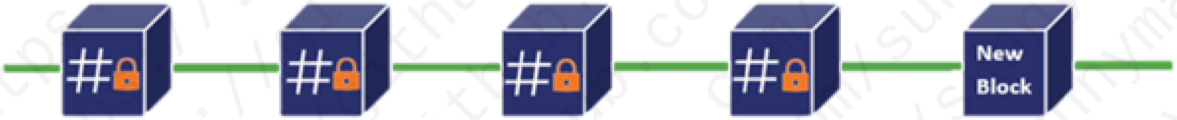
UNIT - 3

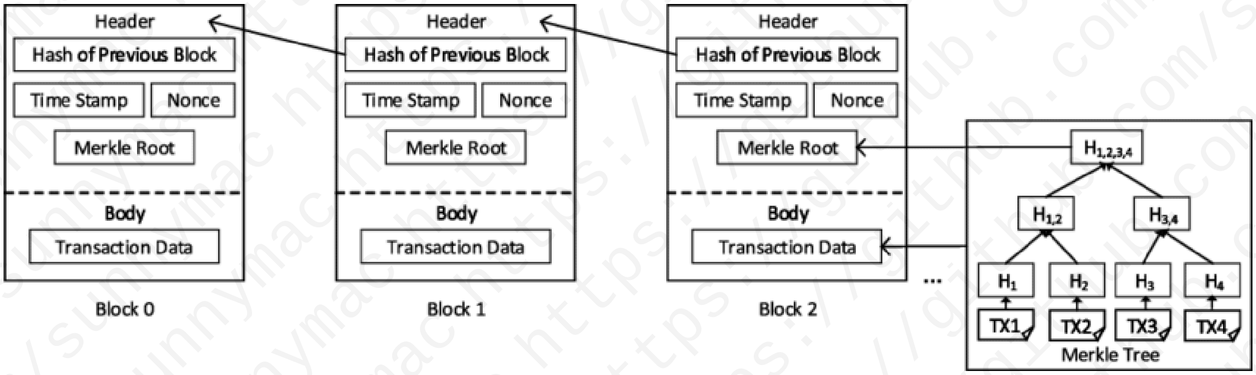
Introduction to Blockchain: A typical block structure, chain of block, distributed ledger, Permissioned and Permission-less Model, Constructing a chain, Orphan block, Block propagation, Introduction to mining

A typical block structure

Block in a Blockchain–Blockchain is a linear chain of blocks.Each block contains a set of transactions and other essential details. Blocks are linearly connected and cryptographically secured.



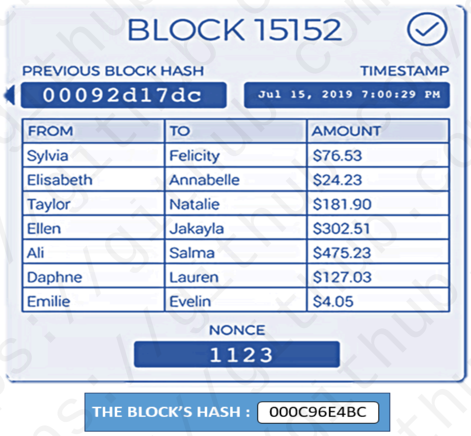
Each block header contains the previous block hash, current block hash, nonce, Merkle root, and other details.



All blocks are connected linearly by carrying the hash of the previous block. The previous block hash is used to compute the current block hash. The first block with no previous block hash is called "Genesis Block." For adding a new block to the network, the blockchain follows consensus mechanisms like proof of work (PoW), proof of stake (PoS), etc.

Structure of a Block

Let's just draw a conceptual image of a block with reference to a ledger of transactions.



BLOCK 15152

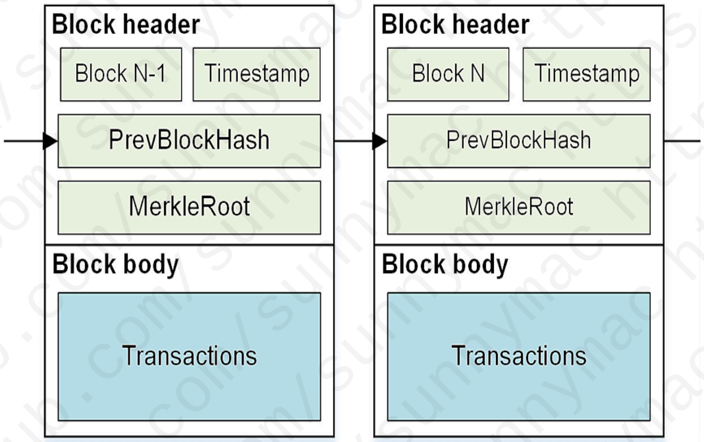
PREVIOUS BLOCK HASH 00092d17dc

TIMESTAMP Jul 15, 2019 7:00:29 PM

FROM	TO	AMOUNT
Sylvia	Felicity	$76.53
Elisabeth	Annabelle	$24.23
Taylor	Natalie	$181.90
Ellen	Jakayla	$302.51
Ali	Salma	$475.23
Daphne	Lauren	$127.03
Emilie	Evelin	$4.05

NONCE 1123

THE BLOCK'S HASH : 000C96E4BC



Block Height : It's the sequence number of the block in the chain of blocks. Block Height: 1 is the genesis block (first block in the network).

Block Size : It's a 4-bytes or 32-bit field that contains the size of the block. It adds size in Bytes. Ex – Block Size: 216 Bytes.

Block Reward : This field contains the amount rewarded to the miner for adding a block of transactions.

Tx Count : The transaction counter shows the number of transactions contained by the block. The field has a maximum size of 9 bytes.

Block Header : The Block header is an 80-Byte field that contains the metadata – the data about the block.

- Time : It's the digitally recorded moment of time when the block has been mined. It is used to validate the transactions.
- Version : It's a 4-bytes field representing the version number of the protocol used. Usually, for bitcoin, it's '0x1'.

- Previous Block Hash : It’s a 32-bytes field that contains a 256-bits hash (created by SHA-256 cryptographic hashing) of the previous block. This helps to create a linear chain of blocks.
- Bits : It’s a 4-bytes field that tells the complexity to add the block. It’s also known as “difficulty bits.” According to PoW, the block hash should be less than the difficulty level.
- Nonce : It’s a 4-bytes field that contains a 32-bit number. These are the only changeable elements in a block of transactions. In PoW, miners alter nonce until they find the right block hash.
- Merkle Root : A 32-bytes field containing a 256-bit root hash. It’s constructed hierarchically combining hashes of the individual transactions in a block.

Distributed ledger

Distributed Ledger Technology (DLT) is centered around an encoded and distributed database where records regarding transactions are stored. A distributed ledger is a database spread across various computers, nodes, institutions, or countries and accessible by multiple people around the globe.

Key Features:

- Decentralized: It is a decentralized technology and every node will maintain the ledger, and if any data changes happen, the ledger will get updated. The process of updating takes place independently at each node. Even small updates or changes made to the ledger are reflected and the history of that change is sent to all participants in a matter of seconds.
- Immutable: Distributed ledger uses cryptography to create a secure database in which data once stored cannot be altered or changed.
- Append only: Distributed ledgers are append-only in comparison to the traditional database where data can be altered.
- Distributed: In this technology, there is no central server or authority managing the database, which makes the technology transparent. To counter the weaknesses of having one ledger to rule all, So that there is no one authoritative copy and have specific rules around changing them. This would make the system much more transparent and will make it a more decentralized authority. In this process, every node or contributor of the ledger will try to verify the transactions with the various consensus

algorithms or voting. the voting or participation of all the nodes depends on the rules of that ledger. In the case of bitcoin, the Proof of Work consensus mechanism is used for the participation of each node.

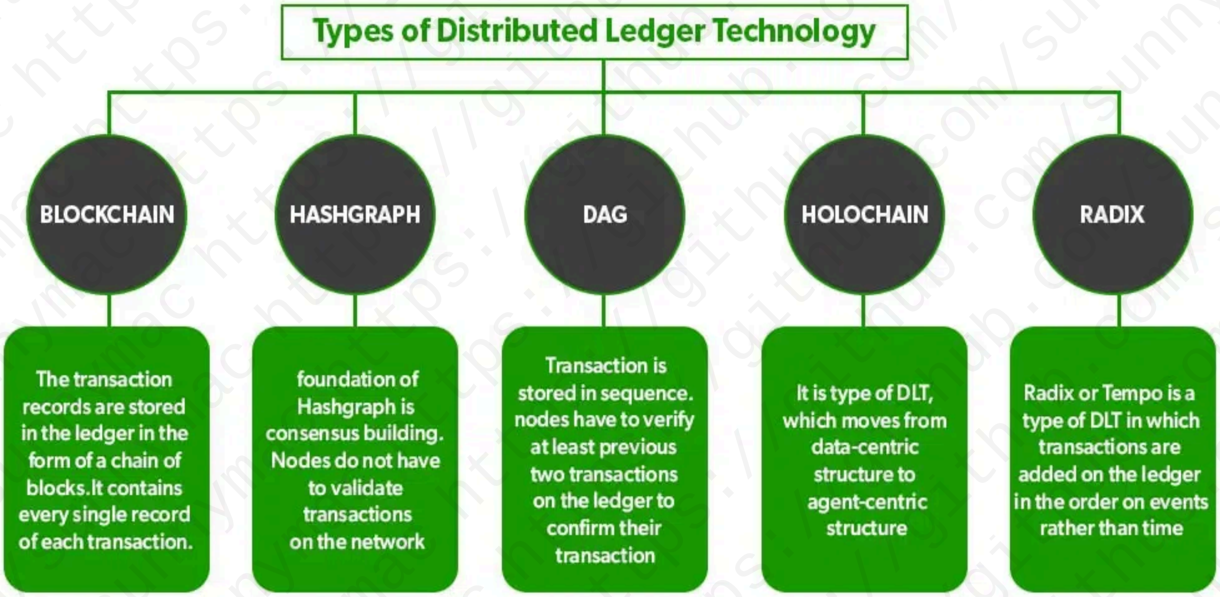
- Shared: The distributed ledger is not associated with any single entity. It is shared among the nodes on the network where some nodes have a full copy of the ledger while some nodes have only the necessary information that is required to make them functional and efficient.
- Smart Contracts: Distributed ledgers can be programmed to execute smart contracts, which are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. This allows for transactions to be automated, secure, and transparent.
- Fault Tolerance: Distributed ledgers are highly fault-tolerant because of their decentralized nature. If one node or participant fails, the data remains available on other nodes.
- Transparency: Distributed ledgers are transparent because every participant can see the transactions that occur on the ledger. This transparency helps in creating trust among the participants.
- Efficiency: The distributed nature of ledgers makes them highly efficient. Transactions can be processed and settled in a matter of seconds, making them much faster than traditional methods.
- Security: Distributed ledgers are highly secure because of their cryptographic nature. Every transaction is recorded with a cryptographic signature that ensures that it cannot be altered. This makes the technology highly secure and resistant to fraud.

Types of Distributed Ledger Technology

- Blockchain: In this type of DLT, transactions are stored in the form chain of blocks and each block produces a unique hash that can be used as proof of valid transactions. Each node has a copy of the ledger which makes it more transparent.
- Directed Acyclic Graphs (DAG): This uses a different data structure to organize the data that brings more consensus. In this type of DLT, validation of transactions mostly requires the majority of support from the nodes in the network. Every node on the network has to provide proof of transactions on the ledger and then can initiate transactions. In this nodes have to verify at

least two of the previous transactions on the ledger to confirm their transaction.

- Hashgraph: In this type of DLT, records are stored in the form of a directed acyclic graph. It uses a different consensus mechanism, using virtual voting as the form consensus mechanism for gaining network consensus. Hence nodes do not have to validate each transaction on the network.
- Holochain: Holochain is termed as the next level of blockchain by some people because it is much more decentralized than blockchain. It is a type of DLT that simply proposes that each node will run on a chain of its own. Therefore nodes or miners have the freedom to operate autonomously. It basically moves to the agent-centric structure. Here agent means computer, node, miner,etc.
- Tempo or Radix: Tempo uses the method of making a partition of the ledger this is termed sharding and then all the events that happened in the network are ordered properly. Basically, transactions are added to the ledger on the basis of the order of events rather than the timestamp.


Types of Distributed Ledger Technology
BLOCKCHAIN
HASHGRAPH
DAG
HOLOCHAIN
RADIX
The transaction records are stored in the ledger in the form of a chain of blocks.It contains every single record of each transaction.
foundation of Hashgraph is consensus building. Nodes do not have to validate transactions on the network
Transaction is stored in sequence. nodes have to verify at least previous two transactions on the ledger to confirm their transaction
It is type of DLT, which moves from data-centric structure to agent-centric structure
Radix or Tempo is a type of DLT in which transactions are added on the ledger in the order on events rather than time

Advantages Of Distributed Ledger Technology

- High Transparency: Distributed ledger presents a high level of transparency because all the transaction records are visible to everyone. The addition of data needs to be validated by nodes by using various consensus mechanisms.

and if anyone tries to alter or change data in the ledger then it is immediately reflected across all nodes of the network which prevents invalid transactions.

- Decentralized: In a centralized network, there may be a single point of failure and it can disrupt the whole network because of mistakes at the central authority level. But in the case of distributed networks, there is no risk of a single point of failure. Because of the decentralized structure, the trust factor also increases in participating nodes. This decentralized nature of validation reduces the cost of transactions drastically.
- Time Efficient: As this network is decentralized so there is no need for a central authority to validate transactions every time. Hence this time for validation of each transaction reduces drastically. In the case of DLT, transactions can be validated by members of the network itself by using various consensus mechanisms.
- Scalable: Distributed ledger technology is more scalable because many different types of consensus mechanisms can be used to make it more reliant, fast, and updated. Because many advanced DLT technologies have been introduced in the last few years. Such as Holochain, hashgraph are considered to be advanced and more secure versions of Blockchain DLT. Blockchain itself is advanced and secure but DLT provides a way to more advanced technologies.

Applications of Distributed Ledger Technology

- Banking: In the banking sector right now transfer of money can be both expensive and time-consuming. Also sending money overseas becomes even more complex due to exchange rates and other hidden fees included. Here DLT can provide a decentralized secure network that will help to reduce the time, complexity, and costs required to transfer money. This decentralized network will eliminate the need for third parties which makes this system more complex and time-consuming.

- Cyber Security: Nowadays cyber security has been emerging as a big threat to governments, enterprises, and individual people also. So it is essential to find an effective solution to secure our data and privacy against unauthorized access. In DLT, all information is authorized and securely encrypted by various cryptographic algorithms. This provides a transparent and secure environment and none of the data can be tempered by any entity.
- Supply chain management: Supply chain is one of the complex structures itself. In this structure, it is hard to trace where the fault happened. So here Distributed ledger technology comes into the picture, Using DLT, you can easily trace the supply chain from the beginning to the end and can easily find out where a mistake or fault has happened. All the data added to the DLT is validated and permanent and can not be altered. This transparency of data enables us to trace from the beginning to the end of the ledger.
- Healthcare: Distributed Ledger eliminates central authority and ensures rapid access to secured and untempered data. Here important medical can be stored securely and no one can change this data, even if someone tries to change it will be reflected everyone immediately. DLT can be used in the insurance sector to trace false claims because of its decentralized system.
- Governance: DLT can be used in the government system to make it transparent among citizens. Many governments have adopted blockchain in the governance system because of the robustness of this system. It can be used as a voting system too. The traditional voting system has many flaws and sometimes it is found that there are many false voting and illegal activities that happen during voting. Online voting systems can be used to vote and with security and fake votes can be easily checked. Everyone will have their own identity. So that any person sitting anywhere in the world can cast his vote.

Youtube Tutorial:
Chain Reaction: Distributed Ledger Technologies (DLT) explained

How are Blockchain And Distributed Ledger Different?

Aspect	Distributed Ledger	Blockchain Technology
Block Structure	In DLT, blocks can be organized in different forms.	In Blockchain, blocks are added in the form of a chain.
Power of Work	It is more scalable because it does not need the power of a work consensus mechanism for the validation of each transaction.	It is a subset of DLT, the power of the work consensus mechanism adds more functionalities and security.
Tokens	It does not require any tokens or digital currency.	In it, tokens must be considered while working with Blockchain.
Sequence	It does not require any specific sequence of data.	All blocks are arranged in a particular series.
Trustability	Trust among participating nodes is high.	Trust among participating nodes is less than DLT. Decision-making powers can be on one hand because everyone can mine.

Advantages of Using Distributed Ledger Technology In Blockchain

- Security: All records of every transaction are securely encrypted. Once the transaction is validated, it is completely secure and no one can update or change it. It is a permanent process.

- Decentralization: All network members or nodes have a copy of the ledger for complete transparency. A decentralized private distributed network improves the reliability of the system and gives assurance of continuous operations without any interruption. It gives control of information and data in the hand of the user.
- Anonymity: The identity of each participant is anonymous and does not possibly reveal their identity.
- Immutable: Any validated transactions can not be changed as they are irreversible.
- Transparency: Distributed technologies offer a high level of transparency. Which is necessary for the sectors like finance, medical science, banking, etc.
- Speed: Distributed Ledger Technology can handle large transactions faster than traditional methods.
- Smart Contracts: Distributed Ledger Technology supports smart contracts which are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. Smart contracts reduce the need for intermediaries and offer transparency and automation in the execution of the contract terms.
- Lower Costs: Distributed Ledger Technology eliminates intermediaries and reduces the costs associated with intermediaries, which makes the system more cost-effective.
- Improved Efficiency: Distributed Ledger Technology reduces the time and costs associated with traditional transaction methods. It offers faster settlement times, reduced paperwork, and increased efficiency.
- Auditing: Distributed Ledger Technology makes auditing easier as every transaction is recorded and the ledger cannot be altered. This improves the transparency and accuracy of financial audits.
- Resilience: Distributed Ledger Technology is more resilient than traditional databases as it is spread across multiple nodes. This means that even if one node goes down, the network can still function as the rest of the nodes can continue to validate transactions.
- Traceability: Distributed Ledger Technology offers complete traceability of assets, from their creation to their current ownership. This improves accountability and reduces the risks of fraud and theft.

Disadvantages Of Distributed Ledger Technology

- 51% Attack: The 51% attack is a bit concerning part of this distributed ledger technology that is to be checked routinely.
- Costs of Transaction: The connected nodes are expected to validate the transaction of a given Distributed Ledger Technology which gives high transaction cost as the other nodes are paid incentives to validate the transaction.
- Slow Transaction Speed: The major disadvantage of this DLT is the slow speed of transactions as multiple nodes are attached to this network and it takes time to validate the transaction by all the other nodes.
- Scalability Issues: Due to low speed and high transaction costs DLT faces very difficulties to expand on a large scale.
- Lack of Regulation: As DLT is a decentralized technology, it operates outside the control of any centralized authority which can lead to a lack of regulation, making it difficult to hold accountable any wrongdoings or fraudulent activities on the network.
- Energy Consumption: Distributed Ledger Technology requires a significant amount of energy to maintain the network and validate transactions, especially in the case of Proof of Work consensus mechanisms, which can lead to a negative impact on the environment.
- Complexity: Implementing and managing Distributed Ledger Technology can be complex and requires a high level of technical expertise, which can be a barrier to entry for many organizations and individuals.
- Privacy Concerns: While the anonymity of participants on the network is considered an advantage, it can also be a disadvantage as it can lead to privacy concerns and illicit activities on the network.
- Lack of Interoperability: Different Distributed Ledger Technologies may use different protocols, which can lead to interoperability issues, making it difficult for different networks to communicate and transact with each other.

Permissioned and Permission-less Model

Permissionless Blockchain

A permissionless blockchain is a type of blockchain network that allows anyone to participate in the network without requiring special permissions or approvals.

- Open Access: Anyone can join the network, validate transactions, and contribute to the blockchain. This openness fosters a decentralized environment where no single entity controls the network.
- Decentralization: Permissionless blockchains operate on a decentralized network of nodes, which helps to distribute power and reduce the risk of censorship or manipulation by any single party.
- Consensus Mechanisms: These blockchains typically use consensus algorithms such as network participants' Proof of Stake (PoS) to validate transactions and secure the network. Participants compete to solve complex mathematical problems (in the case of PoW) or stake their own tokens (in PoS) to earn the right to validate new blocks.
- Transparency: All transactions on a permissionless blockchain are recorded on a public ledger, allowing anyone to view transaction history and verify data integrity.
- Anonymity: While transactions are transparent, participants often remain pseudonymous. Users are identified by their public keys rather than personal information, providing a layer of privacy.

Permissioned Blockchain

A permissioned blockchain is a type of blockchain network that restricts access and participation to a select group of authorized users. Unlike permissionless blockchains, where anyone can join and validate transactions, permissioned blockchains require participants to obtain permission before they can access the network or perform certain actions.

- Access Control: Only authorized participants can join the network, ensuring that all nodes are known and vetted. This allows for greater control over who can validate transactions and access data.

- Centralized Governance: Typically governed by a consortium of organizations or a central authority, which makes decisions about network rules and policies.
- Enhanced Privacy: Transactions and data are often more private, as sensitive information can be kept off-chain or shared only among authorized parties.
- Customizable Protocols: Organizations can customize consensus mechanisms and other protocols to meet their specific needs and requirements.

Types of Blockchain

1. Public Blockchain
2. Private Blockchain
3. Hybrid Blockchain
4. Hybrid Blockchain

1. Public Blockchain

These blockchains are completely open to following the idea of decentralization. They don't have any restrictions, anyone having a computer and internet can participate in the network.

- As the name is public this blockchain is open to the public, which means it is not owned by anyone.
- Anyone having the internet and a computer with good hardware can participate in this public blockchain.
- All the computers in the network hold the copy of other nodes or blocks present in the network
- In this public blockchain, we can also perform verification of transactions or records

Advantages:

- Trustable: There are algorithms to detect fraud. Participants need not worry about the other nodes in the network.
- Secure: This blockchain is large as it is open to the public. In a large size, there is a greater distribution of records.
- Anonymous Nature: It is a secure platform to make your transaction properly at the same time, you are not required to reveal your name and identity to participate.

- Decentralized: There is no single platform that maintains the network, instead every user has a copy of the ledger.

Disadvantages:

- Processing: The rate of the transaction process is very slow, due to its large size. Verification of each node is a very time-consuming process.
- Energy Consumption: Proof of work is highly energy-consuming. It requires good computer hardware to participate in the network.
- Acceptance: No central authority is there so governments are facing the issue of implementing the technology faster.

Use Cases:

Public Blockchain is secured with proof of work or proof of stake; they can be used to displace traditional financial systems. The more advanced side of this blockchain is the smart contract that enabled this blockchain to support decentralization. Examples of public blockchains are Bitcoin and Ethereum.

2. Private Blockchain

These blockchains are not as decentralized as the public blockchain; only selected nodes can participate in the process, making it more secure than the others.

- These are not as open as a public blockchain.
- They are open to some authorized users only.
- These blockchains are operated in a closed network.
- In this few people are allowed to participate in a network within a company/organization.

Advantages:

- Speed: The rate of the transaction is high, due to its small size. Verification of each node is less time-consuming.
- Scalability: We can modify the scalability. The size of the network can be decided manually.
- Privacy: It has increased the level of privacy for confidentiality reasons as the businesses required.
- Balanced: It is more balanced as only some users have access to the transaction which improves the performance of the network.

Disadvantages:

- Security: The number of nodes in this type is limited so chances of manipulation are there. These blockchains are more vulnerable.
- Centralized: Trust building is one of the main disadvantages due to its central nature. Organizations can use this for malpractices.
- Count: Since there are few nodes if nodes go offline the entire system of blockchain can be endangered.

Use Cases:
With proper security and maintenance, this blockchain is a great asset to secure information without exposing it to the public eye. Therefore companies use them for internal auditing, voting, and asset management. An example of private blockchains is Hyperledger, Corda.

3. Hybrid Blockchain

It is the mixed content of the private and public blockchain, where some part is controlled by some organization and other makes are made visible as a public blockchain.

- It is a combination of both public and private blockchain.
- Permission-based and permissionless systems are used.
- User access information via smart contracts
- Even if a primary entity owns a hybrid blockchain it cannot alter the transaction.

Advantages:

- Ecosystem: The most advantageous thing about this blockchain is its hybrid nature. It cannot be hacked as 51% of users don't have access to the network.
- Cost: Transactions are cheap as only a few nodes verify the transaction. All the nodes don't carry the verification hence less computational cost.
- Architecture: It is highly customizable and still maintains integrity, security, and transparency.
- Operations: It can choose the participants in the blockchain and decide which transaction can be made public.

Disadvantages:

- Efficiency: Not everyone is in a position to implement a hybrid Blockchain. The organization also faces some difficulty in terms of efficiency in maintenance.
- Transparency: There is a possibility that someone can hide information from the user. If someone wants to get access through a hybrid blockchain it depends on the organization whether they will give or not.
- Ecosystem: Due to its closed ecosystem this blockchain lacks the incentives for network participation.

Use Case:
It provides a greater solution to the healthcare industry, government, real estate, and financial companies. It provides a remedy where data is to be accessed publicly but needs to be shielded privately. Examples of Hybrid Blockchain are the Ripple network and XRP token.

4.Consortium Blockchain

It is a creative approach that solves the needs of the organization. This blockchain validates the transaction and also initiates or receives transactions.

- Also known as Federated Blockchain.
- This is an innovative method to solve the organization's needs.
- Some parts are public and some parts are private.
- In this type, more than one organization manages the blockchain.

Advantages:

- Speed: A limited number of users make verification fast. The high speed makes this more usable for organizations.
- Authority: Multiple organizations can take part and make it decentralized at every level. Decentralized authority, makes it more secure.
- Privacy: The information of the checked blocks is unknown to the public view. But any member belonging to the blockchain can access it.
- Flexible: There is much divergence in the flexibility of the blockchain. Since it is not a very large decision, it can be taken faster.

Disadvantages:

- Approval: All the members approve the protocol making it less flexible. Since one or more organizations are involved there can be differences in the vision of interest.
- Transparency: It can be hacked if the organization becomes corrupt. Organizations may hide information from the users.
- Vulnerability: If a few nodes are getting compromised there is a greater chance of vulnerability in this blockchain

Use Cases:
It has high potential in businesses, banks, and other payment processors. Food tracking of the organizations frequently collaborates with their sectors making it a federated solution ideal for their use. Examples of consortium Blockchain are Tendermint and Multichain.

Feature	**Public Blockchain**	**Private Blockchain**	**Hybrid Blockchain**	**Consortium Blockchain**
Access Control	Open to everyone	Restricted to specific participants	Limited to a group of organizations	Combination of public and private
Governance	Decentralized	Centralized	Semi-decentralized	Mixed governance structure
Transparency	High transparency	Low transparency	Moderate transparency	Variable transparency
Scalability	Limited scalability	High scalability	Moderate scalability	High scalability potential

Security	High due to decentralization	Lower due to centralization	Moderate security	Variable security
Transaction Speed	Slower due to consensus mechanisms	Faster transactions	Faster than public, slower than private	Variable speed
Use Cases	Cryptocurrencies, decentralized apps	Enterprise solutions, data privacy	Supply chain, banking, collaborations	Various applications need flexibility

Youtube Tutorial:

▶ Crypto Education - Permissioned vs Permissionless Blockchains Explained | A…

▶ Types of Blockchain Explained | Blockchain Types

Orphan block

An **orphan block** in blockchain is a block that is **valid** but **not accepted as part of the longest (or main) blockchain** because it was mined at almost the same time as another block, but eventually **lost the race** to be included in the main chain. These blocks are legitimate and verified, but they do not contribute to the current valid chain.

How Do Orphan Blocks Occur?

- **Simultaneous Mining:**
  Two miners solve a block at approximately the same time.
  Both blocks get broadcasted to different parts of the network.
- **Temporary Fork:**
  For a short time, the blockchain forks because different parts of the network have different versions of the blockchain.

- **Chain Selection:**
  Nodes continue mining on the block they first receive.
  Eventually, **one chain becomes longer** (as more blocks are added to it).
  The blockchain protocol (like Bitcoin) always chooses the **longest chain as the valid chain**.

Feature	**Explanation**
Validity	Fully valid block, but not part of the main chain.
Cause	Network latency or simultaneous block discovery.
Effect on Network	Temporary fork, quickly resolved by longest chain rule.
Impact on Miner	No block reward for orphan blocks in most cases.
Storage	Nodes may still keep orphan block data temporarily for verification.

Why Are Orphan Blocks Important?

- **Security:** Orphan blocks demonstrate that the blockchain can handle temporary forks and maintain consensus.
- **Decentralization:** They show that mining is happening simultaneously around the world.
- **Transaction Confirmation:** Transactions in orphan blocks usually return to the mempool (if not already included in the competing block).

Are Orphan Blocks Dangerous?

No. They are a normal part of blockchain operation. Orphan blocks are discarded and do not cause security risks.However, if orphan blocks are frequent, they may indicate network latency or block propagation delays.

What Happens to the Transactions in Orphan Blocks?If a transaction in an orphan block is not in the competing block (the one that won), it usually returns to the mempool and will be picked up by another miner in the next block.

Block propagation

Block propagation refers to the process of **distributing a newly mined block** across all the nodes in a blockchain network. When a miner successfully mines a new block, it needs to quickly inform the rest of the network so that all nodes can update their copy of the blockchain.

Step-by-Step Process: How Block Propagation Works

1. Block Mining: A miner solves the cryptographic puzzle and mines a new block.
2. Broadcasting the Block: The miner immediately broadcasts the block to its connected peer nodes.
3. Peer-to-Peer Sharing:Each peer node that receives the new block validates it (checking its correctness, transaction validity, and block hash). Once validated, the node forwards (propagates) the block to its own connected peers.
4. Flooding the Network: This process repeats rapidly across the entire network. Within a few seconds, almost all nodes in the network receive the new block.
5. Chain Update: All nodes update their local blockchain by adding the new block to their copy of the chain.

What is Mining in Blockchain?

Mining in blockchain is the process of adding new blocks to the blockchain by solving complex mathematical puzzles.
It is essential for:

- Creating new coins (in cryptocurrencies like Bitcoin).
- Verifying and securing transactions.
- Maintaining the decentralized consensus of the blockchain.

Purpose of Mining

- **Validation:** Ensures that transactions are legitimate and follow the network's rules.
- **Consensus:** Allows all distributed nodes to agree on a single version of the blockchain.

- **New Coin Generation:** In proof-of-work (PoW) systems like Bitcoin, mining introduces new coins into circulation.
- **Security:** Makes it computationally expensive to alter past blocks, protecting the blockchain from attacks.

How Mining Works (Step-by-Step)

1. Collect Transactions
    a. Miners collect pending (unconfirmed) transactions from the mempool.
2. Form a Block
    a. Miners bundle these transactions into a block.
    b. A block contains:
        i. Block header (metadata)
        ii. List of transactions
        iii. Reference to the previous block (hash)
3. Solve the Cryptographic Puzzle
    a. Miners compete to find a nonce (a random number) that solves a hash puzzle.
    b. The puzzle:
        i. Hash(Block Header + Nonce) < Target Difficulty
        ii. The solution must produce a hash that starts with a specific number of leading zeros.
4. Proof of Work
    a. Finding the correct nonce requires billions of trial-and-error attempts.
    b. The miner who solves the puzzle first broadcasts the new block.
5. Block Verification
    a. Other nodes verify:
        i. The block’s hash is valid.
        ii. All transactions inside are correct.
        iii. If valid, the block is added to the blockchain.
6. Mining Reward
    a. The successful miner earns:
        i. Block Reward: Newly created coins.
        ii. Transaction Fees: Fees from all transactions included in the block.

Key Terms in Mining

Term	Meaning
Nonce	Random number miners adjust to solve the puzzle.
Hash Function	Cryptographic function producing a fixed-size output.
Difficulty	Network-adjusted level of how hard the mining puzzle is.
Proof of Work	Consensus mechanism requiring computational effort.

Types of Mining

Type	Description
Solo Mining	Mining individually, keeping full rewards.
Pool Mining	Miners combine resources and share rewards.
Cloud Mining	Renting mining power from remote data centers.

Youtube Tutorial :

▶ How Does Bitcoin Mining ACTUALLY Work? Explained In 3 Minutes

▶ What is Bitcoin Mining for Beginners - Short and Simple