



**ARYA College of Engineering (ACE)**

(Affiliated to RTU | Approved by AICTE, New Delhi)

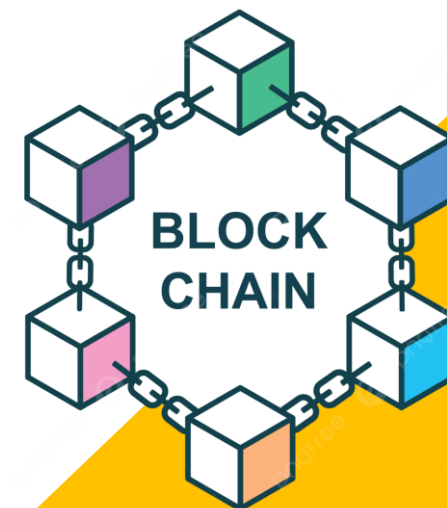
• SP-40, RIICO Industrial Area, Delhi Road,  
Kukas, Jaipur-302028 | Tel. Ph. 0141-2820700

• [www.aryainstitutejpr.com](http://www.aryainstitutejpr.com)  
• Toll Free: 1800 102 1044

# Fundamentals of Blockchain

## Unit-5 Types of Consensus Algorithm

**Er. Harsh Raj**  
(Assistant Professor, CSE)

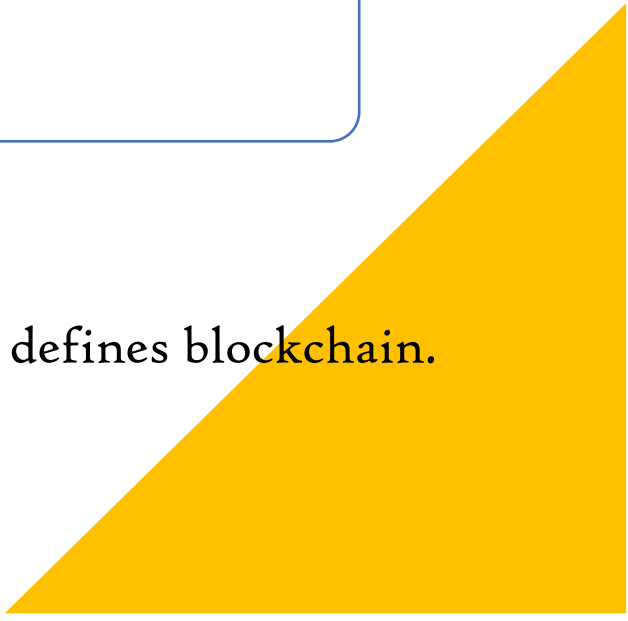




# Course Objectives

1. The students should be able to understand a broad overview of the essential concepts of blockchain technology.
2. To familiarize students with Bitcoin protocol followed by the Ethereum protocol – to lay the foundation necessary for developing applications and programming.
3. Students should be able to learn about different types of blockchain and consensus algorithms.

## Expected Course Outcome

1. To explain the basic notion of distributed systems.
  2. To use the working of an immutable distributed ledger and trust model that defines blockchain.
  3. To illustrate the essential components of a blockchain platform.
- 

# Syllabus

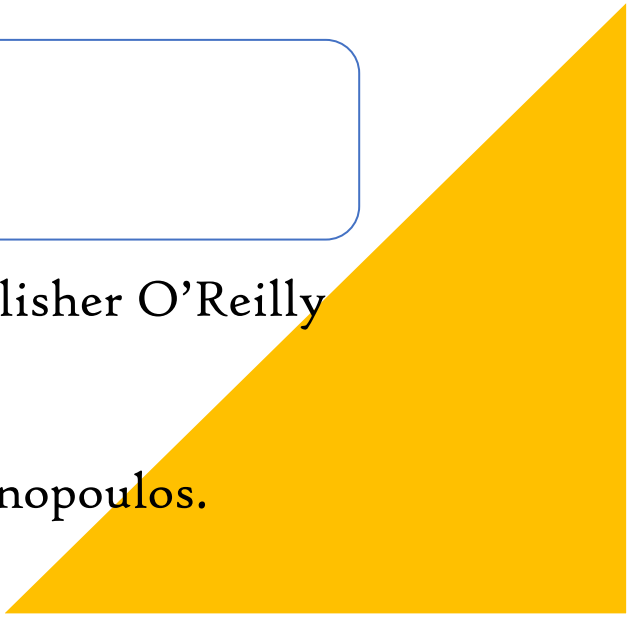
UNIT	Contents
1	Basics: The Double-Spend Problem, Byzantine Generals' Computing Problems, Public-Key Cryptography, Hashing, Distributed Systems, Distributed Consensus.
2	Technology Stack: Blockchain, Protocol, Currency. Bitcoin Blockchain: Structure, Operations, Features, Consensus Model, Incentive Model
3	Ethereum Blockchain: Smart Contracts, Ethereum Structure, Operations, Consensus Model, Incentive Model.
4	Tiers of Blockchain Technology: Blockchain 1.0, Blockchain 2.0, Blockchain 3.0, Types of Blockchain: Public Blockchain, Private Blockchain, Semi-Private Blockchain, Sidechains.
5	Types of Consensus Algorithms: Proof of Stake, Proof of Work, Delegated Proof of Stake, Proof Elapsed Time, Deposit-Based Consensus, Proof of Importance, Federated Consensus or Federated Byzantine Consensus, Practical Byzantine Fault Tolerance. Blockchain Use Case: Supply Chain Management.



# Text Books

1. Kirankalyan Kulkarni, Essentials of Bitcoin and Blockchain, Packt Publishing.
2. Anshul Kaushik, Block Chain & Crypto Currencies, Khanna Publishing House.
3. Tiana Laurence, Blockchain for Dummies, 2nd Edition 2019, John Wiley & Sons.
4. Mastering Blockchain: Deeper insights into decentralization, cryptography, Bitcoin, and popular Blockchain frameworks by Imran Bashir, Packt Publishing (2017).

# Reference Books

1. Blockchain: Blueprint for a New Economy by Melanie Swan, Shroff Publisher O'Reilly Publisher Media; 1st edition (2015).
  2. Mastering Bitcoin: Programming the Open Blockchain by Andreas Antonopoulos.
- 




# Topics

## Types of Consensus Algorithms:

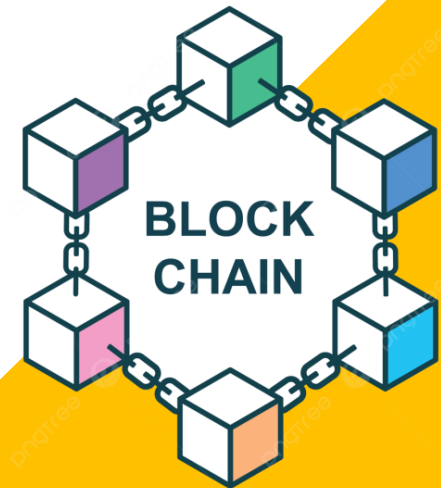
- Proof of Stake
- Proof of Work
- Delegated Proof of Stake
- Proof Elapsed Time
- Deposit-Based Consensus
- Proof of Importance
- Federated Consensus
- Federated Byzantine Consensus
- Practical Byzantine Fault Tolerance

## Blockchain Use Case:

- Supply Chain Management
- 

# Types of Consensus Algorithms:

## Consensus Algorithm



# Consensus Algorithm

A consensus algorithm is a crucial component in distributed computing and blockchain technology that ensures that all participants in a network agree on the current state of the system.


It helps maintain the integrity and consistency of data across multiple nodes in a decentralized network.

Here are a few key consensus algorithms:


1. **Proof of Work (PoW):** PoW is the consensus algorithm used in Bitcoin and many other cryptocurrencies. Participants, called miners, compete to solve complex mathematical puzzles. The first one to solve the puzzle gets the right to add a new block to the blockchain. PoW is energy-intensive but highly secure.
2. **Proof of Stake (PoS):** In PoS, validators are chosen to create new blocks and validate transactions based on the number of coins they hold and are willing to "stake" as collateral. This reduces energy consumption compared to PoW and is used in cryptocurrencies like Ethereum 2.0.

3. **Delegated Proof of Stake (DPoS):** DPoS is a variation of PoS where coin holders vote for a smaller number of delegates who are responsible for validating transactions and creating new blocks. It's faster and more scalable but can be seen as less decentralized.
4. **Proof of Authority (PoA):** In PoA, network participants are known and have a reputation to uphold. A set of authorities is responsible for validating transactions. PoA is often used in private and consortium blockchains.
5. **Practical Byzantine Fault Tolerance (PBFT):** PBFT is a classic consensus algorithm used in permissioned blockchain networks. It ensures consensus among a group of nodes, even if some of them are malicious or faulty.
6. **Raft:** Raft is another consensus algorithm designed for use in distributed systems to achieve consensus. It's often used in systems that need to be available and reliable but don't require the decentralized and trustless nature of blockchain.
7. **Tendermint:** Tendermint is a BFT-based consensus algorithm designed for use in blockchain systems. It combines elements of PoS and BFT to achieve both speed and security.

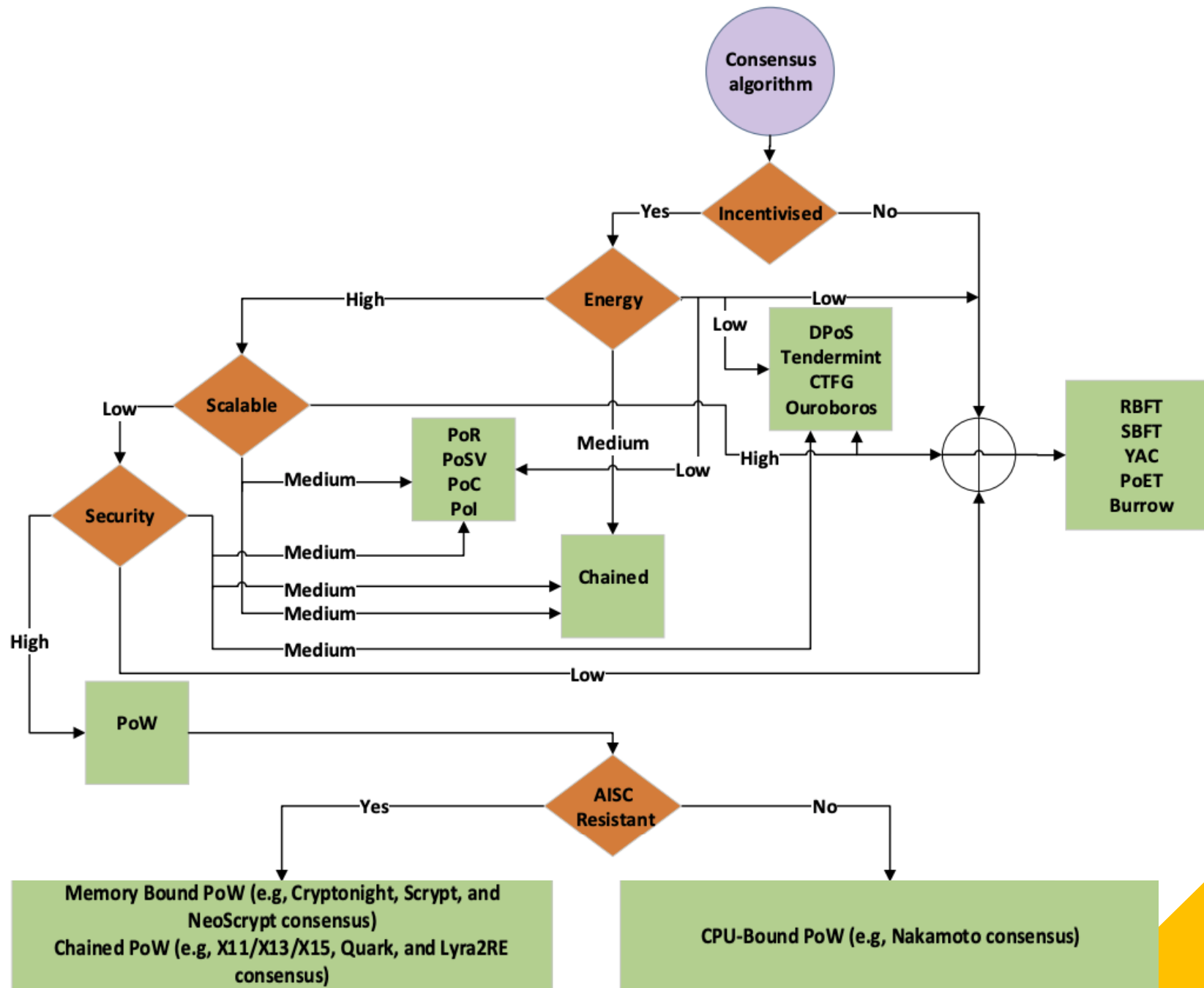


- 
8. **Honey Badger BFT:** This is a more recent BFT-based consensus algorithm designed to be highly resilient and scalable while being suitable for use in decentralized applications and networks.

The choice of consensus algorithm depends on the specific requirements of a network or blockchain. Some prioritize decentralization and security, while others aim for scalability and energy efficiency. Different use cases may require different consensus algorithms to strike the right balance between these factors.

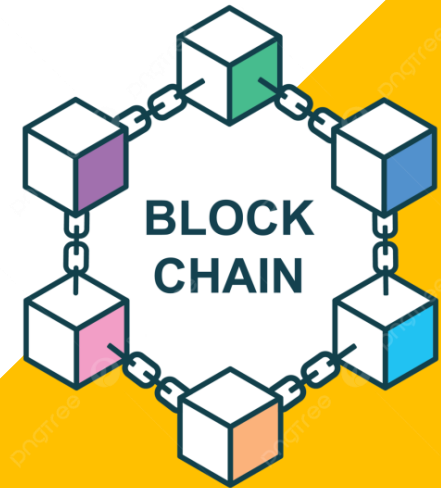


# Blockchain Consensus Algorithm



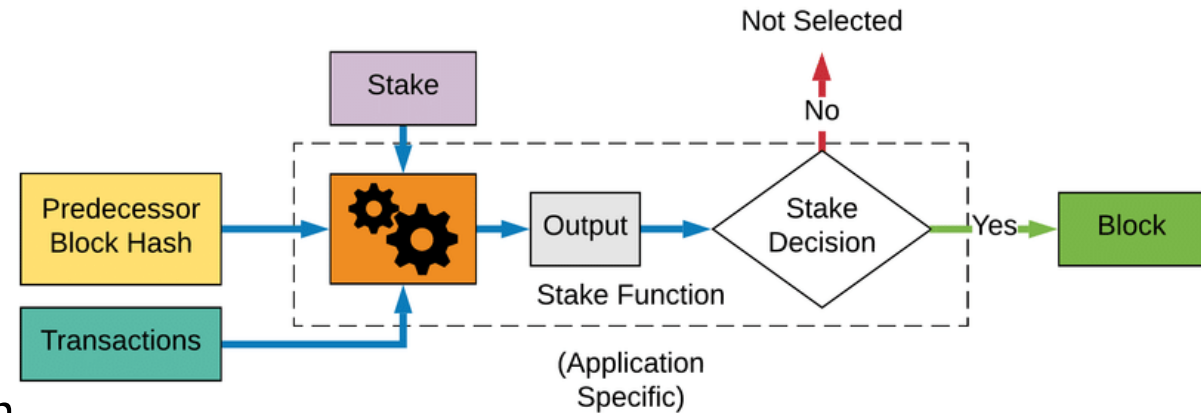
# Types of Consensus Algorithms:

## Proof Of Stake



# Proof Of Stake

- Proof of Stake (PoS) is a consensus mechanism used in blockchain networks to validate and secure transactions and create new blocks in the blockchain.
- It is an alternative to Proof of Work (PoW), which is the consensus mechanism used in popular cryptocurrencies like Bitcoin. PoS was designed to address some of the environmental and scalability concerns associated with PoW.



Here's a brief explanation of how Proof of Stake works:

1. **Validators and Stakers:** In a PoS system, participants are referred to as validators or stakers. These participants are responsible for validating transactions and adding them to the blockchain. Instead of miners solving complex mathematical puzzles like in PoW, validators in PoS are chosen to create new blocks and validate transactions based on the amount of cryptocurrency they hold and are willing to "stake" as collateral.

2. **Stake and Validation:** To become a validator in a PoS network, a participant must lock up a certain amount of the cryptocurrency native to that network as collateral. This collateral is referred to as a "stake." The larger the stake, the higher the probability that the participant will be chosen to validate transactions and create new blocks. This is in contrast to PoW, where miners must invest in expensive hardware and consume electricity to compete for block rewards.
3. **Block Validation:** Validators take turns proposing and validating new blocks. The probability of being selected to propose and validate a block is typically proportional to the size of their stake. Validators are financially incentivized to act honestly, as they have a lot to lose (their staked cryptocurrency) if they attempt to cheat the system.
4. **Block Rewards:** Validators are rewarded with transaction fees and, in some cases, newly created cryptocurrency coins for successfully validating and adding a block to the blockchain. These rewards are distributed in proportion to the size of their stake.
5. **Slashing:** PoS networks often have mechanisms in place to penalize validators who engage in malicious behavior, such as double-spending or attempting to create fraudulent blocks. Validators may lose a portion of their staked cryptocurrency as a penalty in a process called "slashing."

# Benefits Of Proof Of Stake (PoS)

1. **Energy Efficiency:** PoS is more energy-efficient than PoW because it doesn't require the massive computational power that PoW mining does.
2. **Scalability:** PoS is generally considered more scalable because it doesn't involve the same resource-intensive competition as PoW mining.
3. **Security:** PoS incentivizes validators to act honestly, as they have a significant financial stake at risk.
4. **Environmental Impact:** PoS reduces the environmental impact associated with energy-intensive PoW mining.

Many blockchain projects have adopted PoS as their consensus mechanism, including Ethereum 2.0, Cardano, and Tezos, among others. Each PoS system may have its unique rules and variations on the basic principles of PoS, but they all rely on staking and financial incentives to maintain the network's security and integrity.

1 Validators staking some of their coins to get picked up for adding a new block of transactions



2 Coins at "STAKE" in an escrow account



3 Function that randomly picks a validator



4 Joey got selected to add his block to the blockchain network



5 New block is validated by the Validators in the network

VALID

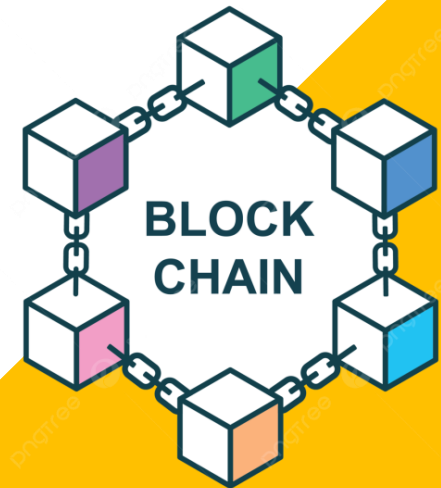
Joey gets to add his new block and receives network fee as a reward

INVALID

Joey loses his staked coins to the network

# Types of Consensus Algorithms:

## Proof Of Work



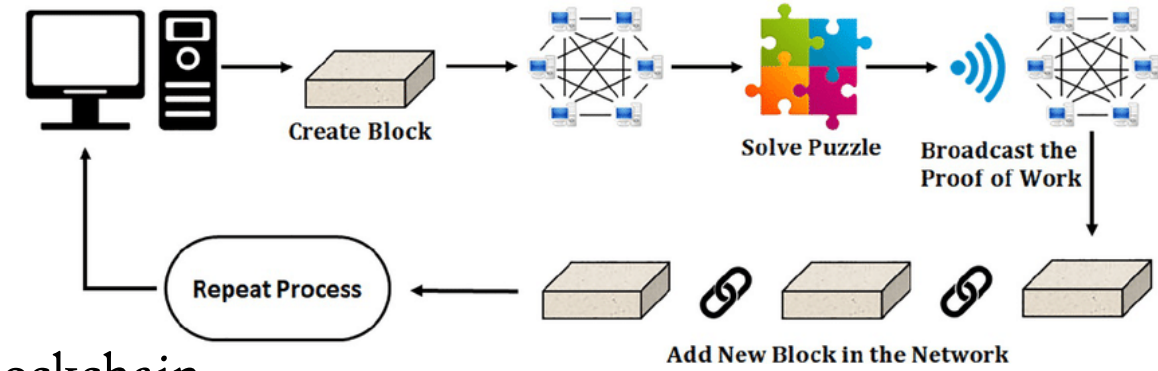


# Proof Of Work

- Proof of Work (PoW) is a consensus mechanism used in blockchain networks to validate and secure transactions, as well as to create new blocks in the blockchain.
- It is the original and most well-known consensus mechanism and is used in cryptocurrencies like Bitcoin. PoW was introduced by Satoshi Nakamoto in the Bitcoin whitepaper in 2008.

Here's how Proof of Work works:

1. **Miners:** Participants in the PoW network are called miners. Miners are responsible for solving complex mathematical puzzles, known as proof-of-work puzzles, to validate transactions and create new blocks. These puzzles require significant computational power and are intentionally difficult to solve.
2. **Mining Process:** Miners compete to solve the proof-of-work puzzle by using their computer's processing power to find a solution. The first miner to solve the puzzle broadcasts the solution to the network, and other nodes verify the solution.



3. **Verification:** Other nodes in the network verify that the proposed solution is correct by applying it to the pending transactions. If the solution is valid, the miner's block is added to the blockchain, and the transactions are considered confirmed.
4. **Block Rewards:** Miners are rewarded for their efforts with cryptocurrency coins, often in the form of transaction fees and newly created coins (block rewards). This incentivizes miners to participate in the network and secure it.
5. **Difficulty Adjustment:** The PoW network adjusts the difficulty of the proof-of-work puzzles over time to ensure that blocks are created at a consistent rate. This adjustment helps maintain the network's security and integrity.



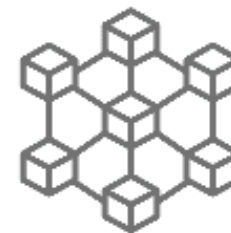
A method

that involves



Monitoring and verifying  
the transactions

taking place  
on a



Blockchain  
Network

# Benefits Of Proof Of Work (PoW)

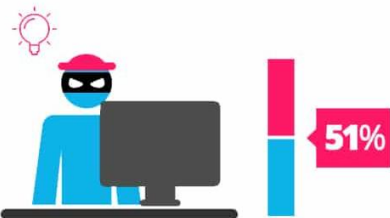
1. **Security:** PoW is considered highly secure because it requires significant computational power to successfully mine new blocks. This makes it difficult and costly for malicious actors to attack the network.
2. **Decentralization:** PoW encourages decentralization, as anyone with the necessary hardware can participate in the network as a miner.
3. **Reliability:** PoW has proven to be a reliable and battle-tested consensus mechanism through the success of cryptocurrencies like Bitcoin.

However, PoW also has some drawbacks, most notably its environmental impact. Mining in PoW consumes vast amounts of electricity and requires specialized hardware, leading to concerns about energy consumption and carbon emissions.

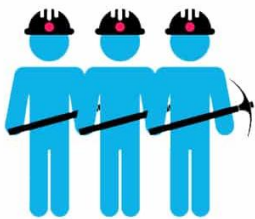
## Proof of Work



To add each block to the chain, miners must compete to solve a difficult puzzle using their computers processing power.



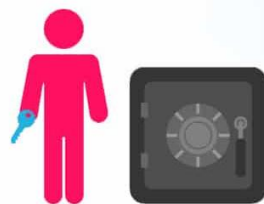
In order to add a malicious block, you'd have to have a computer more powerful than 51% of the network.



The first miner to solve the puzzle is given a reward for their work.

vs.

## Proof of Stake



There is no competition as the block creator is chosen by an algorithm based on the user's stake.



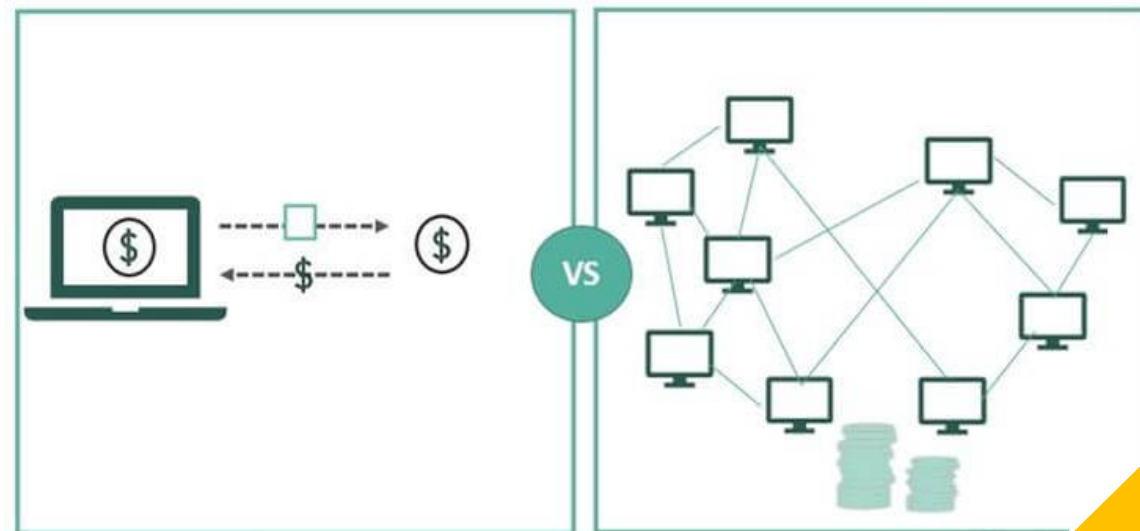
In order to add a malicious block, you'd have to own 51% of all the cryptocurrency on the network.



There is no reward for making a block, so the block creator takes a transaction fee.

# Difference

## Proof of Work vs Proof of Stake



**Proof of Work**

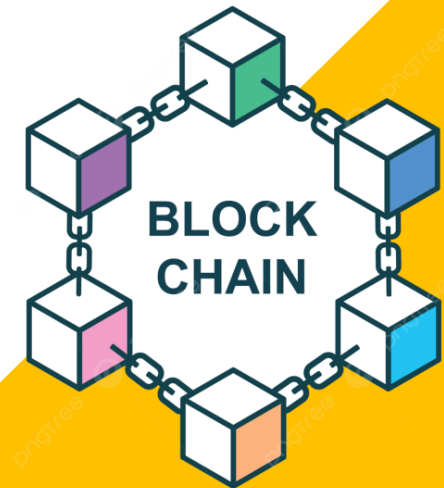
vs



**Proof of Stake**

## Types of Consensus Algorithms:

# Delegated Proof Of Stake



# Delegated Proof Of Stake

- Delegated Proof of Stake (DPoS) is a consensus algorithm used in blockchain technology to validate and confirm transactions and create new blocks in a blockchain.
- DPoS is an alternative to the more traditional Proof of Work (PoW) and Proof of Stake (PoS) consensus mechanisms.
- It was designed to address some of the scalability and energy consumption issues associated with PoW, while also providing faster transaction processing times.
- In a DPoS system, token holders of the blockchain's native cryptocurrency can vote for a select number of delegates (often referred to as "witnesses" or "block producers") who are responsible for validating transactions and creating new blocks.
- These delegates are typically the entities with the most votes and are tasked with running network nodes.
- The number of delegates is limited, which helps maintain efficiency and scalability.



Here's how DPoS generally works:

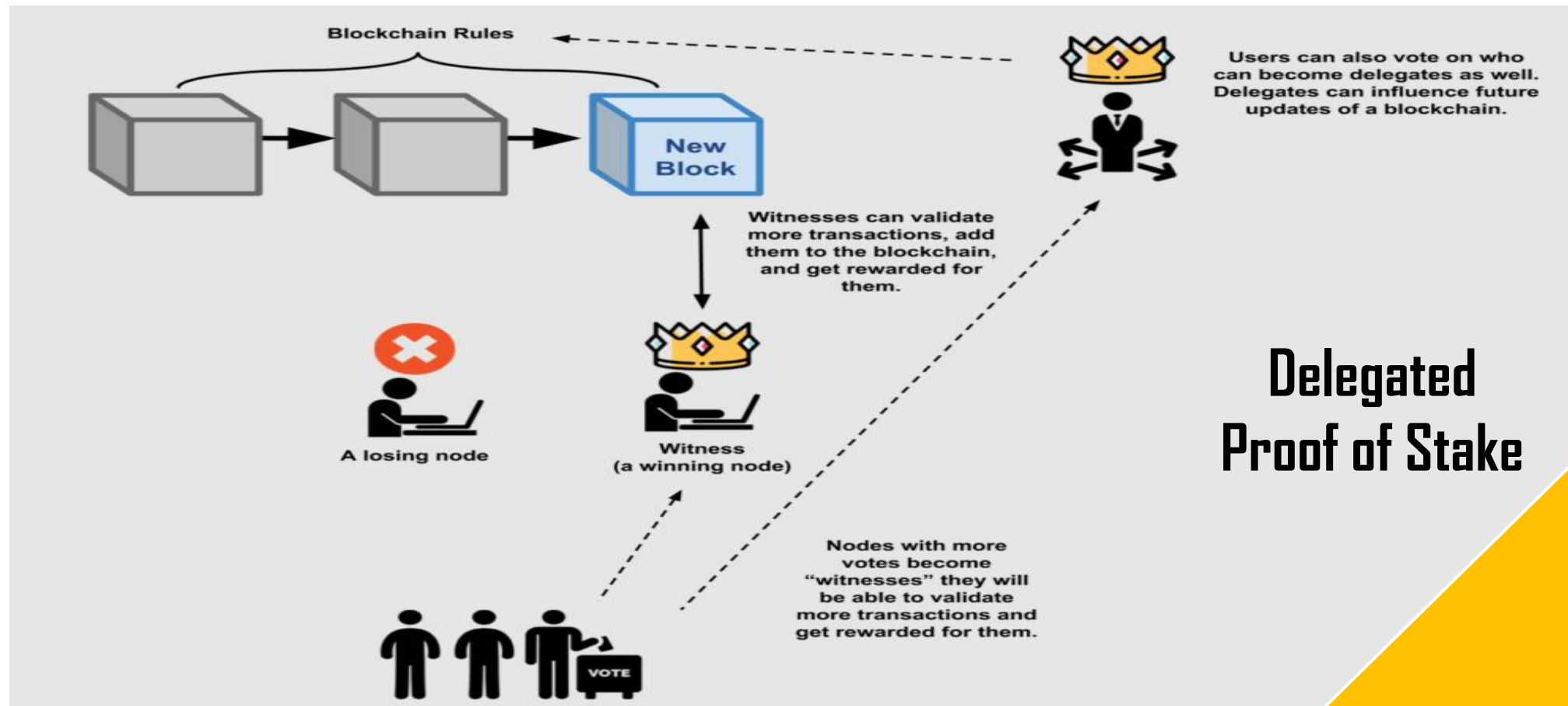
1. **Token Holders Vote:** Token holders in the blockchain network vote for their preferred delegates by staking their tokens. Delegates with the most votes become active participants in block production and validation.
2. **Block Production:** Delegates take turns producing new blocks in a round-robin fashion. This rotation ensures that multiple parties have the opportunity to participate and keeps the network decentralized.
3. **Transaction Validation:** Delegates validate transactions and add them to the blockchain. If a delegate behaves dishonestly or fails to perform their duties, they can be voted out and replaced with more trustworthy candidates.
4. **Block Rewards:** Delegates are rewarded for their services with cryptocurrency tokens. This incentivizes them to perform their duties accurately and maintain the network's security and integrity.

Some well-known blockchain platforms that use DPoS or a similar variant include EOS, TRON, and BitShares.

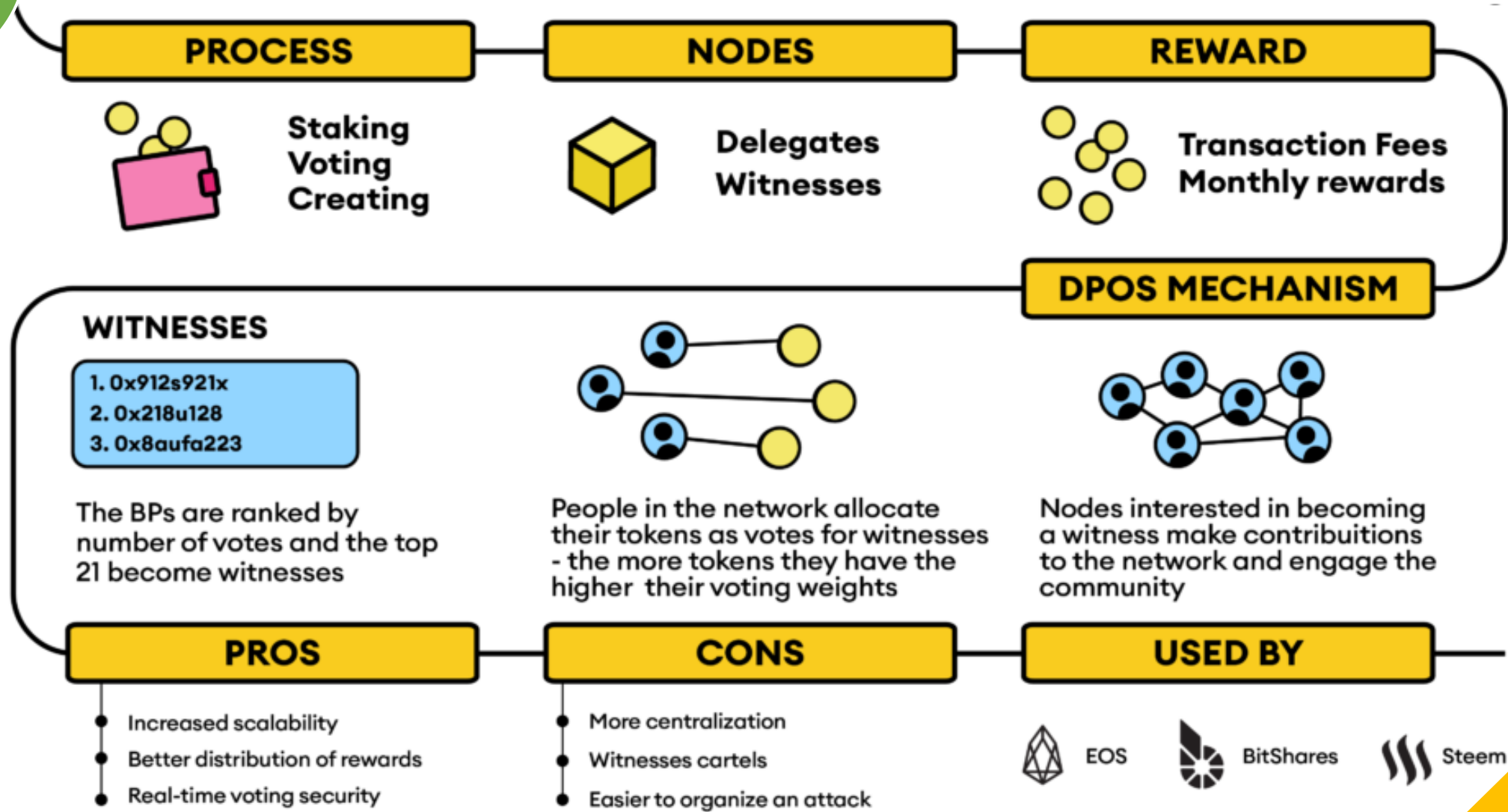




DPoS has the advantage of being more energy-efficient than PoW because it doesn't require the computational "mining" process that consumes significant amounts of electricity. However, it has also faced criticism for potentially centralizing power in the hands of a few major delegates or stakeholders. The governance structure and rules for DPoS can vary between different blockchain projects, and the effectiveness of DPoS largely depends on the design and execution of the specific blockchain system.







## Delegated Proof of Stake

## Types of Consensus Algorithms:

# Proof Elapsed Time



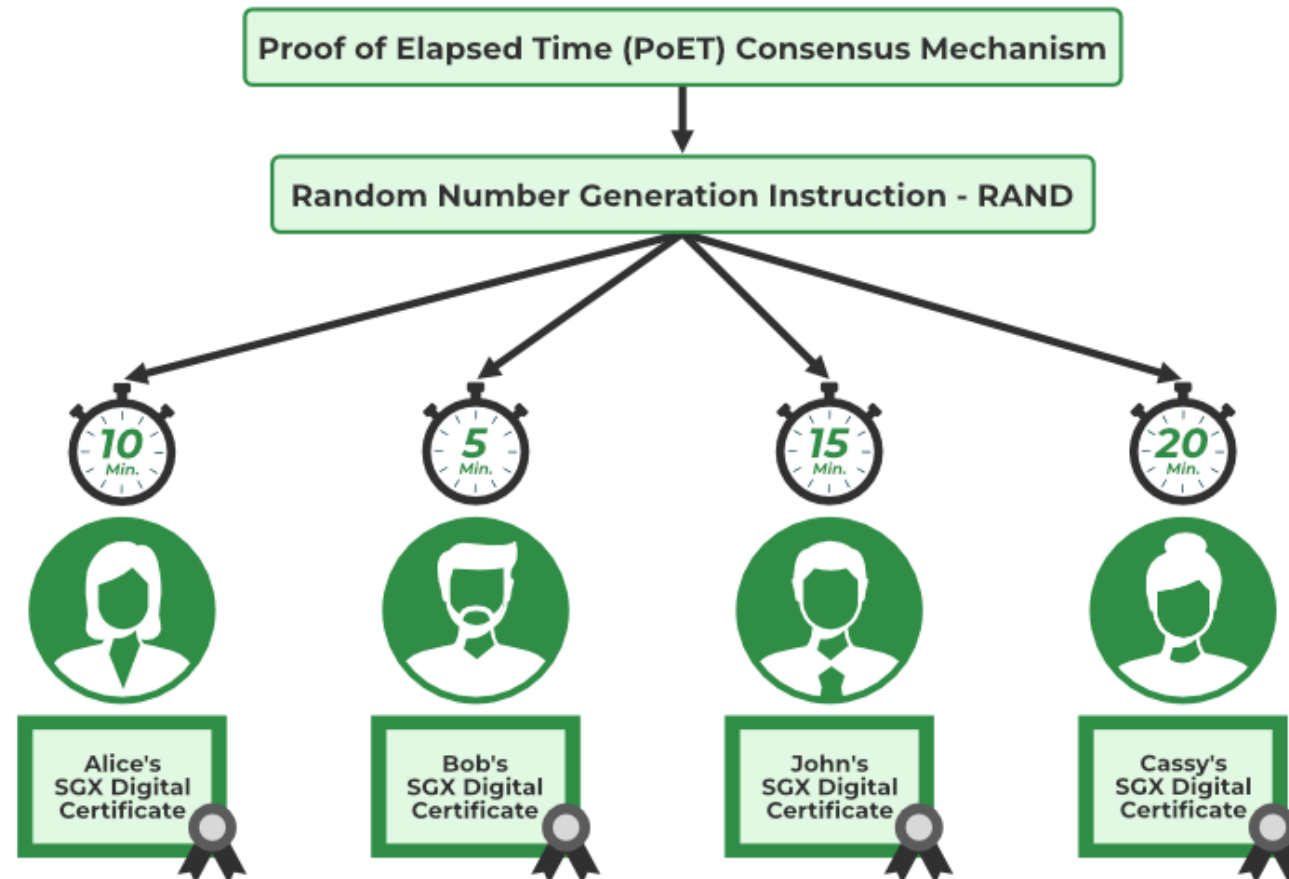
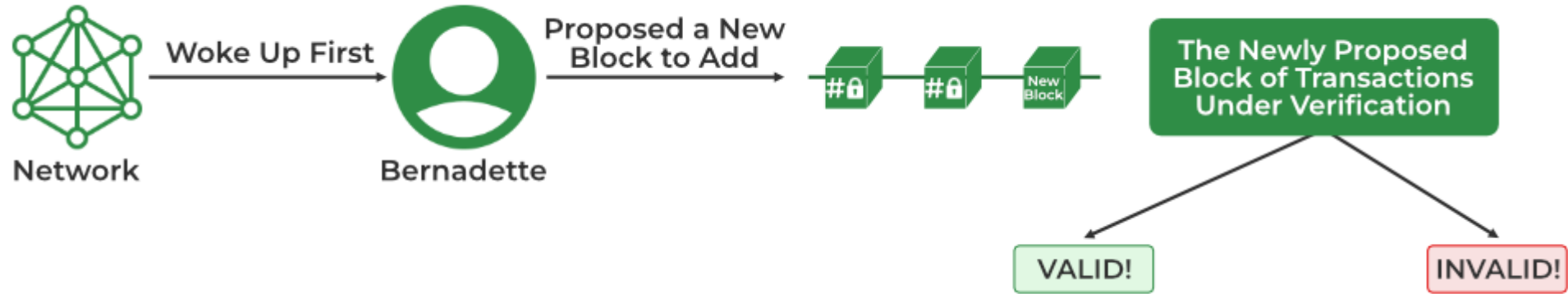
# Proof Of Elapsed Time

- Proof of Elapsed Time (PoET) is a consensus algorithm used in some blockchain systems to achieve consensus and validate transactions.
- It was originally developed by Intel and introduced as part of the Hyperledger Sawtooth framework, an open-source distributed ledger project hosted by the Linux Foundation.
- PoET is designed to address some of the energy efficiency concerns associated with traditional Proof of Work (PoW) algorithms, such as those used in Bitcoin, while still maintaining a decentralized and secure network. It does so by leveraging trusted execution environments (TEEs) provided by modern hardware, such as Intel's Software Guard Extensions (SGX).

Here's how PoET generally works:

1. **Wait Time Lottery:** In PoET, participants in the network must wait for a random amount of time, which is determined by a lottery process. Each participant requests a "wait time" from a trusted function within a TEE.

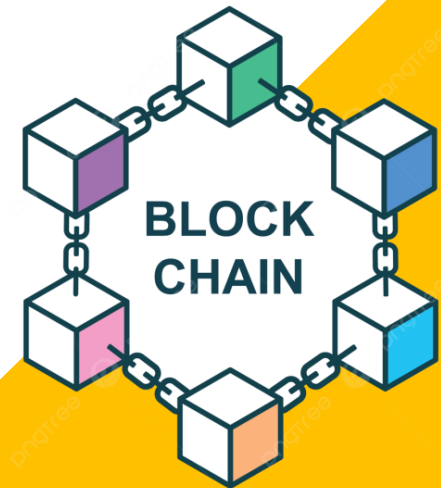
2. **Validation:** The participant who finishes waiting for the shortest amount of time is allowed to create the next block in the blockchain. This is similar to the lottery concept in PoW, where miners compete to solve a difficult computational puzzle to create a new block.
  3. **Creating the Block:** The participant who wins the lottery and creates the new block is rewarded with cryptocurrency tokens and the right to include a set of transactions in the block.
- The idea behind PoET is that it doesn't rely on energy-intensive computations, as in PoW, but rather on a trusted hardware-based randomization process to select the next block producer. This reduces the energy consumption and environmental impact of the consensus mechanism.
  - It's worth noting that PoET relies on trust in the hardware's security properties, specifically the TEEs. If a TEE were compromised, it could undermine the security of the blockchain using PoET. Therefore, the effectiveness of PoET depends on the robustness and security of the hardware involved.
  - While PoET is a novel approach to achieving consensus in a more energy-efficient way, it is not as widely adopted as other consensus mechanisms like Proof of Work (PoW), Proof of Stake (PoS), or Delegated Proof of Stake (DPoS). The choice of consensus mechanism depends on the specific goals and requirements of a blockchain project.



**Working**  
**Proof of Elapsed Time**

## Types of Consensus Algorithms:

# Deposit-Based Consensus

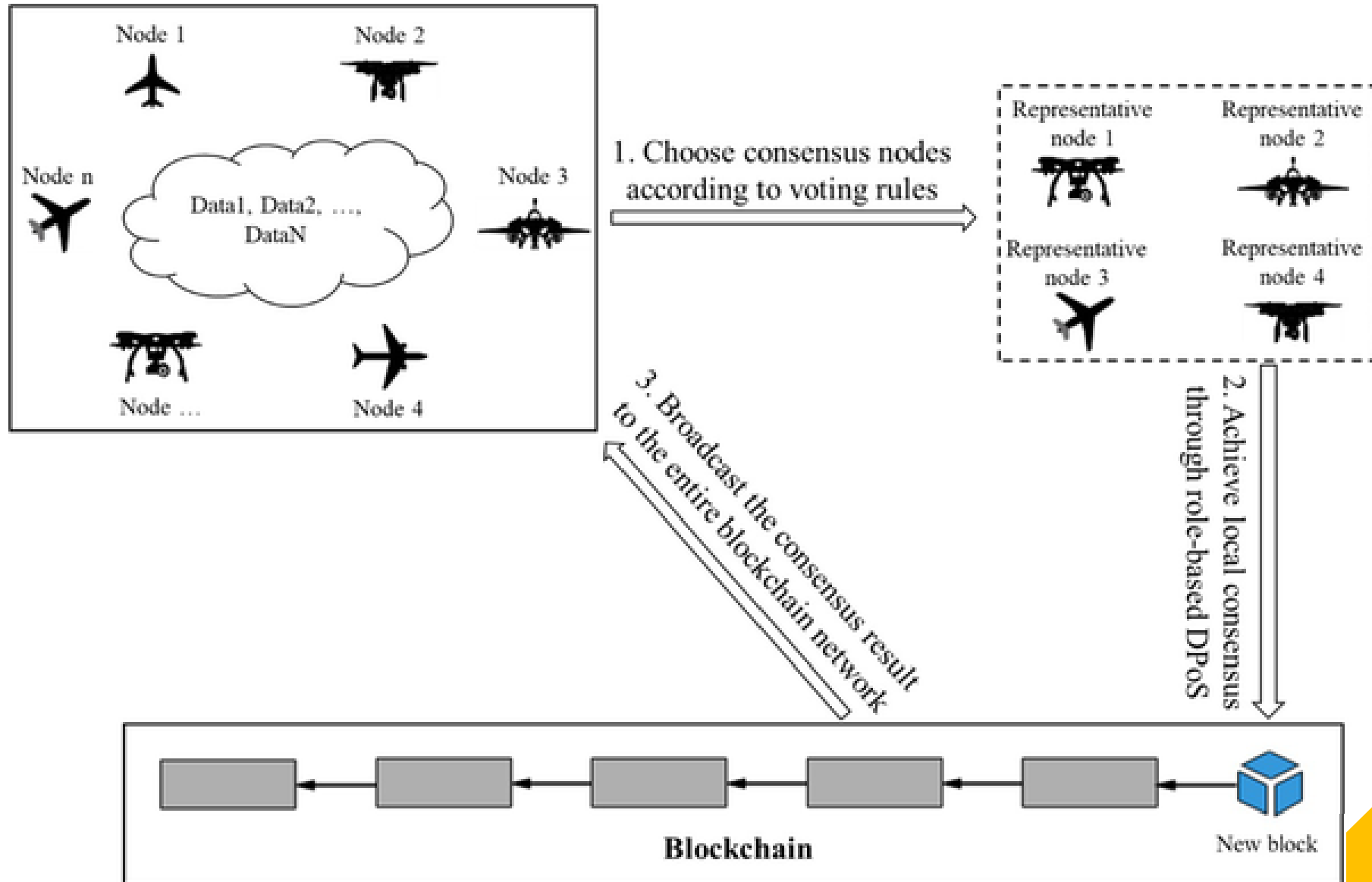


# Deposit-Based Consensus

- "Deposit-based consensus" refers to a consensus mechanism in which participants in a blockchain network are required to make a deposit or stake a certain amount of cryptocurrency or other valuable assets as collateral to participate in the consensus process. The deposits serve as a form of commitment, and they can be forfeited in case a participant acts maliciously or violates the network's rules. This type of consensus mechanism is often used to promote honest and secure behaviour within the network.
- A well-known example of a deposit-based consensus mechanism is "Proof of Stake" (PoS). In PoS, participants, also known as validators or stakes, are required to lock up a certain amount of cryptocurrency as collateral in order to have the chance to create new blocks and validate transactions. The more cryptocurrency a participant stakes, the higher the probability they have of being selected as a validator for the next block. If a validator acts dishonestly or violates the network's rules, they can lose their staked assets as a penalty, which incentivizes them to behave honestly.

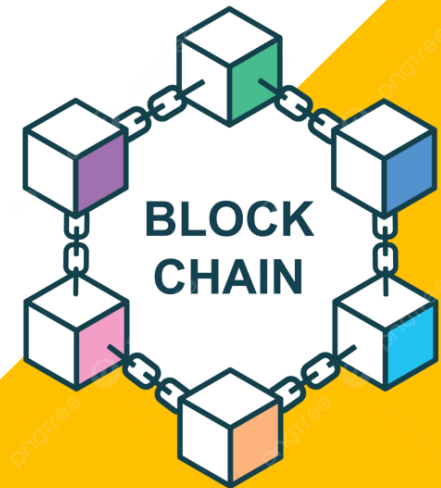
- Another related concept is "Delegated Proof of Stake" (DPoS), where token holders vote for a select number of delegates who are responsible for block validation, and these delegates often have to make a deposit or stake a certain amount of tokens to be eligible for the position. DPoS combines elements of both deposit-based consensus and delegation.
- Deposit-based consensus mechanisms aim to enhance network security and reduce the risk of malicious behaviour by requiring participants to have a vested interest in the network's success. The specific rules and requirements for deposit-based consensus mechanisms can vary from one blockchain project to another, and they are designed to align the interests of participants with the overall integrity and security of the network.





## Types of Consensus Algorithms:

# Proof Of Importance



# Proof Of Importance

"Proof of Importance" (PoI) is a consensus mechanism that was initially introduced by the NEM (New Economy Movement) blockchain platform.

It is designed to determine the likelihood of a node being chosen to validate transactions and create new blocks in a blockchain-based on factors beyond just the amount of cryptocurrency tokens held, as in traditional Proof of Stake (PoS) systems.

PoI aims to encourage active and positive participation within the network.

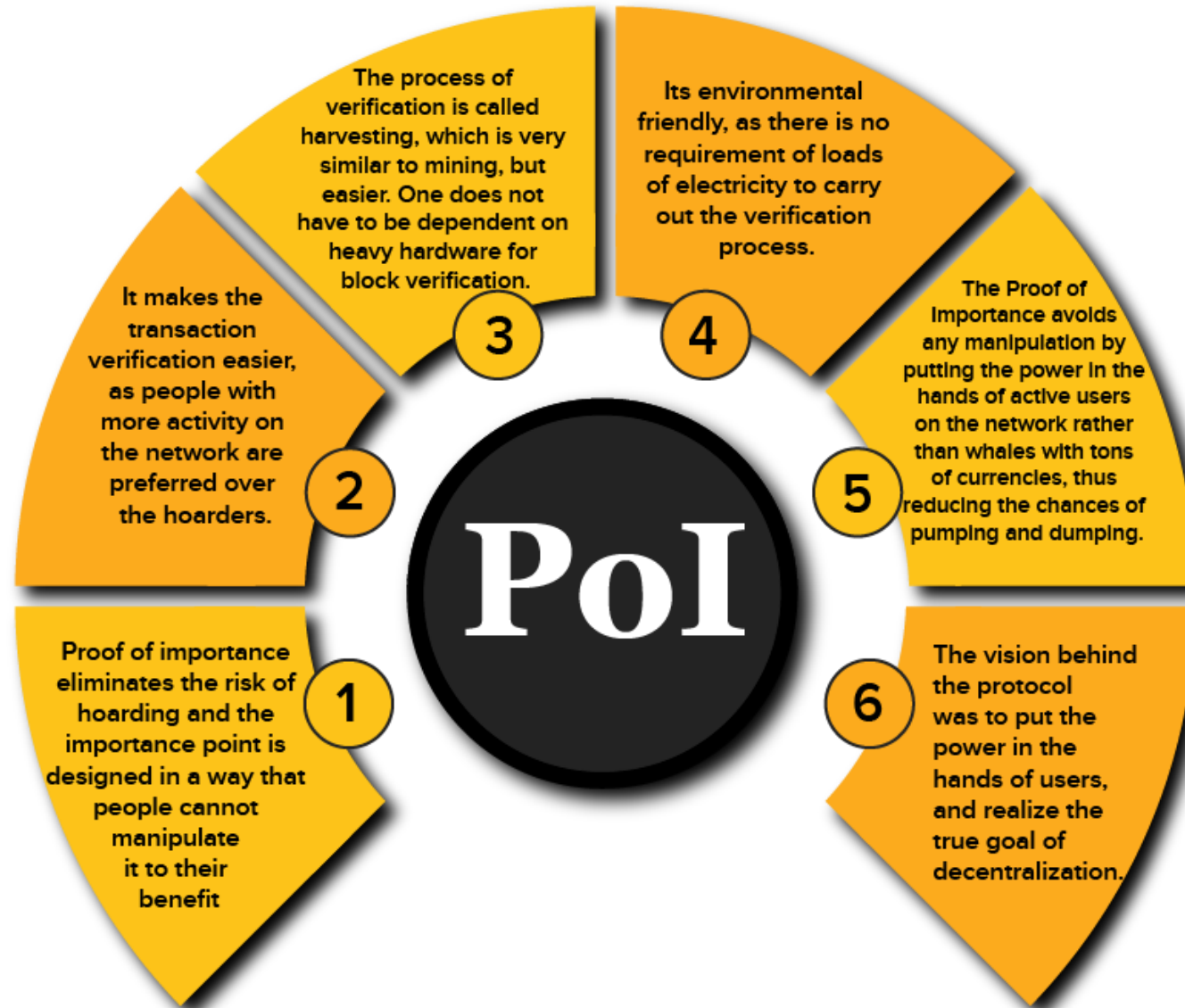
Here are the key concepts of PoI:

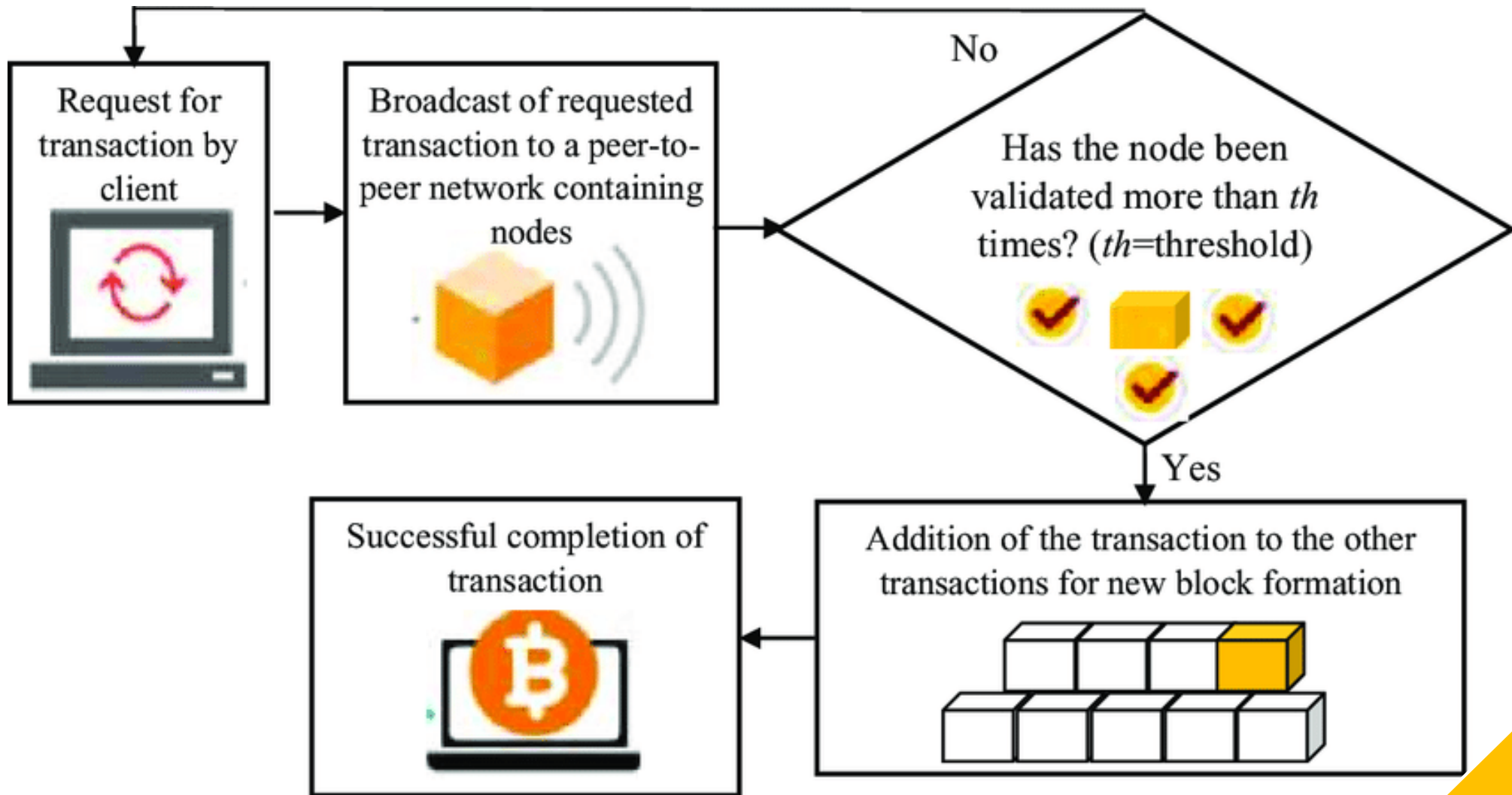
1. **XEM Holdings:** NEM's native cryptocurrency is called "XEM." To participate in PoI, a user needs to hold a certain minimum amount of XEM in their wallet. The more XEM held, the higher the individual's chances of being chosen to participate in the consensus process.
2. **Transactions:** PoI takes into account the number of transactions in which a user has been involved. It values users who both send and receive transactions, which encourages active participation on the network.

3. **Harvesting:** Users can "harvest" on the NEM network, which is similar to the process of mining or validating transactions in other blockchain systems. Harvesting involves actively processing and confirming transactions.
4. **Node Reputation:** A user's reputation is also considered in PoI. Users can improve their reputation by maintaining a higher balance of XEM in their wallet, actively participating in transactions, and generally acting positively within the network.
5. **Proof of Importance Score:** Each user's PoI score is calculated based on these factors, and those with higher scores have a better chance of being chosen as a harvester, responsible for validating transactions and creating new blocks.

The idea behind PoI is to encourage network participation, rather than simply rewarding those who hold large amounts of cryptocurrency. It is designed to promote active engagement in the blockchain network and maintain its security and integrity.

# Why Proof Of Importance (PoW) ?



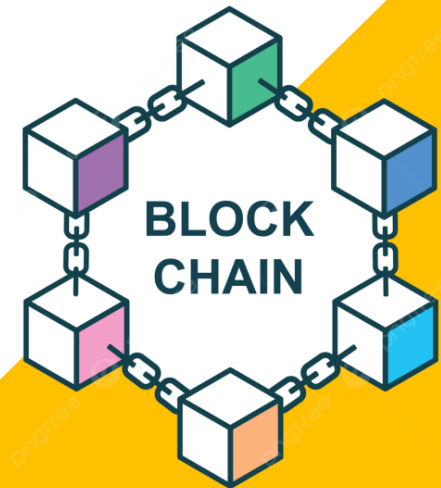


**Working**

**Proof of Importance**

## Types of Consensus Algorithms:

# Federated Consensus



# Federated Consensus

Federated Consensus is a consensus mechanism used in certain blockchain systems to achieve agreement on the state of the blockchain.

It involves a federation or group of trusted validators who collectively make decisions regarding transaction validation and block creation.

Federated consensus is commonly used in private or permissioned blockchain networks, where the participants are known and trusted entities, such as organizations, rather than anonymous participants as in public blockchains like Bitcoin.

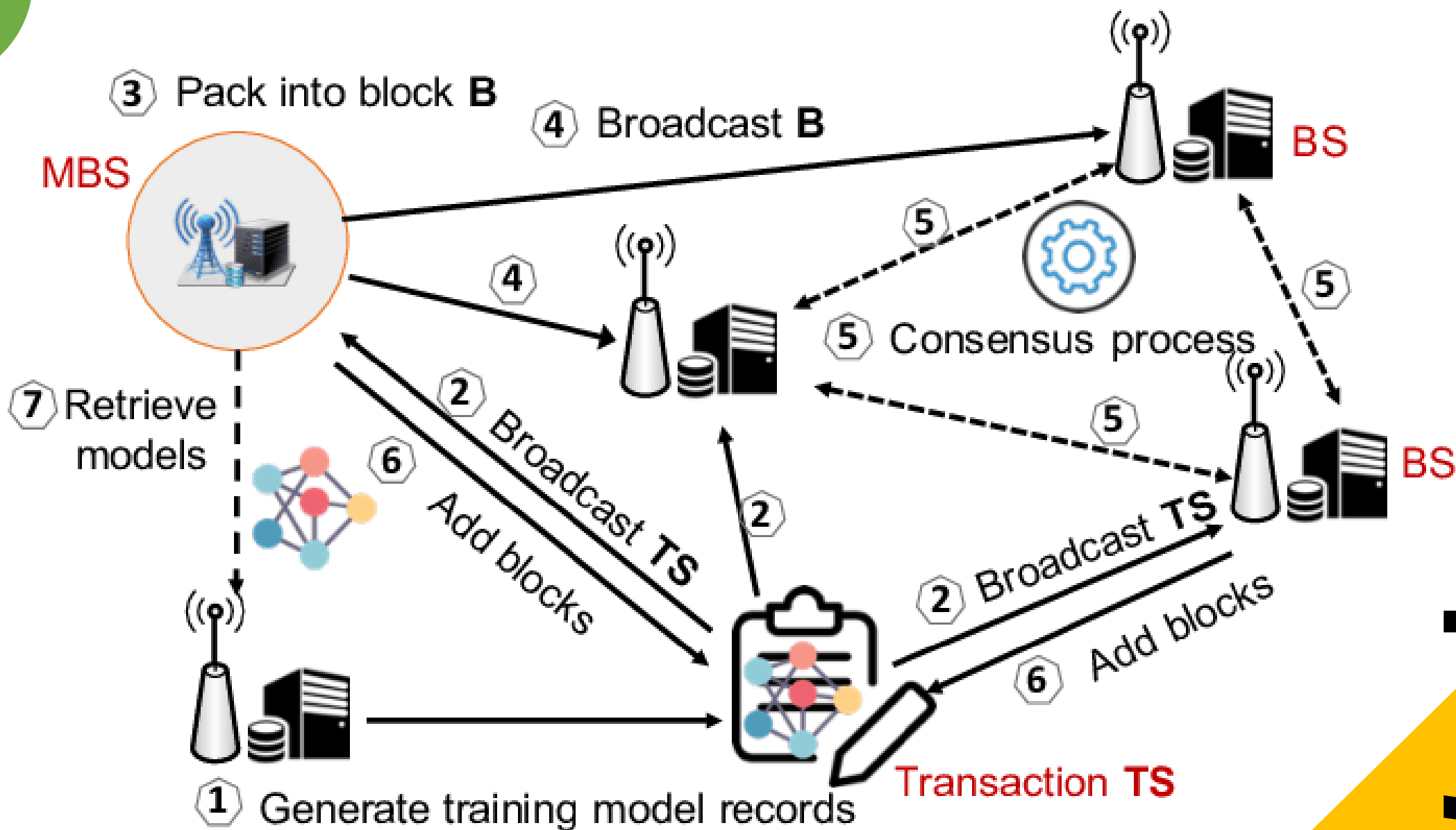
Here are some key features of Federated Consensus:

1. **Trusted Federation:** In a federated consensus system, the network relies on a federation of known validators or nodes to reach consensus. These validators are typically pre-selected and trusted participants who have the authority to validate transactions and create new blocks.
2. **Efficiency:** Federated consensus mechanisms are often more efficient and faster compared to Proof of Work (PoW) or Proof of Stake (PoS) because the trust among participants is established beforehand, eliminating the need for resource-intensive mining or staking.



3. **Security and Control:** Since the validators in a federated consensus system are known and trusted, the network can maintain a higher degree of security and control. This is particularly important in enterprise or consortium blockchain settings where compliance and governance are key concerns.
4. **Scalability:** Federated consensus mechanisms can be more scalable because they don't require the computational work seen in PoW, and the limited number of validators allows for faster decision-making.
5. **Examples:** Examples of blockchain platforms that use federated consensus mechanisms include Hyperledger Fabric and Corda. These platforms are designed for specific use cases, such as supply chain management or financial services, where a consortium of entities works together.

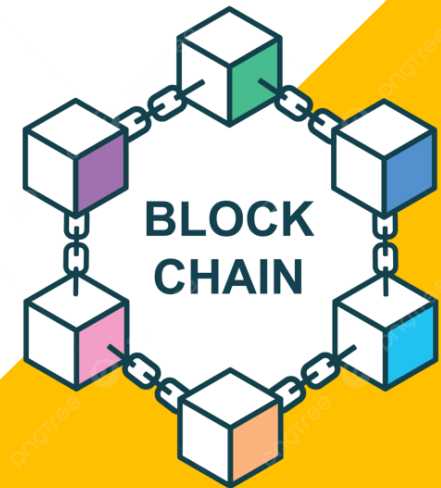
In summary, Federated Consensus is a consensus mechanism that leverages a predefined group of trusted participants to reach agreement on transactions and block creation. It is a suitable choice for private and permissioned blockchains where participants are known and can work together efficiently, securely, and with a high degree of control.



**Working** Federated Consensus

## Types of Consensus Algorithms:

# Federated Byzantine Consensus



# Federated Byzantine Consensus

"Federated Byzantine Consensus" (FBC) is a consensus algorithm that combines the principles of the Byzantine fault-tolerant (BFT) consensus protocol with a federation of trusted validators.

It is designed to provide a high degree of security and consensus in blockchain networks, particularly in private or consortium blockchain settings where participants are known and trusted.

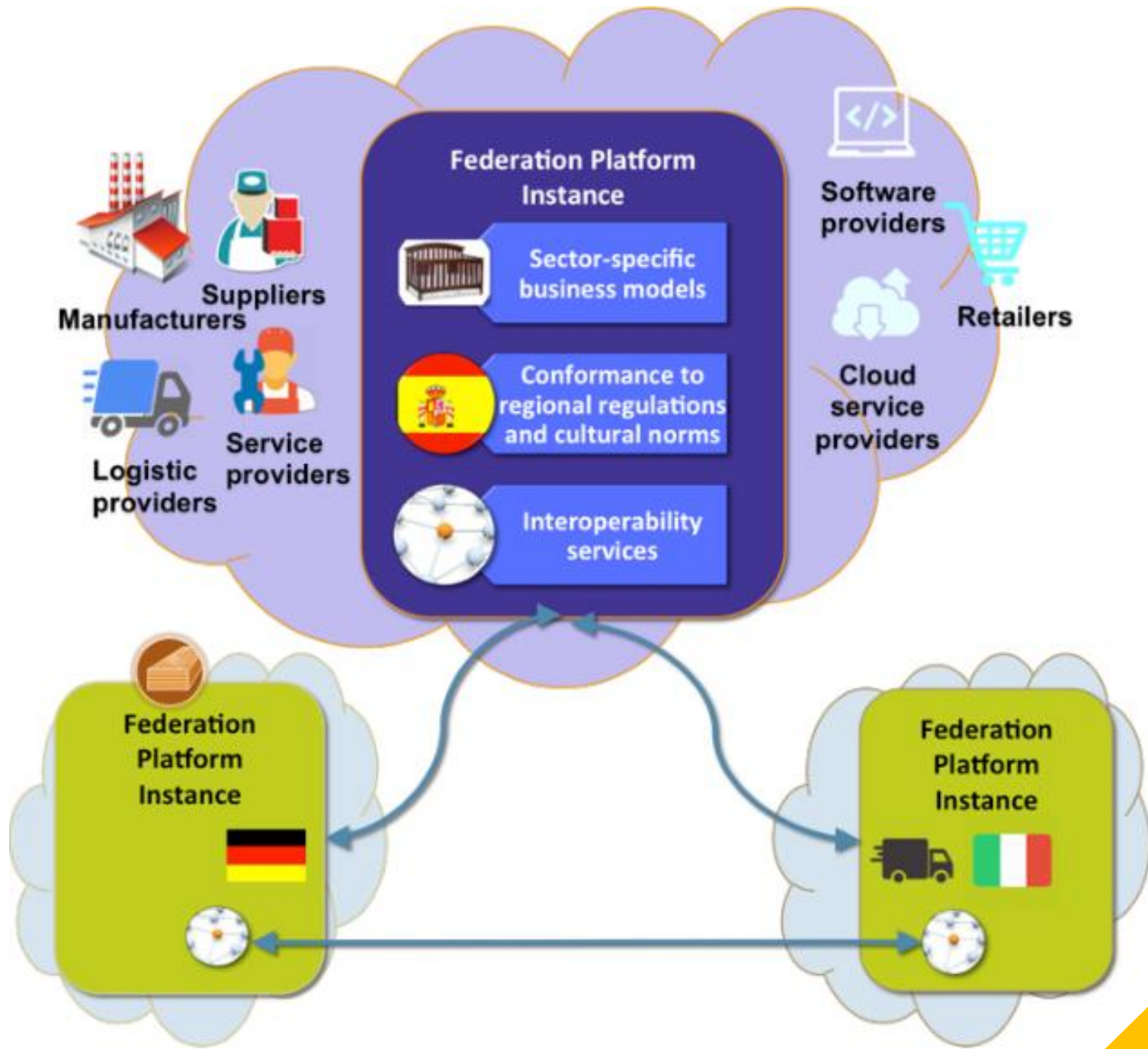
Here are the key features of the Federated Byzantine Consensus:

1. **Byzantine Fault Tolerance:** FBC is designed to address the Byzantine Generals' Problem, which refers to the challenge of achieving consensus in a distributed network when some nodes may be faulty or malicious. FBC ensures that consensus can be reached even in the presence of Byzantine faults.
2. **Federation of Validators:** In FBC, a limited and known set of validators, often referred to as a federation, participate in the consensus process. These validators are selected and trusted by the network's participants.

3. **Voting and Agreement:** Validators in the federation communicate and reach a consensus through a voting process. They agree on the state of the blockchain and validate transactions by signing and confirming them.
4. **Security and Finality:** FBC offers a high level of security and finality. Once a sufficient quorum of validators agrees on a set of transactions, they are considered confirmed and cannot be easily reversed.
5. **Efficiency:** FBC is generally more efficient and scalable compared to Proof of Work (PoW) because it doesn't rely on resource-intensive mining, and it can reach consensus more quickly.
6. **Use Cases:** FBC is often used in private or consortium blockchains where participants are known and trust is established. It is suited for applications in which data privacy and control are important, such as financial services, supply chain management, and government-related use cases.

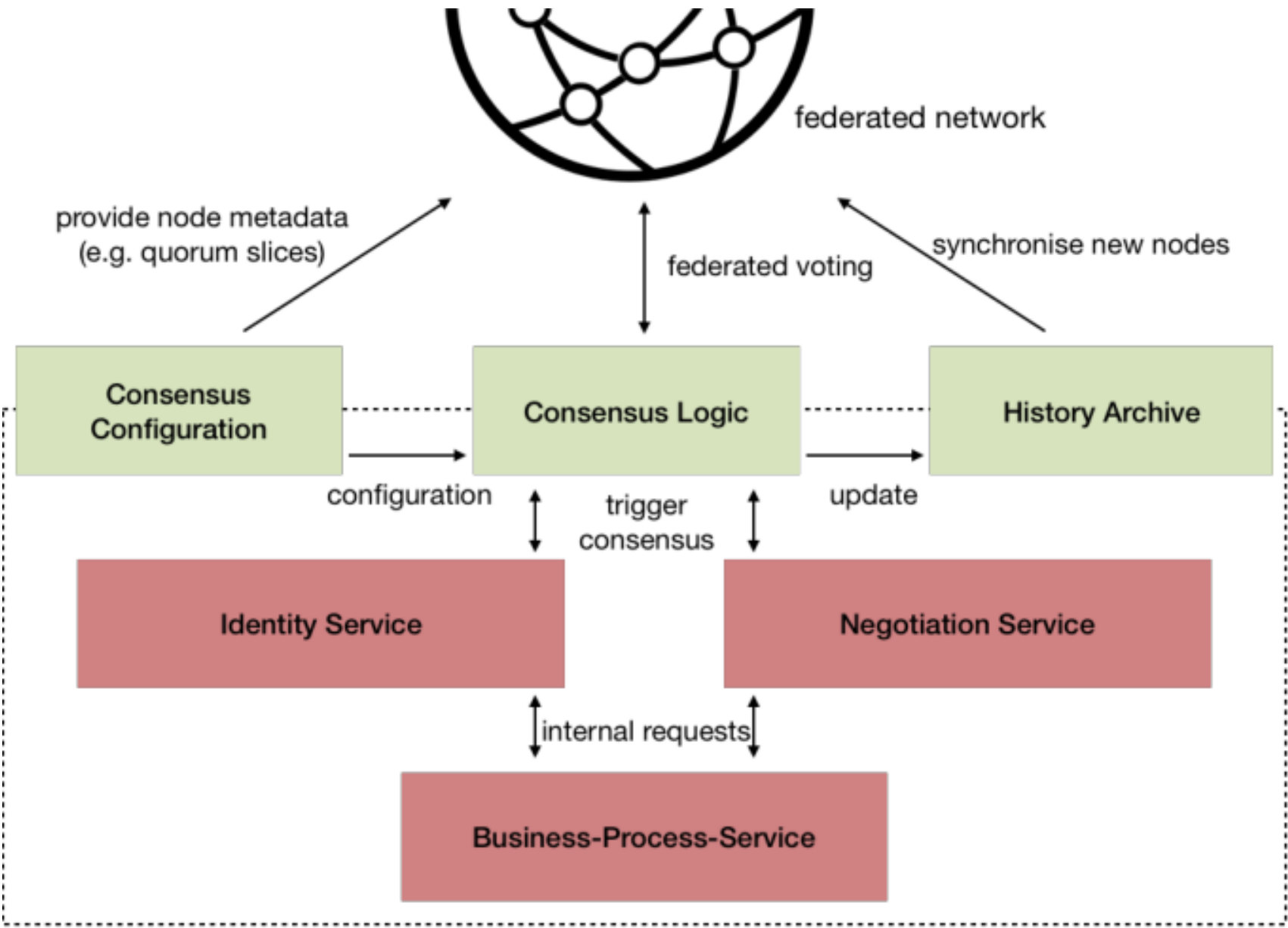
It's important to note that while Federated Byzantine Consensus offers advantages in terms of security and efficiency, it is typically not as decentralized as public blockchains like Bitcoin or Ethereum, where anyone can participate in the consensus process. Instead, it is better suited for use cases where a limited group of known entities collaborates in a more controlled environment

# Benefits



Federated Byzantine Consensus

# Working



# Federated Byzantine Consensus

# Is Federated Consensus and Federated Byzantine Consensus is same or different?

"Federated Consensus" and "Federated Byzantine Consensus" are related terms, but they refer to different concepts in the context of consensus algorithms and blockchain technology.

Let's clarify the difference between the two:

## I. **Federated Consensus:**

- Federated Consensus is a consensus mechanism that involves a group of trusted participants (federated nodes or validators) who collectively make decisions to validate and confirm transactions in a blockchain network.
- It is often used in private or permissioned blockchain networks, where the participants are known and trusted entities, such as organizations or individuals.
- In a federated consensus model, decisions are made by a quorum of participants, and the consensus process is typically more efficient and faster than some other consensus mechanisms, like Proof of Work (PoW) or Proof of Stake (PoS).



- Stellar, for example, uses a Federated Byzantine Agreement (FBA) protocol to achieve consensus among a predefined set of validators.

## 2. Federated Byzantine Consensus:

- Federated Byzantine Consensus, on the other hand, is a specific variant of federated consensus that combines the principles of the Byzantine fault-tolerant consensus protocol with a federated network of validators.
- It is designed to address the Byzantine Generals' Problem, a scenario in distributed computing where some nodes in a network may be malicious or faulty and can send conflicting information.
- In Federated Byzantine Consensus, the network of validators works together to achieve consensus even in the presence of Byzantine faults, ensuring that they agree on the state of the blockchain.
- Stellar's FBA protocol is an example of a Federated Byzantine Consensus algorithm.

## Types of Consensus Algorithms:

# Practical Byzantine Fault Tolerance





# Practical Byzantine Fault Tolerance

Practical Byzantine Fault Tolerance (PBFT) is a consensus algorithm designed to address the Byzantine Generals' Problem, a challenge in distributed computing where nodes in a network may be faulty or malicious, and it's crucial to reach consensus in the presence of such faults.

PBFT is practical because it is known for its efficiency and is often used in permissioned and private blockchain networks where participants are known and trusted.

Here's how PBFT works:

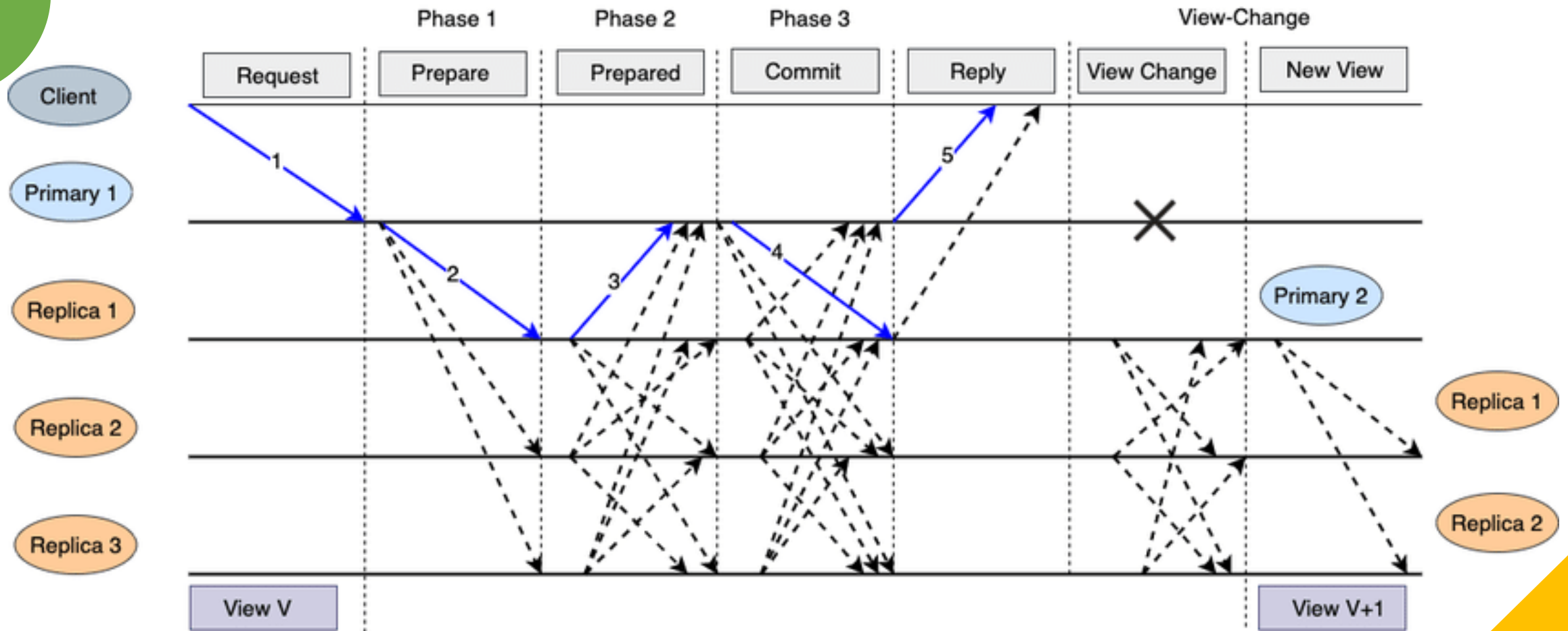
1. **Node Roles:** In PBFT, the network is composed of a set of nodes that take on specific roles. These roles include the primary (leader), replicas, and clients.
2. **Leader Selection:** The primary is chosen among the nodes through a consensus algorithm or a rotating leader selection process. The primary is responsible for proposing new blocks and ordering transactions.
3. **Request and Pre-Prepare Phase:** When a client initiates a transaction, the primary broadcasts a request to all replicas. Each replica verifies the request and replies with a "pre-prepare" message, indicating their readiness to commit the transaction.

- 
- 
3. **Prepare Phase:** Once the primary collects enough pre-prepare messages from replicas, it broadcasts a "prepare" message to the network. Replicas that receive the prepared message, validate it and respond with their own prepare messages, indicating their commitment to the transaction.
  4. **Commit Phase:** When a replica receives enough prepared messages, it broadcasts a "commit" message, confirming its commitment to the transaction.
  5. **Finality:** When a client sees enough commit messages from the replicas, it considers the transaction as finalized and informs the client. Finality means that the transaction is confirmed and cannot be reversed.

# Characteristics Of PBFT

- **Byzantine Fault Tolerance:** PBFT can tolerate up to one-third of the nodes in the network behaving arbitrarily or maliciously while still reaching consensus.
- **Efficiency:** PBFT is known for its efficiency compared to Proof of Work (PoW) and can process transactions quickly, making it suitable for use cases requiring low latency and high throughput.
- **Finality:** PBFT offers finality, meaning that once a consensus is reached on a transaction, it cannot be reversed.
- **Known Participants:** It is typically used in networks where participants are known and trusted, making it more centralized compared to public blockchains.

PBFT is widely used in enterprise and consortium blockchain settings and has been implemented in various blockchain platforms, such as Hyperledger Fabric. It's a practical choice when data privacy, control, and rapid transaction finality are essential requirements.

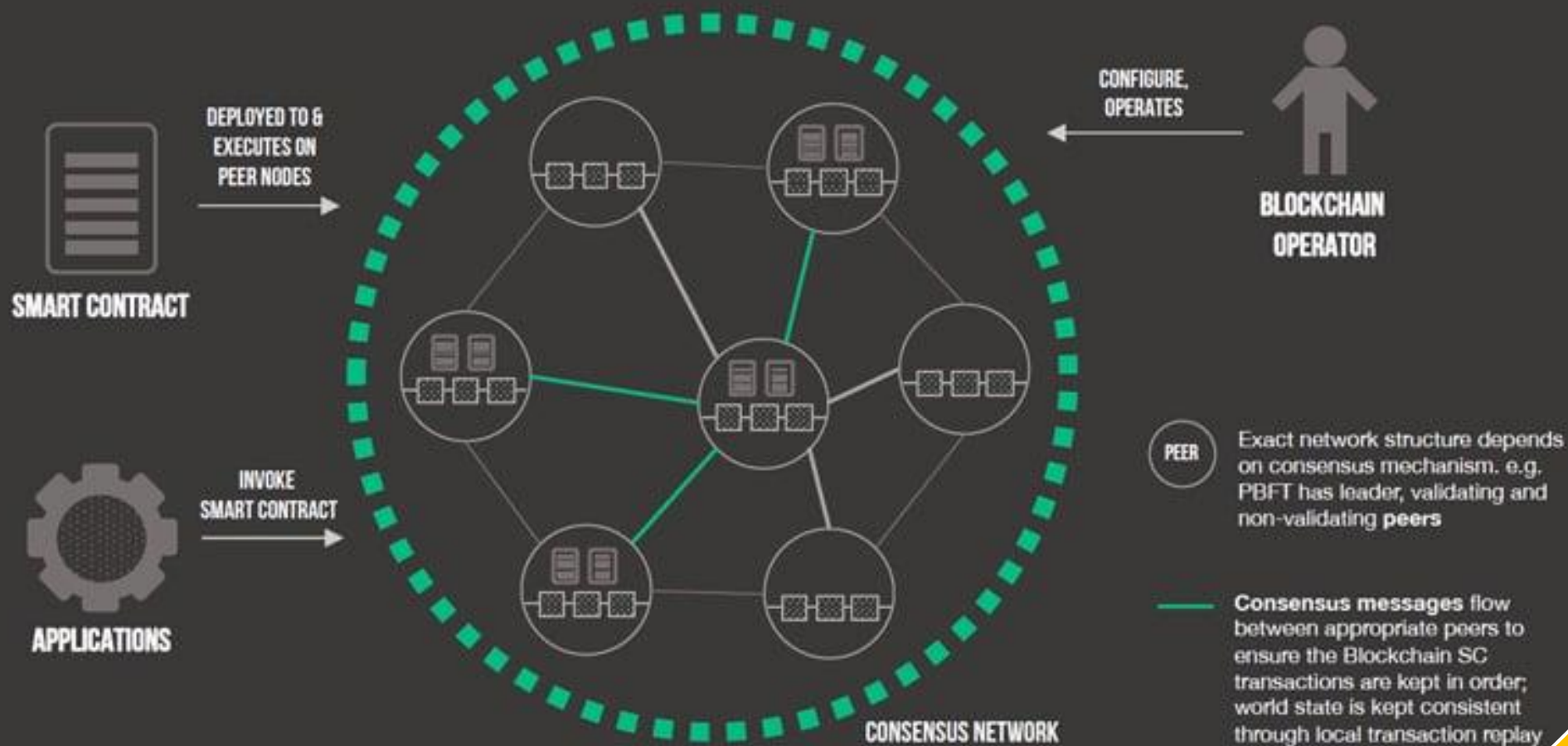


# Working

## Practical Byzantine Fault Tolerance

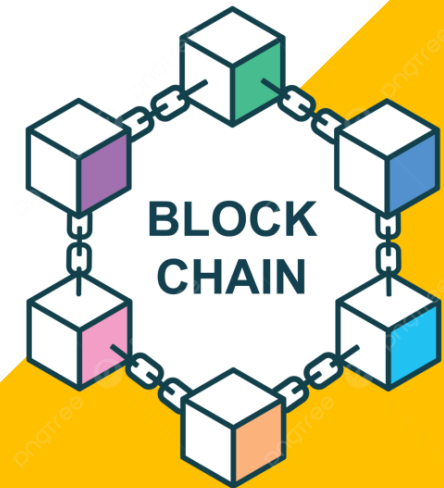
# PRACTICAL BYZANTINE FAULT TOLERANCE

## CONSENSUS AND THE BLOCKCHAIN NETWORK



Practical Byzantine Fault Tolerance

# Supply Chain Management





# Supply Chain Management



- Supply Chain Management (SCM) is one of the prominent use cases for blockchain technology.
- It involves tracking the production, shipment, and delivery of goods or products throughout the entire supply chain, from raw materials to the end consumer.
- Blockchain can address several challenges in supply chain management, providing transparency, traceability, and efficiency.

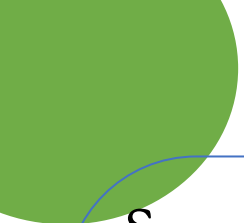


Here's a detailed explanation of how blockchain is used in supply chain management:

1. **Transparency:** Blockchain provides a shared ledger that all participants in the supply chain can access. Each transaction or event in the supply chain is recorded as a block on the blockchain. This transparency ensures that all stakeholders have visibility into the movement and status of products.
2. **Provenance and Traceability:** Blockchain enables the tracking of products from their origin. Every step of the supply chain, from the manufacturer to the distributor to the retailer, can be recorded on the blockchain. This provenance and traceability help identify the source of quality issues or recalls and can reduce fraud and counterfeiting.

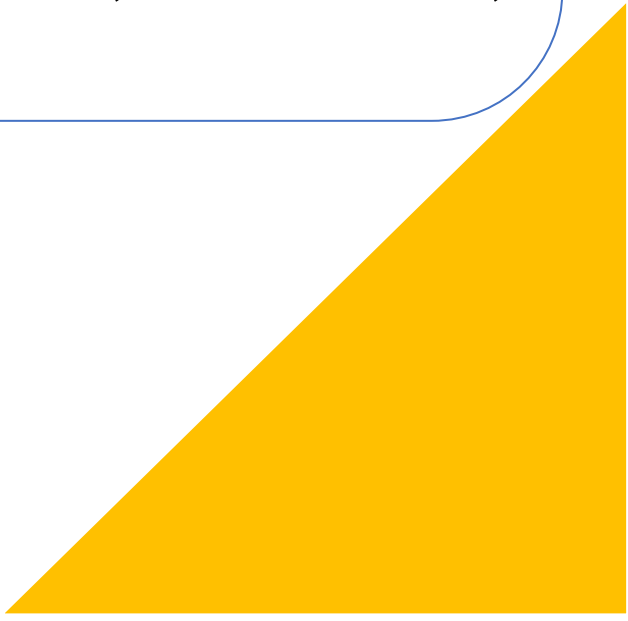
3. **Immutable Records:** Once data is added to the blockchain, it becomes extremely difficult to alter or delete. This immutability ensures that the historical records of the supply chain are secure and trustworthy, preventing data tampering or fraud.
4. **Smart Contracts:** Smart contracts can be integrated into the blockchain to automate various supply chain processes. For example, payment terms can be automatically triggered when products reach certain milestones, reducing the need for manual oversight and reducing administrative costs.
5. **Reducing Fraud:** Counterfeiting and fraud are significant challenges in supply chain management. Blockchain's transparency and immutability make it challenging for bad actors to introduce counterfeit products into the supply chain.
6. **Real-Time Updates:** Blockchain allows real-time updates and alerts, ensuring that all stakeholders are aware of the current status of products. This can be particularly important for perishable goods or those with short shelf lives.
7. **Cost Savings:** By streamlining and automating many supply chain processes, blockchain can lead to cost savings. Reduced paperwork, faster dispute resolution, and efficient tracking can cut down on administrative and operational expenses.

- 
- 
- 8. Efficient Recall Management:** In the event of product recalls or quality issues, blockchain enables swift identification of affected products. This can minimize the impact of recalls on public safety and brand reputation.
  - 9. Compliance and Auditing:** Blockchain records can be used for compliance purposes and auditing. Companies can easily prove adherence to regulations and standards by providing an immutable record of their supply chain activities.
  - 10. Interoperability:** Blockchain can facilitate interoperability among different participants in the supply chain. Organizations with their own systems and databases can connect and share data securely on the blockchain.
  - 11. Environmental and Ethical Concerns:** Blockchain can be used to track the environmental impact of products and ensure ethical sourcing by providing data on the conditions in which products are manufactured.
  - 12. Cross-Border Trade:** In international supply chains, blockchain can simplify customs procedures, reduce fraud, and speed up the movement of goods across borders.

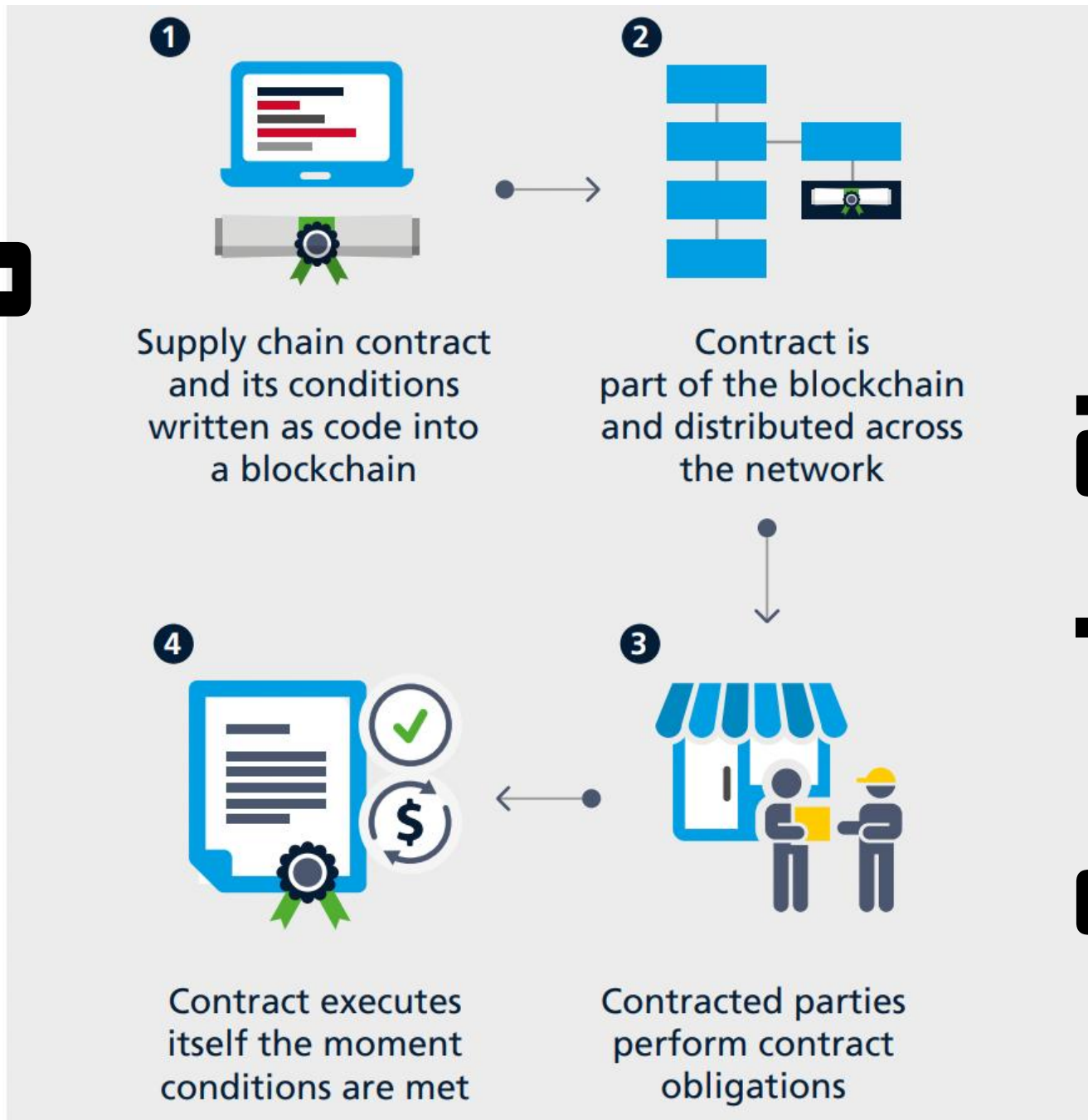


Some notable examples of companies and organizations implementing blockchain for supply chain management include IBM's Food Trust, which tracks the origin and journey of food products, and the TradeLens platform, co-developed by Maersk and IBM, which aims to digitize global trade processes.

In conclusion, blockchain technology in supply chain management offers enhanced transparency, traceability, and automation, which can lead to cost savings, reduce fraud, and improve the overall efficiency and integrity of the supply chain. It's particularly valuable in industries where the provenance and authenticity of products are critical, such as food, pharmaceuticals, and luxury goods.



# Working



# Supply Chain Management

# Top Blockchain Use Cases



Cryptocurrencies



Supply Chains



Voting



Advertising



Insurance



Digital IDs



Credit Ratings



Real Estate

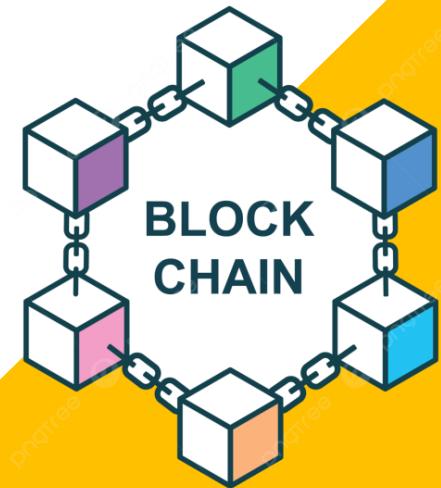


Healthcare



Gaming

# Assignment



# Unit Assignment

1. Define Consensus in the context of Blockchain technology. Why is consensus important in the distributed System?
2. Do the comparison between Proof of Work(PoW) and Proof of Stake(PoS) of the Consensus Algorithm. What are the key differences between each?
3. Explain Proof of Elapsed Time and Proof of Importance.
4. Define Deposit-Based Consensus.
5. Describe Byzantine Fault Tolerance.
6. Write the major differences between the Federated Consensus and Federated Byzantine Consensus.
7. Discuss some real-world use cases of Blockchain Technology.



Thank you

Any  
Queries

