Cryptocurrency wallets: Hardware Vs Software wallets

	SafePal Hardware wallet	SafePal Software Wallet
Private Key Storage Location	Financial grade EAL5 Chip+ secure element	Users' Cellphone
Wallet Type	Decentralized wallet	Decentralized wallet
Access to internet	No	Yes
Management Tool	SafePal APP	SafePal APP
Import method	Mnemonic phrase	Private Key Mnemonic Phrase Keystore Observation Mode
Passphrase	Supported	Supported
Assets	All of the SafePal supported assets (xx chains and 30,000+ tokens)	All of the SafePal supported assets (xx chains and 30,000+ tokens)

Courtesy : SafePal

- **Mnemonic code words**, based on **BIP-39**
- **HD wallets**, based on **BIP-32**
- **Multipurpose HD wallet structure**, based on **BIP-43**
- **Multicurrency and multiaccount wallets**, based on **BIP-44**

Cryptocurrency Usage

Disadvantages of Cryptocurrency

1. **Cryptocurrency claims to be an anonymous form of transaction**, but they are **actually pseudonymous** which means they leave a digital trail that the Federal Bureau of Investigation can decode.
2. constant risk of a **51% attack**

high computational power.

- **No refund or cancellation policy**
  for transaction gone wrongly or mistake

Cryptocurrency Usage

Are Cryptocurrencies Legal In India?

- are **not regulated or issued by any central authority in India.**
- There are **no guidelines laid down for sorting disagreements while dealing with cryptocurrency**.
- Do trade in crypto, **do it at your own risk**.
- **Till 2022, cryptocurrency was unregulated in the country.**
- This changed after the **government set forth a 30% and 1% tax on profits from cryptocurrencies and tax deducted at source** respectively in the **Union Budget of 2022.** This event marked the **Indian government's official regulation of cryptocurrency in the country.**
- While many supported the decision as it marks the very start of the road to getting cryptocurrency recognition, the **Government of India still has to issue an official note for cryptocurrencies to be considered legal in India.**

Courtesy : Forbes.com

Cryptocurrency Usage

Tax on Cryptocurrency in India

- **most confusing investment aspects** in India.
- In the recent **Union Budget 2022, a tax regime for digital or virtual assets** that include cryptocurrency has been introduced.

1. Crypto investors are required to **keep a well-calculated record of losses and gains as a part of their income.**
2. **On the earnings from the transfer of virtual or digital assets,** a **30% tax will be charged.** The tax includes cryptocurrencies, NFTs, etc.
3. **Cost of acquisition along with no deduction will be permitted** while reporting gains from the transfer of virtual or digital assets.
4. A **tax of 1% on tax deducted at source (TDS) on the buyer's payment if it crosses the threshold limit**.
5. If someone **receives cryptocurrency as a gift or it is transferred then it is subjected to tax at the beneficiary's end.**
6. If **investors face any loss from the virtual or digital asset investment, it cannot be recovered against other income.**

Courtesy : Forbes.com

Transactions in Blockchain

UTXO - Unspent transaction output

- Transaction outputs are **indivisible chunks of bitcoin currency,**
  has to be consumed in its entirety
- Bitcoin full nodes track all available and spendable outputs
- **UTXO set** - The collection of all UTXO
  - set grows as new UTXO is created
  - shrinks when UTXO is consumed.
- find the exact grp of utxo that add up to reqd amt by combining smaller values
- or using a utxo worth more than Xn fee itself
- **Users Bitcoin balance = Sum of all UTXO** in the users wallet can detect in the network.
  1. scanning the Blockchain
  2. aggregating the **value of UTXO that wallet can spent using the keys** it stores.

coinbase first transaction. no utxo.

- **locking script / witness script / scriptPubKey / P2PKH (Pay to Public Key Hash)**

Transaction Serialization

- Process of converting the internal representation of a data structure such that it can be transmitted one byte at a time

Transaction Deserialization / Parsing

- Process of converting byte stream representation of a transaction to internal representation of a data structure

Transactions in Blockchain

Transaction inputs

- identify (by reference) which UTXO will be consumed
- provide proof of ownership through an **unlocking script / Digital Signature**

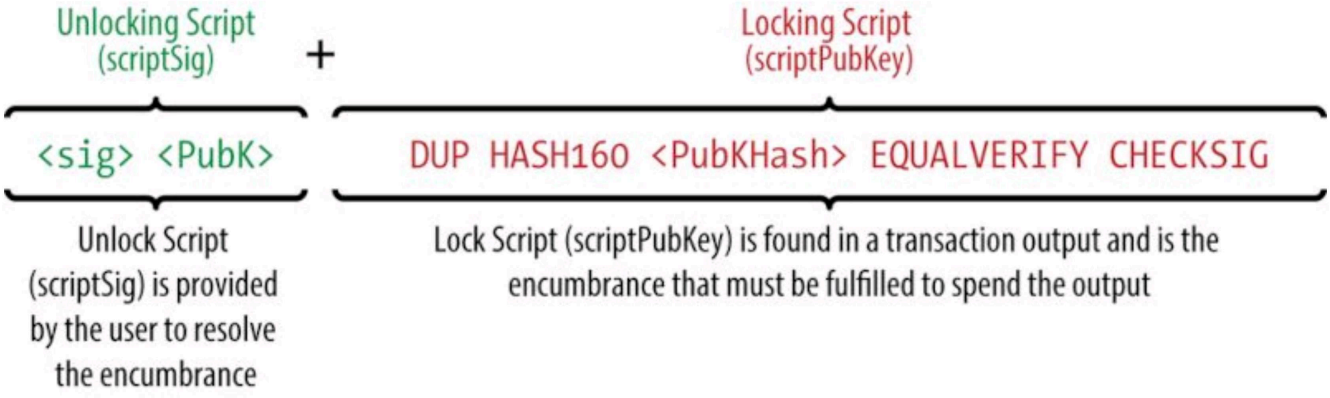
Transaction input contains four elements:

1. A transaction ID, referencing the transaction that contains the UTXO being spent
2. An **output index** (vout), identifying which UTXO from that transaction is referenced (first one is zero)
3. A **scriptSig,** which satisfies the conditions placed on the UTXO, unlocking it for spending
4. A sequence number

Note : Once a transaction is broadcasted, *every validating node needs to retrieve the UTXO reference in the transaction inputs in order to validate the transaction.*

Transactions in Blockchain

Validation - The unlocking script is first copied, then the UTXO that references the input is retrieved, this UTXO consists of a locking script. Both scripts are executed in a sequence. We say the input is valid if the unlocking script satisfies the locking script conditions. Note that a transaction can have multiple inputs, in this case, all inputs are validated independently, this is part of the overall validation of a transaction. Valid transactions satisfying the output conditions are considered 'spent' and removed from the UTXO set



-

- **<u>MinRelayTxFee</u>** (Bitcoin) : Default : **<u>0.00001 BTC</u>**
- If **TxFee < MinRelayFee**
  ⇒ Transaction is free
  ⇒ Relayed only if there is space in mempool / Dropped

CPUs vs GPUs vs ASICs

CPU = Central Processing Unit	General	< 10 MH/s
GPU = Graphics Processing Unit	Specialized	< 1 GH/s
ASIC = Application-Specific Integrated Circuit	Totally Specialized	> 1,000 GH/s

Cloud Mining

Courtesy : Super Data Science

Life of a Miner

ASIC (Application-specific integrated circuits) Miners

- most **effective and powerful mining hardware**
- Manufacturers build these machines with the sole purpose of mining a specific crypto algorithm
- As mining is an intensive and competitive process, it pushes these machines to their **maximum capabilities**.
- The average lifespan of a well-maintained machine : **3 to 5 years**.
- If kept in harsh or poor conditions, they can deteriorate in **a few months**.

Courtesy : Medium, YouTube

Life of a Miner

Common causes for ASIC damage and deterioration are:

1. **Little or no airflow**:
   - ASIC miners release a considerable amount of heat,
   - crucial to keep and run them in a well-ventilated location that keeps air moving and refreshing to avoid overheating.
2. **Humid, damp, or moist environments**:
   - internal components are damaged by humidity, which can cause rust and corrosion.
3. **Extreme temperatures**:
   - can shorten your hardware's lifespan by chipping away its internal components.
   - Cold tends to be less critical, as ASICs release heat that can counter-balance it.
   - Quick swings from below-zero to warm temperatures can cause condensation, provoking irreversible damage.

Courtesy : Medium, YouTube

Life of a Miner

Best practices for preserving ASIC miners

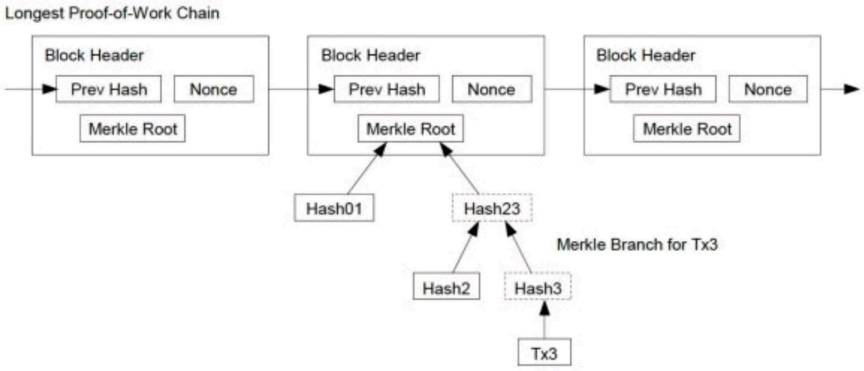
1. **Choosing a suitable location**
   - it must be a **dry** room with good, constant **airflow**, so **wide and open spaces** should be the first choice.
   - consider **installing additional fans** to keep the air moving, maintain the room dry, and avoid condensation.
2. **Mitigating the heat**
   - specialized and advanced cooling systems that reduce temperature,
   - innovative ways to **repurpose the heat produced by ASIC machines**, like heating pools or hot tubs, dehydrating fruit, or redirecting it to greenhouses for growing crops.
     - reduce or even eliminate the damage high temperatures have on miners,
     - enable **increased profitability** either by **reducing costs or adding another source of income**.
     - primary priority is **treating the excess heat** to preserve your miners.
3. **Regular maintenance and cleaning**
   - It is essential to **perform regular maintenance and clean the mining hardware**.
   - Removing accumulated dust not only prolongs lifespan, but also keeps performance high.

Courtesy : Medium, YouTube

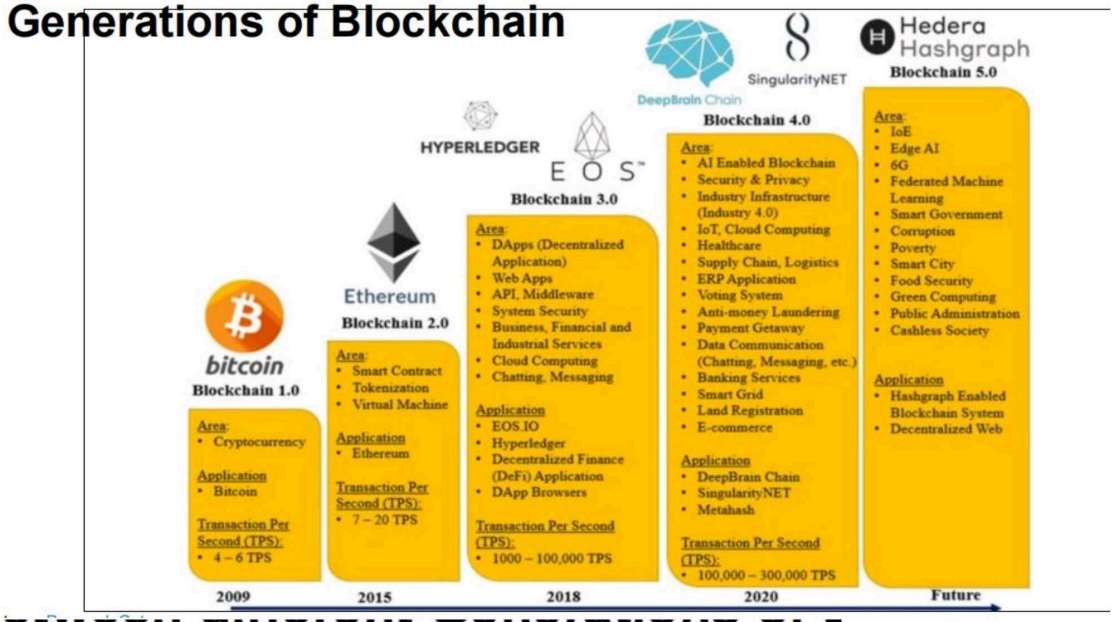
Bitcoin Blockchain- “Bitcoin: A Peer-to-Peer Electronic Cash System”.

Simplified Payment Verification

- Keep a copy of the block headers of the longest proof-of-work chain
- Link the transaction to a space in the chain, if it is accepted by a network, then the transaction is valid
- Vulnerable if the network is overpowered by an attacker



Courtesy : University of Michigan - PPT



Parameter	Blockchain 1.0	Blockchain 2.0	Blockchain 3.0	Blockchain 4.0
Application	Monetary region	Non-monetary region	Commerce platforms	Industry 4.0
Instance	Bitcoin	Ethereum	Cardano, IOTA, Anion	Unibright, SEELE
Energy utilization	Maximum	Reasonable	Power Competent	Very well-organized
Price	Costly	Inexpensive	More Cheaper	Cost efficient
Speed	7 TBS	15 TBS	1000 TBS	1M TBS
Inter communiqué	Not approved	Not approved	approved	approved
Inter operation	No	No	Yes	Highly
Scalability	No	Poor	Scalable	Highly
Verification	Via miners	Via smart contracts	In-built confirmation Via dApps	Sharding Automated confirmation
Consensus mechanism	PoW	Assigned PoW	Proof of stake, authority	Proof of integrity
primary theory	Distributed Ledger	Smart contracts	dApps	Blockchain with AI

bitcoin

Non reversible- as eg. E commerce is
Inflation protection
largest crypocurrency
blockchain 1.0: first virtual currency
pow
why bc: so no 3rd party transaction fees
not issued by govn, acs not managed by banks

stored in digital wallets
offers lower transaction fee compared to traditional online payment methods
currently accepted as a means of payment for products sold or services provided.
BTC
Satoshi Nakamoto is the pseudonymous person or group of individuals who created Bitcoin
Satoshi Nakamoto published a whitepaper titled "Bitcoin: A Peer-to-Peer Electronic Cash System,
Satoshi Nakamoto who first applied the technology of consensus mechanisms in the context of digital currencies.

more than 10k altcoins in existence today
overcome ineff of btc

1. not scalable : if #users increase, transaction proc speed decreases. transaction cost increases. thus less practical for everyday small transactions

2. not energy efficient/ environmental issue: pow uses alot of energy and computational power

to overcome 1. and 2. : altcoin called litecoin.

3. centralization: by large mining pools leads to potential manipulation of the network

4. Lack of Privacy: Bitcoin transactions are pseudonymous, meaning that while wallet addresses are not directly linked to personal identities, transactions can be traced on the public ledger.

.....

1. Project proposal to public: A blockchain-based company can issue a whitepaper, outlining details of its projects, future plans, and issue
size.
2. Fundraising: They can raise funds for that project via an Initial Coin Offering (ICO). by keeping a target
3. which is Similar to an initial public offering (IPO), wherein a firm raises funds by selling its shares to the public.
4. Interested investors can send crytpocurrency to the companies address and receive a new cryptocurrency token issued by the company.
5. This token may have some utility in using the product or service the company is offering.
6. It represent a stake in the company or project.

.....

Liquid: easily convert from asset to coin
The car is like an illiquid asset. If you want to turn it into cash, it takes time and effort to find a buyer, negotiate a price, and complete the sale. It's not something you can easily sell in a hurry without potentially losing some of its value.

The gift card is like a liquid asset. You can quickly use it to buy products at a store or even sell it to someone else for cash without much hassle. It's readily convertible into cash or goods, making it highly liquid.

So, liquidity is about how easily and quickly you can convert an asset into cash or other items of value, with highly liquid assets being easily and quickly convertible, while less liquid assets require more time and effort to convert.

.....

Pros of Bitcoin	Cons of Bitcoin

• The first system of blockchain
  - A success on decentralization
	• Long transaction time
	  ○ Average of 10 mins per block

• Privacy	• Limited throughput
• Hard to modify previous records	
• Transparent	
• Against inflation - Limited throughput	• Large energy consumption

proof of authority
there are a limited number of validators or nodes that have permission to create new blocks and validate transactions.
Relies on their reputation, expertise, or specific criteria set by the network's governance.
limited number of known and trusted validators who take turns creating blocks, private bc

poet
random waiting time lottery based

Poa: activity
After a PoW block is mined, a PoS phase follows, where validators are chosen based on the number of coins they hold or "stake."
pow + pos

dpos
delegated pos : voting + pos
Participants: In a DPoS network, there are two main types of participants:
Delegates (Witnesses): These are individuals or entities elected by token holders to validate transactions and create new blocks. Delegates are responsible for maintaining the network.
Token Holders (Voters): Anyone who holds tokens in the network can vote for their preferred delegates. The number of tokens you hold often determines the weight of your vote.

Tendermint (Byzantine Fault Tolerance): Tendermint combines elements of PoS and Byzantine Fault Tolerance (BFT) to achieve consensus. Validators take turns proposing blocks, and a **two-third**s majority is required for block confirmation.

pbft : practical
dpbft : depived : hyperledger project
rbft : redundant
sbft : simplified

<form id="contactform" action="https://formsubmit.co/put your email here" method="POST">
naked email address= public key

<form id="contactform" action="https://formsubmit.co/unique code or token" method="POST">
unique code= hashed and encrypted form of public key = **bitcoin address**

Incentivization:

1. **Block Reward:** When a miner successfully mines a new block

2. **Transaction Fees:** miners also receive transaction fees for including transactions in the block they mine. Users who want their transactions to be processed quickly may attach transaction fees as an incentive (1. rewards or new coins, 2. Xn fee as in output-input val 3.only Xn fee if inflation max) for miners to prioritize their transactions. Miners typically prioritize transactions with higher fees because it increases their earnings.
Disincentive against abuse or improper use of system. Eg. Chargng Xn fee for all transactions.

3. **Validation and Verification:** Miners validate and verify the transactions within a block they are trying to mine. They ensure that transactions afre legitimate, that the sender has the required funds, and that the transactions follow the network's rules.

.....

inflation: things getting expensive over time

when miners win the golden nonce problem, theyre supposed to get rewards. these rewards are the newly generated cryptocurrency tokens.

creating new tokens as rewards for miners is analogous "printing new notes" irl
only difference being, printing new notes leads to inflation irl while creating new notes controls inflation

thus to avoid inflation, as part of Bitcoin's design, the block reward decreases over time in a process called "halving."
Approximately every four years, the block reward is cut in half.

Initially, when Bitcoin was created, block reward : (50 bitcoins per block).
after the first halving, it became 25 bitcoins per block, then 12.5 bitcoins, and so on.

The gradual reduction in block rewards is designed to limit the creation of new cryptocurrency tokens and control inflation within the network. Eventually, the block reward will become so small that it will approach zero, and the total supply of tokens will reach a predetermined maximum limit (in Bitcoin's case, 21 million bitcoins). This means that there will never be more than 21 milllion bitcoins in existence.

When the block reward reaches zero, there will be no new bitcoins created as rewards for miners. At that point, miners will rely solely on transaction fees as their incentive for securing the network. It's worth noting that the Bitcoin network will continue to operate even after the block reward reaches zero, as transaction fees will provide miners with compensation for their work.
With a limited and decreasing supply of new tokens, there is less potential for excessive token inflation.
price Dynamics: The principles of supply and demand come into play. As the supply of new tokens decreases over time, the value or price of each token may increase if demand remains constant or grows. This price increase can offset the impact of inflation, as each token becomes more valuable.

users want to get their work done
Users create and sign cryptocurrency transactions using their wallets. These transactions include information such as the sender's address, recipient's address, the amount to be transferred, and a transaction fee.
These transactions are sent to mempools

If a transaction is not **relayed** into the mempool, it means that the transaction was not accepted by any of the nodes on the network and, as a result, did not enter the pool of unconfirmed transactions (mempool) where it would wait to be included in a block.

Here are some common reasons why a transaction might not get relayed into the mempool:

- Invalid Transaction: The transaction may be invalid, either due to insufficient funds, incorrect recipient addresses, or other reasons that make it fail the validation checks of network nodes. Invalid transactions are typically rejected and not relayed.
- Low Transaction Fee: Some blockchain networks prioritize transactions with higher fees to incentivize miners to include them in the next block. If a transaction has a very low or no transaction fee, it may not get relayed because miners may not find it profitable to include in a block.
- Double Spending: If the transaction attempts to double-spend a cryptocurrency (spend the same coins more than once), nodes will reject it, preventing it from entering the mempool.
- Node Policies: Individual nodes may have specific policies or rules set by their operators that cause them to reject certain transactions. For example, a node may block transactions from specific addresses or with certain characteristics
- Network Issues: Occasionally, network issues or connectivity problems can prevent transactions from being successfully relayed.
- Congested Mempool: In some cases, the mempool itself may be congested with a large number of pending transactions. When this happens, some transactions may not immediately enter the mempool and could be delayed.

the transactions are broadcasted to all nodes

Miners construct a block by including a set of transactions from the collective mempool. They collectively create one block by selecting transactions.
Miners collect a set of pending transactions from the mempool that they want to include in the next block. They then construct a new block, which includes these selected transactions.
Miner Selection: Miners monitor the collective mempools of the network, not just the mempool of a specific node. They select transactions from the combined set of transactions from mempools across all nodes in the network to create a block.

Miners select what transactions to be added into their blocks (which will be added only when transactions are accepted) based on transaction fees, see if it isnt already spent, basically validate the transactions. Gas fee is paid by users to compensate for the computing energy required to process and validate transactions.
They also include a special transaction called the "coinbase transaction,"
After selecting a transaction, theyre added into blocks.
a block contains multiple transactions bundled together. These transactions can come from various users and involve different transfers of cryptocurrency or other digital assets.
Miners construct a candidate block that includes the selected transactions and a reference to the previous block in the blockchain. They then apply the PoW process by repeatedly changing a value known as the "nonce" in the block's header and calculating the block's hash until they find a nonce that results in a hash meeting certain criteria (usually having a specific number of leading zeros).

Miners pick transactions to include in the blocks they mine based on several factors, with the primary consideration being the potential transaction fees they can earn. Here's how miners typically select transactions:

1. **Transaction Fees:** Transactions on a blockchain network often include a transaction fee paid by the sender to incentivize miners to include the transaction in a block. The higher the fee, the more attractive the transaction is to miners. Miners prioritize transactions with higher fees because they can earn more from including them.

2. **Transaction Size:** Transactions vary in size, depending on the number of inputs and outputs involved. Larger transactions require more data storage in blocks and, consequently, more computational effort to mine. Miners may prioritize smaller, more efficient transactions over larger ones to maximize block space utilization.

3. **Transaction Age:** Some miners may prioritize older transactions in the mempool, giving preference to transactions that have been waiting longer to be confirmed. This practice is known as "first-in, first-out" (FIFO) or "priority" selection.

4. **Block Space:** Each block on the blockchain has a limited size (e.g., 1 MB for Bitcoin). Miners aim to maximize the use of this block space to maximize their earnings. They select transactions that collectively offer the highest total transaction fees while still fitting within the block size limit.

5. **Mining Strategy:** Some miners may have specific strategies or preferences for transaction selection. For example, they might prioritize transactions from certain users or services, or they may choose transactions based on the perceived value of the transactions themselves.

6. **Network Conditions:** Network conditions, including mempool congestion, can influence transaction selection. During times of high network activity, miners may prioritize transactions with significantly higher fees to ensure quicker confirmation.

7. **Inclusivity:** Miners typically aim to be fair and inclusive by selecting a mix of transactions with varying fee levels. This approach helps maintain a competitive and balanced transaction market.

It's important to note that the specific criteria and strategies used by miners can vary between individual miners and mining pools. Additionally, miners must adhere to the network's consensus rules and validation criteria, ensuring that selected transactions are valid and adhere to the network's rules.

Overall, the goal of miners is to maximize their earnings while also serving the interests of users by confirming transactions efficiently and fairly. As a result, transaction selection is a dynamic and competitive process within the blockchain network.

In blockchain technology, a "mempool" (short for "memory pool") is a critical component of the network that temporarily stores pending transactions before they are included in a new block and added to the blockchain.

1. **Transaction Submission:** When a user initiates a cryptocurrency transaction, such as sending bitcoins, they broadcast it to the blockchain network. The transaction includes details like the sender's address, recipient's address, the amount to be transferred, and a transaction fee (a small amount paid to miners as an incentive to include the transaction in a block).

2. **Mempool Entry:** Upon receiving the transaction, nodes on the blockchain network validate it to ensure it meets the network's rules and security requirements. If the transaction is valid, it is temporarily placed in the mempool of the node that received it.

3. **Mempool Storage:** The mempool is essentially a pool of unconfirmed or pending transactions stored in a node's memory. Each node on the network maintains its own mempool. The transactions in the mempool are kept in a queue, ordered by various factors, including transaction fees.

4. **Transaction Priority:** Transactions with higher transaction fees are typically given higher priority in the mempool and by the miners too

5. **Mining and Inclusion:** Miners continuously monitor the mempools across the network to select transactions for inclusion in the next block they are trying to mine. They typically prioritize transactions with higher fees because they can maximize their earnings by doing so.

6. **Confirmation:** Once a miner successfully mines a new block, they include a selection of pending transactions from the mempool into that block. These transactions are considered "confirmed" and are added to the blockchain. The confirmation process provides a record of the transaction's validity and inclusion in the ledger.

7. **Mempool Dynamics:** The size and contents of the mempool can vary over time. During periods of high network activity, the mempool can become congested with a large number of pending transactions. In such cases, users who want their transactions to be processed quickly often attach higher fees to incentivize miners to prioritize their transactions.

8. **Transaction Removal:** Transactions that remain unconfirmed in the mempool for an extended period without being included in a block may eventually be removed from the mempool. Different nodes may have different policies for mempool management.
congestion.

These are the two primary instances of consensus in a blockchain network.

- What transactions to add in a block
- Whether the winner is valid

……..

utility tokens
tokens = programmable assets that buys services. same as coins

security/equity: tokenized assets offerred on stock markets

asset tokens:
An asset token is like a digital certificate that represents ownership of something valuable, such as a piece of real estate (like a house) or a piece of art.

Imagine you have a valuable painting, and instead of having a physical certificate that says you own it, you have a digital token on your computer or smartphone that proves you own the painting.
Each token represents a fraction of the painting's value, and you issue a certain number of these tokens.

1. Share Ownership: You can easily sell a part of the painting by transferring some of these digital tokens to someone else.

2. Split/ fractional Ownership: Many people can own a small piece of the painting by holding a certain number of these digital tokens.

3. Trade/ ownership transfer : You can quickly trade these tokens with others who want to buy or sell a part of the painting. Instead of going through the lengthy and cumbersome process of transferring physical ownership documents, you can transfer these asset tokens digitally to the buyer's digital wallet

4. Keep Records: All transactions with these tokens are recorded on a digital ledger (like a digital book), making it clear who owns the painting at any given time.

5. liquidity high since asset tokens can be easily traded.
In simple terms, asset tokens make it easier and more convenient to own, share, and trade valuable things like real estate or art using digital certificates instead of paper documents.

Stablecoins

tries to keep its value steady, unlike other cryptocurrencies like Bitcoin, which can have big price swings. They do this by either being backed by real assets like regular money or using computer programs to manage their supply. People use stablecoins for

things like buying and selling other cryptocurrencies, protecting their money from inflation, and making smart contracts work more reliably. It's like having digital money that doesn't jump up and down in value all the time.

Memecoin:
Shiba inu dog : meme
Pokemon cards: nostalgia
Novelty souvernier , collectible item. Imagine a limited-edition toy
created more for humor or satire rather than as a serious digital asset or investment.
Lack of Serious Utility
Community-Driven:
High Volatility: Their value can fluctuate wildly, trends
short lived hype
risk.. can decrease in price as soon as they rise

Governance tokens
decentralized autonomous organizations (DAOs)
These tokens are designed to allow holders to participate in the decision-making process, democratic

- **Voting Rights:** Holders of governance tokens typically have the right to vote on proposals or decisions that affect the blockchain network or DAO.

- **Delegated Voting:** In some cases, token holders can delegate/transfer their voting rights to others, allowing experienced or knowledgeable individuals or entities to vote on their behalf.

- whether to implement a new feature
- change transaction fees
- adjust network parameters.
- allocation of resources.
- Token holders may receive rewards or staking incentives for voting or for actively engaging in governance decisions.

Each token usually represents one vote, and the outcome of proposals is determined by majority or supermajority consensus.

coins
- native currency
- independent
- btc eth

tokens
- customizable
- built on existing bc
- erc
- eg. Every time you make a purchase, McDonald's gives you tokens or loyalty points based on the amount you spend. The more you buy, the more tokens you collect.
- u can spend these tokens at any mcdonalds store. but it wont work outside it. to use it outside, ull have to encash them from mcd itself

BUS STATION ANALOGY FOR TRANSACTIONS
The bus station analogy for transactions in blockchain goes like this:

Imagine a busy bus station where people are constantly arriving and departing. Each person represents a transaction in the blockchain network. These transactions are like passengers getting on and off buses, each with a unique destination.

Here's how the analogy relates to blockchain transactions:

1. **Passengers (Transactions):** Passengers at the bus station represent individual transactions in the blockchain. Each passenger (transaction) has a specific purpose or destination.

2. **Buses (Blocks):** Buses waiting at the station are like blocks in the blockchain. Transactions (passengers) are grouped together and loaded onto buses (blocks) to be processed and added to the blockchain.

3. **Bus Routes (Consensus Rules):** Bus routes represent the consensus rules of the blockchain network. Buses (blocks) follow specific routes (consensus rules) to ensure that all passengers (transactions) reach their destinations correctly.

4. **Departure Schedule (Block Time):** The departure schedule for buses is similar to the block time in a blockchain. Buses (blocks) depart at regular intervals, picking up passengers (transactions) during each trip.

5. **Ticket Validation (Validation Process):** Before boarding a bus, passengers must have valid tickets. In the blockchain, transactions go through a validation process to ensure they meet network rules before being added to a block.

6. **Arrival and Departure Records (Transaction History):** The bus station keeps records of when passengers arrive and depart. In blockchain, transactions are recorded in chronological order to create a transaction history.

7. **Bus Station Management (Node Operators):** The bus station is managed by station personnel, just as blockchain nodes are operated by node operators who validate and process transactions.

8. **Traffic Control (Consensus Mechanism):** To maintain order and prevent accidents, the bus station has traffic controllers. In blockchain, the consensus mechanism ensures that transactions are processed correctly and securely.

Unconfirmed Passengers (Unconfirmed Transactions): Passengers (users) whose buses (transactions) have not yet departed are still waiting in the station (mempool). These are unconfirmed transactions

Priority Boarding (Transaction Fees): Passengers can choose to pay extra (transaction fees) to get priority boarding (quicker confirmation) on the next available bus (block). Miners often prioritize processing transactions with higher fees.

Bus Departures (Block Confirmation): When the departure time (block time) for a bus (block) arrives, it leaves the bus station (gets added to the blockchain). Multiple buses can depart together in a group (block), and this is known as a block confirmation

Mempool (Ticket Counter): At the bus station, there is a ticket counter where passengers line up with their tickets. Similarly, in the blockchain, there's a mempool where transactions wait to be included in the next available block. The mempool is

like a queue where transactions are temporarily held before they can board the next bus (block).

Every bus will leave after 10 minutes the prev bus has left in btc world

Potential Privacy Risks: Although HD wallets enhance privacy by generating new addresses for each transaction, blockchain analysis can still reveal patterns of activity. Advanced techniques might be used to link multiple addresses to a single user.

51% attack
controls more than 51% of the total computational power (hashrate) of that network.
potentially reverse recent transactions,
With more than 51% control, they can manipulate transaction records, making it possible to double-spend cryptocurrency (essentially spending the same coins twice).
They can exclude or censor transactions from being confirmed, slowing down or stopping normal network activities.

altcoins not very popular, options to choose from, smaller market, difficult to determine usecase.
eg. subway surfer coins... can be used in game.

cryptocurrency exchanges, allows users to exchange them for fiat currency if they wish to "cash out"
token to coin possible conversion.

.....

analogy of a treasure chest

1. **The Treasure Chest (Bitcoin Address):** Think of the treasure chest as a Bitcoin address where you've stored some cryptocurrency. It's locked, and you want to make sure only the right person can access it.

2. **The Lock (Transaction Input):** To open the treasure chest and spend the Bitcoin inside, you create a transaction input, which is like a lock that needs to be opened. This input has two parts: the locking script and the witness data.

3. **The Locking Script (Witness Script):** The locking script is a set of rules that defines the conditions someone must meet to open the lock (spend the Bitcoin). For

example, it might require providing a valid digital signature or fulfilling certain conditions specified in the script.

4. **The Key (Witness Data):** To open the lock (transaction input), someone needs a key (witness data) that matches the conditions set by the locking script. This key could include digital signatures or other information required by the script.

5. **Unlocking the Chest (Validating the Transaction):** When someone wants to spend the Bitcoin from your address, they create a transaction with the necessary input, including the locking script and witness data. The network checks whether the witness data correctly satisfies the conditions specified in the locking script. If everything matches, the transaction is valid, and the chest (Bitcoin address) can be unlocked, allowing the funds to be moved.

In this analogy, the witness script is like the set of rules that define how the lock (transaction input) must be opened to access the treasure (Bitcoin). The witness data is the actual key that proves the person trying to spend the Bitcoin has met the conditions set by the witness script. This separation of rules (witness script) and proof (witness data) helps improve the security and efficiency of Bitcoin transactions, just as in the real-world example, the rules for opening a treasure chest are separate from the actual key required to open it.

The difficulty target is a numerical value that is used to determine the level of difficulty for miners. It is a 256-bit number in the case of Bitcoin. Miners must find a hash (a long string of numbers and letters) for a new block that, when hashed, produces a value lower than or equal to the current difficulty target. The difficulty target is set by the network's rules and adjusts periodically.

Number of Zeroes: The difficulty target is often represented in hexadecimal format, which includes both numbers and letters. When you convert this hexadecimal target to binary, you get a string of 0s and 1s. Miners aim to find a hash that, when interpreted in binary, starts with a certain number of leading zeroes. The more leading zeroes required, the lower the target value and the higher the difficulty.

Difficulty Adjustment: The network adjusts the difficulty target periodically (typically every 2,016 blocks in Bitcoin)or 10 minutes per block, 2 weeks
the difficulty increases by making it harder to find a hash with the required number of leading zeroes. If blocks were mined slower, the difficulty decreases to make it easier.

Miners change the nonce value in the block header, and then they recompute the hash of the entire block (including the nonce and maybe after manipulating timestamp and other fields) using a cryptographic hash function (such as SHA-256 in the case of Bitcoin). They repeat this process over and over again until they find a hash that meets the current difficulty target.

The nonce serves as a form of randomness that miners can manipulate to generate different hash outputs. By trying different nonce values within the nonce range, miners increase their chances of finding a hash that meets the criteria (e.g., has a certain number of leading zeroes) required by the network's difficulty target.

One nonce range isnt enough. Since more competition, limited number of nonces

highway (bc nw)
toll booths limited (blocks). after every 10 minutes 1 toll booth
lots of buses (Txn)
traffic jam and delay (congestion)

this congestion leads to high fees and slow confirmation times as users compete to get their transactions processed quickly.

soln: **SegWit - segregated witness - optimuzation for digital signature**
Instead of paying at the booth, drivers can prepay their tolls, reducing the time it takes to pass through the booth
60% the percentage of transactions or blocks that are SegWit-enabled.

in this new system, the payment data (fast track previously, witness data) is separated from the car itself (transaction data). This separation allows more cars to flow through the toll booths quickly because the payment process is streamlined.

A smart contract is a self-executing computer program that automatically enforces and executes the terms of an agreement or contract when predefined conditions are met. It runs on a blockchain and eliminates the need for intermediaries, ensuring trust and transparency in digital transactions.

- self executing
- code based
- tamper proof : Once deployed on a blockchain, smart contracts are immutable and secure. They cannot be altered, deleted, or tampered with, providing a high level of trust and transparency.

- **Oracles**: Smart contracts may require external data to function. Oracles are trusted data sources that provide real-world information to smart contracts, enabling them to make informed decisions.
- Software Oracles: These are software-based oracles that retrieve data from publicly available sources on the internet, such as websites, APIs, or data feeds. They are often used for obtaining real-time information like weather updates, stock prices, and sports scores.

- Hardware Oracles: Hardware oracles are physical devices that connect the blockchain to the real world. They can collect data from the physical environment using sensors and feed this data into smart contracts. For example, an IoT device measuring temperature can serve as a hardware oracle for a supply chain smart contract.

- Consensus Oracles: Consensus oracles obtain data from multiple sources and provide a consensus or aggregated result. They help mitigate the risk of incorrect or manipulated data by relying on a majority or predefined algorithm to determine the final data point.

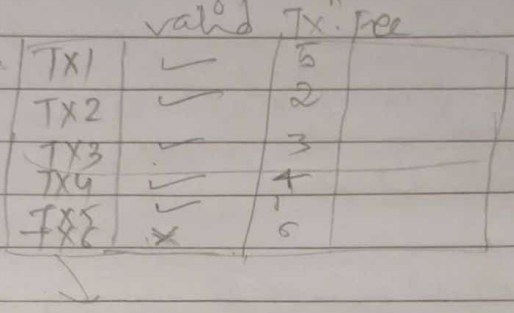
- Anonymous Oracles: These oracles prioritize user privacy by allowing data providers to remain anonymous. They use cryptographic techniques to ensure data integrity while protecting the identity of the providers.

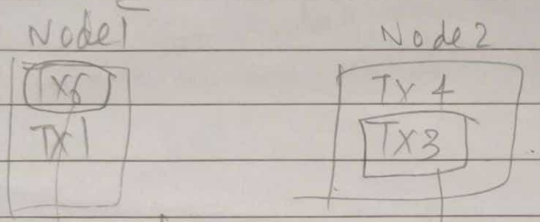
- Authenticated Oracles: Authenticated oracles require data providers to prove their authenticity or reputation before providing data to the blockchain. Users must stake tokens or follow specific verification processes to become data providers.

User A ↓ Tx1 Tx2

User B Tx3 Tx4

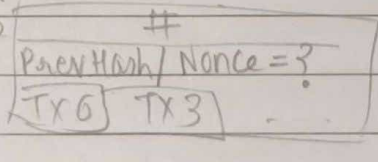
User C Tx5 Tx6





selected for it.

to be in block



Block created ✓ using Consensus.
but nonce field empty

∴ node1 node2 , . . .

Compete to find it

the one who gets it right, gets to add the block into bc