VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

FOUNDATIONS OF BLOCKCHAIN TECHNOLOGY

BCSE324L

Dr. Malathi D.

FOUNDATIONS OF BLOCKCHAIN TECHNOLOGY

Course Objectives

- To understand building blocks of Blockchain.
- To significance of Distributed Ledger Technology and Smart Contract.
- To exploit applications of Blockchain in real world scenarios and their impacts.

Expected Outcomes

- Understand Blockchain ecosystem and its services in real world sceneries
- Apply and Analyze the requirement of Distributed Ledger Technology and Smart Contract
- Design and Demonstrate end-to-end decentralized applications
- Acquaint the protocol and assess their computational requirements

Module – 1

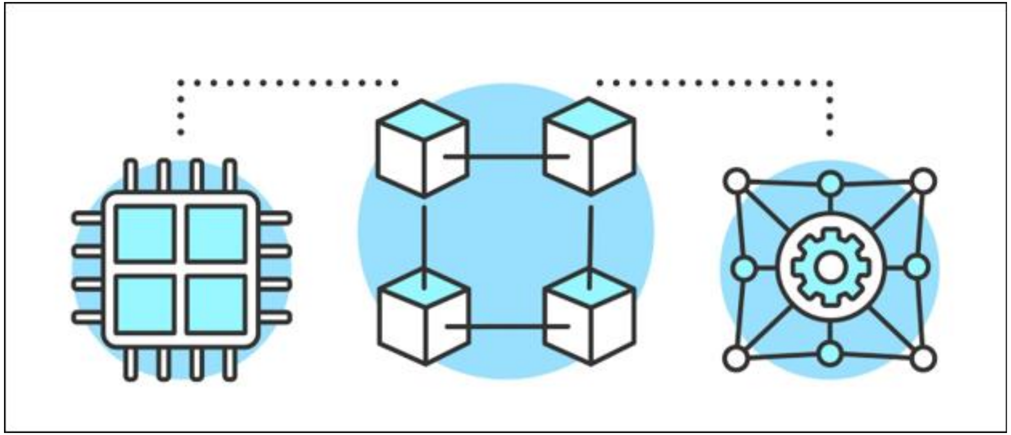
Foundations of Blockchain

Foundations of Blockchain

- Blockchain Architecture
- Challenges and Applications
- Blockchain Design Principles
- The Blockchain Ecosystem
- The consensus problem
- Asynchronous Byzantine Agreement
- AAP protocol and its analysis
- Peer-to-peer network
- Abstract Models
- GARAY model
- RLA Model
- Proof of Work (PoW)
- Proof of Stake (PoS) based Chains
- Hybrid models

Blockchain Architecture

- Blockchain technology is a decentralized distributed ledger with a chain of blocks.
  - Emerged as a revolutionary tool for storing and exchanging digital information.
  - Strength lies in its decentralized nature, which eliminates the need for a central authority
  - Ensures the integrity and immutability of data through cryptography and consensus mechanisms.
  - It is a continuously growing list of records, called blocks, linked together using cryptography to form a chain.
  - Each block in a chain contains a batch of verified transactions added to the blockchain in sequential order, creating a permanent and transparent record of all transactions on the network.



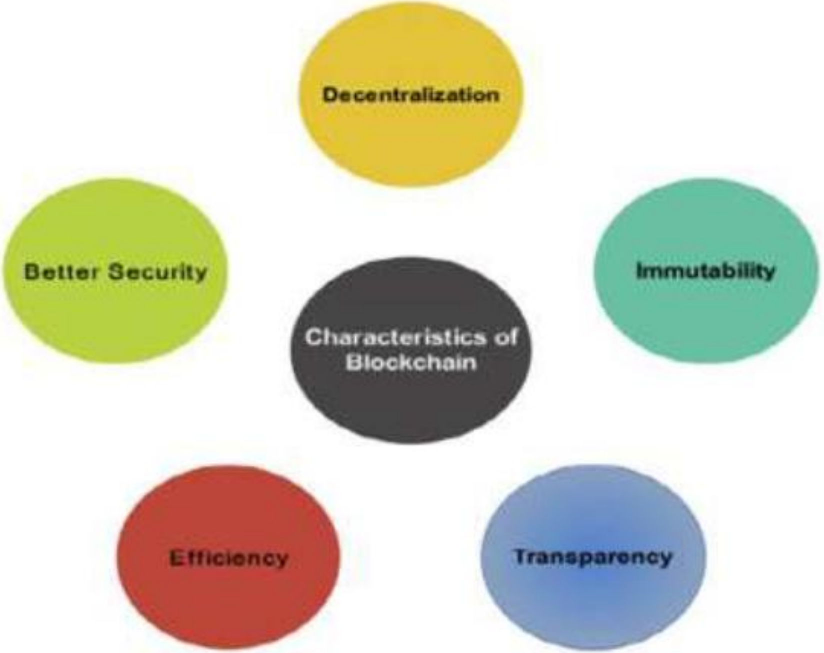
Blockchain Architecture

Characteristics of Blockchain

- A blockchain is a **decentralized structure with built-in security features** that enhance the trust and integrity of transactions. The key features associated with blockchain technology are:
  - **Decentralization**: Unlike centralized systems, which can have a **single point of failure and scalability issues**, blockchain uses a **decentralized, distributed ledger**. This ledger leverages the processing power of all participating users in the network, **reducing latency and eliminating single points of failure**.
  - **Immutability**: **Ensure transaction integrity by creating immutable records**. In traditional centralized models, **databases can be altered, requiring trust in a third party to guarantee data integrity**. Blockchain **links each block in the distributed ledger to the previous one**, forming a chain that is preserved and **unchangeable** as long as the network is maintained by its participants.
  - **Transparency**: Blockchain offers a high level of transparency by **sharing transaction details among all users involved in those transactions**. This transparency **eliminates the need for third-party involvement**, improving business processes and ensuring a trusted workflow.

Blockchain Architecture

- **Security**: Blockchain offers **enhanced security by using a public key system** that protects against malicious attempts **to alter data**. Participants in the blockchain network trust the integrity and security features of the consensus mechanism, and the absence of a single point of failure further strengthens the system's overall security.
- **Efficiency**: Blockchain improves upon traditional centralized models by **distributing database records among multiple users in the network**. This distribution makes it **easier to verify all records** stored in the database. Compared to centralized systems, blockchain is **more efficient in terms of cost, settlement speed, and risk management**.



Blockchain Architecture

Features of blockchain

Header

- A block's header in a blockchain contains necessary metadata about the block, including its version, timestamp, and the Merkle Root of all the transactions in the block.
- Nodes use this header to verify the block's authenticity and contents, ensuring that the data stored on the blockchain is accurate and authentic.

Previous Block Address/Hash

- Each block includes a reference to the previous block in the chain through the hash function.
- Creates an unbreakable link between the blocks in the chain, making it impossible to tamper with any block without changing the hash of every subsequent block.
- Providing a secure and transparent record of all transactions on the network.

Timestamp

- The timestamp in a block's header provides an accurate and immutable record of when a transaction occurred, making it easy to verify the order of transactions and prevent double spending fraud.

Blockchain Architecture

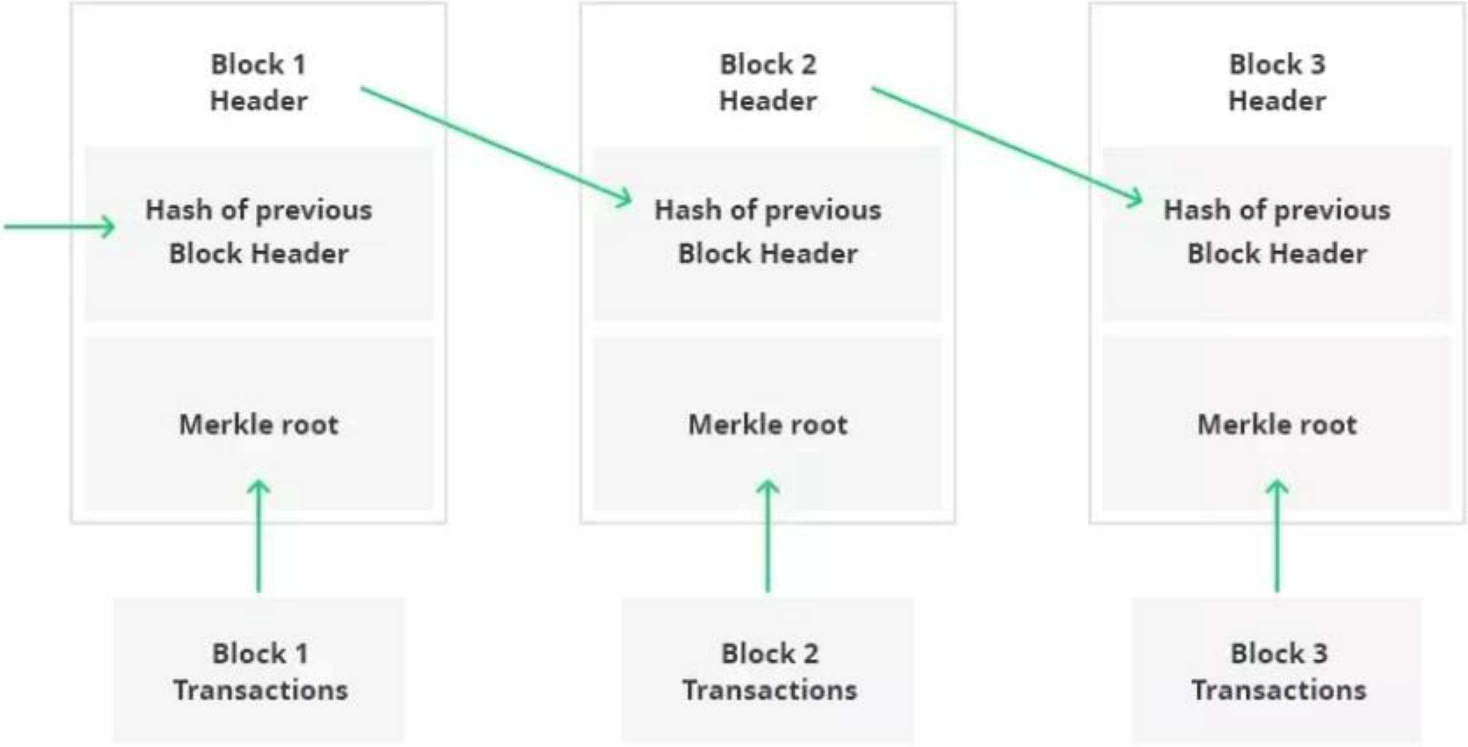
Nonce

- The nonce is a randomly generated number used in the mining process, which is the process by which new blocks get added to a proof-of-work blockchain.
- By finding a nonce that results in a valid hash for a new block, miners can add new blocks to the blockchain and gain rewards in cryptocurrency.
- Using a nonce ensures that the mining process is fair and transparent and that no single entity can control the process.

Merkel Root

- The Merkel Root is a hash of all the transactions within a block, which is included in the block's header.
- This hash provides a compact and secure way to verify the contents of the block, making it easy to ensure the authenticity and accuracy of all transactions on the network.
- Allows for efficient verification of many transactions, making the blockchain scalable and capable of handling large volumes of data.

Blockchain Architecture



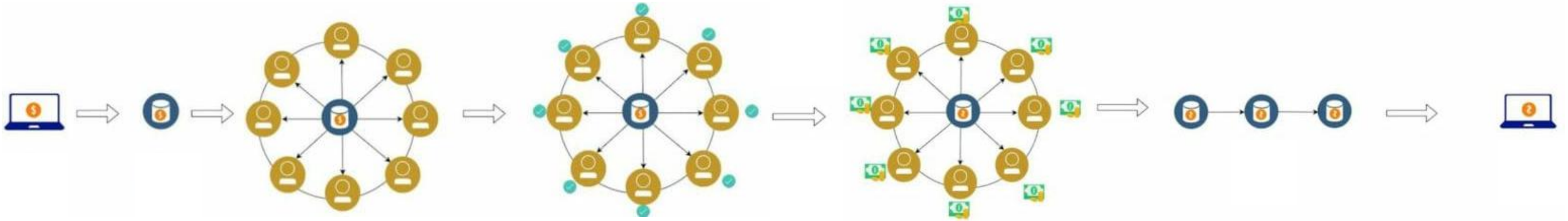
Blockchain Architecture

Core Components of Blockchain Architecture

  - Node - user or computer within the blockchain architecture (each has an independent copy of the whole blockchain ledger)
  - Transaction - smallest building block of a blockchain system (records, information, etc.) that serves as the purpose of blockchain
  - Block - a data structure used for keeping a set of transactions which is distributed to all nodes in the network
  - Chain - a sequence of blocks in a specific order
  - Miners - specific nodes which perform the block verification process before adding anything to the blockchain structure
  - Consensus (consensus protocol) - a set of rules and arrangements to carry out blockchain operations
- Any new record or transaction within the blockchain implies the building of a new block. Each record is then proven and digitally signed to ensure its genuineness. Before this block is added to the network, it should be verified by the majority of nodes in the system.

Blockchain Architecture

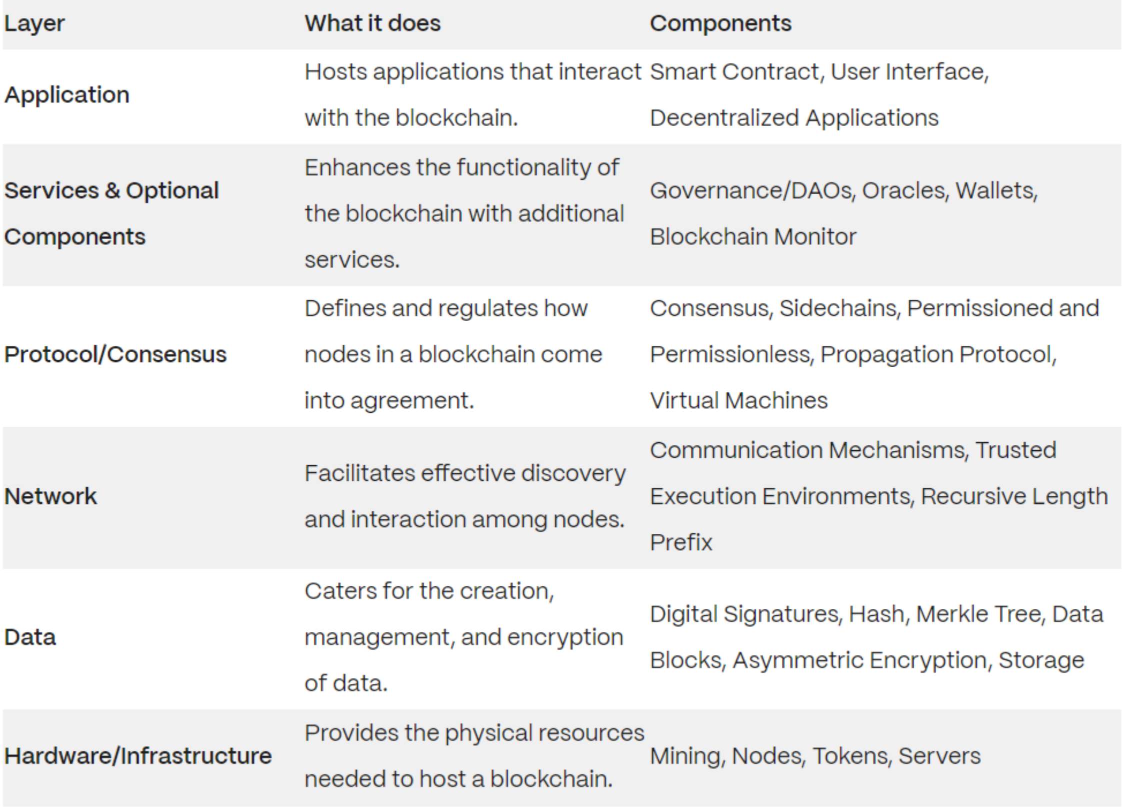
How Blockchain Works?



1. Transaction is Initiated.
2. The Transaction is placed in a Block.
3. The block of a transaction is sent to every node in the network.
4. Miners validate the transaction using consensus mechanism Proof of Work
5. Miners who successfully crack the puzzle in “Proof of Work” will receive the reward.
6. The Block is now successfully placed on the existing Blockchain.
7. The transaction is Successfully Completed.

Blockchain Architecture

Layered Structure Of Blockchain Architecture



Layer	What it does	Components
Application	Hosts applications that interact with the blockchain.	Smart Contract, User Interface, Decentralized Applications
Services & Optional Components	Enhances the functionality of the blockchain with additional services.	Governance/DAOs, Oracles, Wallets, Blockchain Monitor
Protocol/Consensus	Defines and regulates how nodes in a blockchain come into agreement.	Consensus, Sidechains, Permissioned and Permissionless, Propagation Protocol, Virtual Machines
Network	Facilitates effective discovery and interaction among nodes.	Communication Mechanisms, Trusted Execution Environments, Recursive Length Prefix
Data	Caters for the creation, management, and encryption of data.	Digital Signatures, Hash, Merkle Tree, Data Blocks, Asymmetric Encryption, Storage
Hardware/Infrastructure	Provides the physical resources needed to host a blockchain.	Mining, Nodes, Tokens, Servers

Types of Blockchain Architecture

1. Public Blockchain

- Public blockchains are where cryptocurrencies like Bitcoin first emerged, popularizing distributed ledger technology (DLT). Unlike traditional systems that store information in one central place, DLT **distributes data across a peer-to-peer network, enhancing security and transparency**.
- Since there is **no central authority**, public blockchains **use a consensus algorithm to verify and agree on data authenticity**. Common methods include **Proof of Work (PoW) and Proof of Stake (PoS)**.

Key Features

- Open Access: **Anyone with internet access can join a public blockchain**, becoming an authorized node to view, verify, or mine transactions.
- Transparency: The network's code is usually open-source, **allowing anyone to audit transactions, detect bugs, or suggest improvements**.
- Immutability: **Once added** to the ledger, transactions **cannot be altered**.

Advantages

- Independence: Public blockchains **operate independently** of any single organization, continuing to function as long as there are participating computers.
- Security: When users follow proper security protocols, public blockchains are generally **secure due to their transparency and decentralized nature**.

Types of Blockchain Architecture

Disadvantages

- **Speed**: The network can be **slow**, especially **as more nodes join**.
- **Vulnerability**: **If a hacker gains control of 51% or more** of the network's computing power, they **could alter the blockchain**.
- **Scalability**: Public blockchains **struggle to scale efficiently**.

Use Cases

- Public blockchains are ideal for applications requiring transparency and security, such as **cryptocurrency transactions, electronic notarization, and public records of property ownership**.
- **Private businesses may avoid** public blockchains due to the openness of the network.

2. Private Blockchain

- Private blockchains **operate in a closed environment**, typically **controlled by a single entity**. While they **use peer-to-peer connections and decentralization** similar to public blockchains, their scale is much smaller and more controlled. **Only authorized participants** can join and contribute computing power.

Key Features

- **Controlled Access**: The **controlling organization** determines who can view, add, or change data.
- **Permissioned**: Known as **permissioned or enterprise blockchains** because they **restrict participation**.

Types of Blockchain Architecture

Advantages

- **Customization**: Organizations can tailor permission levels, security settings, and accessibility.
- **Speed**: Private blockchains can **process transactions faster due to fewer nodes**.

Disadvantages

- **Centralization**: Critics argue that private blockchains **aren't truly decentralized**, as a central authority controls the network.
- **Security Risks**: Fewer nodes mean the **network could be compromised if some go rogue**.
- **Transparency**: Often proprietary, **limiting the ability to independently verify** the network's security.

Use Cases

- Private blockchains are suitable for **organizations that require secure, private, and fast transactions**, such as in **supply chain management, trade secret protection, and internal audits**.

3. Hybrid Blockchain

- Hybrid blockchains **combine elements of both private and public blockchains**.
- **Allows organizations to control who can access certain data while keeping other data open to the public**.

Types of Blockchain Architecture

- Transactions are usually private but **can be verified when necessary**, using mechanisms like **smart contracts**.

Key Features

- **Controlled Transparency**: Sensitive data remains private but can be verified if needed.
- **User Privacy**: Users' identities are protected unless they engage in a transaction.

Advantages

- **Security**: The closed ecosystem makes it **harder for external hackers** to compromise the network.
- **Flexibility**: Offer a balance of privacy and transparency, with **fast and cost-effective transactions**.

Disadvantages

- **Limited Transparency**: Some information may be hidden, **reducing overall transparency**.
- **Complex Upgrades**: Upgrading the network can be challenging, and there is **little incentive for users to contribute**.

Use Cases

- Hybrid blockchains are ideal for sectors like **real estate, retail, financial services, and healthcare**, where **privacy is crucial**, but certain information still needs to be shared.

Types of Blockchain Architecture

4. Consortium Blockchain

- Consortium blockchains, also known as **federated blockchains, are similar to hybrid blockchains but involve multiple organizations working together on a decentralized network**.
- These networks are **private but governed by a group** rather than a single entity.

Key Features

- **Collaborative Control**: Multiple organizations share control, reducing the risk of a single point of failure.
- **Validator Nodes**: Transactions are validated by predetermined nodes within the consortium.

Advantages

- **Security and Efficiency**: Offer greater security, scalability, and efficiency compared to public blockchains.
- **Access Controls**: Similar to private blockchains, they offer strict access controls.

Disadvantages

- **Transparency**: Like private blockchains, they are **less transparent**.
- **Compromise Risk**: The network **can be compromised** if a member node is breached.

Use Cases

- Consortium blockchains are commonly used in **banking, payments, supply chain management, and research organizations**.

Types of Blockchain Architecture

Permissionless Blockchain

- Also known as **trustless or public blockchains**, permissionless blockchains are **open to anyone who wants to participate**. These networks are typically **used when high transparency is needed**.

Key Features

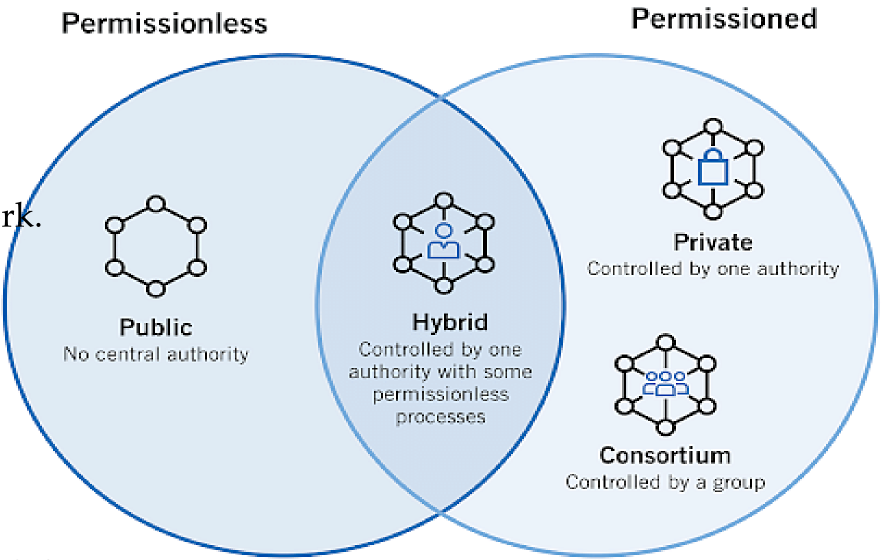
- **No Central Authority**: The network is **completely decentralized and open-source.**
- **Transparency**: Transactions are **fully transparent** and visible to all participants.
- **Token Usage**: Tokens are **heavily used** within the network.

Advantages

- **Open Participation**: Anyone with internet access and suitable hardware can join.
- **Trust:** The high level of transparency builds trust among users.

Disadvantages:

- **Energy Inefficiency**: Large networks consume a lot of energy.
- **Scalability Issues**: As the network grows, performance can degrade.
- **Limited Privacy**: Many details are visible to all participants.



Types of Blockchain Architecture

Permissioned Blockchain

- Permissioned blockchains are **closed networks where only a select group of participants can validate transactions**. These blockchains are used when high privacy and security are necessary.

Key Features

- **Controlled Transparency**: Transparency levels are **set by the organization** based on its objectives.
- **Limited Participation**: Only authorized users can participate, and there is **no central authority**.
- **Private Development**: Typically developed by a private entity.

Advantages

- **Speed**: Fewer nodes mean faster transaction processing.
- **Customizability**: Organizations can tailor the network to their needs.
- **Strong Privacy**: Permission is required to access transaction information.

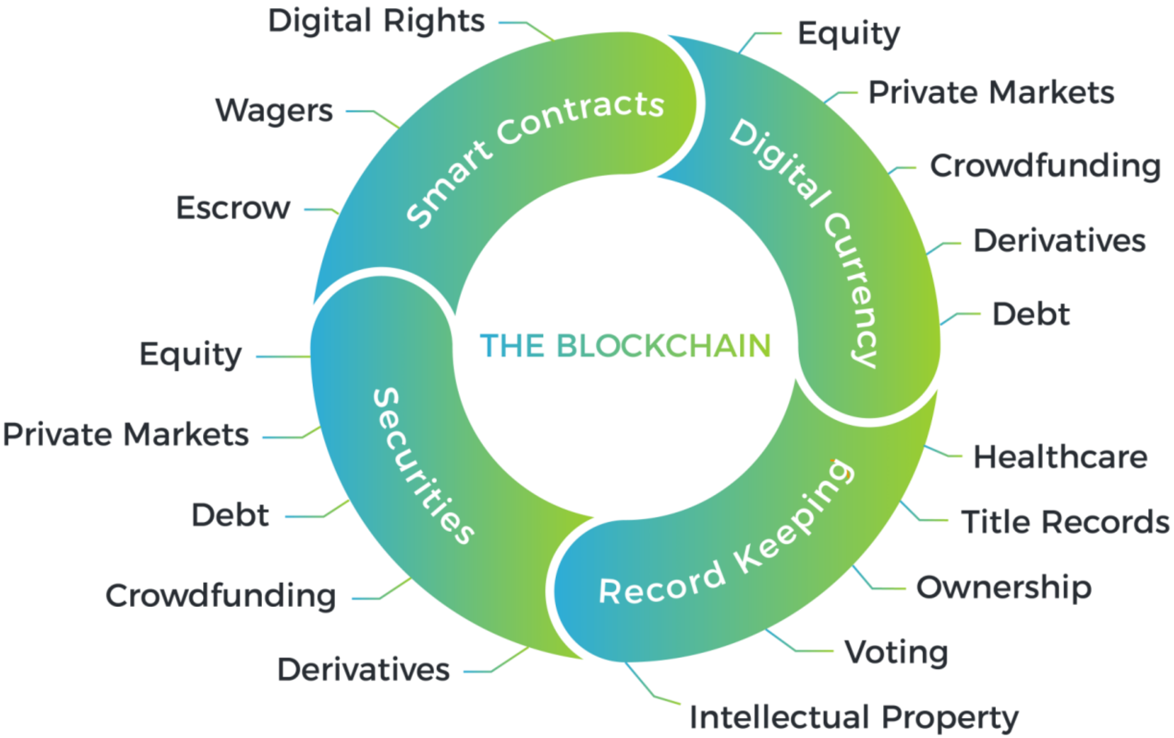
Disadvantages

- **Centralization**: The need for permission means the network is not fully decentralized.
- **Corruption Risk**: With fewer participants, there's a higher risk of corruption.
- **Rule Changes**: The owner or operator can change the network rules at any time.

Challenges of Blockchain Technology

1. **Scalability:** Managing a large number of users simultaneously remains a challenge for the blockchain industry. Blockchain technology **relies on complex algorithms to process each transaction, which can slow down processing speeds when many users are active**.
2. **Hackers and Shadow Dealing: Lack of regulatory oversight**, making it vulnerable to market manipulation. Example is the OneCoin scam, which tricked investors into thinking they were buying the next big digital currency, only to be revealed as a Ponzi scheme. Even if you understand cryptocurrency well, there's always a risk that your online wallet could be hacked or blocked by the government due to suspicious activities.
3. **Complexity in Understanding and Adoption:** Blockchain technology is complicated, making it **difficult for the average person to understand and appreciate its benefits**.
4. **Privacy Concerns:** Blockchain operates as an open ledger, meaning anyone can view the transactions. While transparency is valuable in many situations, it becomes a liability in sensitive environments. For blockchain to be widely adopted, the technology needs to evolve to allow restricted access, ensuring that only authorized individuals can view certain information.
5. **Costs:** Blockchain is often touted as a way to eliminate the costs associated with third parties in value transfers. However, because blockchain technology is still in its early stages, integrating it with existing systems is challenging and expensive. These costs deter both governments and private firms from adopting blockchain on a larger scale.

Applications of Blockchain Technology



Blockchain Design Principles

Principle 1: Decentralization

- allows for transactions without relying on a third party to verify them
- beneficial for businesses that may lack the resources to handle transactions independently
- by separating the network from the miners, blockchain creates a more democratized system, making it less susceptible to centralized control and enabling a fairer distribution of wealth
- decentralization also enhances the system’s resilience against attacks and improves privacy by giving users greater control over their data.

Principle 2: Immutability

- all data and transactions recorded on the blockchain are permanent and cannot be altered
- ensures that information remains accurate and secure, preventing fraudulent activities
- once a transaction is added to the blockchain, it cannot be changed or tampered with, thereby upholding the integrity and security of the entire system.
- helps to reduce transaction costs, as it eliminates the need for third-party verification or reconciliation
- immutability of blockchain fosters greater trust, transparency, and reduced costs in transactions.

Principle 3: Transparency

- allows all users to view transaction details, enhancing the trustworthiness and clarity of the process.

Blockchain Design Principles

- For instance, if you're a business owner selling products online, you can use blockchain to upload detailed product information, such as ingredients or the manufacturing process, directly to the network.
- Customers can then access this information, building trust and increasing engagement with business.
- This level of transparency can strengthen the relationship between businesses and their customers and promote higher levels of customer satisfaction.

Principle 4: Security

- Security is one of the foremost benefits of blockchain technology.
- By making all transactions visible on a public ledger, blockchain ensures that every action is traceable and transparent, enhancing the security of the entire system.
- A blockchain database is stored across the network and accessed using distributed ledger technology, meaning every node has access to the same information.
- When you make a transaction, a new block is created and added to the ledger.
- Miners then verify the block by ensuring it meets certain conditions.
- Once verified, the block is permanently recorded on the chain, accessible to all.
- This process ensures that only authorized parties can complete transactions, making it nearly impossible for anyone to tamper with or falsify data on the blockchain.

Blockchain Design Principles

Principle 5: Scalability

- Scalability refers to the ability of a blockchain system to handle a growing number of transactions without becoming overly complex or slow. Three main factors affect scalability: execution, storage, and consensus.
  - Execution: How quickly transactions are processed, influenced by factors like the number of nodes, their processing power, and available bandwidth.
  - Storage: The amount of data that can be stored, which depends on the size of blocks and how frequently they are generated.
  - Consensus: The process by which all nodes agree on which transactions are valid, often achieved through voting or proof-of-work algorithms.
- Blockchain's scalability allows it to handle many more transactions than traditional systems, making it a significant advantage for widespread adoption.

Principle 6: Privacy

- Privacy in blockchain ensures that data and transactions on the network are transparent yet secure, providing users with a high degree of trust. Since all information is accessible to everyone, it cannot be easily misrepresented, and accountability is enhanced.

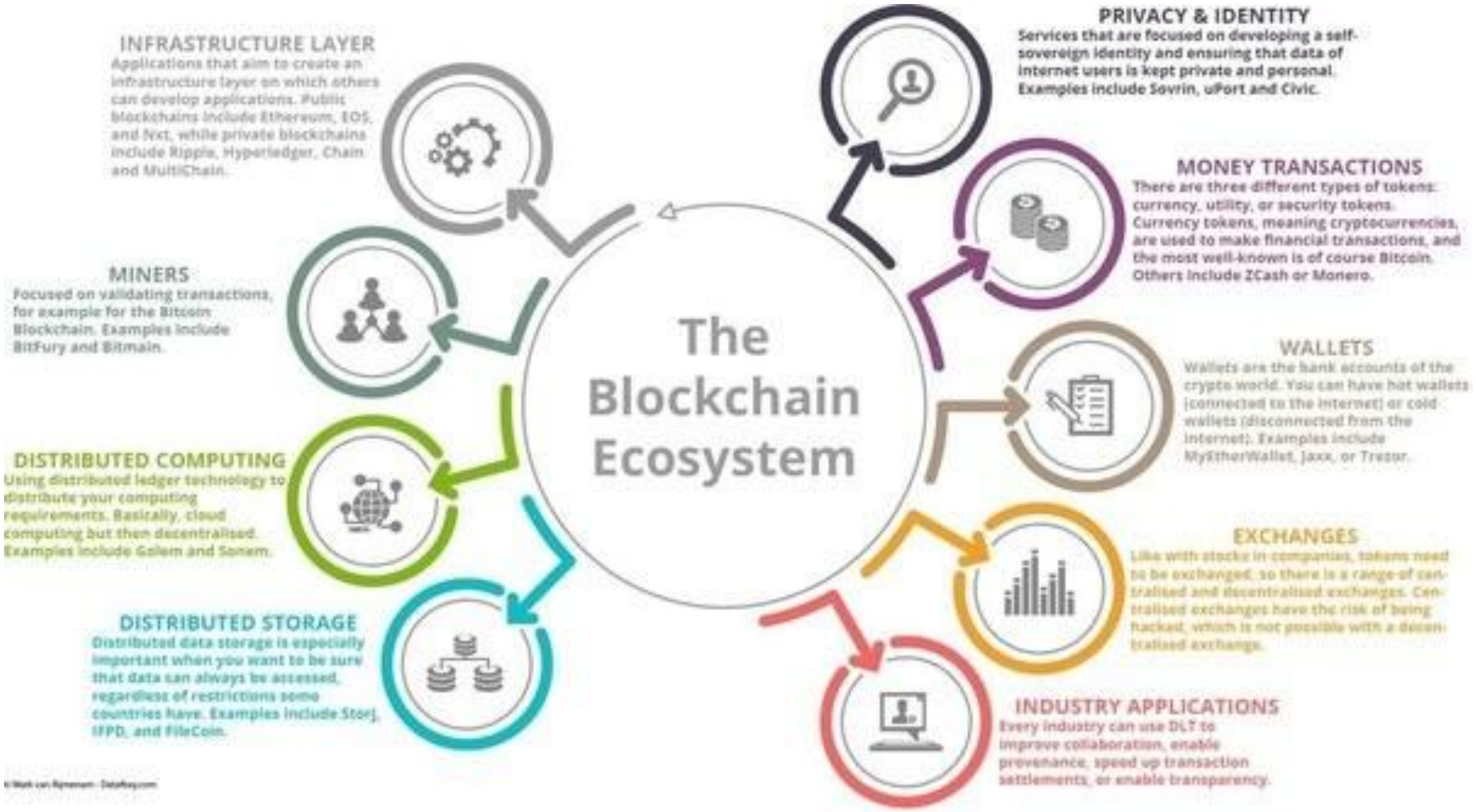
Blockchain Design Principles

- However, privacy is not absolute, as all blockchain data may eventually become publicly accessible.
- To protect privacy, strong cryptography and reliable network nodes are crucial.
- Additionally, private blockchain networks can offer more controlled access than public ones, further safeguarding sensitive information.

Principle 7: Flexibility

- The inherent flexibility of blockchain technology offers several benefits. It allows transactions to be completed quickly and accurately, which is especially important for future system expansion.
- By maintaining a streamlined and manageable network, blockchain minimizes complexity, facilitating growth without placing extra demands on users or developers.

Blockchain Ecosystem



INFRASTRUCTURE LAYER

Applications that aim to create an infrastructure layer on which others can develop applications. Public blockchains include Ethereum, EOS, and Nxt, while private blockchains include Ripple, Hyperledger, Chain and MultiChain.

MINERS

Focused on validating transactions, for example for the Bitcoin Blockchain. Examples include BitFury and Bitmain.

DISTRIBUTED COMPUTING

Using distributed ledger technology to distribute your computing requirements. Basically, cloud computing but then decentralised. Examples include Golem and Sonem.

DISTRIBUTED STORAGE

Distributed data storage is especially important when you want to be sure that data can always be accessed, regardless of restrictions some countries have. Examples include Storj, IFPD, and FileCoin.

PRIVACY & IDENTITY

Services that are focused on developing a self-sovereign identity and ensuring that data of internet users is kept private and personal. Examples include Sovrin, uPort and Civic.

MONEY TRANSACTIONS

There are three different types of tokens: currency, utility, or security tokens. Currency tokens, meaning cryptocurrencies, are used to make financial transactions, and the most well-known is of course Bitcoin. Others include ZCash or Monero.

WALLETS

Wallets are the bank accounts of the crypto world. You can have hot wallets (connected to the internet) or cold wallets (disconnected from the internet). Examples include MyEtherWallet, Jaxx, or Trezor.

EXCHANGES

Like with stocks in companies, tokens need to be exchanged, so there is a range of centralised and decentralised exchanges. Centralised exchanges have the risk of being hacked, which is not possible with a decentralised exchange.

INDUSTRY APPLICATIONS

Every industry can use DLT to improve collaboration, enable provenance, speed up transaction settlements, or enable transparency.

© Mark van Rijmenam · Datafloq.com

Blockchain Consensus Algorithms

- Blockchain technology **offering a decentralized and secure way to store and transfer information**.
- Consensus algorithms are a **set of rules or protocols** that enable nodes in a blockchain network to **agree on a shared state** of the network.
- Used to ensure that all nodes in the network come to a **consensus on the validity of transactions and the order** in which they are added to the blockchain.
- A consensus algorithm is **responsible for maintaining the integrity** of the blockchain by ensuring that **no single node or group of nodes can manipulate** the network.

Blockchain Consensus Algorithms

- Consensus algorithms are critical in blockchain technology for several reasons.
  - **Provide security**
    - by preventing malicious actors from taking control of the network
    - ensuring valid transactions and smooth network operation.
  - **Help achieve decentralization**
    - by ensuring all nodes come to a consensus on transaction validity
    - preventing centralization.
  - **Promote transparency**
    - by making all transactions visible on the blockchain
    - making it easy to track and prevent fraudulent activities.
  - **Improve efficiency**
    - by allowing nodes to quickly agree on transaction validity and add new blocks to the blockchain in a timely manner.

Types of Consensus Algorithms

Proof of Work (PoW)

- Proof of Work is a consensus algorithm used in many blockchain networks **to validate transactions and add new blocks to the chain**.
- PoW was **first introduced by** Bitcoin's creator, **Satoshi Nakamoto**, as a way **to secure the network** and **prevent double-spending**.
- The PoW algorithm **requires miners to solve complex mathematical problems, known as hashes**.
- Hash function used in PoW algorithms is designed to be **computationally difficult to solve**, it requires a **significant amount of computational power** to solve the problem and add a block to the chain.
- **Miners compete with each other** to solve the problem, and the **first one to solve it is rewarded with newly minted cryptocurrency**.
- This **algorithm's security** comes from the fact that it is **difficult to solve** the hash problem, which means that it is **expensive for an attacker** to try to take over the network.
- The attacker would **need to have control** over a significant portion of the network's computational power, known as the **hash rate**, in order **to launch an attack**.
- This is **known as a 51% attack**, and it is difficult to pull off because it would **require a massive amount of resources**.

Types of Consensus Algorithms

Proof of Stake (PoS)

- Unlike PoW, which requires miners to solve complex mathematical problems, **PoS relies on validators** who **hold a certain amount of cryptocurrency** to validate transactions and add new blocks to the chain.
- In a PoS network, **validators are chosen** to add new blocks to the chain **based on the amount of cryptocurrency they hold**, which is known as **their stake**.
- The larger the stake, the **greater the chance of being selected** to add a block to the chain.
- Validators are incentivized to act honestly because **they risk losing their stake if they validate fraudulent transactions** or try to attack the network.

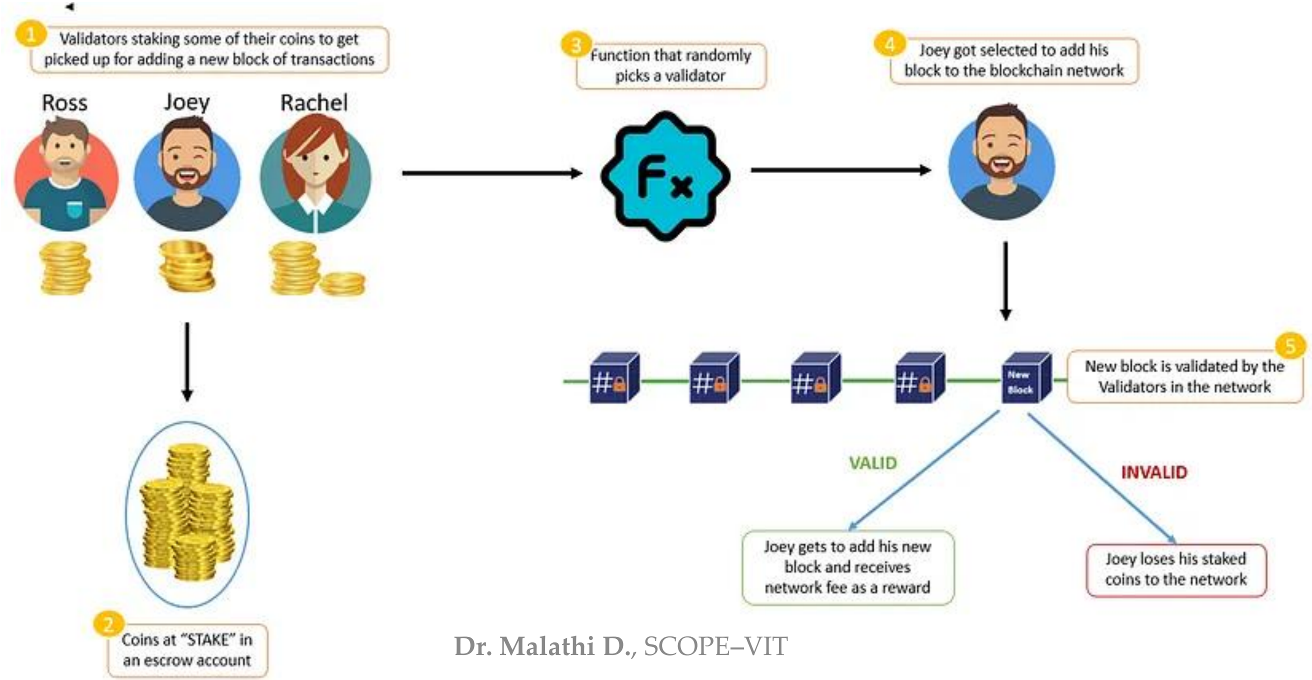
Advantages

- **Less energy-intensive**: PoW requires miners to use significant amounts of computational power to solve complex mathematical problems, while **PoS only requires validators to hold cryptocurrency**. This makes PoS more environmentally friendly and less costly to operate.
- **Promotes decentralization**: In a PoW network, **miners with the largest hash rate have more control** over the network, which can **lead to centralization**. In a PoS network, **validators with the largest stake have more control**, but it is **difficult for a single/group of validators** to gain control of the network because they would need to control a significant amount of cryptocurrency.

Types of Consensus Algorithms

Disadvantages

- **Rich-get-richer**: **Validators with the largest stake continue to earn more cryptocurrency**, making it more difficult for smaller validators to participate in the network.
- **Solution**: Random selection of validators or limiting the amount of cryptocurrency that a single validator can hold.



1 Validators staking some of their coins to get picked up for adding a new block of transactions
Ross
Joey
Rachel
2 Coins at "STAKE" in an escrow account
3 Function that randomly picks a validator
Fx
4 Joey got selected to add his block to the blockchain network
New Block
5 New block is validated by the Validators in the network
VALID
INVALID
Joey gets to add his new block and receives network fee as a reward
Joey loses his staked coins to the network

Types of Consensus Algorithms

Delegated Proof of Stake (DPoS)

- DPoS is a **variation** of Proof of Stake (PoS) that **relies on a smaller group of validators, known as delegates or witnesses**, to validate transactions and add new blocks to the chain.
- In a DPoS network, **token holders vote for delegates to represent them in the validation process**.
- The delegates are **incentivized to act honestly** because they risk losing their position and rewards if they validate fraudulent transactions or try to attack the network.

Advantages

- **Efficient**: **PoS requires all validators to participate** in the validation process, which can lead to inefficiencies if some **validators are not online or not actively participating**. In DPoS, only the **elected delegates participate** in the validation process, which makes it **faster and more efficient**.
- **Promotes decentralization:** In a PoS network, **validators with the largest stake have more control** over the network, which can lead to centralization. In a DPoS network, **token holders have a say in who gets to be a delegate**, which can lead to a more **decentralized network**.

Disadvantages

- It can lead to a **concentration of power in the hands of a small group of delegates.** If a small group of delegates controls a significant amount of voting power, they **could potentially collude to manipulate the network**.
- **Solution**: **Limiting the number of delegates** that any one entity can control.

Types of Consensus Algorithms

Leased Proof of Stake (LPoS)

- LPoS is a variation of Proof of Stake (PoS) that **allows smaller token holders to participate in the validation process by leasing their tokens to larger validators**.
- In a LPoS network, **token holders lease their tokens to a validator**, who uses those tokens to **increase their stake** and **improve their chances of being selected** to validate transactions and add new blocks to the chain.
- The **token holder** retains ownership of their tokens and **receives a share of the rewards** earned by the validator in **proportion to the amount of tokens they leased**.

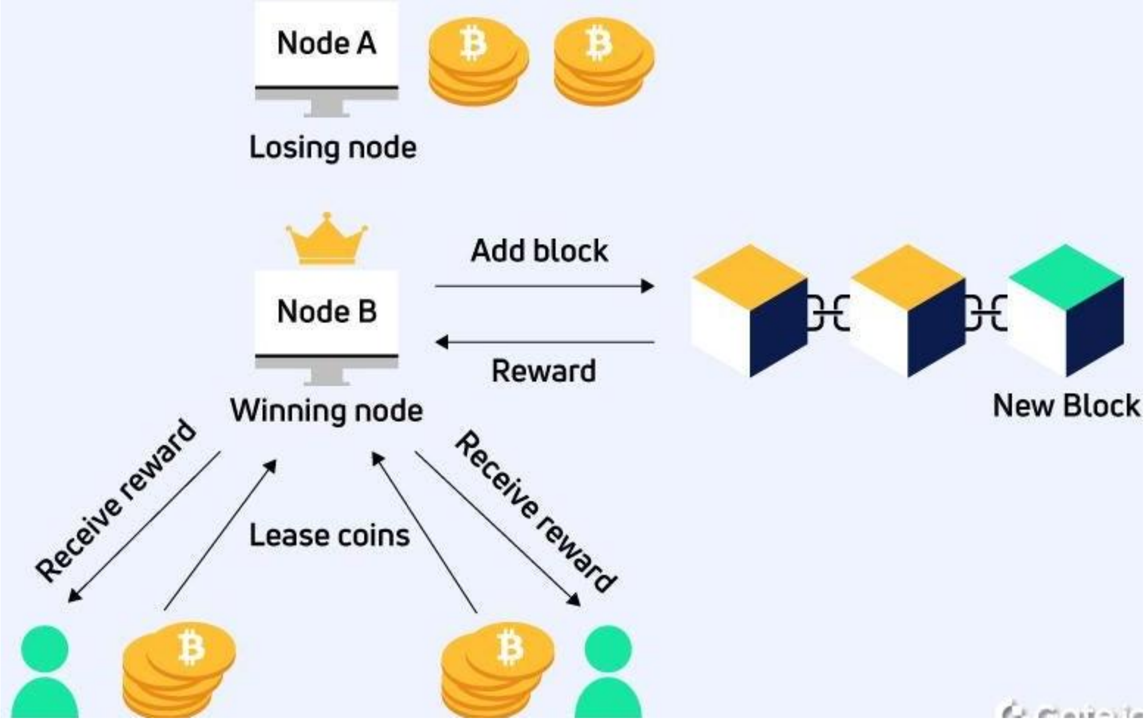
Advantages

- **Allows smaller token holders to participate** in the validation process and earn rewards without having to hold a significant amount of tokens. This **promotes decentralization** and allows for a more **diverse group of participants** in the network.
- **Increase the security**: By allowing more token holders to participate in the validation process, LPoS can **make it more difficult for a single validator or group of validators to gain control of the network and manipulate transactions**.

Types of Consensus Algorithms

Disdvantages

- **More complex** than other consensus algorithms. **Token holders** must understand the **risks and rewards of leasing their tokens** to a validator, and **validators** must **manage the tokens** they have leased in a responsible manner.



Types of Consensus Algorithms

Proof of Authority (PoA)

- Unlike other consensus algorithms such as PoW and PoS, **PoA relies on a group of trusted validators** instead of a decentralized network of nodes.
- In a PoA network, a **group of validators is designated as authoritative and responsible for validating transactions** and adding new blocks to the chain.
- Validators are typically **selected based on their reputation and expertise**, and they are incentivized to act honestly because their reputation is on the line.

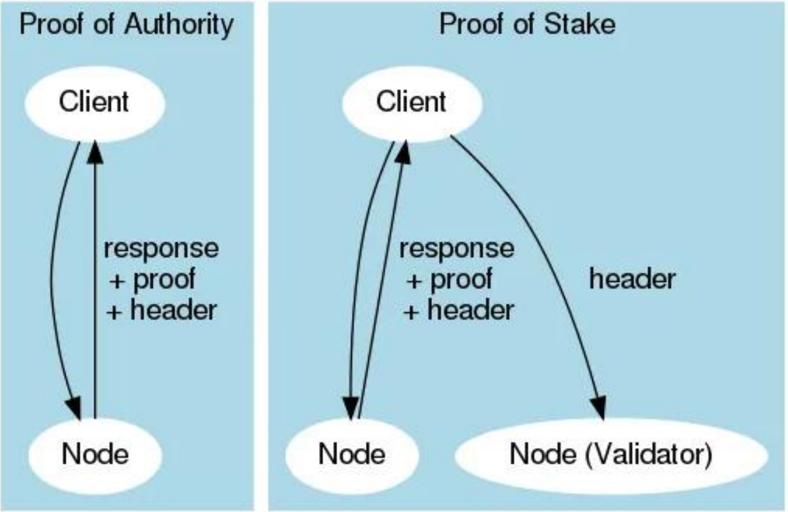
Advantages

- It is **more efficient** than other consensus algorithms.
- **PoW requires a significant amount of computational power** to validate transactions, which can be **costly and time-consuming**. **PoS requires a significant amount of stake** to participate in the validation process, which can **lead to centralization**. **PoA relies on a smaller group of trusted validators**, which makes it **faster and more efficient**.
- More suitable for **private or enterprise blockchain networks**. In these networks, it may **not be feasible** or desirable **to have a decentralized network** of nodes validating transactions. PoA **allows for a more controlled and centralized approach** to validation, which may be more appropriate in these contexts.

Types of Consensus Algorithms

Disadvantages

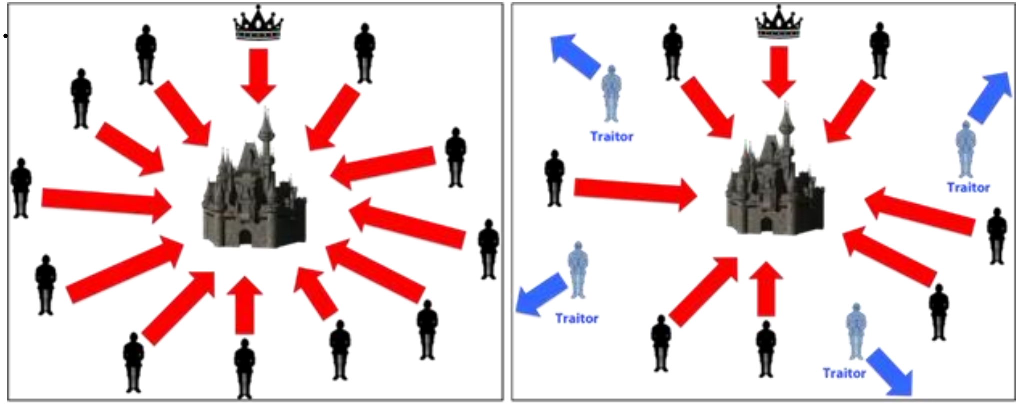
- It is **less secure** than other consensus algorithms.
- Because PoA **relies on a smaller group of validators**, the network is more **vulnerable to attacks** if one or more validators are compromised or act maliciously.
- Some PoA networks have implemented mechanisms **to address this issue**, such as **requiring multiple validators to sign off on transactions**.



Types of Consensus Algorithms

Byzantine Fault Tolerance (BFT)

- In general, it is the **System's ability to function correctly** and reach consensus **even if some of its components fail** or behave maliciously.
- In the context of blockchain technology, BFT is a consensus algorithm that **enables a distributed network of nodes to reach an agreement on the validity of transactions and maintain the integrity** of the blockchain even in the face of **malicious attacks or system failures**.
- BFT is designed **to prevent the "Byzantine Generals' Problem,"**: a scenario in which a group of generals must coordinate an attack on a city, but some of the generals are traitors who may send false information to others.



Coordinated Attack Leading to Victory **Uncoordinated Attack Leading to Defeat**

Types of Consensus Algorithms

- In a blockchain network, the Byzantine Generals' Problem can manifest as **nodes** on the network that **behave maliciously or fail to communicate** correctly.
- BFT addresses this problem by **requiring a certain percentage of nodes to agree** on the validity of transactions before they are added to the blockchain.
- In a **traditional** BFT algorithm, this percentage is set at **two-thirds** of the total number of nodes. If two-thirds of the nodes agree on the validity of a transaction, then it is added to the blockchain. If less than two-thirds of the nodes agree, then the transaction is rejected.

Advantages

- It **does not require** a significant amount of **computational power or stake** to participate in the validation process, it **relies on a smaller group of nodes to reach agreement** on the validity of transactions, which makes it **more efficient and faster** than other consensus algorithms.

Disadvantages

- It **requires a higher level of trust** in the network participants.
- If a significant percentage of **nodes behave maliciously or fail to communicate** correctly, then the network may **not be able to reach a consensus and maintain the integrity** of the blockchain.
- BFT is often used in **private or enterprise blockchain networks** where participants are known and trusted.

Types of Consensus Algorithms

Practical Byzantine Fault Tolerance (PBFT)

- Extends the BFT algorithm **to provide a high level of fault tolerance** in distributed systems.
- PBFT is commonly used in **enterprise blockchain networks** and other distributed systems **where a high level of consensus is required**.
- PBFT works by **breaking down the consensus process into a series of steps** that are repeated for each transaction. Each step **involves a different node** in the network, and **each node is responsible for verifying** the validity of the transaction before passing it on to the next node.
- The PBFT algorithm **requires a certain number of nodes to reach a consensus** on the validity of a transaction before it can be added to the blockchain.
- This number is determined by the formula **f = (n-1)/3**, where f is the maximum number of faulty nodes that the system can tolerate, and n is the total number of nodes in the network.
- PBFT is **designed to be fault-tolerant**, meaning that it can **continue to function correctly** even if some nodes in the network **fail or behave maliciously**.
- If a node fails or behaves maliciously, the **other nodes can detect the problem and exclude the node** from the consensus process.

Types of Consensus Algorithms

Advantages

- It can achieve **high throughput and low latency**, even in networks with a large number of nodes.
- PBFT is also **known for its high level of security**, as it can tolerate up to *f* faulty nodes without compromising the integrity of the blockchain.

Disadvantages

- It **requires a certain number of nodes to reach consensus**, which means that it may **not be suitable for small networks**.
- PBFT **also requires a higher level of computational power** than some other consensus algorithms, which can make it **less energy-efficient**.

Types of Consensus Algorithms

Delegated Byzantine Fault Tolerance (dBFT)

- **Combines the advantages of both BFT and DPoS algorithms**.
- dBFT is commonly used in blockchain networks that **require a high level of consensus and throughput**.
- Like BFT and PBFT, dBFT is **designed to be fault-tolerant**.
- In dBFT, **consensus is reached through a process of voting**, where each node in the network can vote on the validity of a transaction.
- dBFT **uses a delegated model** where network **participants delegate their voting power to** a smaller number of trusted nodes, known as **validators**.
- Validators are responsible for verifying transactions and reaching a consensus on the validity of transactions.
- dBFT is **based on a round-robin system** where **validators take turns** validating transactions.
- Validators are **selected based on their reputation and stake** in the network.

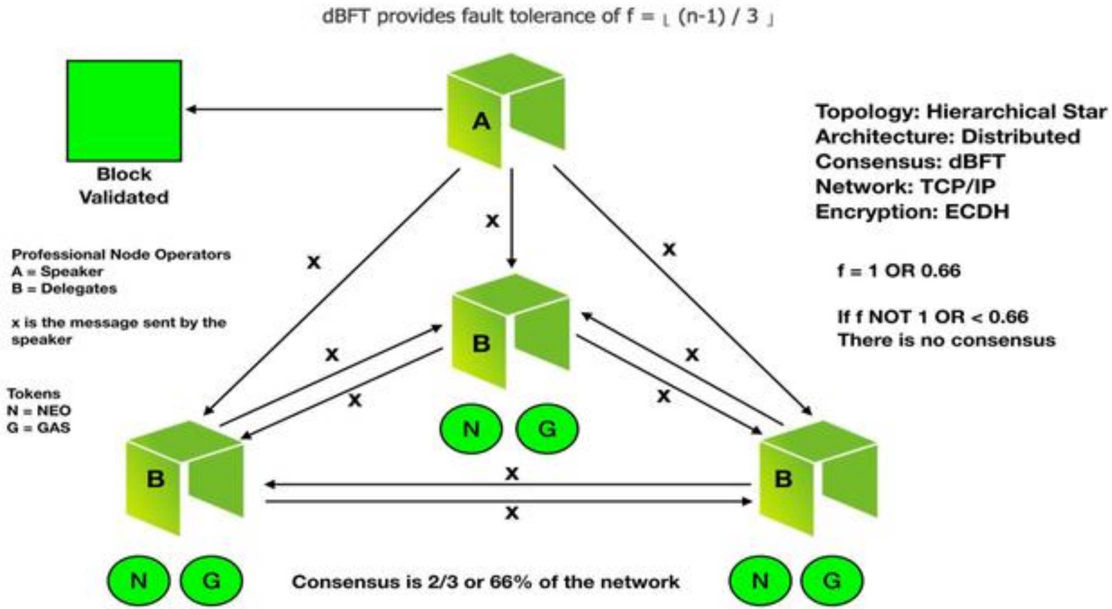
Advantages

- It can **achieve high throughput and low latency**, as only a **small number of validators are required** to reach a consensus, also **reduces the risk of centralization**, as **validators are selected based on their reputation and stake**, rather than their computational power.

Types of Consensus Algorithms

Disadvantages

- It **requires a high level of trust** in the selected validators, which can lead to potential vulnerabilities if a **large number of validators are controlled by a single entity**.
- dBFT is also **not suitable for all types** of blockchain networks, as it may **not be necessary to have such a high level of consensus** for some use cases.



dBFT provides fault tolerance of f = ⌊ (n-1) / 3 ⌋
Block Validated
A
B
B
B
x
x
x
x
x
x
x
x
x
N
G
N
G
N
G
Professional Node Operators
A = Speaker
B = Delegates
x is the message sent by the speaker
Tokens
N = NEO
G = GAS
Topology: Hierarchical Star
Architecture: Distributed
Consensus: dBFT
Network: TCP/IP
Encryption: ECDH
f = 1 OR 0.66
If f NOT 1 OR < 0.66
There is no consensus
Consensus is 2/3 or 66% of the network

Types of Consensus Algorithms

Directed Acyclic Graph (DAG)

- This type of data structure is **often used in distributed ledger technology** and blockchain systems.
- Unlike traditional blockchain architectures, which **organize data in a linear, chronological sequence of blocks**, DAGs allow for a **more flexible and efficient way to store and validate data**.
- **Each vertex represents a transaction and each edge represents a relationship between transactions**.
- In a DAG, **transactions are organized in a more complex structure** where each transaction is linked to multiple other transactions.

BLOCKCHAIN

Types of Consensus Algorithms

Advantages

- They can **achieve high scalability and transaction throughput**.
  - Transactions can be **processed concurrently**, as long as there are no conflicts between them.
  - **Multiple transactions can be validated at the same time**, improving the overall efficiency of the system.
- **Ability to handle forks** in the network.
  - In a traditional blockchain, **when two blocks are created at the same time**, only one of them can be accepted into the chain, lead to a situation where a **block that was previously considered valid is suddenly rejected**, leading to a fork in the chain.
  - In a DAG-based system, **forks are resolved automatically**, as transactions are **validated based on their relationship to other transactions** in the graph.

Disadvantages

- **Need for a complex consensus mechanism** that can determine the **order of transactions** in the graph.
- DAGs may **not be suitable for all types of blockchain applications**, as they may **require a more complex architecture** than traditional blockchain systems.

Types of Consensus Algorithms

Proof of Capacity (PoC)

- PoC is similar to Proof of Work (PoW) in that it requires participants to **solve a computational puzzle** to add new blocks to the blockchain, but it differs in **how it utilizes computer storage** rather than computational power.
- In a PoC system, **participants allocate a portion of their computer's hard drive space to serve as a plot**, which is essentially a pre-computed segment of data that can be **used to generate a solution to the computational puzzle**.
- When a new block needs to be added to the blockchain, the **participant's plot is searched to find a solution to the puzzle**. The first participant to find a valid solution can add the new block to the blockchain and **receive a reward** in the form of cryptocurrency.

Disadvantages: Vulnerable to pre-computation and Sybil attacks.

- **Pre-computation attack**: an attacker could pre-compute a large number of plots and then use them to quickly solve the computational puzzle and add new blocks to the blockchain, giving them an unfair advantage over other participants.
- **Sybil attack**: an attacker could create **multiple identities to increase their chances of finding a solution** to the puzzle.

Types of Consensus Algorithms

Proof of Burn (PoB)

- PoB **requires participants to burn, or destroy, cryptocurrency tokens** to prove their commitment to the network, and **making a financial sacrifice**.
- User must **send a certain amount of cryptocurrency to an address** where it will be permanently destroyed - known as burning.
- Once it is burned, the **user is given the right to add new blocks** to the blockchain and receive rewards.
- **Reduces the likelihood of malicious actors attempting to attack the network**, as they would have to burn a significant amount of cryptocurrency to do so.

Advantages:

- Help to **reduce inflation**, Since tokens are being destroyed rather than created, the **overall supply of tokens decreases**, which can **help stabilize the value of the cryptocurrency**.

Disadvantages:

- **Difficult to determine the value of the burned tokens**, as they are permanently destroyed and cannot be recovered.
- This can make it **difficult to accurately measure the level of commitment and investment** in the network.

Types of Consensus Algorithms

Proof of Identity (PoI)

- It is a consensus mechanism **used to verify the identity of participants** in the network.
- Promote **trust, security, and authenticity** in blockchain transactions.
- PoI works by **requiring participants to provide a digital identity** that is linked to a real-world identity verification process, such as **government-issued IDs, biometric data**, or other forms of verifiable identity credentials.
- It ensures that each **participant is a real, identifiable** individual, which can help **prevent fraudulent or malicious activity** in the network.

Advantages:

- Help **prevent Sybil attacks**, where a single participant **creates multiple identities** in the network to gain control or manipulate the system, ensures each participant is a unique and identifiable entity.

Disadvantages:

- **Difficult to balance anonymity and privacy with identity verification**.
- Some participants may **not want to reveal their identities** to maintain their privacy, while others may **not have access to the necessary identity verification tools**.
- It is **time-consuming and costly**, which may discourage some participants from joining the network.

Asynchronous Byzantine Agreement

- Asynchronous Byzantine Agreement is designed to achieve consensus among a group of nodes even when the network communication is prone to unpredictable delays and message losses or other asynchronous behaviors.
- It aims to allow loyal nodes to agree on a common decision and further ensuring the consensus reached in a fault-tolerant manner.
- Asynchronous Byzantine Agreement protocol works in multiple rounds, allowing nodes to exchange messages and progressively converge towards a shared decision.
- Asynchronous Byzantine Agreement protocol has the following steps
  - Initialization
  - Proposal & Broadcasting
  - Message Exchange
  - Update & Broadcasting
  - Iteration
  - Decision

AAP protocol and its analysis

- Ensures reliable and consistent message delivery in asynchronous distributed systems, like blockchain networks. Guarantees that all processes receive messages in the same order, even in the presence of failures.
- Working Mechanism:
  - Message Sending
    - A node sends a message to a designated sequencer.
  - Sequencing
    - The sequencer assigns a unique sequence number to each message. It broadcasts the message along with its sequence number to all nodes.
  - Message Delivery
    - Nodes deliver messages in sequence number order. If a node misses a message, it requests retransmission from other nodes.

ABSTRACT MODEL FOR BLOCKCHAIN

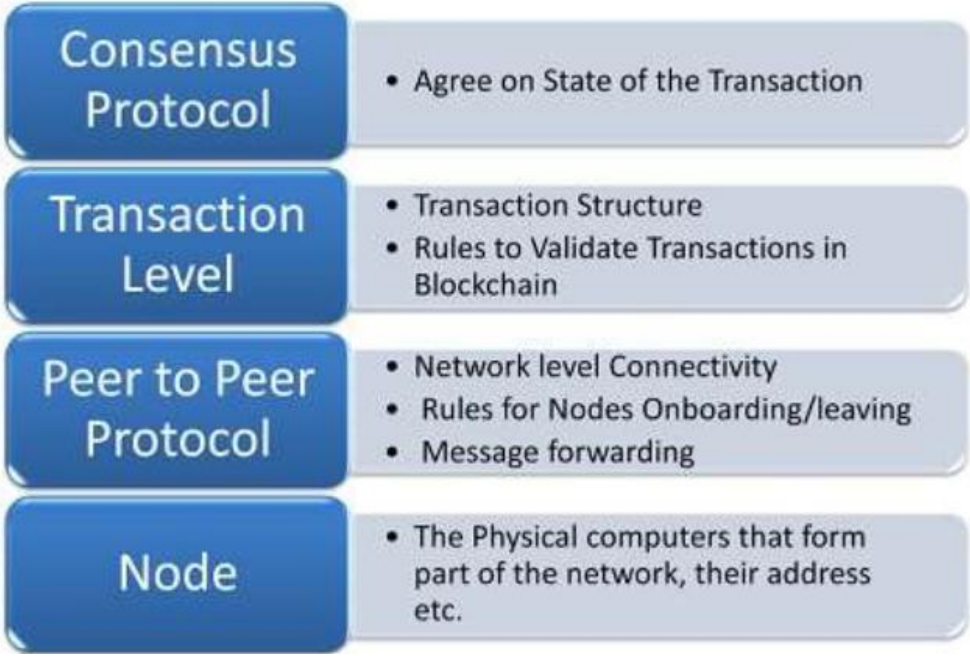
Abstract Interpretation

- Abstract Interpretation is a technique introduced by Cousot and Cousot in 1977 to create a reliable **estimate of how a program will behave during its execution**.
- Used in various fields, such as **security and database management**, and in **different programming environments**.
- The main concept involves **taking the detailed behavior of a program and generalizing it by focusing on key properties instead of specific values**.
- Allows the program's operations to be simulated in a way **that maintains accuracy**.
- Both the detailed and generalized behaviors are often **structured in a way that ranks them based on how precise they are**, with the **highest level indicating a lack of information**.

ABSTRACT MODEL FOR BLOCKCHAIN

IBM Abstract Network model of Blockchain

- Blockchain network is a distributed, decentralized system that **relies on the Internet** as its backbone.
- The network is designed to **balance communication among its nodes** and **uses specific protocols for communication**. This abstract model outlines the activities within the system layer.



Consensus Protocol

- Agree on State of the Transaction

Transaction Level

- Transaction Structure
- Rules to Validate Transactions in Blockchain

Peer to Peer Protocol

- Network level Connectivity
- Rules for Nodes Onboarding/leaving
- Message forwarding

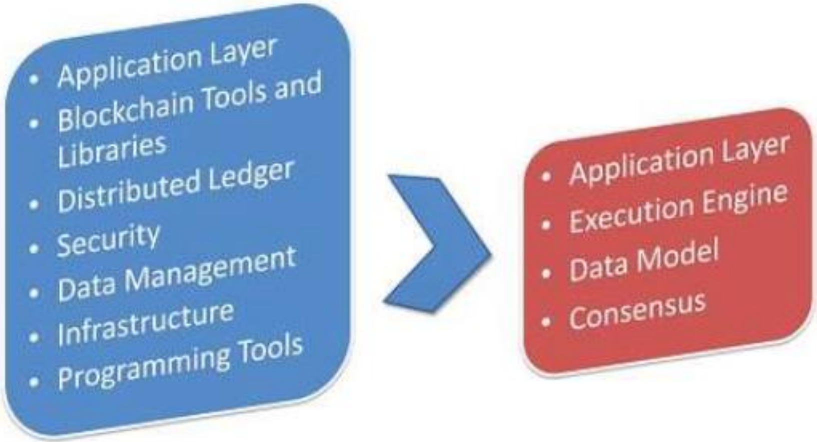
Node

- The Physical computers that form part of the network, their address etc.

ABSTRACT MODEL FOR BLOCKCHAIN

Blockchain Application Model

- As blockchain technology continues to evolve and be explored for new and effective solutions, resource efficiency, and system security, a generic abstract layer model can be defined.
- The Figure below provides a clear picture of the functional focus of each layer and the responsibilities corresponding to that function. It is important to note that this classification is virtual and not physical.



- Application Layer
- Blockchain Tools and Libraries
- Distributed Ledger
- Security
- Data Management
- Infrastructure
- Programming Tools

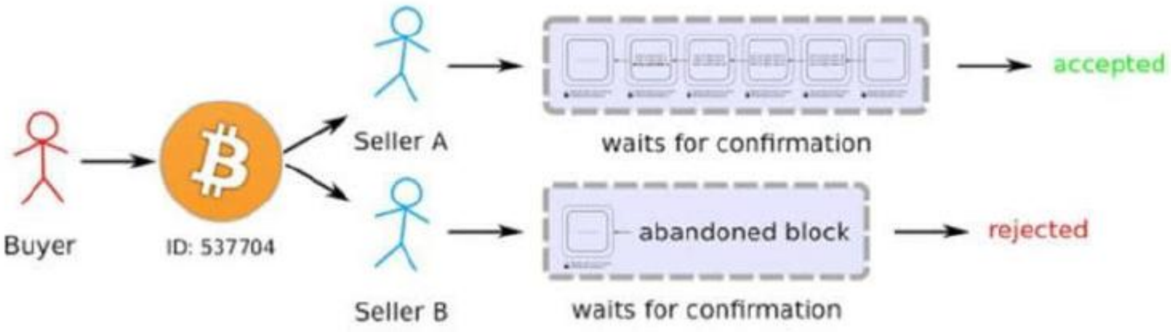
- Application Layer
- Execution Engine
- Data Model
- Consensus

ABSTRACT MODEL FOR BLOCKCHAIN

GARAY model

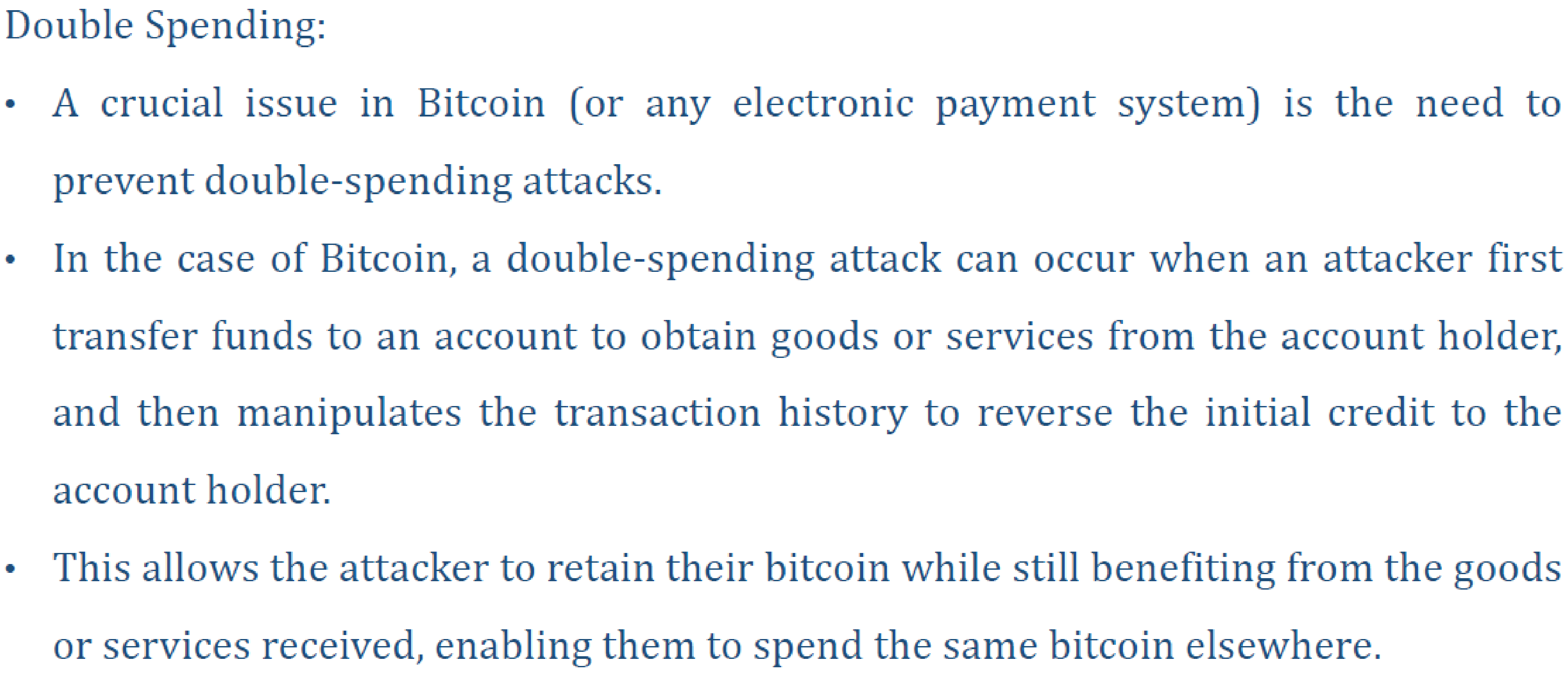
- GARAY model refers to the Bitcoin Backbone protocol, also known as the "Bitcoin Backbone" or the "Garay-Kiayias-Leonardos (GKL) model".
- This model formally analyzes the core security guarantees of consensus mechanisms in blockchains like Bitcoin and Ethereum.
- Properties of Bitcoin Backbone protocol:
  - ✓ Common Prefix
  - ✓ Chain Quality
  - ✓ Chain Growth

Double Spending



ABSTRACT MODEL FOR BLOCKCHAIN

GARAY model



Double Spending:

- A crucial issue in Bitcoin (or any electronic payment system) is the need to prevent double-spending attacks.
- In the case of Bitcoin, a double-spending attack can occur when an attacker first transfer funds to an account to obtain goods or services from the account holder, and then manipulates the transaction history to reverse the initial credit to the account holder.
- This allows the attacker to retain their bitcoin while still benefiting from the goods or services received, enabling them to spend the same bitcoin elsewhere.

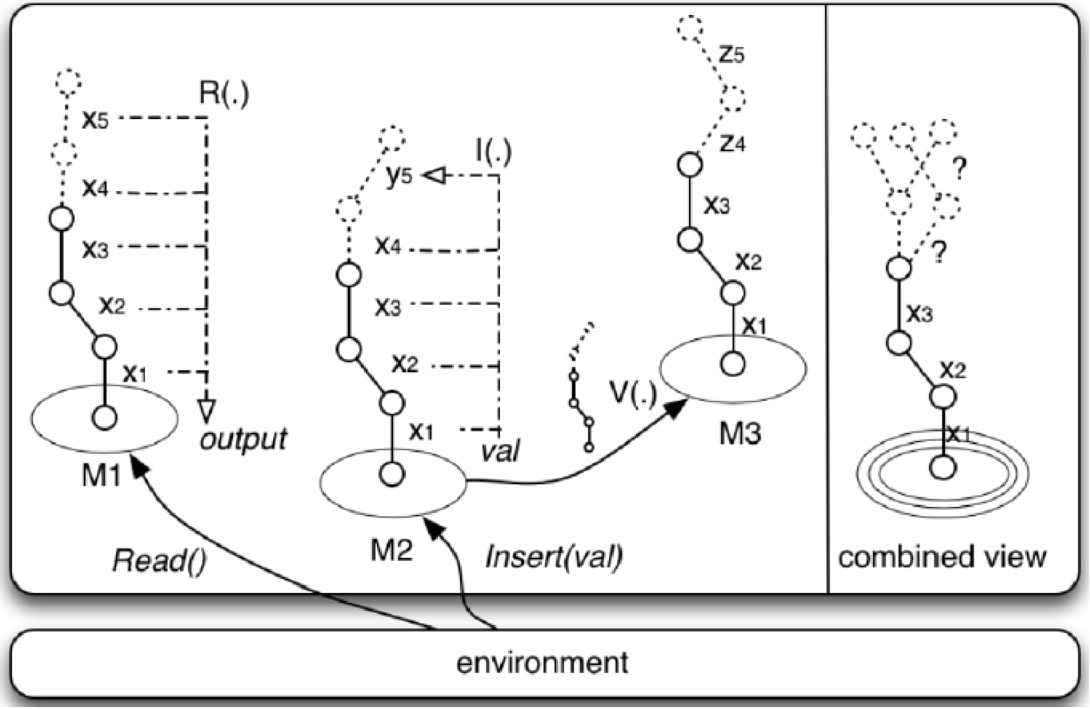
ABSTRACT MODEL FOR BLOCKCHAIN

GARAY model

- Common Prefix (consistency and integrity): The common prefix property Q_{cp} with parameter $k \in N$ states that for any pair of honest players P_1, P_2 adopting the chains C_1, C_2 then it holds as long as removing k blocks from P_1 honest party's chain results to a prefix of P_2 honest party's chain.
- Chain Quality (security and efficiency): The chain quality property Q_{cq} with parameters $\mu \in R$ and $l \in N$ states that for any honest party P with chain C it holds that for any consecutive blocks of length l the ratio of honest blocks is at least μ.
- Chain Growth (reliability and security): The chain growth property Q_{cg} with parameters $\tau \in R$ and $s \in N$ states that for any honest party P that has a chain C it holds that after any s consecutive rounds it adopts a chain that is at least $\tau \cdot s$ blocks longer than C.

ABSTRACT MODEL FOR BLOCKCHAIN

GARAY model



Overview of the basic operation of the Bitcoin backbone protocol

ABSTRACT MODEL FOR BLOCKCHAIN

Proof of Stake (PoS) vs Proof of Work:

Proof of Stake	Proof of Work
Block creators are called validators	Block creators are called miners
Participants must own coins or tokens to become a validator	Participants must buy equipment and energy to become a miner
Energy efficient	Not energy efficient
Security through community control	Robust security due to expensive upfront requirement
Validators receive transactions fees as rewards	Miners receive block rewards

ABSTRACT MODEL FOR BLOCKCHAIN

Hybrid Models (PoW + PoS)

- A hybrid PoW/PoS model **combines Proof of Work (PoW) and Proof of Stake (PoS)** as consensus mechanisms within a blockchain network.
- **Merge** the **security features of PoW** with the **governance and energy efficiency benefits of PoS**.
- The goal of hybrid PoW/PoS systems is to **harness the strengths of both approaches while compensating for their weaknesses**.
- **Decreed** is one of the few **cryptocurrencies that effectively integrates both PoW and PoS**, **creating a multifaceted consensus mechanism**.
- "**Masternode coins**" are also considered hybrids, as they
  - **feature a PoW component similar to Bitcoin**, **along with an additional role for special nodes (masternodes)**.
  - these nodes are typically **required to hold a certain amount of the cryptocurrency as collateral**, demonstrating their commitment to the network's well-being—**similar to Proof of Stake**.
  - **Dash was the first masternode coin, referring to this model as Proof of Service.**

ABSTRACT MODEL FOR BLOCKCHAIN

Decred's Hybrid Model

- Decred’s PoW component **functions like other PoW-based systems** and **uses the Blake-256 hash function.**
- Decred’s **PoS component and its integration into the blockchain are unique**.
  - To participate in Decred’s PoS system, **holders must lock their DCR (Decred tokens) to buy "tickets.“**
  - The **price of each ticket is determined by a market-like mechanism**, with the system targeting a specific number of live tickets (40,960).
  - If there are **more than the target number, the price goes up**; if there are **fewer, the price goes down**.
  - **Once a ticket is purchased**, the **DCR used is locked** and **cannot be spent until the ticket is either called to vote or expires** after roughly **142 days**.
  - This **creates an opportunity cost for PoS participants**, ensuring that they have a vested interest in the network's success.
- **PoS participants**, also known as voters or stakeholders, **have three primary roles**:
  - **Block Voting**: Ensuring the validity of blocks created by PoW miners.
  - **Voting on Consensus Rule Changes**: Deciding on changes to the network’s rules.
  - **Project-Level Governance**: Using the Politeia Proposal System to **vote on proposals** related to the **project’s development and direction**.

ABSTRACT MODEL FOR BLOCKCHAIN

Deciding on Blocks

- **When a PoW miner finds a valid block, they broadcast it to the network**.
- For the **block to be considered valid**, it must **include votes from at least 3/5 randomly selected tickets**.
- **PoS voters must keep their wallets open and ready to respond with votes when their tickets are called** (or they can use Voting Service Providers to do this on their behalf).
- **When a PoS ticket is called and votes, its owner receives a reward**.
- **When tickets vote**, they can **either accept or reject the transactions in the previous block**.
- The network will not **recognize a new block as valid** unless it includes **at least 3 votes**.
- If a **majority of the tickets called reject** the previous block's transactions, those **transactions are returned to the mempool** (**a waiting area for transactions**).
- This mechanism **gives PoS voters the power to deny rewards to miners** without affecting their own rewards. It **limits the power of PoW miners** to block changes to the network's consensus rules, which are decided by the stakeholders.
- PoS voters **can reject any miner behavior** they dislike **by adopting a strategy of voting "no"** when they detect **malicious or inefficient actions**.
- This **prevents bad PoW miners from writing transactions and receiving rewards**.

ABSTRACT MODEL FOR BLOCKCHAIN

- The PoS voting layer significantly **enhances the network's security and resistance to majority attacks**.
- A common method of conducting a majority **double-spend attack** involves **secretly mining an alternative chain and then releasing it after some time**, benefiting from the invalidation of transactions on the "old" chain.
- Since **Decred blocks require input from randomly selected tickets** to be considered valid and **cannot be built upon by PoW miners** without this input, **PoW miners cannot mine secretly** unless they also control a large portion of the live tickets.

Enhanced Security and Governance

- The hybrid PoW/PoS design significantly **increases the cost of attacking the network because an attacker must bypass both systems**.
- The PoS component is designed so that **tickets can only be acquired gradually**. A **limited number of tickets can be bought** in each block/interval, and **purchasing the maximum number causes the price to increase sharply**.
- Once these tickets are purchased, the **funds used are time-locked**, exposing an attacker to any loss in value of their locked coins due to an attack.

ABSTRACT MODEL FOR BLOCKCHAIN

- The requirement that each block is **voted on by randomly selected stakeholders means** that the blockchain must be shared with all participants as it is mined, enhancing the network's security.
- **Decred's hybrid system** is also designed to **give stakeholders control over the PoW miners**.

Consensus Rule Change Voting

- From the beginning, **Decred decided to give PoS stakeholders the primary decision-making power** in the blockchain's governance.
- Built into the consensus rules is an upgrade process through which **any change to the network's rules must go through a voting process**.
- Changes can only be made **if approved by at least 75% of the voting tickets**.
- This process begins once a certain proportion of **miners (95%) and voters (75%)** are running updated software with dormant rule changes.
- If the proposal has **75% support after a one-month voting period**, **it is accepted**; otherwise, it is rejected.
- If it **does not achieve a supermajority**, a **re-vote begins**.
- If a **proposal is accepted**, the **rule change activates one month later**.

Text Book and Reference Books

Text Book

- Dhillon, V., Metcalf, D., and Hooper, M, Blockchain enabled applications, 2017, 1st Edition, CA: Apress, Berkeley.

Reference Books

- Diedrich, H., Ethereum: Blockchains, digital assets, smart contracts, decentralized autonomous organizations, 2016, 1st Edition, Wildfire publishing, Sydney.
- Wattenhofer, R. P, Distributed Ledger Technology: The Science of the Blockchain (Inverted Forest Publishing), 2017, 2nd Edition, Createspace Independent Pub, Scotts Valley, California, US.