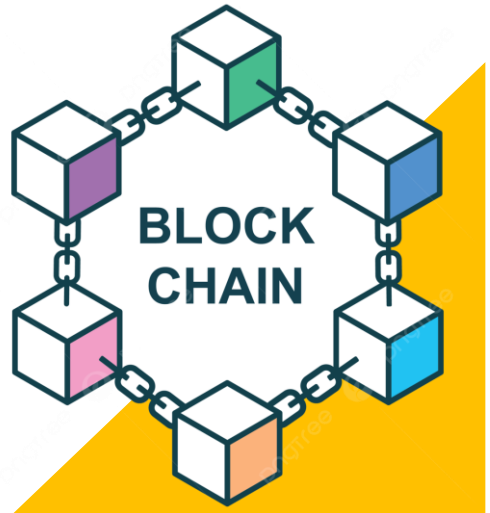
ARYA College of Engineering (ACE)
(Affiliated to RTU | Approved by AICTE, New Delhi)
• SP-40, RIICO Industrial Area, Delhi Road, Kukas, Jaipur-302028 | Tel. Ph. 0141-2820700
• www.aryainstitutejpr.com
• Toll Free: 1800 102 1044

Fundamentals of Blockchain

Unit-4
Tiers of Blockchain Technology



Er. Harsh Raj
(Assistant Professor, CSE)

Course Objectives

1. The students should be able to understand a broad overview of the essential concepts of blockchain technology.

2. To familiarize students with Bitcoin protocol followed by the Ethereum protocol – to lay the foundation necessary for developing applications and programming.

3. Students should be able to learn about different types of blockchain and consensus algorithms.

Expected Course Outcome

1. To explain the basic notion of distributed systems.

2. To use the working of an immutable distributed ledger and trust model that defines blockchain.

3. To illustrate the essential components of a blockchain platform.

Syllabus

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

Text Books

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

Reference Books

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

Topics

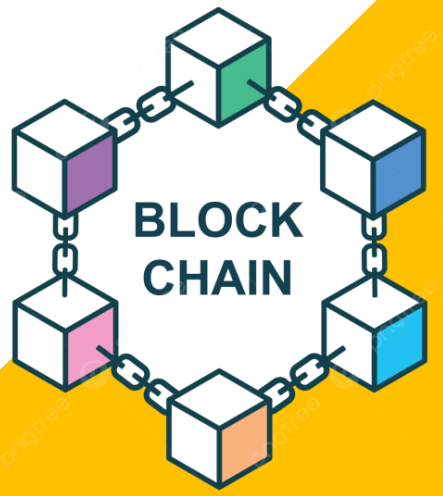
Tiers of Blockchain Technology:

- Blockchain 1.0
- Blockchain 2.0
- Blockchain 3.0

Types of Blockchain:

- Public Blockchain
- Private Blockchain
- Semi-Private Blockchain
- Sidechains

Tiers of Blockchain

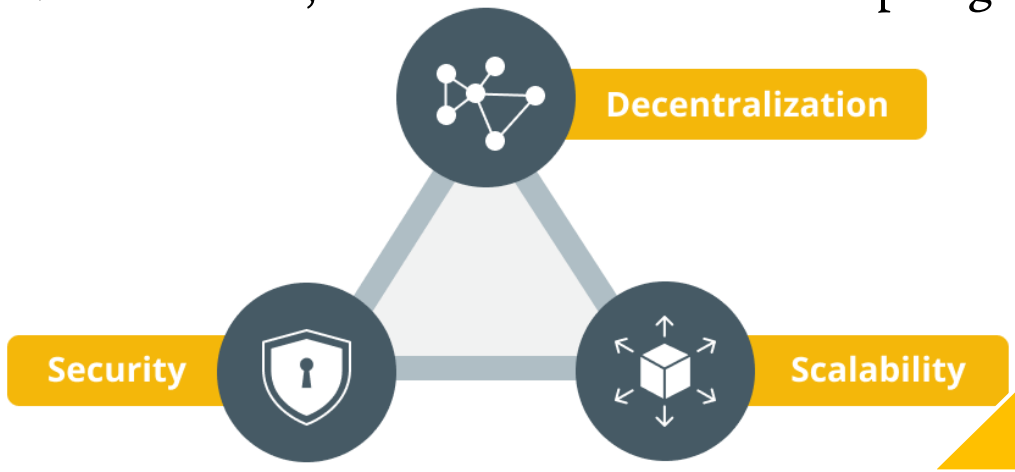


Tiers of Blockchain

Blockchain technology can be divided into different tiers or generations, each representing advancements and improvements over the previous one.
As of my last knowledge update in September 2021, here are the three primary tiers of blockchain technology:

1. First Generation Blockchain (Blockchain 1.0):

- Bitcoin, created by an anonymous entity known as Satoshi Nakamoto, introduced the first generation of blockchain technology.
- Bitcoin's primary use case is as a decentralized digital currency (cryptocurrency).
- It relies on a Proof of Work (PoW) consensus mechanism for securing the network.
- Transactions are transparent and immutable, but the blockchain's scripting language is limited, allowing only basic operations.



2. Second Generation Blockchain (Blockchain 2.0):

- Ethereum, launched by Vitalik Buterin in 2015, is often considered the pioneer of the second generation of blockchain technology.
- Ethereum introduced the concept of smart contracts, which are self-executing contracts with predefined rules and conditions.
- Smart contracts allow for the creation of decentralized applications (DApps) on the Ethereum platform.
- Ethereum uses a PoW consensus mechanism, similar to Bitcoin, but has plans to transition to Proof of Stake (PoS) in Ethereum 2.0 to improve scalability and energy efficiency.
- Other second-generation blockchains, such as EOS, Cardano, and Tezos, also emerged with their own features and improvements.

3. Third Generation Blockchain (Blockchain 3.0):

- Third-generation blockchains aim to address scalability, interoperability, and sustainability issues that have arisen in earlier generations.
- They often employ innovative consensus mechanisms like PoS, Delegated Proof of Stake (DPoS), or Proof of Authority (PoA) to improve efficiency.
- These blockchains prioritize interoperability, allowing different blockchains to communicate and exchange information seamlessly.
- They focus on sustainability by addressing energy consumption concerns, often by utilizing PoS or other eco-friendly consensus mechanisms.
- Examples of third-generation blockchains include Polkadot, Cosmos, and Algorand.

It's worth noting that the blockchain space is continually evolving, and new generations of blockchain technology may have emerged since my last update in September 2021. Additionally, individual projects within each generation may have unique features and capabilities that differentiate them from others in the same generation.

BLOCKCHAIN 1.0

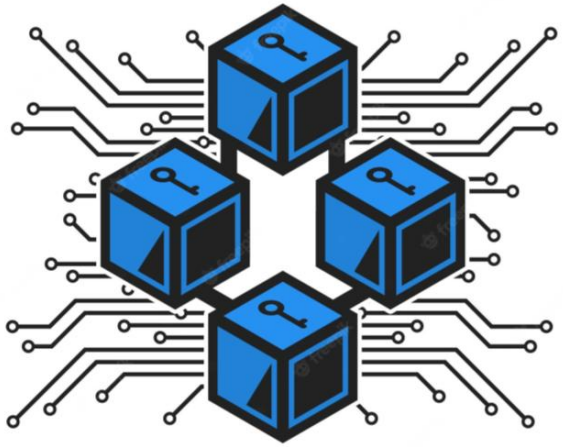
BLOCKCHAIN 2.0

BLOCKCHAIN 3.0

Tiers of Blockchain Technology:

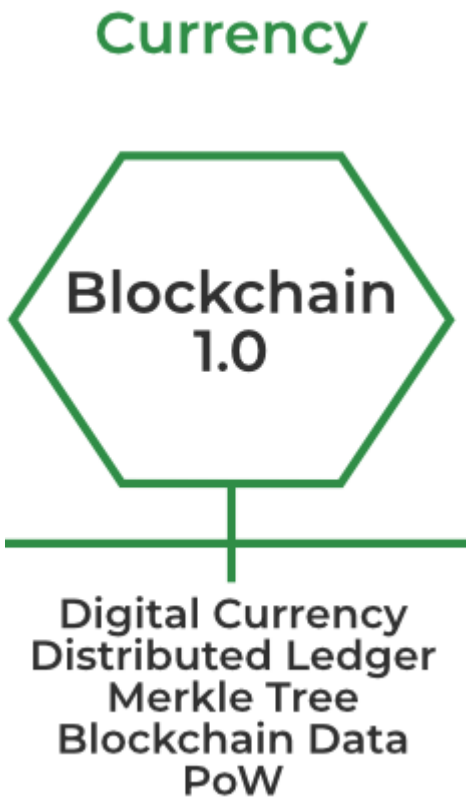
Blockchain 1.0

Blockchain 1.0



- Blockchain 1.0 is also used for **Cryptocurrency**.
- Version 1.0 was introduced in 2005 by Hall Finley, who implements DLT (Distributed Ledger Technology) and represents its first application based on Cryptocurrency.
- This allows Financial Transactions based on Blockchain technology or DTL which is executed with the help of Bitcoin.
- This type of Version is permissionless as any participant will perform a valid transaction of Bitcoin. This type is mainly used in Currency and Payments.
- Blockchain 1.0 or Blockchain Version 1.0 aimed to introduce a transparent, publicly accessible, completely decentralized, immutable ledger and distributed system of transactions in the global financial market.

- Blockchain 1.0 was developed on the idea and structure of Bitcoin.
- It primarily focused on the development and creation of new cryptocurrencies.
- Blockchain 1.0 is often termed a digital, decentralized, distributed ledger that records transactions in a database shared by all nodes, updated by blockchain miners and maintained and monitored by everyone with no individual ownership.



Key Characteristics of Blockchain 1.0

1. **Bitcoin:** The first and most well-known application of blockchain technology is Bitcoin, which was introduced in a whitepaper by an anonymous person or group of people using the pseudonym Satoshi Nakamoto in 2008. Bitcoin is a decentralized digital currency that uses blockchain technology to record transactions and manage the issuance of new coins. It served as the prototype for many other cryptocurrencies that followed.

2. **Cryptocurrency:** Blockchain 1.0 primarily focused on the development and use of cryptocurrencies as a digital form of money. These cryptocurrencies were built on blockchain technology and operated independently of traditional financial institutions.

3. **Proof of Work (PoW):** Most Blockchain 1.0 networks, including Bitcoin, relied on the PoW consensus algorithm. PoW requires participants (miners) to solve complex mathematical puzzles to validate transactions and add new blocks to the blockchain. This energy-intensive process was used to secure the network.

4. **Limited Smart Contract Functionality:** While Bitcoin's scripting language allowed for some basic smart contract capabilities, it was limited compared to what later generations of blockchain (Blockchain 2.0 and 3.0) would offer. Smart contracts are self-executing contracts with the terms of the agreement directly written into code.

5. **Focus on Digital Currency:** Blockchain 1.0 was primarily associated with the creation and transfer of digital currencies. Its main use case was as a decentralized digital cash system.

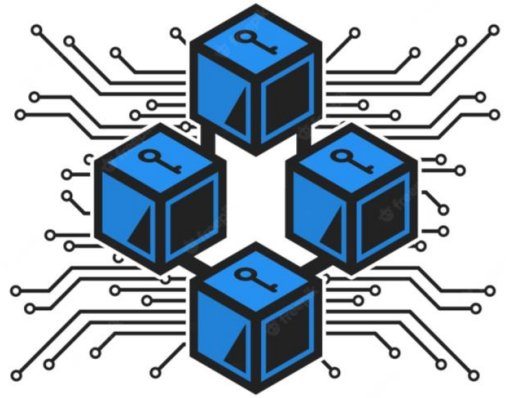
6. **Public and Permissionless:** Most Blockchain 1.0 networks were public and permissionless, meaning that anyone could participate in the network, view the blockchain's ledger, and mine or transact with the cryptocurrency.

7. **Scalability Challenges:** Blockchain 1.0 networks, especially Bitcoin, faced scalability challenges in terms of transaction processing speed and cost.

Blockchain 1.0 set the stage for further developments in the blockchain space, including the emergence of more advanced blockchain platforms and the expansion of use cases beyond digital currency. These subsequent generations of blockchain, often referred to as Blockchain 2.0 and Blockchain 3.0, introduced features like smart contracts, decentralized applications (DApps), and interoperability between different blockchains.

Blockchain 2.0

Blockchain 2.0



- Blockchain 2.0 is also used for **Smart Contracts**.
- The new Version of Blockchain came because there was a problem in version 1.0 which was Mining of Bitcoin was Wasteful and there was also a lack of Scalability of the Network in it. So the problem is improved in Version 2.0.
- In this version, the Blockchain is not just limited to Cryptocurrencies but it will extend up to Smart Contracts.
- Thus, Small Contracts are Small computers which live in the Chains of Blocks.
- These Small computers are free computer programs that execute automatically, and check the conditions defined earlier like facilitation, verification or enforcement and reduce transaction cost efficiency.

- In Blockchain 2.0, Bitcoin is replaced with Ethereum. Thus, Blockchain 2.0 was successfully processing a high number of Transactions on Public networks rapidly.

Key Aspects Of Blockchain 2.0

1. **Smart Contracts:** One of the defining features of Blockchain 2.0 is the introduction of smart contracts. Smart contracts are self-executing contracts with the terms of the agreement directly encoded in code. They allow for the automation of complex processes and transactions without the need for intermediaries. Ethereum, launched in 2015 by Vitalik Buterin, is the most notable example of a Blockchain 2.0 platform that popularized smart contracts.

2. **Decentralized Applications (DApps):** Blockchain 2.0 platforms enable the development of DApps. These are applications that run on blockchain networks, utilizing smart contracts to execute various functions. DApps can be built for a wide range of use cases, from finance and supply chain management to gaming and social networking.

3. **Ethereum:** Ethereum is the most prominent Blockchain 2.0 platform. It introduced the concept of a "world computer" where developers could build and deploy decentralized applications using smart contracts. Ethereum's native cryptocurrency, Ether (ETH), is used to pay for transaction fees and computational services on the network.

4. **Tokens and Token Standards:** Blockchain 2.0 saw the emergence of various token standards, such as the Ethereum-based ERC-20 standard. These standards enable the creation of fungible and non-fungible tokens (NFTs), which have found applications in areas like tokenized assets, collectables, and gaming.

5. **Interoperability:** Some Blockchain 2.0 projects aimed to address interoperability challenges by allowing different blockchains to communicate and share data. This was an important step toward creating a more connected and versatile blockchain ecosystem.

6. **Scalability Solutions:** To address scalability issues that became apparent in Blockchain 1.0 (e.g., slow transaction processing and high fees), Blockchain 2.0 platforms began exploring solutions like sharding and Layer 2 scaling solutions.

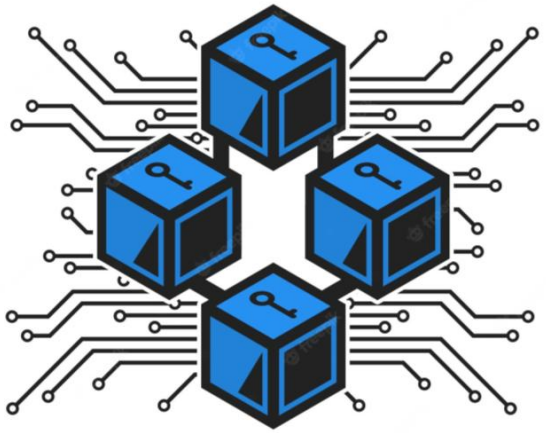
7. **ICO Boom:** Blockchain 2.0 was marked by the Initial Coin Offering (ICO) boom, where startups and projects raised funds by issuing their own tokens on platforms like Ethereum. While ICOs offered a new way to raise capital, they also faced regulatory scrutiny due to potential fraud and lack of investor protection.

8. **Use Cases Beyond Currency:** With the introduction of smart contracts and DApps, Blockchain 2.0 expanded use cases beyond digital currency. It became a platform for building decentralized applications for various industries, including finance, healthcare, supply chain, and more.

Blockchain 2.0 represented a significant step forward in the blockchain space, enabling greater flexibility and versatility in the development of decentralized applications and smart contracts. It laid the foundation for further innovations in Blockchain 3.0 and beyond.

Blockchain 3.0

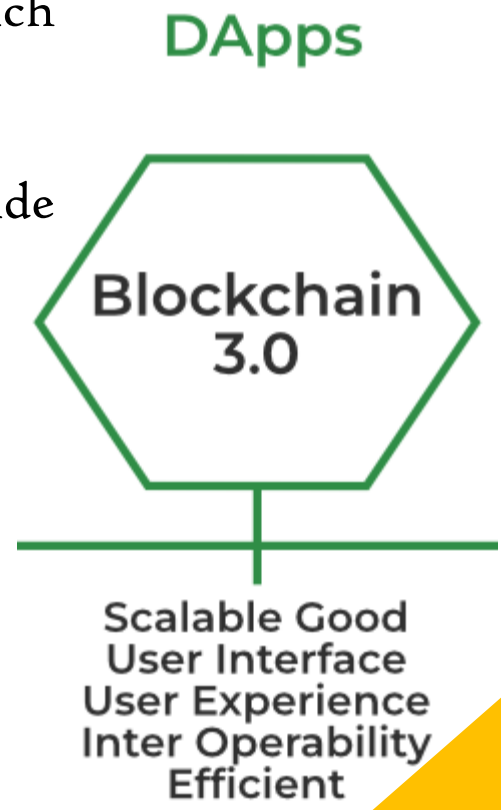
Blockchain 3.0



- Blockchain 2.0 is also used for **Smart Contracts.**
- After Version 2.0, a new version was introduced which includes DApps which is known as Decentralized Apps.
- A DApp is like a conventional app, it can have frontend written in any language that makes calls to its backend, and its backend code is running on a decentralized Peer-To-Peer Network.
- It makes use of decentralized storage and communication which can be Ethereum Swarm etc. DApps is decentralised, i.e. no single owner/authority that ensures transparency, improved security, data accessible to all, no censorship and flexible development.
- DApps bring many benefits such as zero downtime, ensuring privacy, data integrity and trustless yet secure communication (business, transaction, etc.).
- There are many decentralized Applications like BitMessage, BitTorrent, Tor, Popcorn, etc.

Advantages :

- Transaction takes place without requiring and Third Party Intermediary which ensures the security of Details and Data.
- Blockchain uses Cryptography in order to make sure the information is locked inside the Blockchain.
- Blockchain removes Double records which accelerates Transactions.



Disadvantages :

- There is always the risk of Error as long as the human factor is evolved.
- The transaction cost of Bitcoin is quite High.
- Blockchain technology is immutable which means we cannot make any changes when data or information is inserted.

Key Aspects Of Blockchain 3.0

1. **Scalability Solutions:** Blockchain 3.0 platforms aim to overcome the scalability challenges faced by earlier generations. They implement various techniques such as sharding, sidechains, and consensus algorithms like Proof of Stake (PoS) or Delegated Proof of Stake (DPoS) to achieve higher transaction throughput and lower latency.

2. **Interoperability:** Blockchain 3.0 emphasizes interoperability between different blockchain networks. It aims to create a more connected and seamless blockchain ecosystem where data and assets can flow between different blockchains without friction. Cross-chain communication protocols and standards are developed to enable this interoperability.

3. **Security Enhancements:** To improve security, Blockchain 3.0 platforms often implement advanced consensus algorithms, robust encryption methods, and formal verification techniques for smart contracts. Security breaches and vulnerabilities are addressed more comprehensively.

4. **Sustainability and Energy Efficiency:** Concerns about the energy consumption of blockchain networks, particularly those using Proof of Work (PoW) consensus, have led Blockchain 3.0 projects to adopt more eco-friendly consensus mechanisms like Proof of Stake (PoS) or variations of PoS. These mechanisms require significantly less energy for transaction validation.

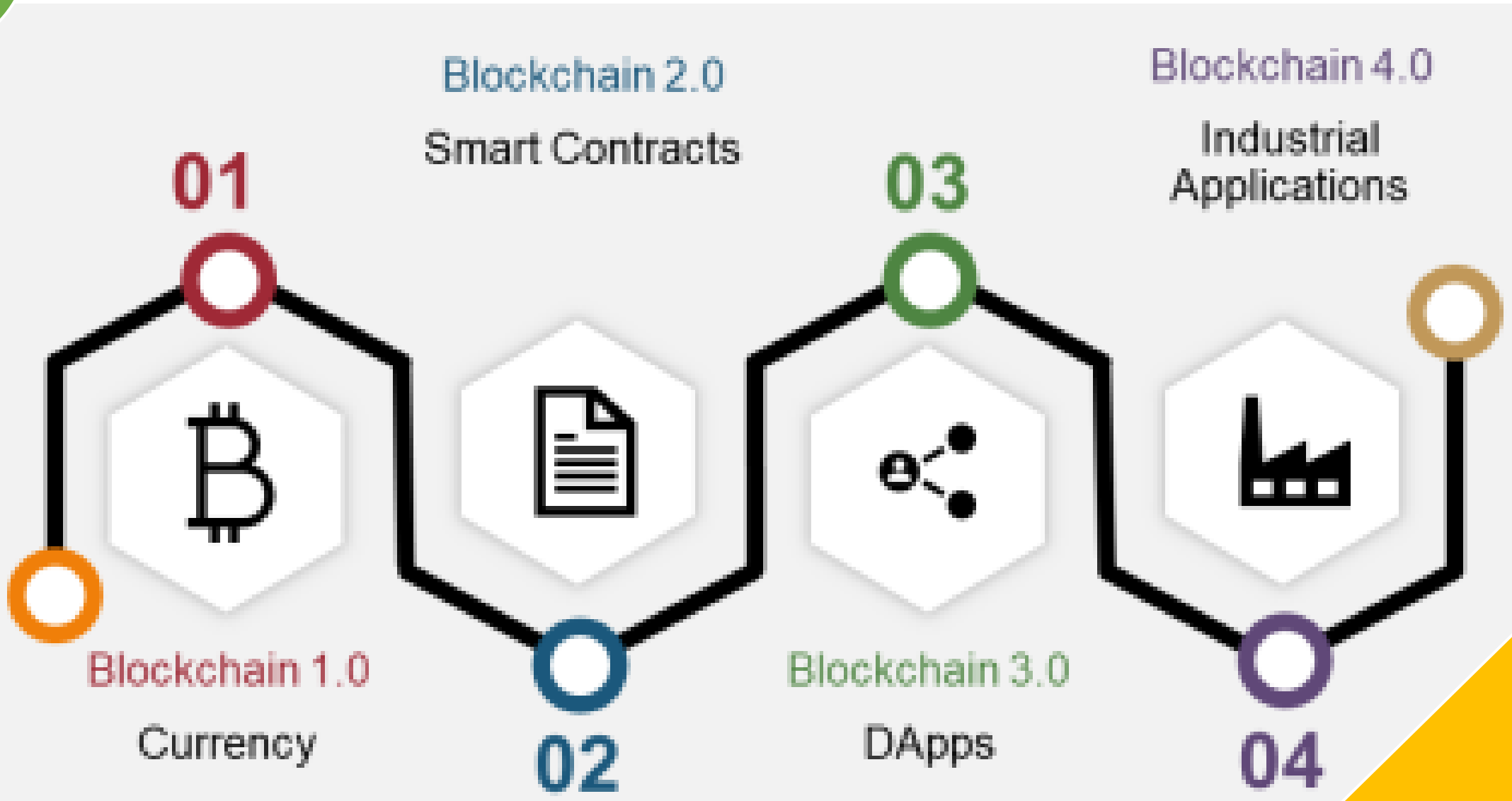
5. **Privacy Features:** Blockchain 3.0 platforms often incorporate enhanced privacy features, such as zero-knowledge proofs, ring signatures, and confidential transactions. These technologies allow users to conduct private transactions and share data selectively, while still maintaining the transparency of the blockchain.

6. **Enterprise Adoption:** Blockchain 3.0 platforms aim to be more attractive to enterprises by providing enterprise-grade features like permissioned networks, customizable governance models, and tools for regulatory compliance. They seek to address the specific needs of businesses looking to leverage blockchain technology.

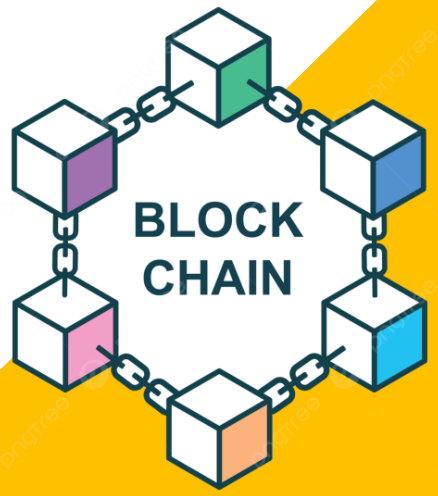
7. **Tokenization of Real Assets:** Blockchain 3.0 facilitates the tokenization of real-world assets, such as real estate, stocks, and commodities. This allows for easier and more efficient trading and ownership of physical assets through digital tokens on the blockchain.

8. **DeFi (Decentralized Finance) and NFTs (Non-Fungible Tokens):** Blockchain 3.0 has seen the explosive growth of DeFi, where financial services like lending, borrowing, and trading are decentralized and accessible to anyone. Additionally, NFTs, which gained prominence in Blockchain 2.0, continued to flourish in this generation, with more diverse use cases beyond digital art and collectables.

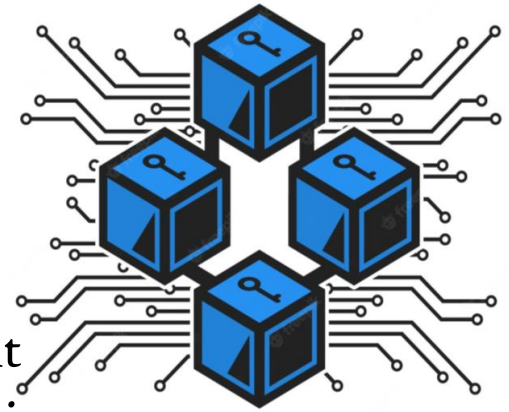
Examples of Blockchain 3.0 projects and platforms include Polkadot, Cardano, Solana, and Avalanche, among others. These platforms aim to provide a more scalable, secure, and interconnected blockchain ecosystem that can support a wide range of applications and use cases beyond digital currencies.


Blockchain 2.0
Smart Contracts
Blockchain 4.0
Industrial Applications
01
03
Blockchain 1.0
Currency
02
Blockchain 3.0
DApps
04

Types Of Blockchain



Types Of Blockchain



- The basic application of the blockchain is to perform transactions in a secure network. That's why people use blockchain and ledger technology in different scenarios. One can set up multichain to prevent unauthorized access to sensitive data.

- It is not available to the public, and can only be available to authorized entities in the organization.

- It depends on the organization which type it requires to choose for their work.

- By using blockchain we can track orders and payments from end to end.

Advantages of using blockchain :

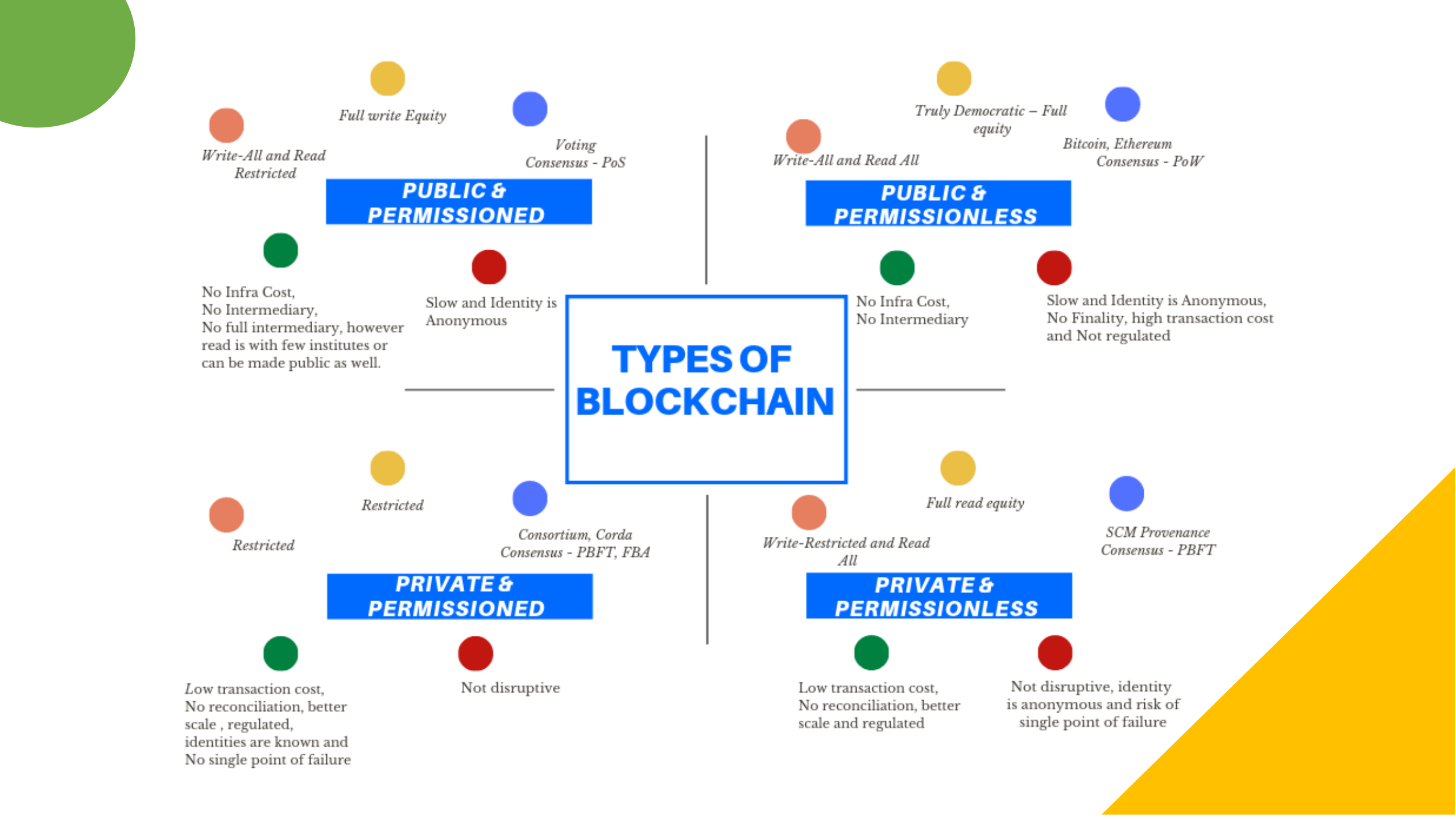
- It provides greater trust among users.
- It provides greater security among data.
- Reduce the cost of production.
- Improve Speed.
- Invocation and tokenization.
- It provides immutable records.
- Smart contracts

Disadvantages of using blockchain :

- Data modification is not possible.
- It requires large storage for a large database.
- The owner cannot access the private key again if they forget or lose it.

Real-Life Application Of Blockchain

1. In a secure and full-proof voting management system.
2. To supply chain management.
3. In healthcare management.
4. Real estate projects.
5. NFT marketplace.
6. Avoid copyright and original content creation.
7. In the personal identity system
8. To make an immutable data backup.
9. Internet of Things


TYPES OF BLOCKCHAIN
PUBLIC & PERMISSIONED
Full write Equity
Write-All and Read Restricted
Voting Consensus - PoS
No Infra Cost, No Intermediary, No full intermediary, however read is with few institutes or can be made public as well.
Slow and Identity is Anonymous
PUBLIC & PERMISSIONLESS
Truly Democratic – Full equity
Write-All and Read All
Bitcoin, Ethereum Consensus - PoW
No Infra Cost, No Intermediary
Slow and Identity is Anonymous, No Finality, high transaction cost and Not regulated
PRIVATE & PERMISSIONED
Restricted
Restricted
Consortium, Corda Consensus - PBFT, FBA
Low transaction cost, No reconciliation, better scale , regulated, identities are known and No single point of failure
Not disruptive
PRIVATE & PERMISSIONLESS
Full read equity
Write-Restricted and Read All
SCM Provenance Consensus - PBFT
Low transaction cost, No reconciliation, better scale and regulated
Not disruptive, identity is anonymous and risk of single point of failure

Permissionless Blockchain

It is also known as trustless or public blockchains, which are available to everyone to participate in the blockchain process that is used to validate transactions and data.

These are used in the network where high transparency is required.

Characteristics:

- Permissionless blockchain has no central authority.
- The platform is completely open-source.
- Full transparency of the transaction.
- Heavy use of tokens.

Advantages:

- Everyone can participate only requirement is good hardware and internet.
- Bring trust among users or entities.
- It has a high level of transparency as it's a larger network.
- Broader decentralization of access to more participants.

Disadvantages:

- Poor energy efficiency due to large network.
- Lower performance scalability.
- Less privacy as many of the things are visible.

Permissioned Blockchain

These are the closed networks only a set of groups are allowed to validate transactions or data in a given blockchain network.

These are used in the network where high privacy and security are required.

Characteristics:

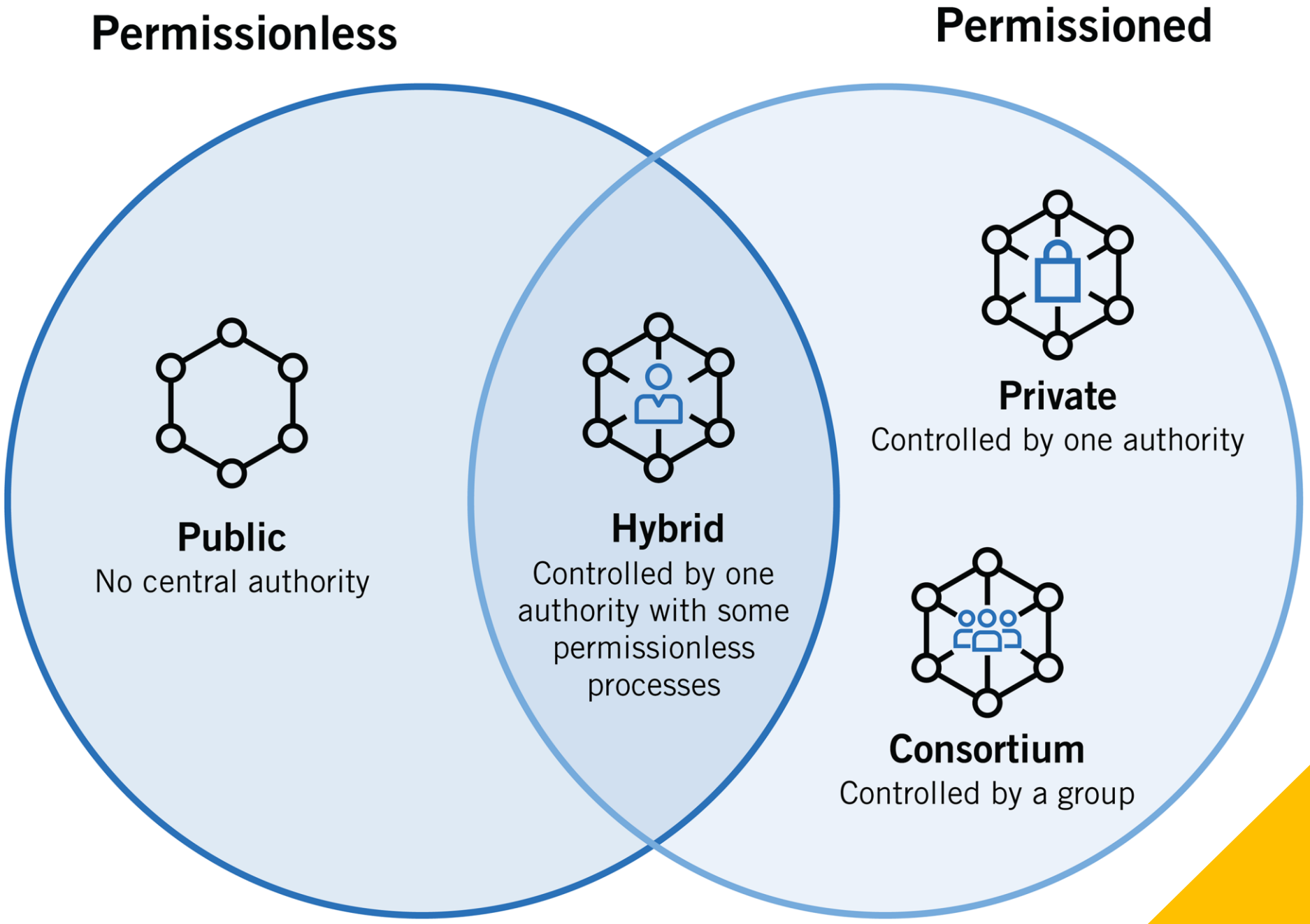
- A major feature is transparency based on the objective of the organization.
- Another feature is the lack of anatomy as only a limited number of users are allowed.
- It does not have a central authority.
- Developed by private authority.

Advantages:

- This blockchain tends to be faster as it has some nodes for validations.
- They can offer customizability.
- Strong Privacy as permission is needed for accessing transaction information.
- As few nodes are involved performance and scalability are increased.

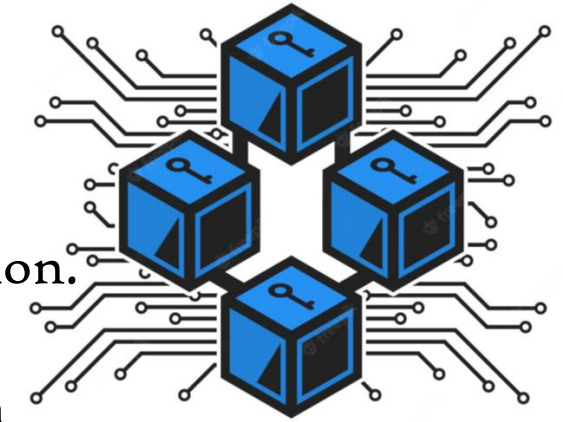
Disadvantages:

- Not truly decentralized as it requires permission
- Risk of corruption as only a few participants are involved.
- Anytime owner and operator can change the rules as per their need.


Permissionless
Permissioned
Public
No central authority
Hybrid
Controlled by one authority with some permissionless processes
Private
Controlled by one authority
Consortium
Controlled by a group

Public Blockchain

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 internet and a computer with good hardware can participate in this public blockchain.
- All the computer in the network hold the copy of other nodes or block present in the network
- In this public blockchain, we can also perform verification of transactions or records.

Advantages:

- **Trustable:** There are algorithms to detect no fraud. Participants need not worry about the other nodes in the network
- **Secure:** This blockchain is large in size 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 in order 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 high 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.highly

Use Cases:

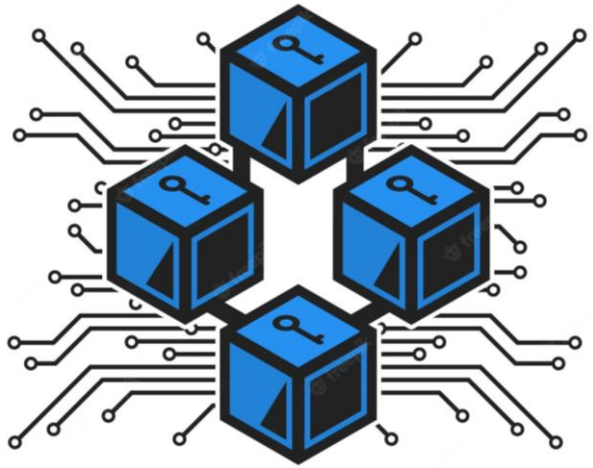
Public Blockchain is secured with proof of work or proof of stake they can be used to displace traditional financial systems.

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.

Private Blockchain

Private Blockchain



These blockchains are not as decentralized as the public blockchains 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 user has 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.

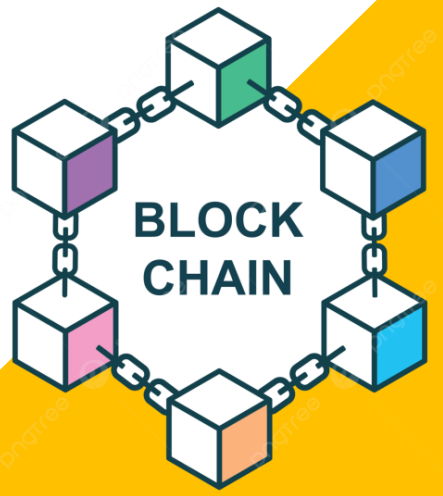
Use Cases:

With proper security and maintenance, this blockchain is a great asset to secure information without exposing it to the public eye.

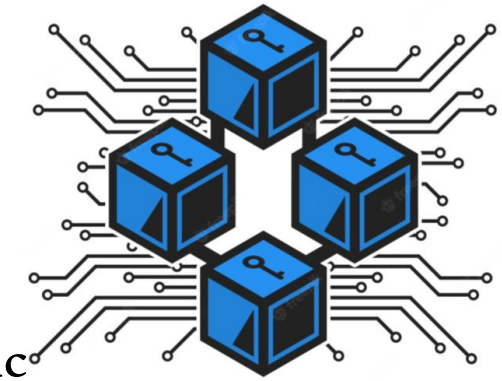
Therefore companies use them for internal auditing, voting, and asset management.

An example of private blockchains is Hyperledger, Corda.

Hybrid Blockchain



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 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 Cases:

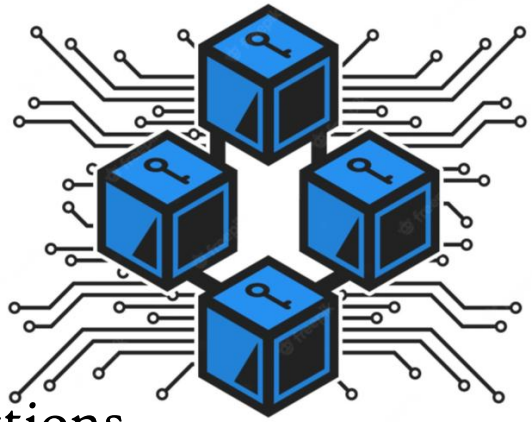
It provides a greater solution to the healthcare industry, government, real estate, and financial companies.

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.

Consortium Blockchain

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 part is public and some part is 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 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.

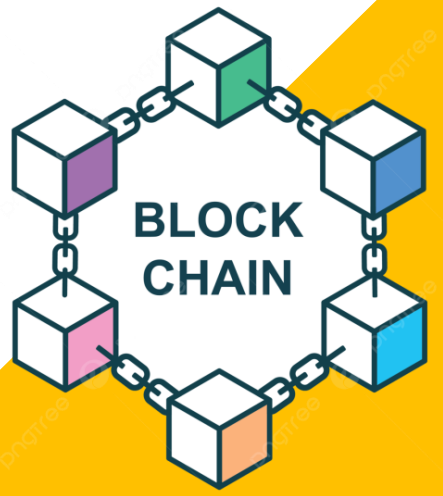
Use Cases:

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.

Sidechains

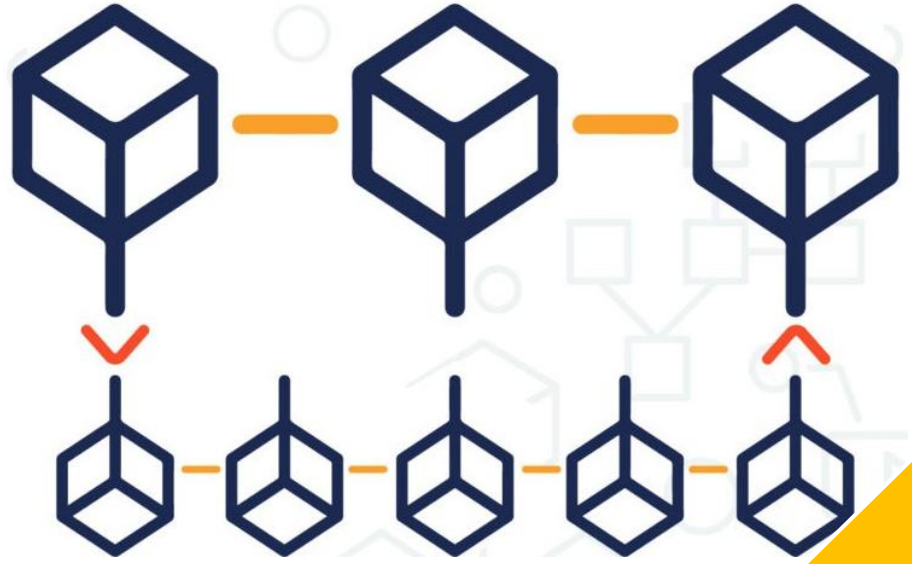


Sidechains

- Sidechains are separate blockchains that are attached to a parent blockchain using an asymmetric two-way peg.

- Sidechains are a concept in blockchain technology that refers to separate and parallel blockchains connected to a main blockchain, often referred to as the "mainchain" or "parent chain."

- These sidechains are designed to work alongside the mainchain, enabling the transfer of assets, data, or value between them in a secure and interoperable manner.



Key Characteristics & Concept Related To Sidechains

1. Purpose and Functionality:

Parallel Chains: Sidechains are separate blockchains that run alongside the main chain (often referred to as the "parent chain"). These side chains can be thought of as parallel chains with their own set of rules and functionalities.

2. Interoperability:

Two-Way Peg: One of the key features of sidechains is the ability to transfer assets or data between the mainchain and the sidechain through a two-way peg mechanism.

Locking and Unlocking: Users can lock a certain amount of cryptocurrency or assets on the mainchain, which will then generate an equivalent amount of tokens on the sidechain. Conversely, users can unlock these tokens on the sidechain, which will then release the equivalent assets on the mainchain.

3. Customization:

Tailored Functionality: Sidechains can be customized to serve specific purposes or use cases. For example, a sidechain might be designed for faster transaction processing, confidential transactions, or to support unique smart contract features.

Consensus Mechanisms: Sidechains can employ different consensus mechanisms than the mainchain. For instance, a sidechain might use a Proof of Stake (PoS) consensus while the mainchain uses Proof of Work (PoW).

4. Scalability:

Scalability Relief: Sidechains can help alleviate scalability challenges that might be faced by the main chain. By offloading some transactions or computations to sidechains, the mainchain can focus on its core functions.

5. Security:

Security Measures: Maintaining security when assets move between the mainchain and sidechain is paramount. Various security measures like cryptographic proofs and decentralized validators are employed to ensure the integrity and safety of assets during transfers.

Decentralization: Sidechains aim to maintain decentralization similar to the mainchain, ensuring that a single entity or group does not have excessive control.

6. Use Cases:

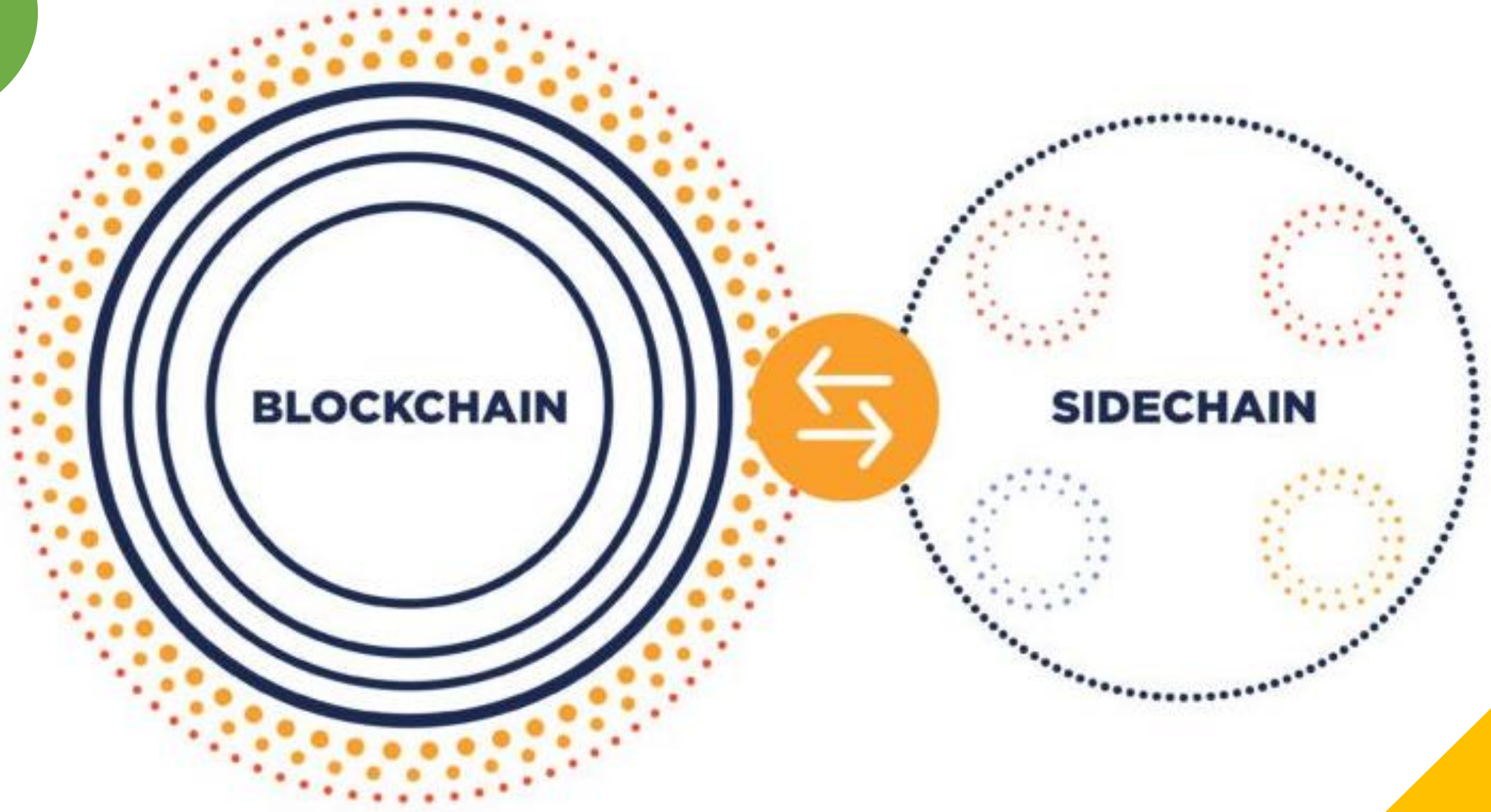
Asset Tokenization: Sidechains are used for asset tokenization, where real-world assets like real estate, stocks, or commodities are represented as blockchain tokens on a sidechain. This facilitates easier trading and transfer of these assets.

Privacy and Anonymity: Some sidechains focus on enhancing privacy and anonymity features, making them suitable for confidential transactions and data.

Experimentation: Blockchain projects often use sidechains as sandboxes for experimenting with new consensus mechanisms or smart contract functionality without risking the stability of the main chain.

Specific Applications: Sidechains can cater to specific applications such as gaming, supply chain management, and identity verification by tailoring their functionalities to the unique requirements of these use cases.

Sidechains are a fundamental concept in blockchain technology that allows for the creation of specialized, parallel chains connected to a main blockchain. They offer flexibility, scalability, and interoperability while maintaining a focus on security and decentralization. Sidechains play a vital role in expanding the capabilities and use cases of blockchain networks.



2-way Peg Between Parent Blockchain And Sidechains

Assignment

Unit Assignment

1. Explain the tiers of blockchain technology in detail.
2. What is the difference between Blockchain 1.0, Blockchain 2.0 and Blockchain 3.0 with examples and diagrams of each?
3. What are the types of blockchain?
4. Write the difference between public blockchain, private blockchain, hybrid and consortium blockchain with examples.
5. What do you understand by the terms Sidechains?

thank you

Any Queries