BLOCKCHAIN TECHNOLOGY

Consensus protocol –

- ✓ Consensus decision-making is a group decision-making process in which group members develop, and agree to support a decision in the best interest of the whole.

- ✓ Basically, it states that the longest valid chain in the Blockchain network should exist on every node in the Network. Blockchain is a distributed decentralized network that provides immutability, privacy, security, and transparency.

- ✓ There is no central authority present to validate and verify the transactions, yet every transaction in the Blockchain is considered to be completely secured and verified.
- ✓This is possible only because of the presence of the consensus protocol which is a core part of any Blockchain network.

- ✓A consensus algorithm is a procedure through which all the peers of the Blockchain network reach a common agreement about the present state of the distributed ledger.

Consensus protocol –

- ❑ Consensus is a process of ensuring that all the different users in a blockchain come to an agreement regarding the current state of blockchain.

- ✓In this way, consensus algorithms achieve reliability in the Blockchain network and establish trust between unknown peers in a distributed computing environment.

- ✓ Essentially, the consensus protocol makes sure that every new block that is added to the Blockchain is the one and only version of the truth that is agreed upon by all the nodes in the Blockchain.

- ✓ The Blockchain consensus protocol consists of some specific objectives such as coming to an agreement, collaboration, co-operation, equal rights to every node, and mandatory participation of each node in the consensus process.
- ✓ Thus, a consensus algorithm aims at finding a common agreement that is a win for the entire network.

- ❑ Various consensus algorithms and how they work.:

- ❑ Proof of Work (PoW):

- ✓ This consensus algorithm is used to select a miner for the next block generation.

- ✓ Bitcoin uses this PoW consensus algorithm.

- ✓ The central idea behind this algorithm is to solve a complex mathematical puzzle and easily give out a solution.

- ✓ This mathematical puzzle requires a lot of computational power and thus, the node who solves the puzzle as soon as possible gets to mine the next block.

- ❑ Various consensus algorithms and how they work.:

- ❑ Proof of Stake (PoS):

- ✓ This is the most common alternative to PoW.
- ✓ Ethereum has shifted from PoW to PoS consensus.

- ✓ In this type of consensus algorithm, instead of investing in expensive hardware to solve a complex puzzle, validators invest in the coins of the system by locking up some of their coins as stake.

- ✓ After that, all the validators will start validating the blocks.

- ✓Validators will validate blocks by placing a bet on it if they discover a block which they think can be added to the chain.

- ❑ Various consensus algorithms and how they work.:

- ❑ Proof of Stake (PoS):

- ✓ Based on the actual blocks added in the Blockchain, all the validators get a reward proportionate to their bets and their stake increase accordingly.

- ✓ In the end, a validator is chosen to generate a new block based on their economic stake in the network. Thus, PoS encourages validators through an incentive mechanism to reach to an agreement.

Proof of Work(Pow): Basic introduction:

- ✓This idea was first proposed by Dwork and Naor (1992) to combat junk emails. To discourage the attacker from sending junk emails, the sender had to do some work for the validation of email.
- ✓The work is given by Service provider to the Service requester. This work is moderately hard but feasible for the requester and is easy for the provider to validate.
- ✓The puzzle friendliness property of cryptographic hash functions make them useful to be used as PoW.
- ✓Most implementations of Bitcoin PoW use double SHA256 hash function.
- ✓The probability of getting a PoW is low.
- ✓It is difficult to say which miner will be able to generate the block. Hence, no single miner will be able to control the network.

Proof of Work (PoW) :

- ✓Proof of Work (PoW) is a blockchain consensus protocol in which nodes on a blockchain network validate transactions and prevent double-spending.
- ✓HashCash PoW:

- ✓Hashcash is a proof-of-work system used to limit email spam and denial-of-service attacks, and more recently has become known for its use in bitcoin (and other cryptocurrencies) as part of the mining algorithm. Hashcash was proposed in 1997 by Adam Back.
- ✓In this a textual encoding of a hashcash stamp is included in an email header to check that the sender has expended a modest amount of CPU time calculating the stamp before sending the email.

Proof of Work (PoW) :

HashCash:

- ✓Many of the ideas evolved into HashCash what we understand to be a Proof of Work mechanism today.
- ✓HashCash even included “Double Spending Protection,” a foundational concept in blockchain for keeping networks secure from double spend attacks.
- ✓Moreover, Satoshi Nakamoto cited HashCash as an influence in Bitcoin, writing that in order “to implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash.”
- ✓on 2008, Satoshi clear that proof of work was a key element of the Bitcoin protocol:

Proof of Work (PoW) :

- ✓It propose a solution to the double-spending problem using a peer-to-peer network.
- ✓ The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work.

- ✓Proof of Work system is one that forces computers to do a little extra work before a requested process is executed.
- ✓The extra work results in a solution, which is then presented to the other computers in a network.
- ✓The other computers can easily verify that the solution is accurate and approve whatever action the original computer is requesting.

Proof of Work Blockchain :

- ✓Imagine that there is a reward for being the first one to solve a specific mathematical problem.
- ✓Suppose further that millions of computers are all competing to earn that reward.
- ✓The first one to complete the problem gets the prize. Once a solution is found, the reward is distributed and a new problem is presented.
- ✓All the machines begin competing to solve the new problem, and so on.
- ✓ In a very simplified way, this is how Proof of Work networks function.
- ✓Each “block” in a Proof of Work blockchain is really just a list of completed transactions .
- ✓In an ultra-simplified way, each transaction is really just a transfer of data in a ledger from one Bitcoin wallet address to another.

Proof of Work Blockchain :

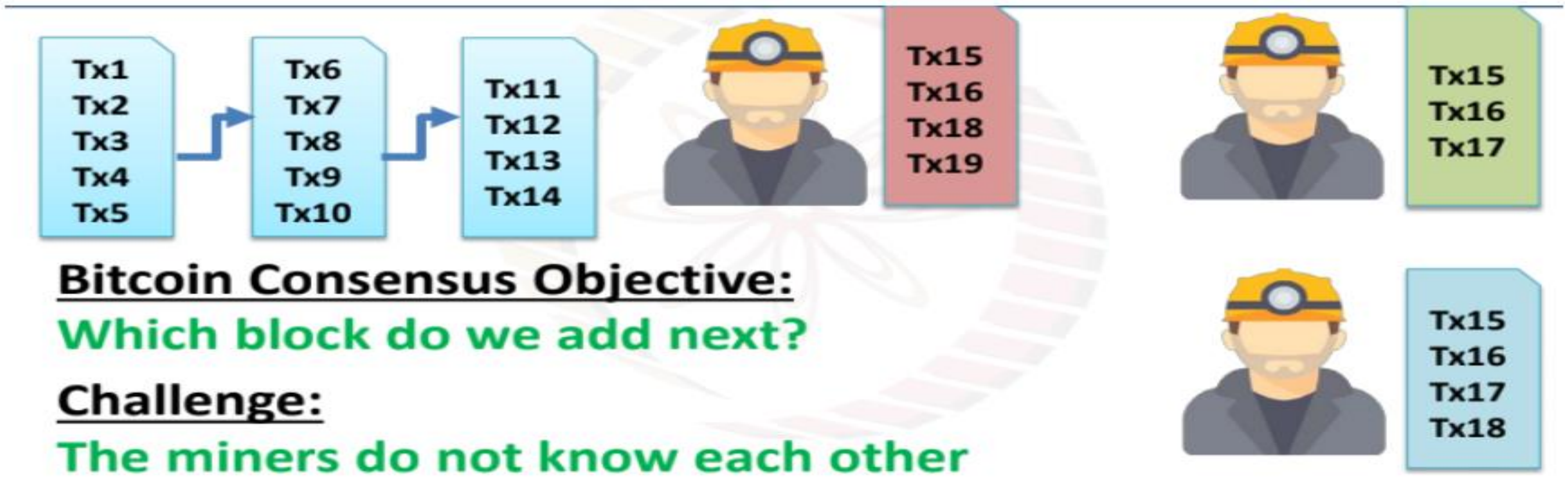
- In order for the network to complete a transfer of funds, the transaction must be confirmed and written into a block on the blockchain.
- A block is mined every time a miner finds a solution to a mathematical problem and broadcasts their solution to the rest of the network.
- In other words, the miner solves the problem and proves their work to the other machines that were trying to solve the same problem.
- All the machines on the network verify the solution. If the solution is true, the miner who found it is given a reward.
- Then, a new problem is presented and the competition begins again. That's how Proof of Work blockchain function.

Proof of Work Blockchains :

- ❖ Proof of work (PoW) is a form of adding new blocks of transactions to a cryptocurrency's blockchain.

Consensus in Bitcoin:

- ❖ All the nodes in this network need to agree on the correctness of a transaction. Some nodes can also initiate malicious transactions.
- ❖ Whenever the multiple miners mine new blocks simultaneously, the objective of consensus is to decide which block is to be added next.



Bitcoin Consensus Objective:

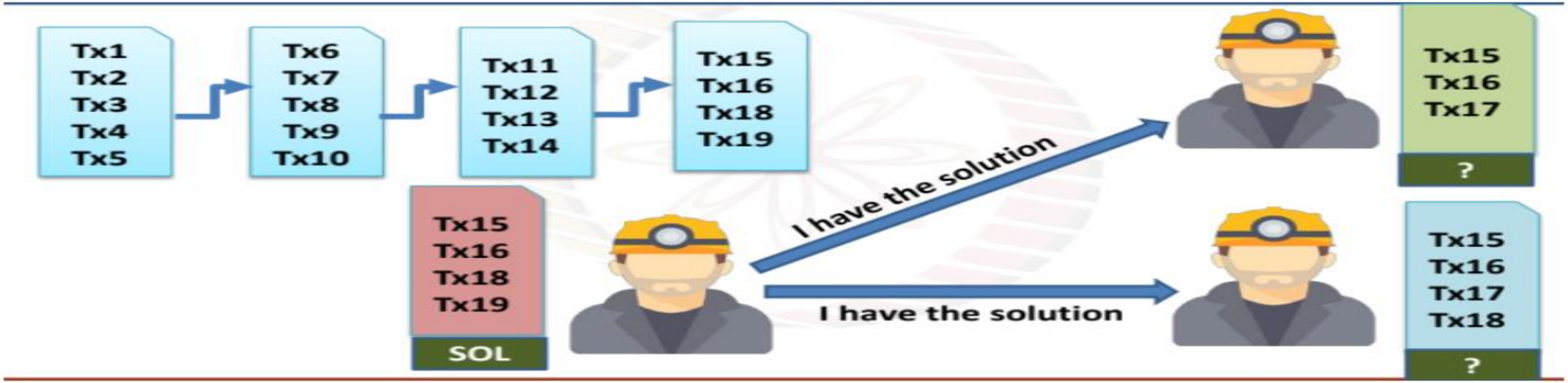
Which block do we add next?

Challenge:

The miners do not know each other

Proof of Work Blockchain : Consensus in Bitcoin:

- Here the miners don’t know each other.
- Every miner solves a challenge independently. The miner who completes the challenge first will add the block mined by him to blockchain. This is his Proof of Work(PoW).
- Now the miner sends the solution to all the other miners and this block is included in the blockchain. In case any transactions are not logged in the block, they will be included in the next round.



Proof of Work Blockchain :

- Proof of work (PoW) is a form of adding new blocks of transactions to a cryptocurrency's blockchain.
- The work, in this case, is generating a hash that matches the target hash for the current block.
- The crypto miner who does this, wins the right to add that block to the blockchain and receive rewards.
- The proof-of-work model is a consensus mechanism used to confirm and record cryptocurrency transactions.

Proof of Work Blockchain :

- Every cryptocurrency has a blockchain, which is a public ledger made up of blocks of transactions.
- With proof-of-work cryptocurrencies, each block of transactions has a specific hash.
- For the block to be confirmed, a crypto miner must generate a target hash that's less than or equal to that of the block.
- To accomplish this, miners use mining devices that quickly generate computations.
- The aim is to be the first miner with the target hash because that miner is the one who can update the blockchain and receive crypto rewards.

Proof of Work Blockchain :

- An example of how Bitcoin uses proof of work to maintain the integrity of its blockchain.
- When Bitcoin transactions occur, they go through a security verification and are grouped into a block to be mined.
- Bitcoin's proof-of-work algorithm then generates a hash for the block.
- The algorithm Bitcoin uses is called SHA-256, and it always generates hashes with 64 characters.
- Miners race to be the first to generate a target hash that's below the block hash.
- The winner gets to add the latest block of transactions to Bitcoin Blockchain.

Proof of Work Blockchain :

- ✓ They also receive Bitcoin rewards in the form of newly minted coins and transaction fees.
- ✓ Bitcoin has a fixed maximum supply of 21 million coins, but, after that, miners will continue receiving transaction fees for their service.
- ✓ The proof-of-work algorithm used by Bitcoin aims to add a new block every 10 minutes.
- ✓ To do that, it adjusts the difficulty of mining Bitcoin depending on how quickly miners are adding blocks.
- ✓ If mining is happening too quickly, the hash computations get harder. If it's going too slowly, they get easier.

Advantages and disadvantages of proof of work:

PROS	CONS
High level of security.	Inefficient with slow transaction speeds and expensive fees.
Provides a decentralized method of verifying transactions.	High energy usage.
Allows miners to earn crypto rewards.	Mining often requires expensive equipment.

Proof of work vs. proof of stake

- Proof of work was the first cryptocurrency consensus mechanism.
- An alternative, proof of stake, came out in 2012 with the launch of Peercoin (CRYPTO:PPC).
- It chooses transaction validators based on how many coins they've staked, or locked up, to the network.
- Because proof of stake doesn't require nearly as much computing power as proof of work, it's more scalable.
- It can process transactions more quickly for lower fees and with less energy usage, making proof-of-stake cryptocurrencies more environmentally friendly.
- It's also much easier to start staking crypto than mining since there's no expensive hardware required.

Proof of work vs. proof of stake

However, proof of work is more proven from a security perspective. One potential problem with proof of stake is that parties with large crypto holdings could have too much power, which is an issue that proof of work doesn't have.

SN	Proof of work	Proof of stake
1	The probability of mining a block is determined by how much computational work is done by miner.	The probability of validating a new block is determined by how large of a stake a person holds (how many coins they possess).
2	A reward is given to first miner to solve cryptographic puzzle of each block.	The validator do not receive a block reward instead they collect network fee as their reward.
3	Bitcoin is most well known crypto with a Proof-of-Work consensus building algorithm which uses most well known proof-of-work function is called SHA256.	Some of cryptocurrencies that use different variants of proof-of-stake consensus are: EOS (EOS), Tezos (XTZ), Cardano (ADA), Cosmos (ATOM), Lisk (LSK).

SN	Proof of work	Proof of stake
4	To add each block to chain, miners must compete to solve difficult puzzles using their computer process power	There is no competition as block creator is chosen by an algorithm based on user stake.
5	Hackers would need to have 51% of computation power to add malicious block.	Hackers would need to own 51% of all cryptocurrency on network, which is practically impossible.
6	Proof of work systems are less energy efficient and are less costly but more proven.	Proof of Stake systems are much more cost and energy efficient than POW systems but less proven.
7	Specialized equipment to optimize processing power.	Standard server grade unit is more than enough.
8	Initial investment to buy hardware.	Initial investment to buy stake and build reputation.

Attacks on PoW :

Tampering Blockchain:

- Each block is mined after doing some work. Thus, the blockchain together contains a large amount of work. If an attacker wants to change any block, he needs to compute all the hashes in the blockchain. This will need a large amount of work which is difficult with current hardware.

Double Spending Problem:

- We have already seen this problem in the previous article. This problem arises when the attacker tries to send the same amount of bitcoin to two different persons.

Attacks on PoW :

Sybil Attack:

- In Sybil attacks, the attacker attempts to fill the network with the clients under its control.
- When this thing happens the attacker can actually control or get a monopoly over the network and these clients can do different kinds of tractions based on the instruction from the attacker.
- They can refuse to relay the valid blocks or they can only relay the blocks which are generated by the attackers and those blocks can lead to double-spending. In Simple language, The attacker can include multiple nodes in the network who can collectively compromise the Proof of Work mechanism

Denial of Service(DoS) Attack:

- The attacker sends a lot of data in the network to make it busy so that the actual transactions are not able to take place.

Monopoly Problem.

- During bitcoin’s early days, anyone could “mine” it using their home computer.
- But as the price of digital currency climbed towards $100 in 2013 (it’s now over $4,000), professional mining groups with specialized computer chips emerged.
- Today, these groups, or pools — have become concentrated and now dominate the production of new bitcoins.

Why monopoly problem existed?

- Miners are getting less rewards over the time. So, they are discouraged to join as a miner. The difficulty of puzzle is increasing which is not possible to be solved by normal hardware.

Solution of Monopoly Problem:

- Proof of Stake(PoS) emerged as a solution to this problem.

Proof of Stake(PoS):

- A person can mine or validate block transactions according to how many coins he or she holds.
- This means that the more Bitcoin owned by a miner, the more mining power he or she has.
- The first cryptocurrency to adopt the PoS method was Peercoin.
- In Peercoin, the coinage is used as a variation of stake. Coinage is calculated by multiplying number of coins by the number of days the coins have been held.
- If an attacker wants to attack, he/she should have more number of Bitcoin. If the attacker holds majority of bitcoins, then the majority affect will be on attacker only.

Advantages And Disadvantages of Proof-of-stake :

Advantages

- Does not require expensive equipment for participation.
- Fast and inexpensive transaction speed.
- Energy-efficient.

Disadvantages

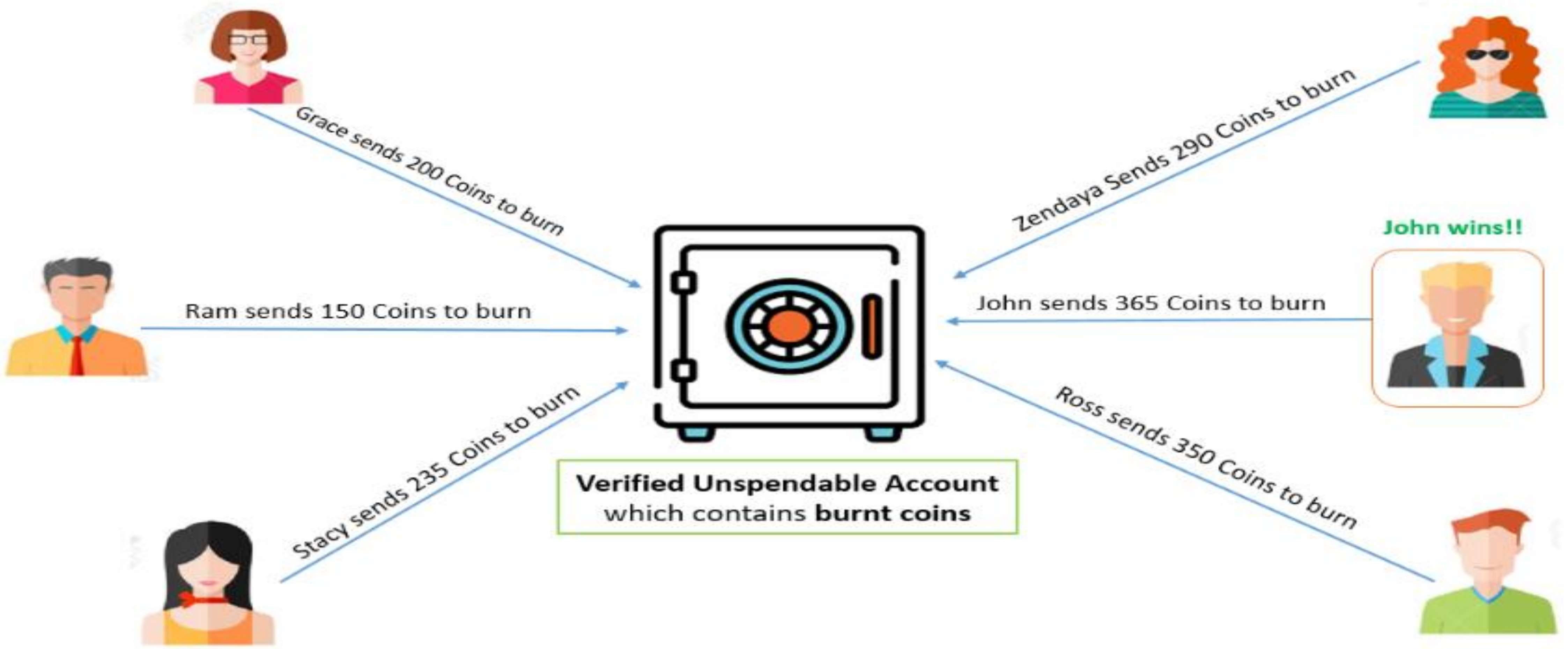
- Lacks in terms of security when compared to proof-of-work.
- Validators with large holdings can influence the verification of transactions.
- Few of the PoS cryptos require locking up staked coins for a certain period of time.

Proof of Burn(PoB):

- PoB works on the principle of allowing the miners to “burn” or “destroy” the virtual currency tokens, which grants them the right to write blocks in proportion to the coins burnt.
- To burn the coins, miners send them to a verifiably un-spendable address. These publicly verified unspendable accounts are randomly created with no private keys associated.
- Once coins get received by burn address/accounts, it becomes useless and inaccessible.
- Eventually, the burnt coins in the account are used for strengthening the security of the network.
- This process does not consume many resources other than the burned coins. PoB works by burning PoW mined cryptocurrencies. It is power efficient unlike PoW.

Proof of Burn(PoB):

John wins as he burns the maximum number of coins. Hence, he gets the chance to add his block of transactions to the network.


Grace sends 200 Coins to burn
Zendaya Sends 290 Coins to burn
John wins!!
Ram sends 150 Coins to burn
John sends 365 Coins to burn
Stacy sends 235 Coins to burn
Ross sends 350 Coins to burn
Verified Unspendable Account
which contains burnt coins

Proof of Burn(PoB):

PoB works on the principle of allowing the miners to “burn” or “destroy”.

Advantages of PoB:

- It required very little power compared to PoW.
- It reduces energy consumption by wasting insignificant resources when coins are burned.
- It encourages long-term involvement in a project as a consumer is displaying a big commitment to the currency by foregoing a narrow profit in exchange for a long-term profit.
- The coin distribution is more fair compared to all other consensuses.

Proof of Burn(PoB):

Disadvantages of PoB:

- It is risky because one doesn’t know that will they gain the wealth they have burnt in the future or not.
- As coins are burnt, so technically if we see then resources are wasted.
- It may suffer from rich getting richer phenomena. In which those who are wealthy are getting wealthier by having more coins.

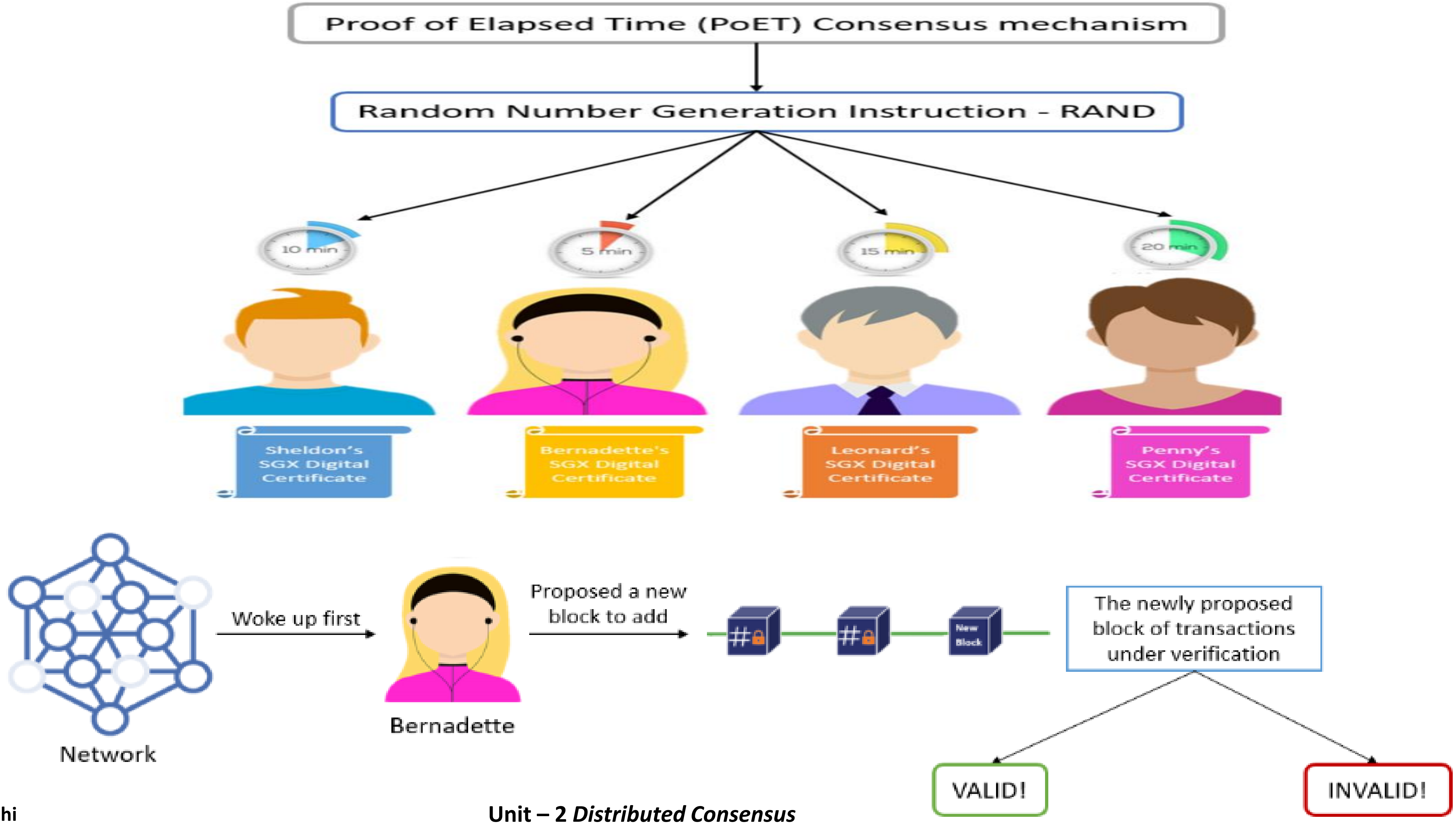
Proof of Elapsed Time(PoET):

- PoET is a consensus algorithm used in a Permissioned blockchain network to decide mining rights and next block miner.
- A Permissioned blockchain network requires participants to prove their identity, whether they are allowed to join.
- Hence, it needs permission (or invitation) to join the decentralized network as a new participant (or node).
- The PoET algorithm was developed by Intel Corporation, the processor chip giant, in early 2016.
- Intel associated with Linux Foundation in the development of Hyperledger Sawtooth.
- They aimed to build a highly scalable private blockchain network.

Proof of Elapsed Time(PoET):

- Intel introduced PoET as a time-lottery-based consensus algorithm secured by cryptography.
- The concept basically motivates the ideology of giving equal chances of getting a reward like a lottery.
- PoET Mechanism assigns an amount of time to each node in the network randomly.
- The node must sleep or do another task for that random wait time.
- Whichever node gets the shortest waiting time wakes up and add their block to the network.
- Later, the new update information floods among other network participants.

Proof of Elapsed Time(PoET):



Proof of Elapsed Time (PoET) Consensus mechanism

Random Number Generation Instruction - RAND

Sheldon's SGX Digital Certificate

Bernadette's SGX Digital Certificate

Leonard's SGX Digital Certificate

Penny's SGX Digital Certificate

Network

Woke up first

Bernadette

Proposed a new block to add

The newly proposed block of transactions under verification

VALID!

INVALID!

Proof of Elapsed Time(PoET):

Benefits of Proof of Elapsed Time (PoET) :

.

- PoET can go up to a million transactions per second.
- It is highly energy-efficient and easily scalable.
- It’s a block generation consensus algorithm, unlike proof of stake (PoS).
- PoET is for privately controlled spaces like business organizations.
- It ensures the same opportunity for network participants with time object and activation.
- As it’s a Permissioned blockchain network, the process of selecting validators ensures network security against cyber attacks.

Proof of Elapsed Time(PoET):

Disadvantages of the PoET consensus mechanism:

- PoET is a Permissioned and closed network, unlike Bitcoin and Ethereum.
- The mechanism highly depends on tools by Intel technology which might raise compatibility issues with other tools later.

1) Proof of Work (PoW)

.

Principle: it is difficult to find a solution, but it is easy to check the result.

Performance: low.

DLT environment: public blockchain.

Completion: probabilistic.

Example of use: Bitcoin, Ethereum, Litecoin.

2) Proof of Burn (PoB)

.

Principle: burning a mined PoW cryptocurrencies in exchange for mining privileges or the coins/tokens of an alternative currency

Performance: medium

DLT environment: Public

Example of use: Slimcoin and Counterparty

3) Proof of Stake (PoS)

Principle: the network trusts the validator, who puts his own resources as a pledge for the ability to create blocks: the larger the share, the higher the probability that the network will allow the creation of a block.

Performance: high.

DLT environment: public / private blockchain.

Completion: probabilistic.

Example of use: NXT, Tezos, soon Ethereum.

4) Proof-of-Elapsed-Time (PoET):

Principle: blocks are created in a trusted environment with equal periods.

Performance: average.

DLT environment: private blockchain, with and without permissions.

Completion: probabilistic.

Usage example: Intel.

Comparison between Pow, PoS and PoET

Parameters	**PoW**	**PoS**	**PoET**
Blockchain type	Permissionless	Both	Both
Transaction finality	Probabilistic	Probabilistic	Probabilistic
Transaction rate	Low	High	Medium
Token needed	Yes	Yes	No
Cost of participation	Yes	Yes	No
Scalability of peer network	High	High	High
Trust model	Untrusted	Untrusted	Untrusted

Creation of coins :

- A cryptocurrency is a digital currency, which uses cryptography for secure transactions.
- 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.

Creation of coins :

- 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.

Creation of coins :

- 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.

SN	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 of coins :

- 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.

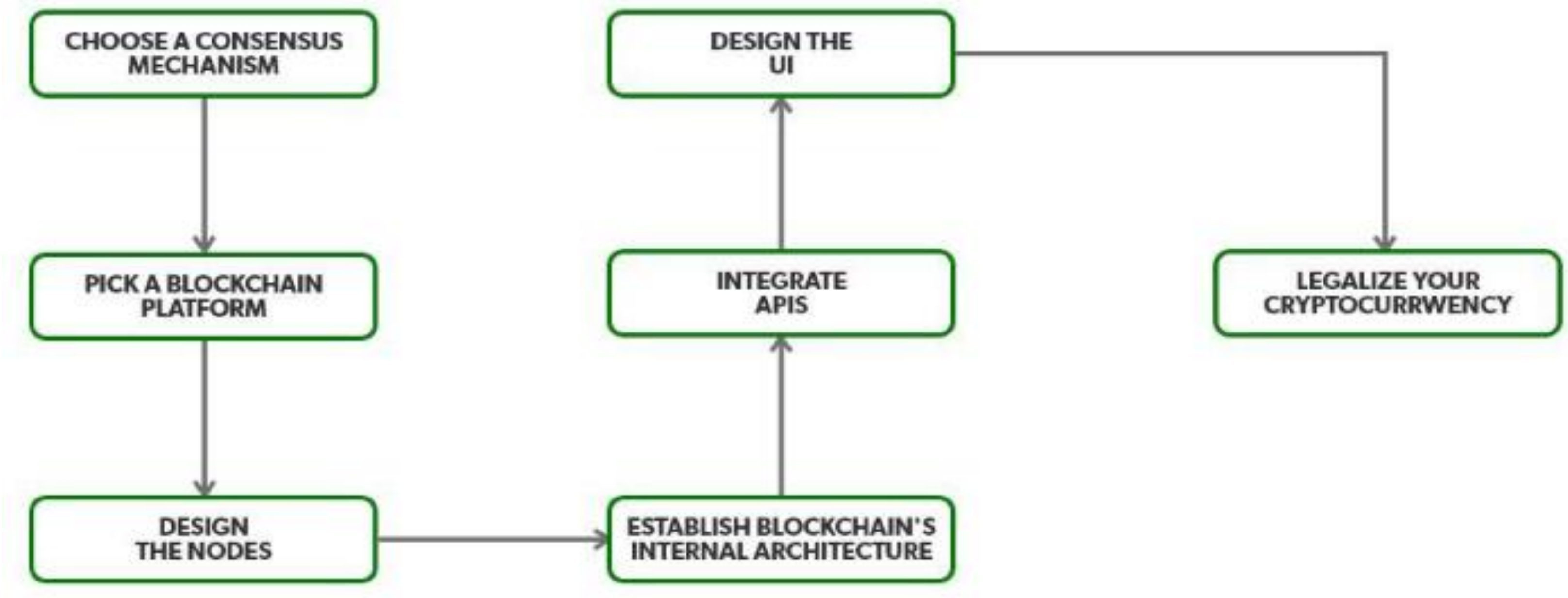
2. Creating a Token:

- 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.

Steps to Create a Cryptocurrency

Below are the steps to create a cryptocurrency:

.


CHOOSE A CONSENSUS MECHANISM
PICK A BLOCKCHAIN PLATFORM
DESIGN THE NODES
ESTABLISH BLOCKCHAIN'S INTERNAL ARCHITECTURE
INTEGRATE APIS
DESIGN THE UI
LEGALIZE YOUR CRYPTOCURRWENCY

2. Pick a Blockchain Platform: Choosing the right blockchain platform for the business depends on the consensus mechanism which is choose.

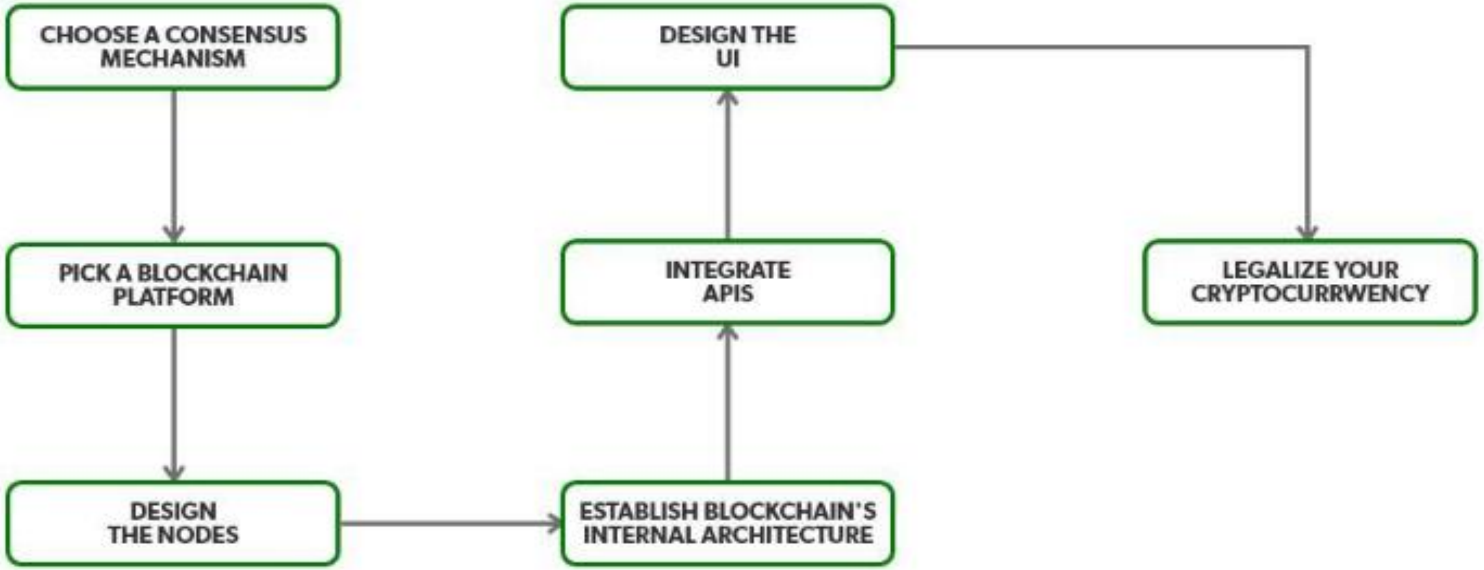
3. Design The Nodes: Need to determine how blockchain will work and function, and design the nodes accordingly.

Steps to Create a Cryptocurrency

4. Establish Blockchain 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.

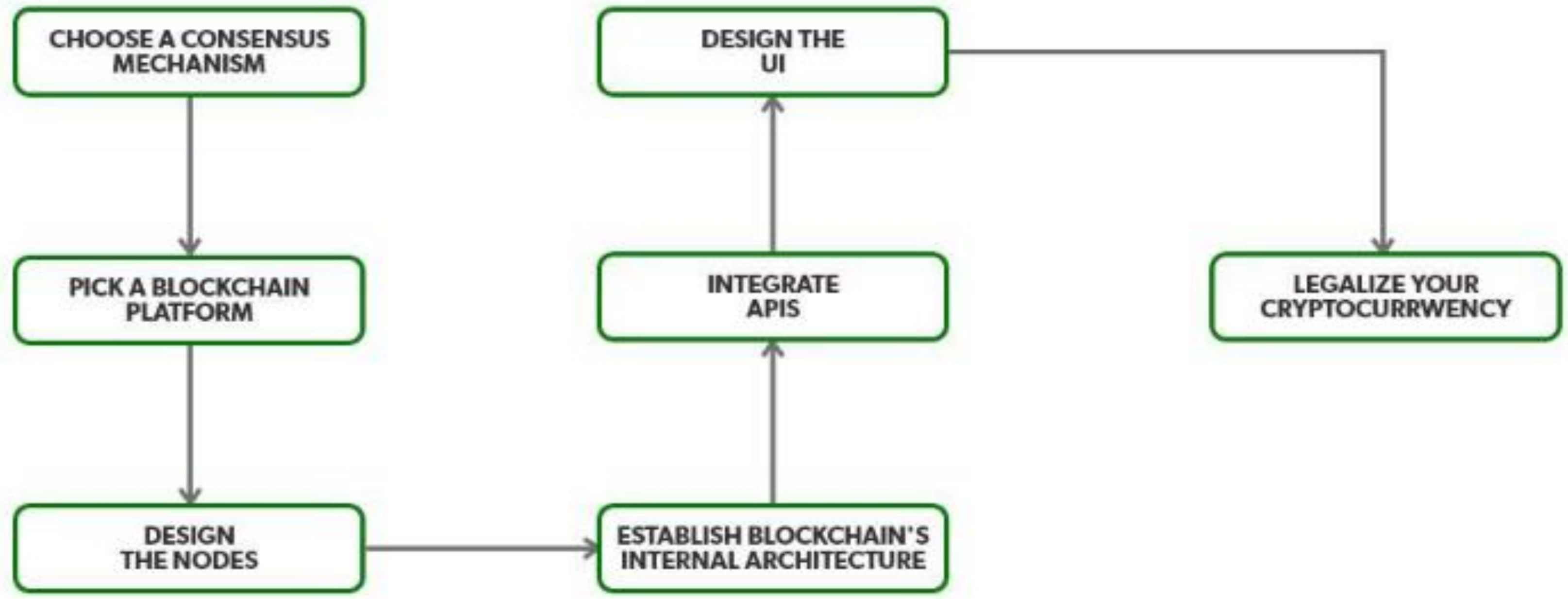
5. Integrate APIs: Some platforms don’t offer pre-built APIs. There are several third-party blockchain API providers like ChromaWay, Gem, Colu, BlockCypher, etc.


CHOOSE A CONSENSUS MECHANISM
PICK A BLOCKCHAIN PLATFORM
DESIGN THE NODES
ESTABLISH BLOCKCHAIN'S INTERNAL ARCHITECTURE
INTEGRATE APIS
DESIGN THE UI
LEGALIZE YOUR CRYPTOCURRWENCY

Steps to Create a Cryptocurrency

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.



CHOOSE A CONSENSUS MECHANISM

PICK A BLOCKCHAIN PLATFORM

DESIGN THE NODES

ESTABLISH BLOCKCHAIN'S INTERNAL ARCHITECTURE

INTEGRATE APIS

DESIGN THE UI

LEGALIZE YOUR CRYPTOCURRWENCY

Double-spending :

- Double-spending is simply the process of making two payments with the same currency or funds in order to deceive the recipient of those funds.
- With physical currency, this really isn’t possible. You can’t give two people the same coin.

- With most online payments, you trust a third party to make sure funds are sent and received properly.
- Banks, credit card companies, and payment processors validate the transactions themselves and minimize the risk of double-spending.
- With cryptocurrency, however, there’s no third-party intermediary — just the sender and the recipient.
- How can crypto holders protect themselves against double-spending?
- The answer is on the blockchain.

Double-spending :

- The Bitcoin blockchain is a public ledger of transactions that’s secured by miners who receive mining rewards as an incentive to protect the blockchain.

- When you initially make a transaction, it’s an unconfirmed, or pending, transaction waiting to be included in a block.
  New blocks are added to the Bitcoin blockchain approximately every 10 minutes.
- Once an unconfirmed transaction is included in a block, it’s been “written” to the blockchain public ledger and is now a “confirmed” transaction.
- A confirmed transaction is assigned to the recipient and is verified by the network through specialized cryptographic proofs, meaning it can’t be double-spent, or “copied.”

Double-spending :

- You don’t need permission from anyone to send the transaction; all you need is a cryptocurrency wallet and an internet connection.
- Double-spending would seriously damage the network and remove one of its most important features: trustless, immutable, and decentralized transactions.

How Does Double Spending Happen?

- Double spending can happen in online transactions only.

  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’.

Double-spending :

How Does Double Spending Happen?

- ✓ 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.

Double-spending :

- ✓ As long as you don’t accept unconfirmed transactions, you shouldn’t need to worry about double-spending attacks.
- ✓ Most wallets and exchanges will label transactions that haven’t been confirmed as “unconfirmed.”

Types of Double-Spending Attacks

- ✓ Although many consider the double-spending problem largely solved by the blockchain, there have been some attempts to exploit the Bitcoin protocol, via race attacks,
  Finney attacks,
  and 51% attacks.

Double-spending :

- In a race attack, the hacker sends two transactions in quick succession and only one is later confirmed on the blockchain.
- The goal is to purchase something with the unconfirmed transaction and then invalidate it before it's confirmed.
- This is possible only if the recipient or merchant accepts an unconfirmed transaction.
- Only miners can perform Finney attacks. The miner pre-mines a transaction into a block from one wallet to another.
- Then, they use the first wallet to make a second transaction and broadcast the pre-mined block, which includes the first transaction.
- This requires a very specific sequence to work. Like a race attack, a Finney attack is possible only if the recipient accepts an unconfirmed transaction.

Double-spending :

- A 51% attack occurs when a group or individual controls more than 50% of a network’s hashing power in order to alter a blockchain.
- With this control, the hacker(s) can launch a double-spend attack. However, because of Bitcoin’s enormous hash rate, this scenario is highly improbable on the Bitcoin protocol.

Bitcoin Peer to Peer Network.

- It is an ad-hoc network with random topology, Bitcoin protocol runs on TCP port 8333.
- All nodes (users) in the bitcoin network are treated equally.
- New nodes can join any time, non-responding nodes are removed after 3 hours.

How to join this P2P network?

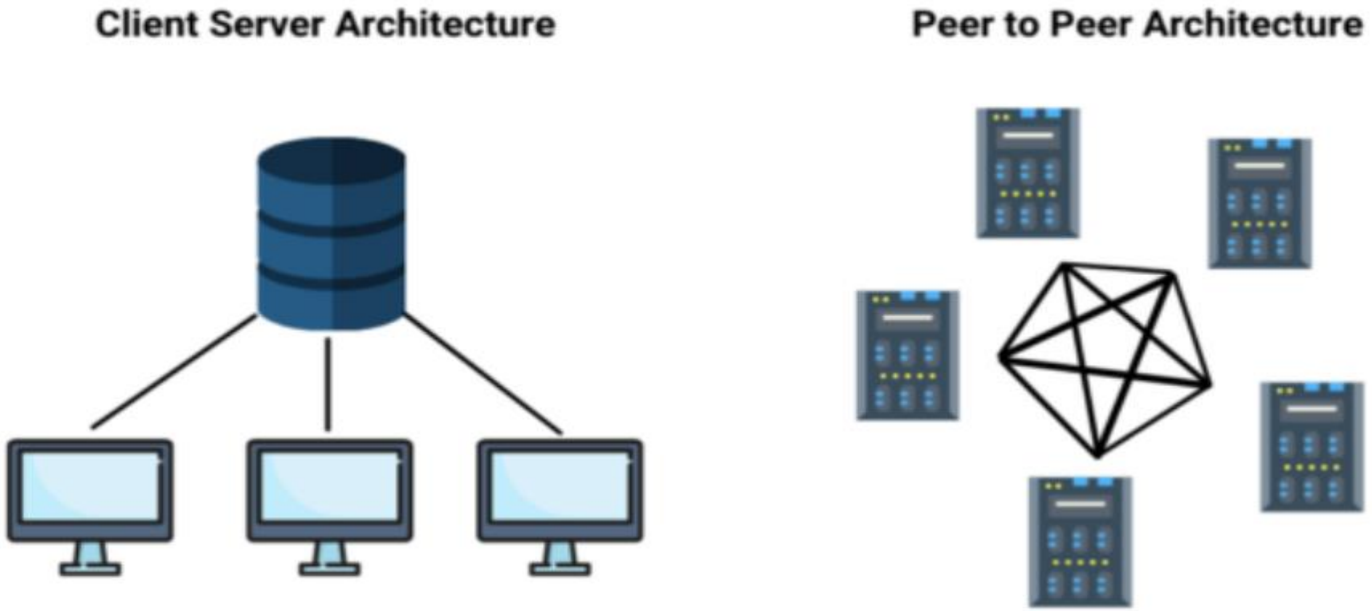
- Suppose you want to join an existing Bitcoin P2P network, then you will follow the following steps:
- You send the request message to join the network. There are certain nodes in the network known as seed nodes which provide the initial information to the new node.
- You send a message to seed node to provide the peer addresses.
- In response, seed node sends a set of addresses to consider as peers.
- Among this set, you select some random addresses and make them as peers by making virtual links with them.
- You ask the peers to send the most recent information of blockchain. After you receive the information, you compare it and keep the copy which is transferred by most number of peers(>50%).

How to join this P2P network?

- The term P2P refers to decentralized networks of interconnected computer systems containing peers, or nodes.
- All nodes are equal, and the exchange of data occurs without a central server — that is, each computer or node can act as both a file server and a client.
- Bitcoin is open-source; its design is public, nobody owns or controls Bitcoin and everyone can take part.
- Peers make a portion of their resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by servers or stable hosts.
- Peers are both suppliers and consumers of resources, in contrast to the traditional client-server model in which the consumption and supply of resources is divided.

How to join this P2P network?

- Each node in a network shares files with every other node without going through a central authority or administrator.
- As mentioned, nodes play the dual roles of client and server to other nodes on the network.
- P2P networks differ from traditional client/server networks, where clients request specific resources from central servers.



Benefits of P2P Networks:

- **Improved network efficiency:**

  In P2P networks, each node participates in the routing and forwarding of data. This can improve network efficiency, as there’s no need for dedicated routers or servers.

- **Resilience to failure:**

  P2P networks are more resilient to failure than centralized networks, as the loss of a single node doesn’t cripple the entire network.

- **Privacy:**

  P2P networks are often viewed as more privacy-friendly than centralized networks, as there’s no need for a central authority to store or access user data.

Benefits of P2P Networks:

- Scalability:

P2P networks are designed to be scalable. Each node or peer can be a server, preventing bottlenecks encountered in centralized systems when the number of clients increases. With a P2P network, an increase in the number of clients means an equal increase in the number of servers.

- Cost:

P2P networks are considerably cost-effective, as costs don't aggregate around a centralized authority but are instead distributed.

In addition, these networks are highly scalable and efficient, due to the multiple roles of every node.

Types of peer-to-peer (P2P) networks :

.

The network is categorized into three types of P2P networks based on their architectural differences.

Structured peer-to-peer networks

In this network, an organized structure is used in which the nodes interact, making it possible for the nodes to easily search for files even if the data is unavailable.

Due to this organized structure, some amount of centralization exists in this type of network.

Despite providing easy access to data, a structured P2P network is more challenging and costly to set up.

Types of peer-to-peer (P2P) networks :

Unstructured peer-to-peer networks

In this type of network, there is no set structure for the nodes to follow.
Participants can join or leave the network as and when they desire.
This lack of a definite structure leads participants to communicate randomly with each other.
This network is easy to build, but it requires high CPU power as all nodes must remain active to process a high number of transactions.
Memory usage is also increased as search queries are sent to the whole network.
An unstructured peer-to-peer network is best applicable for high churn activity, such as for a social platform.

Types of peer-to-peer (P2P) networks :

Hybrid peer-to-peer networks:

A hybrid P2P network is a combination of a peer-to-peer and client-server model.
The network has a central server that stores information on the location of resources and uses this server to conduct searches.
In comparison to the structured and unstructured P2P network, a hybrid P2P network has better performance.
It provides centralization, which is required for specific queries while providing the benefits of a decentralized network.

Transactions in Bitcoin Network:

- Representation of transaction:

  When Alice sends 10 bitcoins to Bob, it will be represented as:

  A->B: BTC 10

- Mechanism:

  Alice sends 10 bitcoins (along with scripts) to Bob after getting the most recent information.

  This transaction will be broadcast to all the peers.

  They will validate the transaction using script.

  If it is valid, they will broadcast this to neighboring peers.

Transactions in Bitcoin Network:

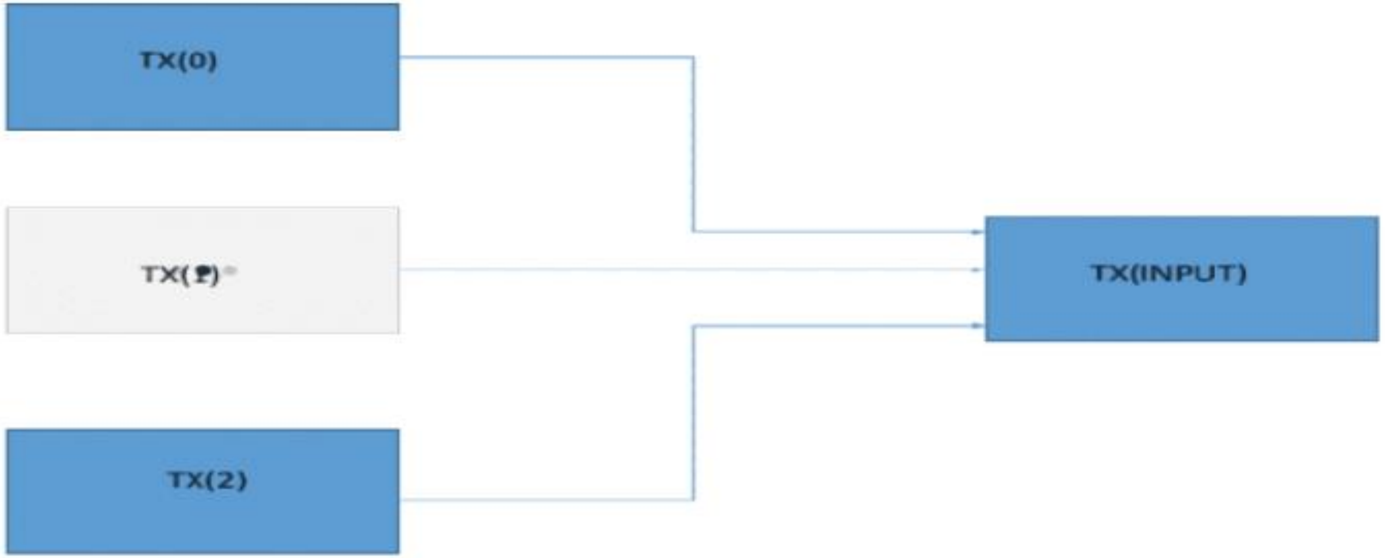
- This process will continue and each node will receive copy of transaction.
- If a node gets the same transaction information from more than one neighboring peer, it will keep the copy first received and discard all copies.
- If there is more than one transaction happening in the network, then the transactions are stored in order they are received by the node.

  So, different nodes may have different transaction pools.

- Reliable Transactions:
- There should be no conflict between two transactions.
- User must not be able to double spend the bitcoin.
- The script matches with a pre-given set of white list scripts — avoid unusual scripts, avoid infinite loops.

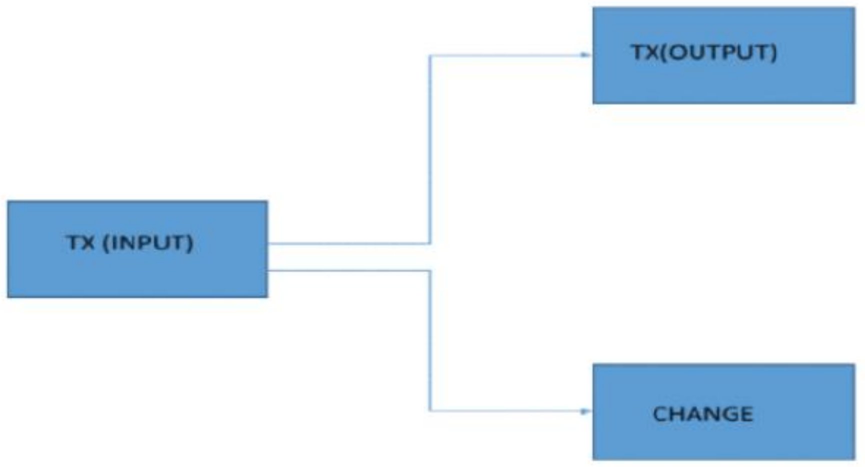
Transactions in Bitcoin Network:

- Transaction Input: In order to make this transaction happen, Alice needs to get bitcoin which she has received from various previous transactions.
- So, suppose Alice needs to pull bitcoin from the following transactions which we shall name TX(0), TX(1) and TX(2).
- These three transactions will be added together and that will give you the input transaction which we shall call TX(Input).



Transactions in Bitcoin Network:

- Transaction Output: The output basically will have the number of bitcoin that Bob will possess, post-transaction and any remaining change that is left over, which is then sent back to Alice. This change then becomes her input value for all future transactions. A pictorial representation of the output side looks like this:



- Conditions of a transaction :

  TX(Input) > TX(output). The input transaction has to be always greater than the output transaction.

Transactions in Bitcoin Network:

- Conditions of a transaction :

In any transaction, the deficit between the input and the output (output+ change) is the transaction fees that miners collect. So:
Transaction fees = TX(Input) – (TX(output) + Change).

- In the input side: TX(0) + TX(1) + TX(2) = TX(Input).

If Alice doesn’t have the funds necessary to carry out the transactions then the miners will simply reject the transactions.

- Transaction in Bitcoin Network
- As a new user, you can get started with Bitcoin without understanding the technical details.
- Once you've installed a Bitcoin wallet on your computer or mobile phone, it will generate your first Bitcoin address and you can create more whenever you need one.

Transactions in Bitcoin Network:

- You can disclose your addresses to your friends so that they can pay you or vice versa.

  In fact, this is pretty similar to how email works, except that Bitcoin addresses should be used only once.
- The block chain is a shared public ledger on which the entire Bitcoin network relies.
- All confirmed transactions are included in the block chain.
- It allows Bitcoin wallets to calculate their spendable balance so that new transactions can be verified thereby ensuring they're actually owned by the spender.
- The integrity and the chronological order of the block chain are enforced with cryptography.

Transactions in Bitcoin Network:

✓ Transactions - private keys:

.

✓ A transaction is a transfer of value between Bitcoin wallets that gets included in the block chain.

✓ Bitcoin wallets keep a secret piece of data called a private key or seed, which is used to sign transactions, providing a mathematical proof that they have come from the owner of the wallet.

✓ The signature also prevents the transaction from being altered by anybody once it has been issued.

✓ All transactions are broadcast to the network and usually begin to be confirmed within 10-20 minutes, through a process called mining.

What Is Bitcoin Mining?

- ✓ Bitcoin mining refers to ensuring that transactions are valid and added to the
- ✓ Bitcoin blockchain correctly using a global network of computers running the Bitcoin code.
- ✓ The process of mining is also the means by which new Bitcoin are created.
- ✓ The process of bitcoin mining involves the verification of new transactions against the Bitcoin network, which results in the production of new bitcoin.
- ✓ Bitcoin mining is the process by which Bitcoin transactions are validated digitally on the Bitcoin network and added to the blockchain ledger.
- ✓ Bitcoin mining is the process of creating new bitcoin by solving puzzles. Solving these puzzles requires powerful computing power and sophisticated equipment.

What Is Bitcoin Mining?

- ✓ It consists of computing systems equipped with specialized chips competing to solve mathematical puzzles.
- ✓ It is done by solving complex cryptographic hash puzzles to verify blocks of transactions that are updated on the decentralized blockchain ledger.
- ✓ In return, miners are rewarded with Bitcoin, which is then released into circulation hence the name Bitcoin mining.

➢ Mining Mechanism:

- ✓ Miners are certain nodes in the network that have great computational power. Not all the nodes in network are miners.
- ✓ Miners collect all the transactions flooded in the network and start mining. The miner who solves the puzzle first generates a new block in the network.

Mining Mechanism:

- ✓ That new block will get flooded in the network.
- ✓ It may be possible that multiple miners mine same new block for a transaction or different blocks for different transactions simultaneously.
- ✓ Mining is a distributed consensus system that is used to confirm pending transactions by including them in the block chain.
- ✓ It enforces a chronological order in the block chain, protects the neutrality of the network, and allows different computers to agree on the state of the system.
- ✓ To be confirmed, transactions must be packed in a block that fits very strict cryptographic rules that will be verified by the network.

Mining Mechanism:

- ✓ These rules prevent previous blocks from being modified because doing so would invalidate all the subsequent blocks.
- ✓ Mining also creates the equivalent of a competitive lottery that prevents any individual from easily adding new blocks consecutively to the block chain.
- ✓ In this way, no group or individuals can control what is included in block chain or replace parts of the block chain to roll back their own spends.

▪ Block propagation in bitcoin

- ✓ Mined blocks are propagated to all participating nodes in the network through compact block relay (CBR) protocol.
- ✓ Therefore, reducing the block relay time between nodes can reduce the block propagation time to all nodes and ultimately improve the performance of Bitcoin.

Block propagation in bitcoin :

- ✓ Block propagation time or block propagation delay determines the limits of Bitcoin’s scaling.
- ✓ It’s an average time that is needed for the new block to reach the majority of nodes in the network.
- ✓ In a large decentralized network like Bitcoin, whenever the new block is generated, it is broadcasted according to the Gossip protocol.
- ✓ If some node has got the new valid block, it informs nodes connected to it about its new possession.
- ✓ Then the node transfers this block to those nodes which asked it to do that.
- ✓ Before the block reaches each full-node in the network, it passes through 7 intermediary nodes.
- ✓ It’s important that every honest node verifies the block before relaying it to other peers.

Transactions in Bitcoin Network:

- Block propagation in bitcoin

.

- ✓ Since data transmission is the most time-consuming part of the block relay, researchers got interested in determining how much time is required for a data packet of a certain size to reach 50%, 90%, or 95% of nodes in the network.
- ✓ It was found that for blocks of a size larger than 20kB, the block propagation delay is nearly proportional to the block size.
- ✓ According to research published in 2013, every extra kB of data in the block caused an extra 80ms of block propagation delay.
- ✓ The block propagation time has a massive effect on the blockchain security.
- ✓ The longer the propagation time in the network, the more often miners mine on top of old blocks.

Transactions in Bitcoin Network:

- Block propagation in bitcoin

✓ Long propagation delay reduces the node’s resistance against 51% attacks and selfish mining.

✓ The propagation delay should be reasonable so that miners will keep their nodes synchronized most of the time, and will always verify proposed blocks.

✓ Bitcoin’s P2P network is formed of miner nodes where the nodes randomly connect with each other.

✓ Transactions and blocks are transmitted over this network by these nodes, until each has received the message.

Block propagation in bitcoin :

.

- ✓ For a message to be diffused through the network, the transaction travel in hops.
- ✓ With each iteration a set of 2 nodes are sent the message, and the network diffusion grows by a factor of 2^n.
- ✓ The diffusion increases exponentially as the hops increase, and after 12–15 hops, the entire network receives the message.

Block Propagation on Network Plane:

.

- ✓ Blockchain throughput is measured by the number of transactions per second that it can support and is measured as
  (Throughput = Transactions/Block * Blocks/second (Inverse of Block interval)
  where Transactions/Block is a factor of Bitcoin's current block capacity and average transaction size
  (Transactions/Block = Bitcoin capacity /average Transaction size)
- ✓ The current Block capacity for Bitcoin is 1MB for a Block interval of 10 minutes and given the average transaction size of nearly 540 bytes, the Bitcoin network currently processes ~1950 transactions per Block, which translates to ~3 transactions per second (TPS).

Block Propagation on Network Plane:

- ✓ To increase the throughput one can either increase the Transactions/Block or Blocks/second.

Block Relay:

- ✓ The Bitcoin Relay Network is a high-speed block-relay system primarily for miners.
- ✓ It relays blocks around the globe (see map below) in low multiples of global latency (usually 100-300ms, see the stats page).
- ✓ It is in use in one way or another by the majority of major miners.

General relay network information:

.

- ✓ The Bitcoin Relay Network is a system of peering between nodes in the network by creating a system of high-speed relay nodes for miners and merchants/exchanges.
- ✓ This system

  a) acts as a fall back in the case that the public Bitcoin network encounters issues and

  b) decreases block propagation times between miners.
- ✓ It is NOT designed to in any way replace or decrease the need for the public Bitcoin P2P network.
- ✓ It is NOT any kind of attempt at centralization

General relay network information:

.

✓ The Bitcoin Relay Network consists of a few nodes scattered around the globe, all of which peer with each other.

✓ In order to participate, simply run the local client (it will automatically select the server closest to you).