UNIT III

Consensus Algorithm

Consensus Algorithms

We know that 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.

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

What is Proof of Work?

Proof of Work is a type of consensus mechanism. Here, users (a.k.a. miners) use their computational devices to solve complex mathematical problems in order to verify and add blocks to the ledger system.

It needs heavy computational power to function properly.

Working Principles of Proof of Work

- Miners solve complex mathematical problems. After that new block gets created and the transaction is confirmed.
- Depends on the number of users available on the network, overall load of the network and minimum current power.
- Each block will contain a new hash function and the hash function of the previous block.

Advantages of Proof of Work

- Proof of Work consensus offers a high level of security compared to other consensus mechanisms.
- It can establish a true decentralized network and offers a transparent transaction verifying process for every user.
- This process also offers a reward system for the users participating in the mining process.

Issues with Proof of Work Consensus Algorithm

- It does not offer efficiency. The process is slow and can amount to high expensive fees.
- It needs a massive amount of energy to function, which is not an environmentally friendly process.
- The mining process damages hardware; therefore, miners have to invest in expensive equipment. It's vulnerable to 51% attack.

What Is Proof of Stake?

Proof of Stake is a consensus mechanism that addresses the issues of Proof of Work and offers a better solution.

Here, users will need to stake their coins in order to participate in the verification process. This one does not need computational resources like PoW.

How Does It Work?

- In Proof of Stake, users have to be qualified to take participate in the verification process. To qualify one needs to store a certain amount of coin in their wallets.
- Once you are qualified, you will need to deposit or stake an amount of coin to take part in the voting system. This voting system will choose the validators.
- The more you stake the more you can mine or validate a new block.

Advantages of Proof of Stake

- Proof of Stake is a highly efficient consensus protocol as it does not need heavy computational power to function.
- It can offer inexpensive transaction processing fees and can also verify and process a transaction faster.
- It does not need any special hardware or equipment to function.

Key Differences between PoW and PoS

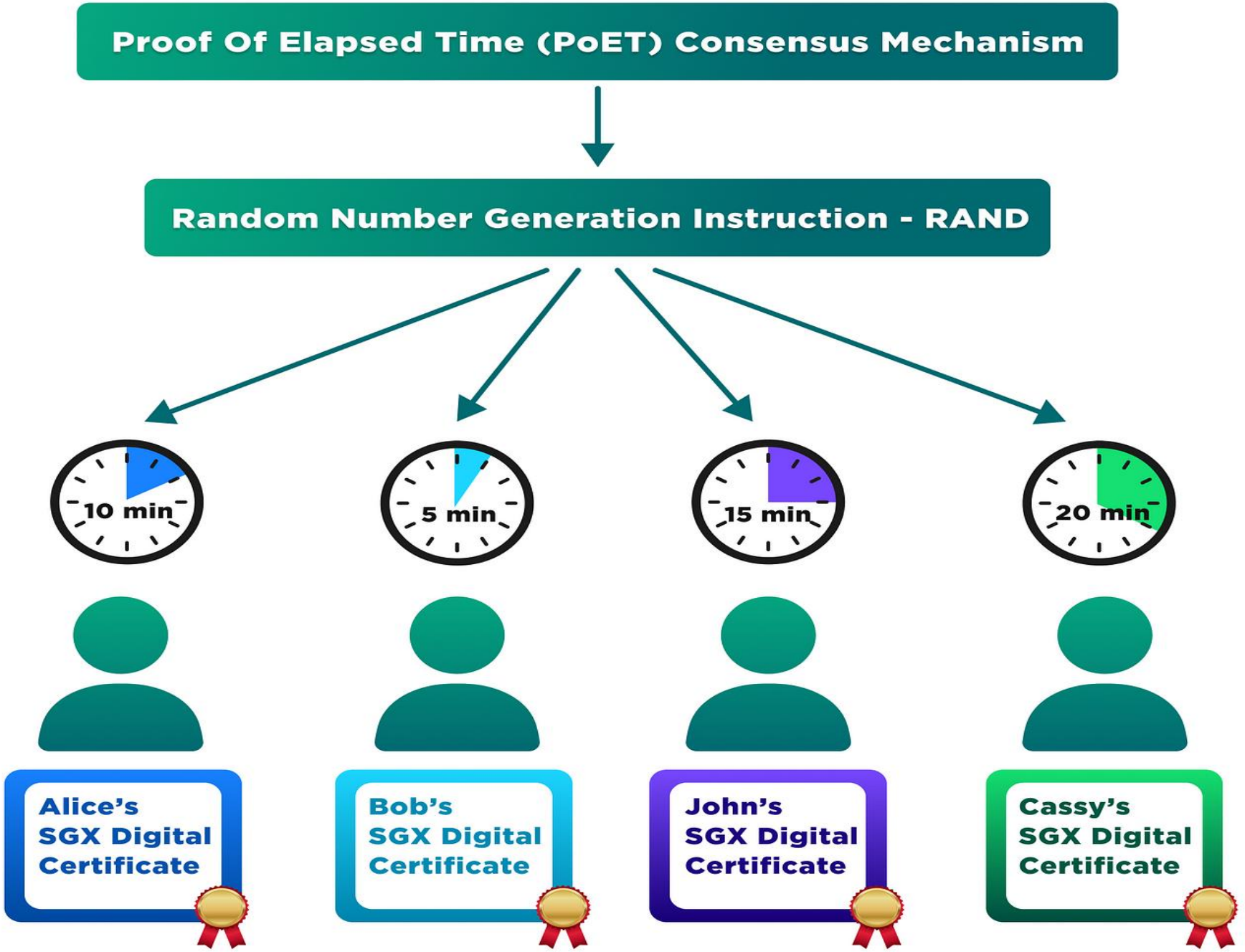
	PoW	PoS
Verification Mechanism	Mining	Validators
Incentive Policy	Transaction fees + new coins	Transaction fees
Vulnerability	51% attack	Nothing at stake
Motivation	Profit	Loyalty
Requirement	Hash Power/Computational Power	Number of coins owned
Scalability	Low	High
Main Issues	Energy Inefficient	Wealth concentration

Proof of Elapsed Time

- **What Is Proof of Elapsed Time (PoET)?**

  Proof of elapsed time (PoET) is a blockchain network consensus mechanism that prevents high resource utilization and energy consumption; it keeps the process more efficient by following a fair lottery system.

- The algorithm uses a randomly generated elapsed time to decide mining rights and block winners on a blockchain network. By running a trusted code within a secure environment, the PoET algorithm also enhances transparency by ensuring lottery results are verifiable by external participants.


Proof Of Elapsed Time (PoET) Consensus Mechanism
Random Number Generation Instruction - RAND
10 min
5 min
15 min
20 min
Alice's SGX Digital Certificate
Bob's SGX Digital Certificate
John's SGX Digital Certificate
Cassy's SGX Digital Certificate

Key points

- The PoET algorithm is for permissioned blockchain networks. That is, a special verification is required from a node when it tries to join the network. This verification is achieved using Intel's Software Guard Extension (SGX) A set of instructions built into the Intel CPUs technology which was first introduced in 2015

- PoET enables permissioned blockchain networks to determine who creates the next block.

- PoET follows a lottery system that spreads the chances of winning equally across network participants, giving every node the same chance.

The PoET algorithm generates a random wait time for each node in the blockchain network; each node must sleep for that duration.

- The node with the shortest wait time will wake up first and win the block, thus being allowed to commit a new block to the blockchain.

- The PoET workflow is similar to Bitcoin's proof of work (PoW) but consumes less power because it allows a node to sleep and switch to other tasks for the specified time, thereby increasing network energy efficiency

Benefits of Proof of Elapsed Time (PoET)

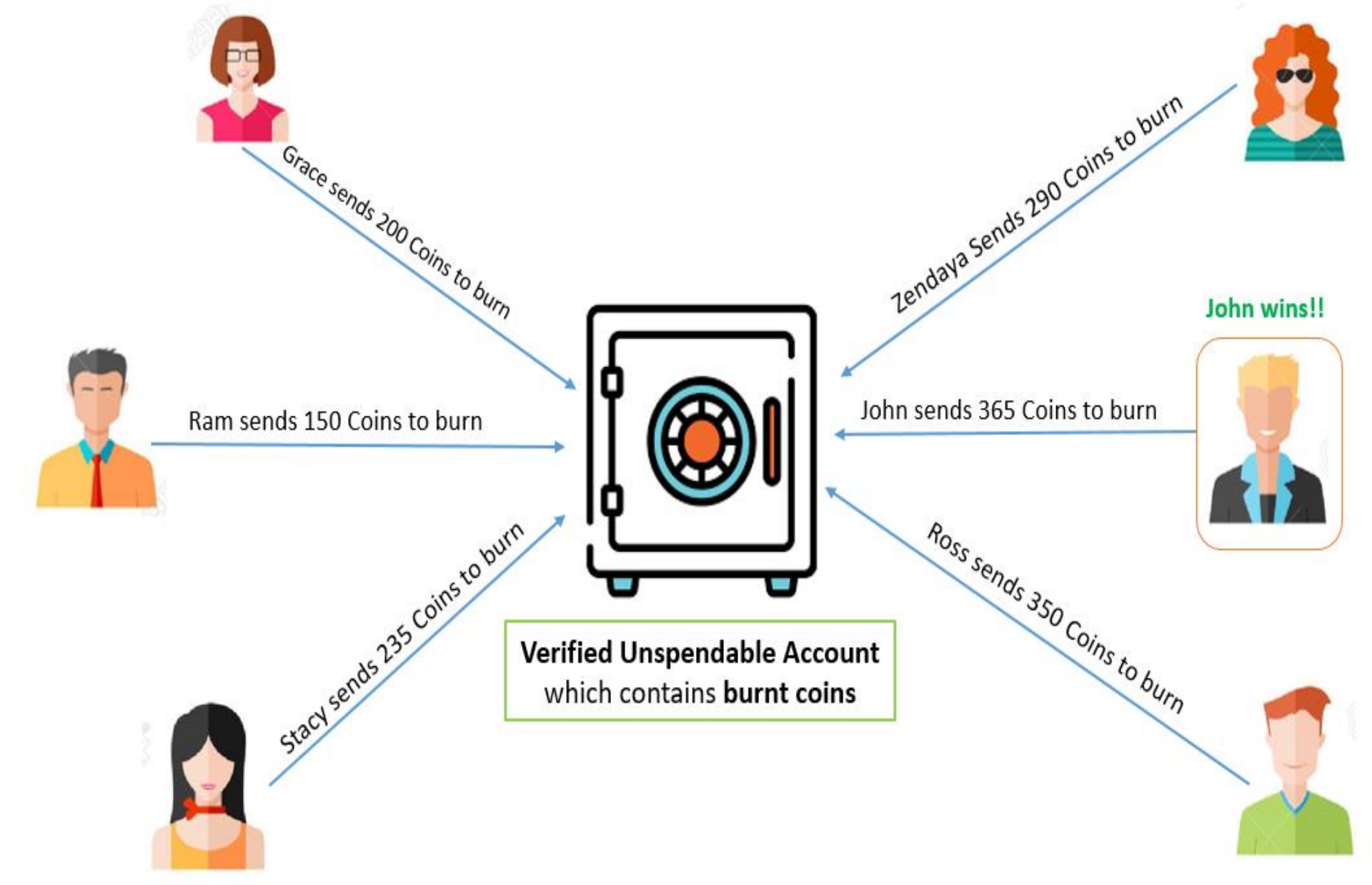
- Following are the advantages of the PoET consensus mechanism:
- PoET can go up to **a million transactions per second**.
- It is **highly energy-efficient** and easily scalable.
- PoET is for **privately controlled** spaces like business organizations.
- It ensures the **same opportunity for network participants** with time object and activation.

What Is a Proof of Burn

- In the Proof of Burn (PoB) : algorithm, miners reach a consensus by burning the coins. It's a process in which crypto coins get permanently eliminated from regular circulation. In such cases, the burning of coins mechanism is used to validate transactions. Hence, the more coins a miner burns, the higher the chances of adding the block to the network.

- This algorithm is implemented to avoid the possibility of any cryptocurrency coin double-spending.

Proof of Burn in Blockchain



Let's take an example to understand the working of proof of Burn (PoB)?

- We have 6 miners, each having their own block of transactions. As per the process, the miners have to burn some amount of coins to get an opportunity to add their block to the network.
- See the below diagram. Each miner sends some of their coins to the burn address or unspendable escrow account.
- John wins as he burns the maximum number of coins. Hence, he gets the chance to add his block of transactions to the network.
- Moreover, the block added by John will be verified by other network validators. If the block is found invalid, then the second-highest (Ross) gets the chance to add a new block.

Benefits of PoB

Following are the advantages of Proof of Burn in blockchain:

- Less power and energy consumption.
- Motivates miners to make regular transactions using cryptocurrency.
- PoB is more sustainable and doesn't need hardware for heavy computation.
- Used for long-term commitments

Attacks

- Double spending attacks
- Sybil attack
- Denial of service attack

Double spending attacks

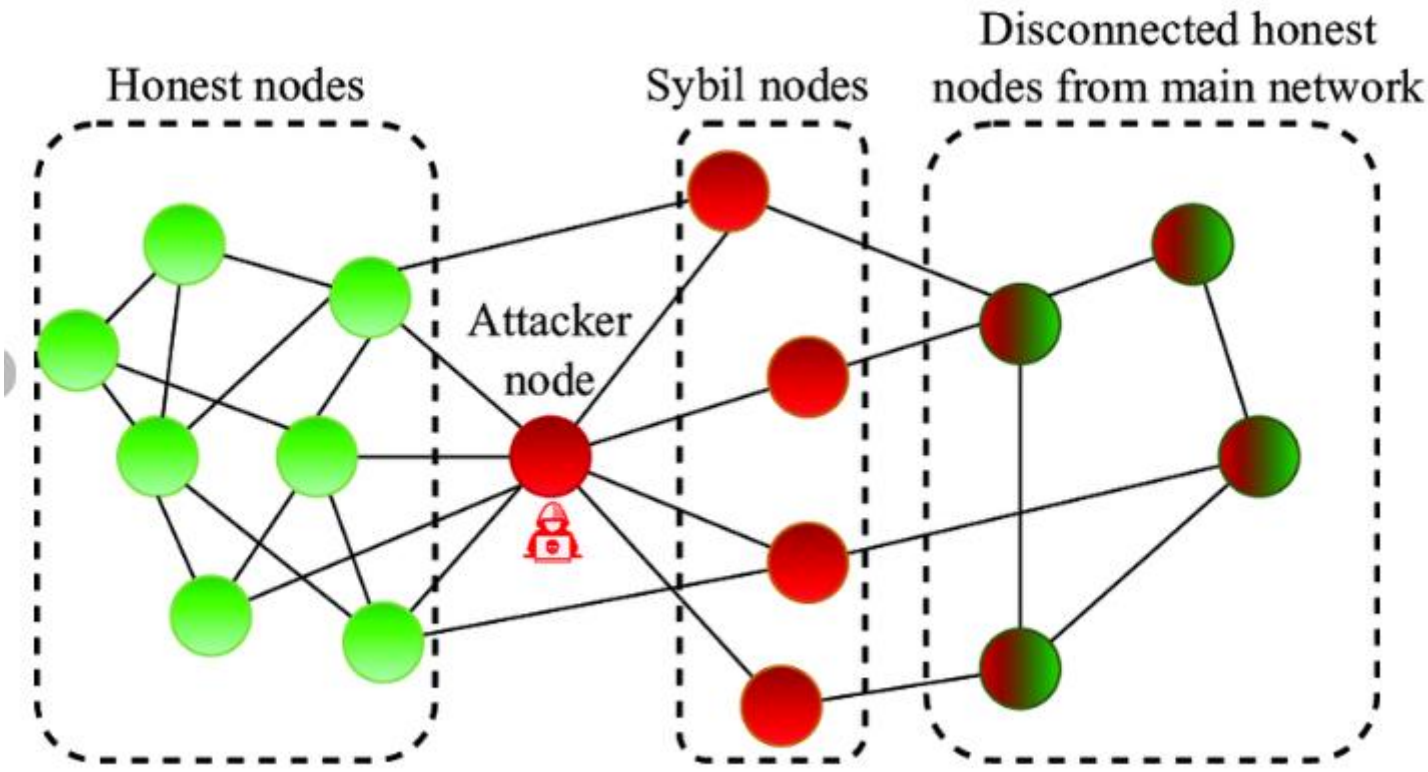
- Double-spending is a situation in which the same digital funds are spent multiple times.
- In the blockchain-based decentralized network, a reliable consensus mechanism has to be put in place to prevent double-spending.
- Bitcoin network, double spending attacks are prevented by evaluating and verifying the authenticity of each transaction using the transaction logs stored in Bitcoin's blockchain protocol.

Sybil Attacks

- The name of this attack was inspired by a 1973 book called Sybil, a woman diagnosed with a dissociative identity disorder. In the context of attacks, the term was originally coined by Brian Zill, and initially discussed in a paper by John R. Douceur, both at Microsoft Research.

- A successful Sybil attack provides threat actors with the ability to perform unauthorized actions in the system. For example, it enables a single entity, such as a computer, to create and operate several identities, such as user accounts and IP address-based accounts. All of these fake identities, tricking systems and users into perceiving them as real.

Sybil attack example



Sybil attack scenario in a P2P network.

What Problems Can Sybil Attacks Cause?

- Here are several problems a Sybil attack may cause:

- **Block users from the network**—a Sybil attack that creates enough identities enables threat actors to out-vote honest nodes and refuse to transmit or receive blocks.

- **Carry out a 51% attack**—a Sybil attack that enables one threat actor to control over half (51% or more) of a network's total hash rate or computing power. This attack damages the integrity of a blockchain system and can potentially cause network disruption.

What is the Ideal Solution for Preventing Sybil Attacks

- **Developing a Reputation System:** The reputation mechanism can validate older members as honest nodes and give them the power to override Sybil nodes.
- **Identity Validation Mechanism :** You can use identity validation mechanisms for direct/indirect validation in which a central authority would validate all the new nodes(losing your privacy).
- **Social Trust Graphs :** Another trusted addition among measures for preventing Sybil attacks points at social trust graphs. Social trust graphs work through a comprehensive analysis of connectivity data between the nodes. Therefore, it can help in identifying and stopping abnormal nodes before they impose any damage.

Denial of service attack

- Traditional Distributed Denial of Service (DDoS) attacks are designed to exploit bottlenecks within a system. This is accomplished by sending it more traffic than its network card can handle, overwhelming an application with more requests than it can manage, etc.

- One of the main selling points of blockchain technology is its resistance to DDoS attacks. A traditional DDoS attack targets a fixed single point of failure within a system such as a web server. If the web server goes down, then an organization's website may not be available to visitors.

Solution

To prevent DOS attacks there are several rules bitcoin have which are:

- No forwarding of orphaned blocks.
- No forwarding of double-spend transactions.
- No forwarding of same block or transactions Disconnect a peer that sends too many messages
- Restrict the block size to 1 MB (1mb according to Satoshi Nakamoto)
- Limit the size of the bitcoin script up to 10000 bytes.

Mining Difficulty

- For mining a block, a miner must solve complex mathematical problems by finding a valid hash.
- As the process progresses, the network adjusts the rate so miners can find valid hashes.
- Each blockchain has its algorithm to regulate this adjustment.
- The algorithm increases or decreases the mining difficulty based on the rate at which miners can mine a block.

- In recent times, the number of miners has increased manifold. Thus automatically, the mining difficulty of blockchains has also increased. Let’s take an example for you to understand better.
- Bitcoin is a cryptocurrency that has become very popular. As a result, the number of miners on that blockchain has also increased.
- The more the number of miners, the more computing power is used in the peer-to-peer network. And as a result, greater is the competition for the limited block rewards. Thus to adjust the rate at which miners can find blocks, the network raises its hash power.

Benefits of Mining difficulty

- Mining difficulty may seem to you as a hindrance on your path to getting block rewards. However, it has its benefits too. They are:

- **Security of the Network:** As the mining difficulty increases, it becomes more difficult for a hacker to conduct a malicious attack on the network. Due to the increasing difficulty, miners use special ASIC mining computers that make trillions of guesses each second to find the correct hash for a block.

- **A steady mining rate:** A miner's computing power differs from person to person and pool to pool. Thus to maintain parity in the mining process, the blockchain network raises or lowers its mining difficulty. This ensures that the network is generating blocks at a steady rate.

permissioned and permissionless blockchain

Category	Permissioned	Permissionless
Speed	Faster	Slower
Privacy	Privacy Membership	Transparent and open – anyone can become a member
Ownership	Managed by a group of nodes predefined	Public ownership no one owns the network
Decentralization	Partially decentralized	Truly decentralized
Cost	Cost effective	No cost effective
Security	Less secure	More secure
Transparency	Controlled	Complete

Smart Contracts

- In 1994, Nick Szabo, a legal scholar, and cryptographer realized that the decentralized ledger could be used for smart contracts, otherwise called self-executing contracts, blockchain contracts, or digital contracts.

- Smart contracts are lines of code that are stored on a blockchain and automatically execute when predetermined terms and conditions are met.

- The execution of smart contracts is controlled by relatively easy "if/when…then…" statements written in code on the blockchain.

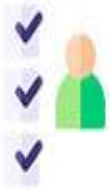
- As Vitalik Buterin, founder of ethereum, says that, in a smart contract approach, an asset or currency is transferred into a program “and the program runs this code and at some point it automatically validates a condition.

- Smart Contracts:
- They are logic or code that operate on block chain
- They are part of the block chain in Ethereum
- They are immutable, it should be carefully coded
- Solidity is popular to code smart contract, EVM (Ethereum virtual machine) is the computer that runs the code.
- EVM is the engine of ethereum. Gas is the fuel for the engine.

How does a Smart Contract Work?

Identify Agreement

Multiple parties identify the cooperative opportunity and desired outcomes.



Set conditions

Smart contracts are executed automatically when certain conditions are met.

Code business logic

A computer program is written

Encryption and blockchain technology

Encryption provides a secure transfer of messages between parties.

Execution and processing

The code is executed and outcomes are memorialized.

Network updates

All the nodes on the network update their ledger.

Difference between Traditional and Smart Contracts

Sl.No.	Traditional Contracts	Smart Contracts
1	Created by legal team	Created by Programmers
2	Physical contracts	Digital contracts
3	Legal language	Programming language
4	Enforcement depends on Third party	Code is automatically executed
5	It takes days	It takes minutes
6	Escrow may be necessary	Escrow may not be necessary