UNIT 5

Ethereum

Ethereum is a decentralised blockchain platform that establishes a peer-to-peer network that securely executes and verifies application code, called smart contracts. Smart contracts allow participants to transact with each other without a trusted central authority. Transaction records are immutable, verifiable, and securely distributed across the network, giving participants full ownership and visibility into transaction data. Transactions are sent from and received by user-created Ethereum accounts. A sender must sign transactions and spend Ether, Ethereum's native cryptocurrency, as a cost of processing transactions on the network.

Benefits of building on Ethereum

Ethereum offers an extremely flexible platform on which to build decentralised applications using the native Solidity scripting language and Ethereum Virtual Machine. Ethereum's large user base encourages developers to deploy their applications on the network, which further reinforces Ethereum as the primary home for decentralised applications like DeFi and NFTs. In the future, the backwards-compatible Ethereum 2.0 protocol, currently under development, will provide a more scalable network on which to build decentralised applications that require higher transaction throughput.

IOTA

IOTA is an open-source, decentralised blockchain technology that was designed to enable secure and efficient data transfer and management for the Internet of Things (IoT) ecosystem. Unlike traditional blockchain technologies, which use a linear chain of blocks to record transactions, IOTA uses a directed acyclic graph (DAG) called the Tangle to record and verify transactions.

How does the IOTA Blockchain Work?

IOTA uses a unique data structure called the Tangle, which is a Directed Acyclic Graph (DAG) that enables feeless transactions and near-instant confirmation times. The Tangle operates differently from traditional blockchain technologies, which rely on miners to validate transactions and create new blocks.

In the IOTA Tangle, each transaction must confirm two previous transactions before it can be confirmed itself. Because there are no miners in the IOTA Tangle, there are no transaction fees associated with sending transactions.

One potential downside of the IOTA Tangle is that it can be more susceptible to certain types of attacks, such as the double-spending attack.

To mitigate this risk, IOTA uses a consensus mechanism called the Markov Chain Monte Carlo (MCMC) algorithm, which helps to prevent double-spending by ensuring that each transaction is validated by the network before it can be confirmed.

Overall, the IOTA Tangle operates differently from traditional blockchain technologies and offers several unique features and advantages for IoT applications.

Transactions on IOTA Blockchain

Transactions on the IOTA Tangle, which is the distributed ledger technology used by IOTA, work differently than transactions on traditional blockchain networks. Here is an overview of how transactions work on the IOTA Tangle:

Creating a transaction: To create a transaction on the IOTA Tangle, a user must generate a new transaction bundle containing information about the transaction, such as the sender’s address, the recipient’s address, and the amount of IOTA being sent.

Confirming transactions: Before a new transaction can be confirmed on the IOTA Tangle, it must confirm two previous transactions. This confirmation process adds to the security and scalability of the network, as more users participate and confirm transactions.

No fees: One of the unique features of the IOTA Tangle is that there are no fees associated with sending transactions. This makes it well-suited for microtransactions in IoT applications, where small amounts of data or value are exchanged between devices.

Consensus mechanism: To prevent double-spending attacks, the IOTA Tangle uses a consensus mechanism called the Markov Chain Monte Carlo (MCMC) algorithm. This algorithm ensures that each transaction is validated by the network before it can be confirmed.

Transaction history: Because the IOTA Tangle operates as a distributed ledger, each transaction is recorded on the network and forms a part of the transaction history. This history can be audited and verified by any user on the network, adding to the transparency and immutability of the system.

Features of IOTA Blockchain

The IOTA blockchain, or Tangle, offers several unique features and advantages for users and developers. Here are some of the key features of IOTA:

Feeless transactions: Unlike traditional blockchain networks, IOTA does not charge transaction fees. This makes it well-suited for microtransactions in IoT applications, where small amounts of data or value are exchanged between devices.

Scalability: The IOTA Tangle is designed to be highly scalable, with confirmation times that decrease as more users participate in the network. This makes it well-suited for applications that require high throughput and low latency.

Decentralisation: IOTA is designed to be a decentralised network, with no central authority controlling the system. This means that users can transact and interact with each other directly, without the need for intermediaries.

Security: The IOTA Tangle uses a consensus mechanism called the Markov Chain Monte Carlo (MCMC) algorithm to prevent double-spending attacks and ensure the security of the network.

Quantum-resistant: IOTA uses a cryptographic algorithm called Winternitz One-Time Signature Scheme (WOTS+) that is quantum-resistant. This means that the network is more secure against attacks from quantum computers, which are expected to become more prevalent in the future.

Green technology: Because IOTA does not rely on mining to validate transactions, it is more energy-efficient than traditional blockchain networks. This makes it a more environmentally friendly alternative for distributed ledger technology.

Flexibility: The IOTA Tangle is designed to be a flexible platform that can support a wide range of applications and use cases, from micropayments to supply chain management.

Use Case of IOTA

The IOTA blockchain, with its unique architecture and features, has several potential use cases across a wide range of industries. Here are some examples of the potential use cases for IOTA:

1. Internet of Things (IoT)

IOTA was originally designed to serve as a secure and efficient platform for the growing ecosystem of connected devices in the IoT space. The Tangle's feeless transactions and scalability make it well-suited for microtransactions between IoT devices, such as for data transfer, device-to-device payments, and supply chain management.

2. Mobility

IOTA has also been explored as a potential platform for decentralised mobility applications, such as autonomous vehicles and ride-sharing services. The Tangle's scalability and real-time data transfer capabilities could help enable secure and efficient micro-payments between vehicles and other devices in a mobility network.

3. Energy

IOTA has been explored as a potential platform for energy trading and management. The Tangle's feeless transactions and scalability make it well-suited for micro-payments between energy producers and consumers, as well as for managing data exchange between smart grids and IoT devices.

4. Supply Chain

The IOTA Tangle's data transfer and security features make it well-suited for supply chain management applications. The ability to record and verify transactions in real time can help improve transparency and efficiency in supply chain networks.

5. Healthcare

IOTA has also been explored as a potential platform for secure and efficient data exchange in healthcare applications. The Tangle's security and data transfer capabilities could help enable the secure and efficient sharing of medical data between providers and patients.

Benefits of IOTA

The IOTA blockchain offers several potential benefits to users and businesses, including:

Scalability: The IOTA Tangle architecture is designed to be highly scalable, with the potential to handle large volumes of transactions without slowing down the network. This scalability makes it well-suited for applications such as the Internet of Things (IoT), where large numbers of devices are constantly sending and receiving data.

Feeless transactions: IOTA uses a feeless transaction model, which means that there are no fees associated with sending MIOTA tokens on the network. This makes it well-suited for micropayments and high-volume data transfer applications.

Security: The IOTA Tangle uses a unique consensus mechanism called "Coordinator," which helps ensure the security of the network by preventing double-spending attacks and other types of malicious activity.

Data integrity: The IOTA Tangle can be utilized to securely and impenetrably record and validate data. This makes it ideal for applications like supply chain management, where it's crucial to monitor the flow of items and guarantee data integrity.

Decentralisation: Because the IOTA blockchain is decentralised, no single entity is in charge of running the network. As there is no single point of failure, this helps to assure the network's resilience and endurance.

Interoperability: The IOTA blockchain is made to work with other networks and blockchains, which could make it easier to integrate various technologies.

The real need for mining

1. Validating Transactions

Bitcoin transactions take place in huge figures every day. Cryptocurrencies function without a central administrator and the insecurity can be substantial with the transactions that transpire. So, what is the authentication method with such cryptocurrencies? With each transaction, new blocks are added to the blockchain in the network and the validation lies in the mining results from the blockchain miners.

2. Confirming Transactions

Miners work the blockchain mining process to confirm whether the transaction is authentic or not. All confirmed transactions are then included in the blockchain.

3. Securing Network

To secure the transaction network, bitcoin miners work together. With more users mining the blockchain, blockchain network security increases. Network security ensures that there are no fraudulent activities happening with cryptocurrencies.

CONSENSUS

Consensus plays a key role in building trust among crypto coin traders worldwide. Due to the decentralised nature of the crypto world, it is essential to have complete transparency while trading a particular coin. This minimises the chances of a buyer becoming a victim of fraud.

If you are a beginner in crypto trading, you must know the vital details about consensus regarding blockchain.

So keep scrolling to know everything about consensus in the blockchain.

What Is The Meaning Of Consensus?

Generally, consensus means that the majority of a group has agreed in favour of a decision. When it comes to blockchain, reaching a consensus is important. At least 51% of the traders and miners associated with a particular coin must agree to finalise the next global status of the coin.

What Is A Consensus Mechanism?

In the blockchain, a consensus mechanism is a system that validates a transaction and marks it as authentic. This mechanism lists all valid transactions of a coin in a blockchain to build trust in the coin among traders. Several currencies, such as Bitcoin, Ethereum etc., use this system for security purposes.

How Does The Consensus Mechanism Work?

It achieves the agreement of most users on a single network. The consensus mechanism maintains the security of the blockchain by keeping a record of all legitimate transactions. Since crypto trading is a decentralised process, this becomes important to stop sellers from deliberately cheating a buyer.

To build trust for a blockchain, the consensus mechanism ensures that a transaction is reflected in the blockchain as soon as it gets validated. There are a variety of methodologies that are essential to ensure security and trust and achieve agreement across a blockchain network. Consensus mechanisms also ensure that all the transactions for a coin are rightly listed in the blockchain.

What Are The Types Of Consensus Mechanisms?

Several mechanisms are used as a consensus mechanism during coin trading. These mechanisms are as follows:

Proof of Work

'Proof' refers to the solution of a highly-complex problem, and 'work' refers to the process of solving the same. Crypto coin miners compete to solve the problem and gain the right to process the transaction. The fastest solver receives a mining fee from the traders of these coins.

This mechanism tracks and verifies the creation and transactions across blockchain networks. It enables miners by allowing them to validate new transactions and is extremely secure. However, it has several cons, such as high electricity requirements and difficulty for individual miners.

Proof of Stake

This mechanism randomly chooses a maximum coin owner to validate a transaction. It also allows the owner to create a block for the same coin. This mechanism requires comparatively less energy, transaction time and a lower fee. Coins like Etherium 2.0, Polkadot, Cosmos, Cardano, ThorChain, Nxt and Algorand use this mechanism extensively. There is a security risk as if an owner owns 51% or more coins of a particular coin, then that person will get sole ownership of its network.

Proof of Capacity

The PoC mechanism heavily relies on free space available in the hard drive. This is because there are many solutions to a coin's hash problem that a trader needs to store. It is highly efficient as compared to PoW and PoC mechanisms. Coins such as Burst, Storj, SpaceMint and Chia use these mechanisms.

Proof of Activity

This mechanism is a combination of both Proof of Work and Proof of Stake. It has been designed to combine the best features of PoW and PoS. In the beginning, the Proof-of-Activity mechanism functions like PoW. Once a new block is completed, it starts to function like a Proof-Of-Stake mechanism. Coins such as DCR (Decred) use this mechanism.

Proof of Authority

Different organisations and private companies created this unique mechanism. There are validators with approved accounts which authorise transactions and the creation of new blocks. These validators must disclose their true identity to get the right to validate a transaction.

Proof of Burn

PoB aims to improve the quality of blockchain so that it can be used easily and extensively as a tool for faster and more secured transactions. After PoW and PoS, PoB is designed to prevent fraud activities on a blockchain network. Cryptocurrencies such as Bitcoin use this mechanism to offer secure transactions to traders.

Proof of Elapsed Time

Intel Corporation created this mechanism to permit blockchain to decide the person who will create the next block. It uses a lottery system to decide the next block creator. Thus, it gives a fair chance to all traders to create the next block. It is an efficient process involving utilising lesser resources and low energy consumption.

What are the advantages of the consensus mechanism?

Consensus mechanisms offer several advantages, such as:

- No barriers to participation
- Any crypto trader or miner across the globe can participate in a consensus mechanism. There are few barriers to participation in a consensus for any crypto coin.
- Builds trust among users
- Traders and miners of a particular coin across the globe must agree to approve a decision. This, in turn, builds trust among the users.
- Establishes security
- Consensus mechanisms maintain the transparency of trading for all coins. Thus, traders can ensure that no fraud occurs during a transaction.

What are the disadvantages of the consensus mechanism?

The minor disadvantages of a consensus mechanism include:

- Severe chances of hacking
- There lies a chance of hacking known as 51% hack, which stands out as a potential attack on a consensus mechanism.
- Excessive use of electricity
- There is a heavy requirement for electricity for the PoW mechanism to function.

With very few associated disadvantages, the consensus mechanism is a great security tool for a decentralised form of trade. This allows traders and miners across the globe to establish a connection and trust among themselves and benefit from the mechanism.

The benefits in the case of traders are trade security and faster transactions. On the other hand, miners get several rewards for solving complex problems faster and gaining authority to validate a trade.

What is the Byzantine General’s Problem?

In 1982, The Byzantine General’s Problem was invented by Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine Generals Problem is an impossibility result which means that the solution to this problem has not been found yet as well as helps us to understand the importance of blockchain. It is basically a game theory problem that provides a description of the extent to which decentralised parties experience difficulties in reaching consensus without any trusted central parties.

The Byzantine army is divided into many battalions in this classic problem called the Byzantine General’s problem, with each division led by a general.

The generals connect via messenger in order to agree to a joint plan of action in which all battalions coordinate and attack from all sides in order to achieve success.

It is probable that traitors will try to sabotage their plan by intercepting or changing the messages.

As a result, the purpose of this challenge is for all of the faithful commanders to reach an agreement without the imposters tampering with their plans.

How Bitcoin Solves the Byzantine General’s Problem?

In the Byzantine Generals Problem, the untampered agreement that all the loyal generals need to agree to is the blockchain. Blockchain is a public, distributed ledger that contains the records of all transactions. If all users of the Bitcoin network, known as nodes, could agree on which transactions occurred and in what order, they could verify the ownership and create a functioning, trustless money system without the need for a centralised authority. Due to its decentralised nature, blockchain relies heavily on a consensus technique to validate transactions. It is a peer-to-peer network that offers its users transparency as well as trust. Its distributed ledger is what sets it apart from other systems. Blockchain technology can be applied to any system that requires proper verification.

Proof Of Work: The network would have to be provable, counterfeit-resistant, and trust-free in order to solve the Byzantine General's Problem. Bitcoin overcame the Byzantine General's Problem by employing a Proof-of-Work technique to create a clear, objective regulation for the blockchain. Proof of work (PoW) is a method of adding fresh blocks of transactions to the blockchain of a cryptocurrency. In this scenario, the task consists of creating a hash (a long string of characters) that matches the desired hash for the current block.

Counterfeit Resistant: Proof-of-Work requires network participants to present proof of their work in the form of a valid hash in order for their block, i.e. piece of information, to be regarded as valid. Proof-of-Work requires miners to expend significant amounts of energy and money in order to generate blocks, encouraging them to broadcast accurate information and so protecting the network. Proof-of-Work is one of the only ways for a decentralised network to agree on a single source of truth, which is essential for a monetary system. There can be no disagreement or tampering with the information on the blockchain network because the rules are objective. The ruleset defining which transactions are valid and which are invalid, as well as the system for choosing who can mint new bitcoin, are both objectives.

Provable: Once a block is uploaded to the blockchain, it is incredibly difficult to erase, rendering Bitcoin's history immutable. As a result, participants of the blockchain network may always agree on the state of the blockchain and all transactions inside it. Each node independently verifies whether blocks satisfy the Proof-of-Work criterion and whether transactions satisfy additional requirements.

Trust-free: If any network member attempts to broadcast misleading information, all network nodes immediately detect it as objectively invalid and ignore it. Because each node on the Bitcoin network can verify every information on the network, there is no need to trust other network members, making Bitcoin a trustless system.

Byzantine Fault Tolerance (BFT)

The Byzantine Fault Tolerance was developed as inspiration in order to address the Byzantine General's Problem. The Byzantine General's Problem, a logical thought experiment where multiple generals must attack a city, is where the idea for BFT originated.

Byzantine Fault Tolerance is one of the core characteristics of developing trustworthy blockchain rules or features is tolerance.

When two-thirds of the network can agree or reach a consensus and the system still continues to operate properly, it is said to have BFT.

Blockchain networks' most popular consensus protocols, such as proof-of-work, proof-of-stake, and proof-of-authority, all have some BFT characteristics.

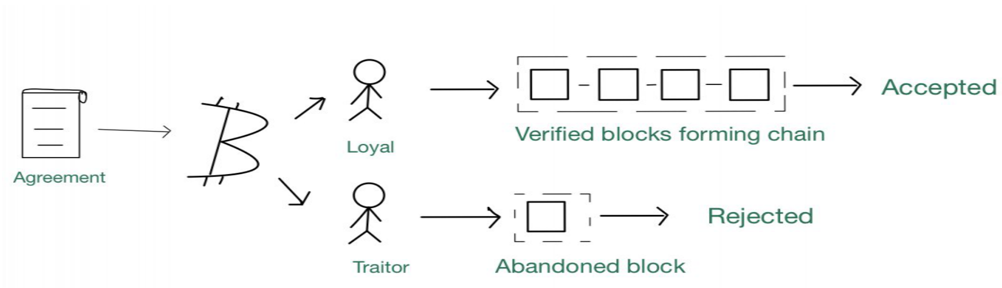
In order to create a decentralised network, the BFT is essential.

The consensus method determines the precise network structure. For instance, BFT has a leader as well as peers who can and cannot validate.

In order to maintain the sequence of the Blockchain SC transactions and the consistency of the global state through local transaction replay, consensus messages must pass between the relevant peers.

More inventive approaches to designing BFT systems will be found and put into practice as more individuals and companies investigate distributed and decentralised systems. Systems that use BFT are also employed in sectors outside of blockchains, such as nuclear power, space exploration, and aviation.

Proof Of Work in Blockchain for the Byzantine General's Problem



Byzantine General's Problem in a Distributed System

In order to address this issue, honest nodes (such as computers or other physical devices) must be able to establish an agreement in the presence of dishonest nodes.

In the Byzantine agreement issue, an arbitrary processor initialises a single value that must be agreed upon, and all non faulty processes must agree on that value. Every processor has its own beginning value in the consensus issue, and all non faulty processors must agree on a single common value.

The Byzantine army's position can be seen in computer networks.

The divisions can be viewed as computer nodes in the network, and the commanders as programs running a ledger that records transactions and events in the order that they occur. The ledgers are the same for all systems, and if any of them is changed, the other ledgers are updated as well if the changes are shown to be true, so all distributed ledgers should be in agreement.

Byzantine General's Problem Example

A basic Byzantine fault is a digital signal that is stuck at "1/2," i.e. a voltage that is anywhere between the voltages for a valid logical "0" and a valid logical "1." Because these voltages are in the region of a gate's transfer function's maximum gain, little quantities of noise on the gate's input become enormous amounts of noise on the gate's output. This is due to the fact that "digital circuits are simply analog circuitry driven to extremes."

This problem is solvable because, with a dominating input, even a Byzantine input has no output impact.

An excellent composite example is the well-known 3-input majority logic "voter."

If one of the inputs is "1/2" and the other two are both 0 or both 1, the result is 0 or 1 (due to masking within the voter).

When one of the inputs is "1/2" and the other two are different values, the output can be 0, "1/2," or 1, depending on the precise gain and threshold voltages of the voter gates and the properties of the "1/2" signal.

PRIVATE OR PERMISSIONED BLOCKCHAINS:

Permissioned blockchains - Closed networks with limited decentralisation, an additional access control layer, and designated entities.

Permissioned blockchains

Now, let’s take a closer look at permissioned blockchains. Permissioned blockchains are blockchains that are closed (i.e., not publicly accessible) or have an access control layer. This additional layer of security means that the blockchain can only be accessed by users with permissions. Permissioned users are only able to perform blockchain operations within the strict confines of roles assigned to them by the ledger administrators and require that they authenticate themselves through certificates or digital identifier methods.

Aspects of a permissioned blockchain

Decisions are authorised by a private group

Decisions are made by the owners of the network through a central, pre-defined level.

Security

Permissioned blockchains provide the operating organisation granular control over permissions, data access, and the scope of user roles.

Decentralisation isn’t fixed

Permissioned blockchains can either be fully centralised or partially decentralised. Its members typically decide on the network’s level of decentralisation and the mechanisms for consensus.

Transparency is not required

Unlike permissionless blockchains, permissioned blockchains do not need to be transparent. Transparency is optional, as most permissioned blockchain networks are specifically intended to not be transparent for security purposes. Levels of transparency usually depend on the goals of the organisation running the blockchain network.

In the meantime, the ledger maintains a record of every transaction and the identities of the participating parties.

Lack of anonymity

Access to the identity of every transactional participant can be crucial information for private entities concerned with accountability and a provable chain of custody. Every change is tracked to a specific user, so network administrators can have instantaneous access to has made a change to the system and when.

Consensus mechanisms

Because of the structure of permissioned blockchains, they don’t use the same types of consensus protocols as permissionless ones. Most commonly, organisations that deploy permissioned blockchains use one (or more) of the following three protocols: Practical Byzantine Fault Tolerance (PBFT), federated, or round-robin consensus.

PBFT – PBFT is an improved version of the original BFT protocol where all voting nodes must reach a consensus, but one or more parties are considered unreliable. In this model, a network’s safety and stability are guaranteed so long as the required minimum percentage of nodes are behaving honestly and properly.

Federated (or Federated Byzantine Consensus) - In a federated consensus, there’s a set of transaction validators trusted by each node in the blockchain that receives and sorts the transactions. Once a minimum number of these validators agree, a consensus is reached.

Round-robin - In a round-robin consensus, nodes are selected pseudo-randomly to create blocks. Once chosen, a node must pass through a cooling-off period before it can reenter the pool and be available again for consensus participation.

Advantages of permissioned blockchain

One of the most significant advantages of permissioned blockchains is the high level of privacy and security they can provide. Without a verified set of credentials and access, no user can access or alter transaction information without permission.

Another advantage is flexibility when it comes to decentralisation. It can be incremental or fully centralised, giving businesses more freedom to participate without having to worry about the risks associated with a highly centralised network.

Permissioned blockchains are also highly customizable and can accommodate configurations and integrations based on an organisation's needs. And with knowledge of every user and their actions on the network, a verifiable chain of custody can be established for every transaction.

Lastly, these types of blockchains are both scalable and highly performant due to the limited number of nodes needed to manage transaction verifications.

Disadvantages of permissioned blockchain

While lack of transparency can be a potential point of concern for permissioned blockchains, the issue is usually mitigated by the implicit trust placed in the governing authority. In a business context, consensus mechanisms and the smart contracts that moderate transactions on the network are agreed upon by the participating parties and maintained in secure, isolated containers. With this additional layer of computational security and measure of implicit trust, a properly provisioned permissioned blockchain can offset the security risk posed by bad actors.

Why permissioned blockchains are ideal for business applications

Many enterprise use cases require performance characteristics that permissionless blockchain technologies are presently unable to deliver because of limitations due to inefficiency and scalability. Additionally, in instances where permissioned blockchains are replacing existing secure, centralised networks, the identity of the participants is an essential requirement, such as in the case of financial transactions where Know-Your-Customer (KYC), Anti-Money Laundering (AML), and supply-chain provenance regulations must be followed.

In general, then, for a blockchain network to be ready for enterprise use, it should possess the following requirements:

- Participants must be identified/identifiable
- Networks need to be permissioned
- High transaction throughput performance
- Low latency of transaction confirmation
- Privacy and confidentiality of transactions and data pertaining to business transactions

- Business value

Let’s quickly review and see how permissioned blockchains stack up against these requirements. In terms of added value, permissioned blockchains:

- Increase business velocity by accelerating transactions, enabling new business models and revenue streams
- Automate multi-party business processes
- Reduce the cost and risk of using intermediaries
- Reduce the cost of fraud and regulatory compliance
- Improve data quality and timeliness by avoiding offline reconciliation and manual exception handling
- Increase auditability and trust; reduce audit costs

INTRODUCTION TO HYPER LEDGER

Hyperledger is an open-source project under the Linux Foundation where people can come and work on the platform to develop blockchain-related use cases. According to Brian behlendorf, executive director of Hyperledger

“Hyperledger is an open source community to benefit an ecosystem of hyperledger based solution providers and users focused on blockchain related use-cases that will work on a variety of industrial sectors”.

Hyperledger

Hyperledger provides the platform to create personalised blockchain services according to the need of business work. Unlike other platforms for developing blockchain-based software, Hyperledger has the advantage of creating a secured and personalised blockchain network.

- It is created to support the development of blockchain-based distributed ledgers.
- It includes a variety of enterprise-ready permissioned blockchain platforms.
- It is a global collaboration for developing high-performance and reliable blockchain and distributed ledger-based technology frameworks.

Example: Consider a situation when person X wants to buy medicine from person Y, who was a doctor living in another country.

- As a medical requirement is one person's private needs, they need to maintain the data confidentially.
- But Dr. Y is selling medicine in the network to so many people, in the case of the public blockchain, every transaction will get updated in the network to all the peers.
- That's where hyperledger finds its significance. In the hyperledger, the parties are directly connected and the concerned people's ledger will be updated.
- Hence providing privacy and confidentiality.

TOKEN

Technically, "token" is just another word for "cryptocurrency" or "crypto asset." But increasingly it has taken on a couple of more specific meanings depending on context. The first is to describe all cryptocurrencies *besides* Bitcoin and Ethereum (even though they are technically also tokens). The second is to describe certain digital assets that run *on top of* other cryptocurrencies' blockchain, as many decentralised finance (or DeFi) tokens do. Tokens have a huge range of potential functions, from helping make decentralised exchanges possible to selling rare items in video games. But they can all be traded or held like any other cryptocurrency.

- DeFi tokens A new world of cryptocurrency-based protocols that aim to reproduce traditional financial-system functions (lending and saving, insurance, trading) has emerged in recent years. These protocols issue tokens that perform a wide variety of functions but can also be traded or held like any other cryptocurrency.
- Governance tokens These are specialised DeFi tokens that give holders a say in the future of a protocol or app, which (being decentralised) don't have boards of directors or any other central authority. The popular savings protocol Compound, for example, issues all users a token called COMP. This token gives holders a vote in how Compound is upgraded. The more COMP tokens you have, the more votes you get.
- Non-Fungible Tokens (NFTs) NFTs represent ownership rights to a unique digital or real-world asset. They can be used to make it more difficult for digital creations to be

copied and shared (an issue anyone who has ever visited a Torrent site full of the latest movies and video games understands). They’ve also been used to issue a limited number of digital artworks or sell unique virtual assets like rare items in a video game.

- Security tokens Security tokens are a new class of assets that aim to be the crypto equivalent of traditional securities like stocks and bonds. Their main use case is to sell shares in a company (very much like the shares or fractional shares sold via conventional markets) or other enterprises (for instance, real estate) without the need for a broker. Major companies and startups have been reported to be investigating security tokens as a potential alternative to other methods of fundraising.

coin drop as a stratergy for public adoption

Coin drops, also known as "airdrops," are a strategy used to distribute cryptocurrency tokens to a large number of people. They can be an effective method for promoting public adoption of a blockchain project when done correctly. Here are some key points to consider when using coin drops as a strategy for public adoption in blockchain:

1. Clear Objectives: Determine your objectives for the coin drop. Are you aiming to increase awareness, attract new users, or incentivize specific actions within your blockchain ecosystem? Setting clear goals will help you design the coin drop accordingly.
2. Target Audience: Identify your target audience. Are you looking to reach out to existing cryptocurrency enthusiasts, potential users of your blockchain project, or a broader demographic? Understanding your audience will help tailor the coin drop to their preferences and needs.
3. Token Utility: Clearly communicate the utility and purpose of your tokens. If people don't understand why they're receiving tokens or how they can use them, the coin drop may not be as effective.
4. Timing: Choose an appropriate time for the coin drop. Coin drops can be used to coincide with the launch of a project, an upgrade, or other significant events to maximise their impact.

5. Marketing and Promotion: Promote the coin drop through various channels, including social media, cryptocurrency forums, and partnerships with influencers. Create engaging content to generate interest and excitement.
6. User Engagement: Encourage recipients to actively engage with your project. This could involve holding onto the tokens, participating in your platform, or referring others to your ecosystem.
7. Compliance: Ensure that your coin drop complies with relevant regulations and legal requirements. Different countries have different rules regarding the distribution of cryptocurrency tokens.
8. Avoid Spam: Be mindful not to overdo it. Excessive airdrops or poorly targeted distributions can lead to spam and dilute the value of your tokens.
9. Transparency: Maintain transparency by providing clear information about the coin drop, the number of tokens distributed, and how they were allocated.
10. Community Building: Use the coin drop as an opportunity to build a supportive and engaged community around your project. Engage with your audience, answer questions, and take feedback seriously.
11. Evaluation: Continuously evaluate the impact of your coin drop. Assess whether it met your objectives and adapt your strategy as needed.

Coin drops can be a powerful tool for public adoption, as they allow individuals to get hands-on experience with a project's tokens and blockchain technology. However, they should be part of a comprehensive marketing and user acquisition strategy, and careful planning is essential to make them effective.

CURRENCY MULTIPLICITY

Currency multiplicity in blockchain refers to the existence of multiple different cryptocurrencies or digital tokens within the blockchain ecosystem. In the world of blockchain and cryptocurrencies, there are thousands of different cryptocurrencies, each with its own unique characteristics, use cases, and underlying technologies. This multiplicity of currencies can be attributed to several factors:

1. Forking: Forking is a process in which a blockchain splits into two separate chains, each with its own set of rules and potentially its own cryptocurrency. This results in the creation of a new cryptocurrency while maintaining the old one. Examples of this include the Bitcoin and Bitcoin Cash fork or the Ethereum and Ethereum Classic split.

2. Tokenization: Many blockchains support the creation of custom tokens, often referred to as "tokens" or "coins." These tokens can represent various assets, from digital collectibles (NFTs) to stablecoins, and each serves its unique purpose within the blockchain's ecosystem.

3. Blockchain Platforms: Many blockchain platforms, such as Ethereum, Binance Smart Chain, and Cardano, enable developers to create their own tokens and cryptocurrencies using their smart contract capabilities. This has led to an explosion of new tokens with various use cases.

4. Specialised Tokens: Some blockchain projects issue tokens for specific purposes, like governance tokens for decision-making, utility tokens for accessing a particular service, and security tokens representing ownership in a real-world asset.

5. Competition and Innovation: The competitive nature of the cryptocurrency space encourages innovation, leading to the development of new currencies and tokens to address perceived shortcomings or improve upon existing solutions.

6. Local and Niche Currencies: Some blockchain projects and communities create their own local or niche currencies, often for experimental or community-specific use.

While currency multiplicity can be seen as a sign of innovation and diversity in the blockchain space, it also presents some challenges:

- Fragmentation: With so many different cryptocurrencies, users and businesses may find it challenging to navigate and choose the right ones for their needs.
- Volatility: The values of cryptocurrencies can be highly volatile, which can make them unsuitable for certain financial transactions or store of value purposes.
- Interoperability: The lack of interoperability between different blockchains and their native currencies can be a barrier to seamless transactions and cross-chain compatibility.
- Regulatory Challenges: The proliferation of cryptocurrencies can create regulatory complexities for governments and authorities trying to oversee this evolving space.

As the blockchain and cryptocurrency space continues to evolve, projects are working on improving interoperability and reducing some of the fragmentation issues associated with currency multiplicity. Technologies like cross-chain protocols and standards are being developed to enable better connectivity between different blockchain networks and their native tokens.

DEMURRAGE CURRENCIES

Currency is one such core concept in blockchain technology that can be extended and re-understood. Currency which is usually referred to as digital token facilitates quantified transfer mechanism. This idea is known as Demur-rage currency.

Demur-rage means “cost of carrying”- that is the cost to carry an asset. The Demur-rage originated from the freight and shipping industry which is used to indicate the extra cost or charge associated with detention in port of a vessel by the ship owner, as in loading or unloading in a given time.

In the cryptocurrency sense, demur-rage can lose value over time i.e., deflationary. Thus, there should be some sort of action taken to realise value before it is lost i.e., spending. Therefore it encourages economic activity. Another important aspect of demur-rage currencies is automatic redistribution of the currency across the network at a certain time specified. In addition to the value loss, this periodic redistribution is another important factor.

Demur-rage currency features could become a dominant and standard currency tool. Freicoin and Healthcoin are two examples of demur-rage currency.Here several health-related services can be paid by using “Healthcoin”, for instance in United States many health related services or plans are usually paid in Healthcoin, where as Freicoin can be used basic needs like living expenditures. As the currency loses its value over time the main goal is to spend it or to use it as soon as possible. Thus inducement to spend and redistribution are the main features of demur-rage currency. This concept of demur-rage currency is not only in the context of currency but it is also used for financial purposes, in economic activities and so on.

However the main goal of demur-rage currency is to provide trust and motivate the people to spend the money before it loses its value.