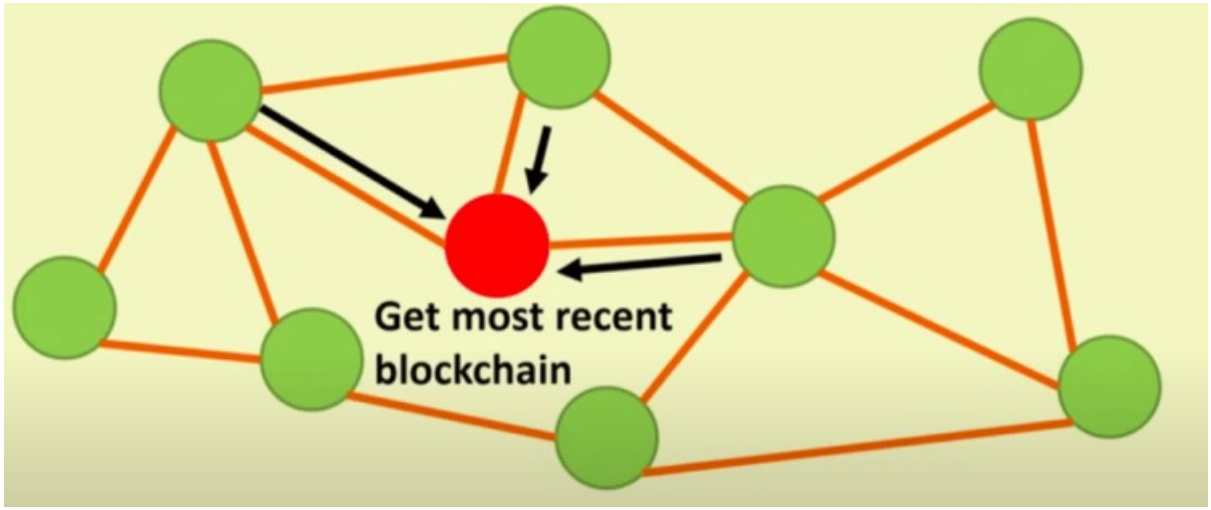
The task of seed node is to provide the initial information to the new nodes who are going to join in the network.



Example of seed node in the network.

Operations:

Once a node joins the network, the first task of a node is to get the most recent blockchain from the peer nodes and update the local copy of the blockchain. It is required as a node may be offline for a certain duration, and as time progresses, blockchain has increased with new transactions.



Get most recent blockchain

Once the peer nodes transfer the most recent blockchain information to the new joint node, It compares the block and accepts the block received from more than 50 percent of peer nodes. The individual nodes must follow this scheme as the entire ecosystem is decentralized, and nodes may collude for malicious intent. In simple words, accept the blockchain copy, which most peer nodes have transferred.

While accepting the blockchain copy, the node also needs to ensure that it only accepts the longest chain in the current blockchain. Once a node receives the most recent copy of the blockchain, it can start the transaction procedure

TRANSACTION IN BITCOIN NETWORK

Bitcoin is basically a digital currency that is currently used as a form of payment. Bitcoin is a cryptocurrency and the transactions related to bitcoins take place in the blockchain network. Every bitcoin is stored in a virtual wallet and transaction involves the transfer of bitcoin from one wallet to another. Bitcoins can be sent from peer to peer irrespective of geographical location without any intermediator in between(for example bank per se). it works in a decentralized way, meaning nobody can interfere with your digital money, only you are responsible for your bitcoins.

Bitcoin Transaction

Bitcoin transaction means sending bitcoin from one person to the other in the secured blockchain network. These are messages that are digitally signed using cryptography and are verified by the miners that are present in the blockchain network. The miner is the person who solves mathematical puzzles(also called proof of work) to validate the transaction. Anyone with mining hardware and high processing power can take part in this. Numerous miners take part simultaneously to solve the complex mathematical puzzle, the one who solves it first, wins 12.5 bitcoin as a reward. miner verifies the transactions(after solving the puzzle) and then adds the block to the blockchain when confirmed. The transaction input is the bitcoin address from which the money was sent, and the transaction output is the bitcoin address to which the money was sent. Generally, a bitcoin transaction takes 10 to 20 minutes to confirm any transactions. if network congestion takes place, then time might take even 60 minutes.

Example: Suppose Hari wants to send 5 BTC(bitcoins) to Senorita.

Input- It consists of the bitcoin address from which hari got his bitcoins previously.

Amount- This deals the specific amount of money that hari wishes to send to senorita, in this case, its 5BTC.

Output- This is the bitcoin address of senorita which hari needs to know in order to transfer the bitcoins to her wallet. Bitcoin address of senorita is also known as public key.

Transaction Fees

The transaction rate or speed is dependent on the amount the user pays for it. If a user pays a small amount, the transaction rate will be slow, the transaction will take more time to happen, vice versa is applicable here. Due to limited space, only a limited number of transactions are possible at one point in time.
Consider a case where heavy network traffic occurs, then the miners prioritize those transactions that have the highest fees so that even in the hectic congestion, the highest-paid transaction gets executed.
Many bitcoin wallets allow users to set transaction fees manually. The fees are directly sent to the miners. When the bitcoin hits a bull run, the transaction fees shoot up to an all-time high. there is no such minimum transaction fee a user must pay, but the highest transaction fees mainly lie between $24 to $31. as the highest-paid transaction gets confirmed first, therefore the fees tend to fluctuate based on the demand of the user.

Why Do Some Bitcoin Transaction Confirmations Take So Long?

Time is taken for transaction confirmation mainly depends on two factors:

- **Transaction fees:** As discussed above, if the user pays minimal transaction fees, then the time taken for confirmation of a particular transaction would take a longer time. the mining process needs significant technology and efforts, therefore the importance of transaction fees comes into play.
- **Network load:** Every transaction gets stored temporarily in the memory pool till the miners confirm it. When the transaction activities reach a certain high threshold, the memory pool gets jammed thereby slowing the confirmation time of the transaction even more. Due to this, all the subsequent transactions become susceptible to delay.

How Bitcoin Transaction Works?

Sending or exchanging bitcoins undergoes lots of procedures underneath. The bitcoin wallet and the network ensures that the digital currency reaches the receiver properly. There are two basic terminologies related to this-

- **Public key:** Also known as a bitcoin address, these are publicly known to all like your username in social media handles. In order to receive bitcoins, the user must share his public key with the other user.
- **Private key:** These are kept secret and must not be shared with anyone, similar to the user's password of social media accounts. Private keys are the most important thing in the whole cryptocurrency concept. The private key allows the user to have access to bitcoins, if the user forgets the private keys, there's no way to recover the bitcoins or the private key. Therefore, it is advised to make a proper backup of the private key in a safe place.

Transaction input is nothing but the address of the sender which gets registered in the network and remains in an encrypted and inaccessible state. Transaction output is the receiver's address which is registered on the bitcoin network.

In the previous example, Hari opens his bitcoin account and signs a transaction detail with his private key, and then broadcasted to a bitcoin network called blockchain, where miners compete with each other to find a hash value called nonce which solves the mathematical puzzle thereby verifying the transaction. The miners create new blocks by abiding by the fact that the transaction volume must be less than 21 million. 21 million is the total number of bitcoins that can be generated. The verified transaction gets a unique identification code and is linked with the previous verified transaction.

In the bitcoin network, every transaction is traceable via linked blocks. Anyone can understand who sent it to who at any point in time. thus, bitcoin works in a transparent manner

Different Types of Bitcoin Address

There are mainly three types of bitcoin addresses:

1. **P2PKH addresses:** These addresses start with number 1. For example 1WX23.
2. **P2SH addresses:** These addresses start with number 2. For example 2WX23.
3. **Bech32 addresses:** These addresses start with bc1. For example bc12WX23.

Internal Vs External Transactions

- An internal transaction is a transaction that doesn't come under any external third party.it works inside the internal function of business thereby doesn't exchange any sort of resources. Internal transaction doesn't have any impact on the cash flow as it deals only with interdepartmental transactions.

- An External transaction is a transaction that comes under any external third party.it basically is an exchange medium between an internal organization and a third party. Since it involves exchange with third parties, it has a huge impact on the cash flow.

How To Send Bitcoin

In order to send or receive bitcoins, one must possess a bitcoin wallet application.

- After installing the bitcoin wallet app, select the type of currency you want to send. For example ethereum, bitcoin, etc.
- Write in the receiver's address.
- Type the amount of bitcoin you wish to send.
- Pay the required transaction fee.
- Press the "send bitcoin" button and the cryptocurrency will be transferred.

How to Receive Bitcoin?

In order to receive bitcoins, do the following steps:

- Open the wallet and click receive.
- Share the public key address. It can be a QR code or a combination of numbers and letters.
- Anyone with a public address can send the cryptocurrency.

BLOCK MINING

Bitcoin Mining is the process of verifying bitcoin transactions and storing them in a blockchain(ledger). It is a process similar to gold mining but instead, it is a computer process that creates new bitcoin in addition to tracking Bitcoin transactions. Let's further study bitcoin and the various concepts related to it.

What is Bitcoin Mining?

Bitcoin mining is a computation-intensive process that uses complicated computer code to generate a secure cryptographic system. The bitcoin miner is the person who solves mathematical puzzles(also called proof of work) to validate the transaction. Anyone with mining hardware and computing power can take part in this. Numerous miners take part simultaneously to solve the complex mathematical puzzle, the one who solves it first, wins 6.25 bitcoin as a part of the reward. Miner verifies the transactions(after solving the puzzle) and then adds the block to the blockchain when confirmed. The blockchain contains the history of every transaction that has taken place in the blockchain network. Once the minor adds the block to the blockchain, bitcoins are then transferred which were associated with the transaction.

For the miners to earn rewards from verifying the bitcoin Transactions, two things must be ensured:

1. The miners must verify the one-megabyte size of the transaction.
2. For the addition of a new block of transaction in the blockchain, miners must have the ability to solve complex computational maths problems called proof for work by finding a 64-bit hexadecimal hash value.

Why Do Bitcoin Needs To Be Mined?

Bitcoin is a digital currency where there are chances of copying, counterfeiting, or double-spending the same coin more than once. Mining solves these problems by making the above illicit activities extremely expensive and resource-intensive. Thus, it can be concluded that it is more beneficial and cost-effective to join the network as a miner than to try to undermine it.

Why Does Bitcoin Needs Miners?

Bitcoin miners are very essential for the smooth functioning of the bitcoin network for the following reasons:

- Miners' job is just like auditors i.e. to verify the legitimacy of the bitcoin transactions.
- Miners help to prevent the double-spending problem.
- Miners are minting the currency. In the absence of miners, Bitcoin as the network would still exist and be usable but there would be no additional bitcoin.

Why Mine Bitcoins?

There are several pros of mining a bitcoin:

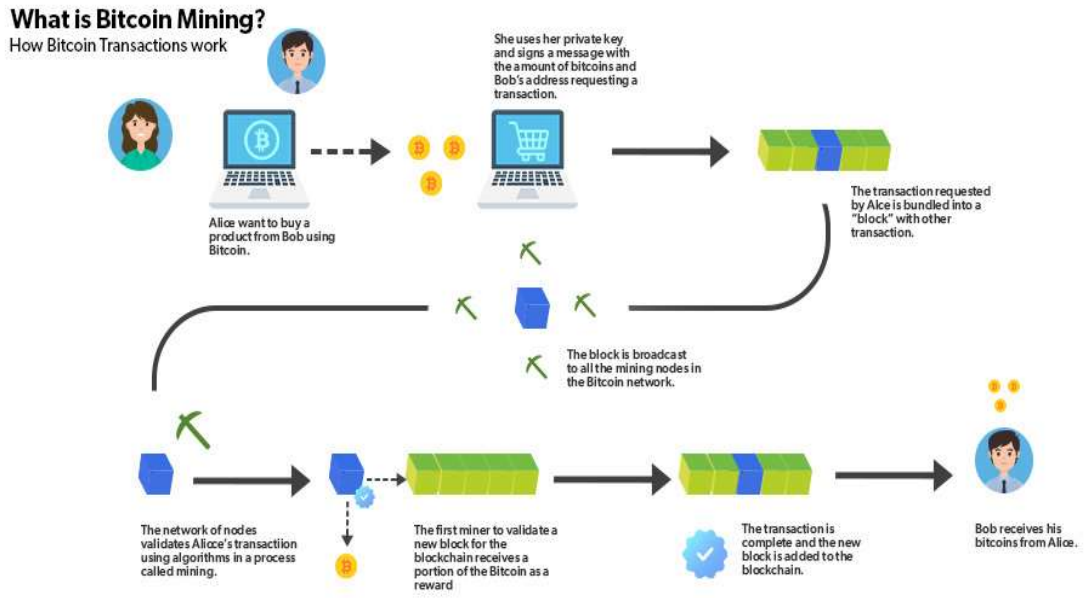
- Mining bitcoin helps support the Bitcoin ecosystem.
- Bitcoin mining helps miners to earn rewards in form of bitcoins.
- It is the only way to release new cryptocurrencies into circulation.
- It is used to check counterfeiting and double spending.

How Does Bitcoin Mining Work?

The nodes of the blockchain network are based on the concept that no one in the network can be trusted. Proof of work is accepted by nodes to validate any transaction. Proof of work involves doing hefty calculations to find a 32-bit hash value called nonce to solve the mathematical puzzle. The miners create new blocks by abiding by the fact that the transaction volume must be less than 21 million. 21 million is the total number of bitcoins that can be generated. The verified transaction gets a unique identification code and is linked with the previous verified transaction.

Let's understand this with the help of an example-

- Suppose Alice wants to transfer 10 BTC to Bob.
- Now the transaction data of A is shared with the miners from the memory pool. A memory pool is a place where an unconfirmed or unverified transaction waits for its confirmation.
- Miners start competing with themselves to solve the mathematical riddle in order to validate and verify the transaction using proof of work.
- The miner who solves the problem first shares his result with other nodes(miners).
- Once maximum nodes agree with the solution, the transaction block is verified and is then added to the blockchain.
- At the same time, the miner who solved the puzzle gets a reward of 6.25 bitcoins.
- Now, after the addition of the transaction block, the 10 BTC associated with the transaction data is transferred to Bob from Alice.



Requirements to Mine Bitcoin

In past, users of the system used to mine bitcoins using their home computers but as the technology has improved, this is no longer the case. The general time a bitcoin network takes to verify a new transaction is 10min. Within that time, there are more than one million miners competing with each other to find the hash value. When there is more computing power working together to mine for bitcoins, the difficulty level of mining increases. Therefore, in order to mine bitcoins, the user must possess-

- Specialized mining hardware is called "application-specific integrated circuits," or ASICs.
- A Bitcoin mining software to join the Blockchain network.
- Powerful GPU (graphics processing unit).

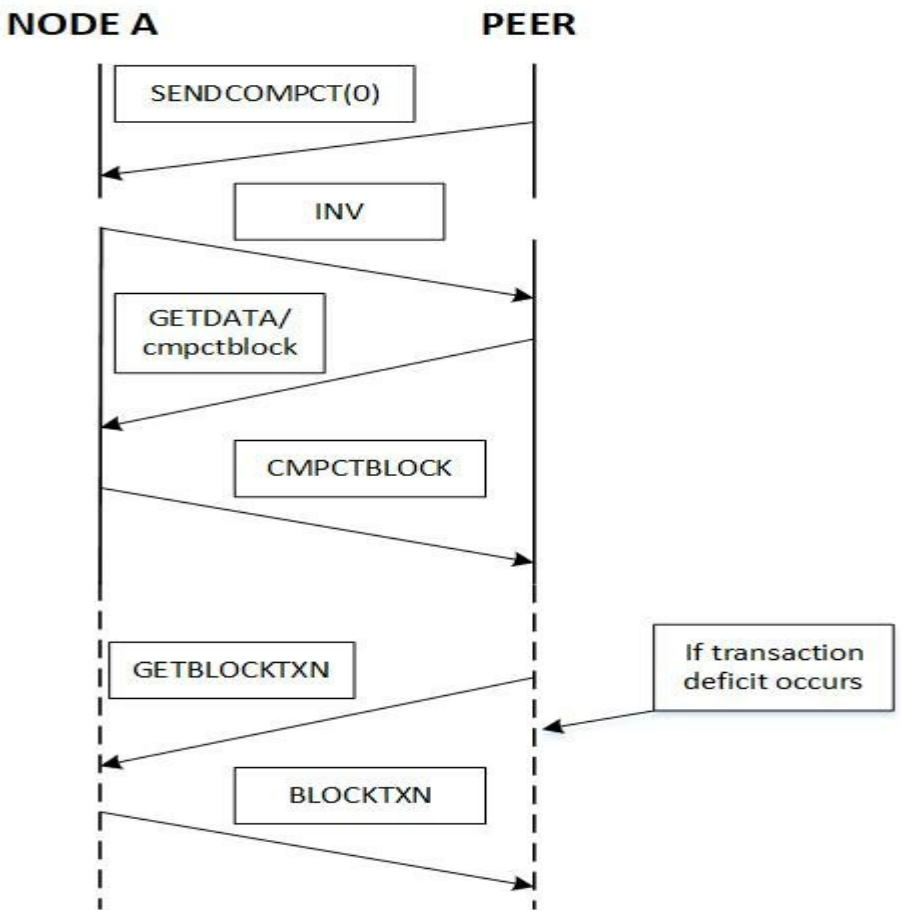
How to Start Mining Bitcoin?

The following steps display the ways to mine bitcoins:

1. **Profit calculation:** One must, first of all, calculate the profit by taking hardware costs, electricity costs, and bitcoin costs into consideration.
2. **Buying the Mining Hardware:** After ensuring the feasibility of mining bitcoins, the user must purchase mining hardware like ASICs.
3. **Mining Software:** For proper access to bitcoin, mining software provides a pathway to join the Blockchain network. There are lots of free mining software available online.
4. **Installing Bitcoin Wallet:** After the user receives bitcoins as a reward for mining, the bitcoins are to be kept in the bitcoin wallet.
5. **Joining a Mining Pool:** This increases the possibility of mining bitcoins efficiently.

BLOCK PROPAGATION AND BLOCK RELAY

Block propagation and block relay are important processes in the functioning of a **blockchain** network. Here is an explanation of these concepts in easy language:



- 1. **Block Propagation**: Block propagation refers to the dissemination of newly created blocks across the blockchain network. When a miner successfully mines a new block, it needs to be quickly shared with other nodes in the network so that they can validate and add it to their copy of the blockchain.
- 2. **Block Relay**: Block relay is the process of transmitting the newly created block from one node to another within the network. It involves sending the block's data and metadata to neighboring nodes or peers in order to propagate it throughout the network.
- 3. **Efficiency and Speed**: Efficient block propagation and relay are crucial for the overall performance and security of the blockchain network. Fast propagation ensures that new blocks are disseminated quickly, reducing the chances of forks and improving the network's consensus mechanism.
- 4. **Peer-to-Peer Network**: Blockchain networks typically operate on a peer-to-peer (P2P) basis, where each node communicates directly with its neighboring nodes. During block propagation and relay, nodes exchange information using a peer-to-peer protocol, ensuring a decentralized and resilient network architecture.
- 5. **Consensus Mechanism**: Block propagation and relay play a significant role in the consensus mechanism of the blockchain network. Nodes need to agree on the validity of each block, and the speed and efficiency of block propagation directly impact the consensus algorithm's performance.
- 6. **Challenges**: Block propagation and relay face challenges such as network latency, bandwidth limitations, and the possibility of malicious actors trying to disrupt the network. Innovations and optimization techniques are continuously being developed to address these challenges and improve the overall efficiency of block propagation.