Unit - 1 - .blockchin

Blockchain Technology (Jawaharlal Nehru Technological University, Hyderabad)

Introduction

Blockchain could be a data structure that could be a growing list of information blocks. The knowledge blocks area unit coupled along, such recent blocks can't be removed or altered. Blockchain is the backbone Technology of Digital CryptoCurrency BitCoin. The blockchain is a distributed database of records of all transactions or digital event that have been executed and shared among participating parties. Each transaction verified by the majority of participants of the system.

It contains every single record of each transaction. BitCoin is the most popular cryptocurrency an example of the blockchain. Blockchain Technology first came to light when a person or Group of individuals name 'Satoshi Nakamoto' published a white paper on "BitCoin: A peer-to-peer electronic cash system" in 2008. Blockchain Technology Records Transaction in Digital Ledger which is distributed over the Network thus making it incorruptible. Anything of value like Land Assets, Cars, etc. can be recorded on Blockchain as a Transaction.

Blockchain

- Blockchain is a type of shared database that differs from a typical database in the way that it stores information; blockchains store data in blocks that are then linked together via cryptography.
- As new data comes in, it is entered into a fresh block. Once the block is filled with data, it is chained onto the previous block, which makes the data chained together in chronological order.
- Different types of information can be stored on a blockchain, but the most common use so far has been as a ledger for transactions.
- In Bitcoin's case, blockchain is used in a decentralized way so that no single person or group has control—rather, all users collectively retain control.
- Decentralized blockchains are immutable, which means that the data entered is irreversible. For Bitcoin, this means that transactions are permanently recorded and viewable to anyone.
- A blockchain is a distributed database or ledger that is shared among the nodes of a computer network.

- As a database, a blockchain stores information electronically in digital format. Blockchains are best known for their crucial role in cryptocurrency systems, such as Bitcoin, for maintaining a secure and decentralized record of transactions.

- The innovation with a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party.

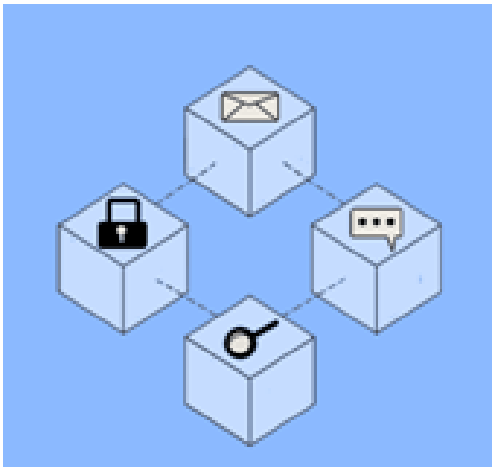


Fig : Blockchain

Block Chain Technology

- Blockchain technology is an advanced database mechanism that allows transparent information sharing within a business network.
- A blockchain database stores data in blocks that are linked together in a chain.
- The data is chronologically consistent because you cannot delete or modify the chain without consensus from the network.
- As a result, you can use blockchain technology to create an unalterable or immutable ledger for tracking orders, payments, accounts, and other transactions.
- The system has built-in mechanisms that prevent unauthorized transaction entries and create consistency in the shared view of these transactions.
- Blockchain technology has been garnering great hype recently.
- It gained popularity after the introduction of Bitcoin in 2009 by the person or group of people by the pseudonym Satoshi Nakamoto.

- Many people confuse and believe blockchain to be bitcoin. But, bitcoin is one application of the blockchain technology.
- There are many other applications and use cases that can be solved using blockchain other than just payment systems.

Fig : Blockchain Technology

Bitcoin vs. Blockchain

Blockchain technology was first outlined in 1991 by Stuart Haber and W. Scott Stornetta, two researchers who wanted to implement a system where document timestamps could not be tampered with. But it wasn't until almost two decades later, with the launch of Bitcoin in January 2009, that blockchain had its first real-world application.

The Bitcoin protocol is built on a blockchain. In a research paper introducing the digital currency, Bitcoin's pseudonymous creator, Satoshi Nakamoto, referred to it as "a new electronic cash system that's fully peer-to-peer, with no trusted third party."

The key thing to understand is that Bitcoin uses blockchain as a means to transparently record a ledger of payments or other transactions between parties.

Blockchain vs. Banks

Blockchains have been heralded as a disruptive force in the finance sector, especially with the functions of payments and banking. However, banks and decentralized blockchains are vastly different. To see how a bank differs from blockchain, let's compare the banking system to Bitcoin's blockchain implementation.

How Are Blockchains Used?

As we now know, blocks on Bitcoin's blockchain store transactional data. Today, more than 23,000 other cryptocurrency systems are running on a blockchain. But it turns out that blockchain is a reliable way of storing data about other types of transactions.

Some companies experimenting with blockchain include Walmart, Pfizer, AIG, Siemens, and Unilever, among others. For example, IBM has created its Food Trust blockchain to trace the journey that food products take to get to their locations.

IBM. "IBM Food Trust."

Why do this? The food industry has seen countless outbreaks of E. coli, salmonella, and listeria; in some cases, hazardous materials were accidentally introduced to foods. In the past, it has taken weeks to find the source of these outbreaks or the cause of sickness from what people are eating.

Using blockchain allows brands to track a food product's route from its origin, through each stop it makes, to delivery. Not only that, but these companies can also now see everything else it may have come in contact with, allowing the identification of the problem to occur far sooner—potentially saving lives. This is one example of blockchain in practice, but many other forms of blockchain implementation exist.

Banking and Finance

Perhaps no industry stands to benefit from integrating blockchain into its business operations more than banking. Financial institutions only operate during business hours, usually five days a week. That means if you try to deposit a check on Friday at 6 p.m., you will likely have to wait until Monday morning to see that money hit your account.

Even if you make your deposit during business hours, the transaction can still take one to three days to verify due to the sheer volume of transactions that banks need to settle. Blockchain, on the other hand, never sleeps.

By integrating blockchain into banks, consumers might see their transactions processed in minutes or seconds—the time it takes to add a block to the blockchain, regardless of holidays or the time of day or week. With blockchain, banks also have the opportunity to exchange funds between institutions more quickly and securely. Given the size of the sums involved, even the few days the money is in transit can carry significant costs and risks for banks.

The settlement and clearing process for stock traders can take up to three days (or longer if trading internationally), meaning that the money and shares are frozen for that period. Blockchain could drastically reduce that time.

Currency

Blockchain forms the bedrock for cryptocurrencies like Bitcoin. The U.S. dollar is controlled by the Federal Reserve. Under this central authority system, a user's data and currency are technically at the whim of their bank or government. If a user's bank is hacked, the client's private information is at risk.

If the client's bank collapses or the client lives in a country with an unstable government, the value of their currency may be at risk. In 2008, several failing banks were bailed out—partially using taxpayer money. These are the worries out of which Bitcoin was first conceived and developed.

Blockchain can also give those in countries with unstable currencies or financial infrastructures a more stable currency and financial system. They would have access to more applications and a wider network of individuals and institutions with whom they can do domestic and international business.

By spreading its operations across a network of computers, blockchain allows Bitcoin and other cryptocurrencies to operate without the need for a central authority. This not only reduces risk but also the processing and transaction fees.

Using cryptocurrency wallets for savings accounts or as a means of payment is especially profound for those without state identification. Some countries may be war-torn or have governments lacking any real identification infrastructure. Citizens of such countries may not have access to savings or brokerage accounts—and, therefore, no way to safely store wealth.

Healthcare

Healthcare providers can leverage blockchain to store their patients' medical records securely. When a medical record is generated and signed, it can be written into the blockchain, which provides patients with the proof and confidence that the record cannot be changed. These personal health records could be encoded and stored on the blockchain with a private key so that they are only accessible to specific individuals, thereby ensuring privacy.

Property Records

If you have ever spent time in your local Recorder's Office, you will know that recording property rights is both burdensome and inefficient. Today, a physical deed must be delivered to a government employee at the local recording office, where it is manually entered into the county's central database and public index. In the case of a property dispute, claims to the property must be reconciled with the public index.

This process is not just costly and time-consuming, it is also prone to human error, where each inaccuracy makes tracking property ownership less efficient. Blockchain has the potential to eliminate the need for scanning documents and tracking down physical files in a local recording office. If property ownership is stored and verified on the blockchain, owners can trust that their deed is accurate and permanently recorded.

In war-torn countries or areas with little to no government or financial infrastructure and no Recorder's Office, proving property ownership can be nearly impossible. If a group of people living in such an area can leverage blockchain, then transparent and clear timelines of property ownership could be established.

Smart Contracts

A smart contract is a computer code that can be built into the blockchain to facilitate a contract agreement. Smart contracts operate under a set of conditions to which users agree. When those conditions are met, the terms of the agreement are automatically carried out.

Say, for example, that a potential tenant would like to lease an apartment using a smart contract. The landlord agrees to give the tenant the door code to the apartment as soon as the tenant pays the security deposit. The smart contract would automatically send the door code to the tenant when it was paid. It could also be programmed to change the code if rent wasn't paid or other conditions were met.

Supply Chains

As in the IBM Food Trust example, suppliers can use blockchain to record the origins of materials that they have purchased. This would allow companies to verify the authenticity of not only their products but also common labels such as “Organic,” “Local,” and “Fair Trade.”

As reported by Forbes, the food industry is increasingly adopting the use of blockchain to track the path and safety of food throughout the farm-to-user journey.

Voting

As mentioned above, blockchain could facilitate a modern voting system. Voting with blockchain carries the potential to eliminate election fraud and boost voter turnout, as was tested in the November 2018 midterm elections in West Virginia.

Using blockchain in this way would make votes nearly impossible to tamper with. The blockchain protocol would also maintain transparency in the electoral process, reducing the personnel needed to conduct an election and providing officials with nearly instant results. This would eliminate the need for recounts or any real concern that fraud might threaten the election.

Pros and Cons of Blockchain

For all of its complexity, blockchain’s potential as a decentralized form of record-keeping is almost without limit. From greater user privacy and heightened security to lower processing fees and fewer errors, blockchain technology may very well see applications beyond those outlined above. But there are also some disadvantages.

Pros

- Improved accuracy by removing human involvement in verification
- Cost reductions by eliminating third-party verification
- Decentralization makes it harder to tamper with
- Transactions are secure, private, and efficient
- Transparent technology
- Provides a banking alternative and a way to secure personal information for citizens of countries with unstable or underdeveloped governments

Cons

- Significant technology cost associated with some blockchains
- Low transactions per second
- History of use in illicit activities, such as on the dark web
- Regulation varies by jurisdiction and remains uncertain
- Data storage limitations

Features of Blockchain Technology :

These are the ten features of Blockchain Technology :

1. Immutable
2. Distributed
3. Decentralized
4. Secure
5. Consensus
6. Unanimous
7. Faster Settlement
8. Proof of work / Transparency
9. Miners
10. Public Distributed Ledger

Fig : Features of Blockchain

1. Immutable

Immutability means that the blockchain is a permanent and unalterable network. Blockchain technology functions through a collection of nodes.

- Every node in the network has a copy of the digital ledger. To add a transaction every node checks the validity of the transaction and if the majority of the nodes think that it is a valid transaction then it is added to the network.
- This means that without the approval of a majority of nodes no one can add any transaction blocks to the ledger.
- Any validated records are irreversible and cannot be changed. This means that any user on the network won't be able to edit, change or delete it.

2. Distributed

All network participants have a copy of the ledger for complete transparency. A public ledger will provide complete information about all the participants on the network and transactions. The distributed computational power across the computers ensures a better outcome. Distributed

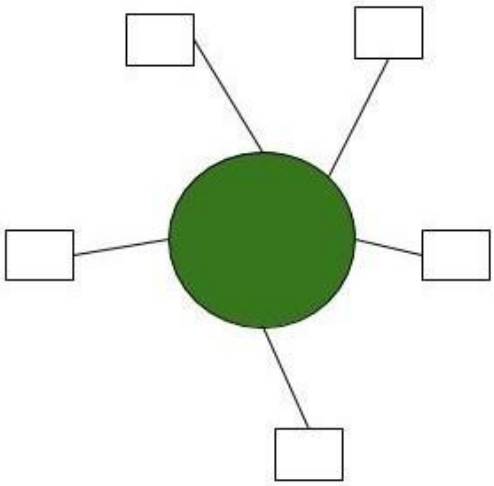
ledger is one of the important features of blockchains due to many reasons like:

- In distributed ledger tracking what's happening in the ledger is easy as changes propagate really fast in a distributed ledger.
- Every node on the blockchain network must maintain the ledger and participate in the validation.
- Any change in the ledger will be updated in seconds or minutes and due to no involvement of intermediaries in the blockchain, the validation for the change will be done quickly.
- If a user wants to add a new block then other participating nodes have to verify the transaction. For a new block to be added to the blockchain network it must be approved by a majority of the nodes on the network.
- In a blockchain network, no node will get any sort of special treatment or favors from the network. Everyone will have to follow the standard procedure to add a new block to the network.

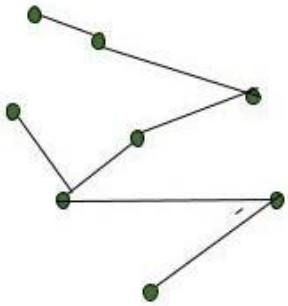
3. Decentralized

The blockchain network is decentralized which means that there is no central governing authority that will responsible for all the decisions. Rather a group of nodes makes and maintain the network. Each and every node in the blockchain network has the same copy of the ledger. Decentralization property offers many advantages in the blockchain network:

- As a blockchain network does not depend on human calculations it is fully organized and fault-tolerant.
- The blockchain network is less prone to failure due to the decentralized nature of the network. Attacking the system is more expensive for the hackers hence it is less likely to fail.
- There is no third-party involved hence no added risk in the system.
- The decentralized nature of blockchain facilitates creating a transparent profile for every participant on the network. Thus, every change is traceable, and more concreate.
- Users now have control over their properties and they don't have to rely on third-party to maintain and manage their assets.



Centralised Network



Decentralised network

4. Secure

All the records in the blockchain are individually encrypted. Using encryption adds another layer of security to the entire process on the blockchain network. Since there is no central authority, it does not mean that one can simply add, update or delete data on the network.Every information on the blockchain is hashed cryptographically which means that every piece of data has a unique identity on the network. All the blocks contain a unique hash of their own and the hash of the previous block. Due to this property, the blocks are cryptographically linked with each other. Any attempt to modify the data means to change all the hash IDs which is quite impossible.

5. Consensus

Every blockchain has a consensus to help the network to make quick and unbiased decisions. Consensus is a decision-making algorithm for the group of nodes active on the network to reach an agreement quickly and faster and for the smooth functioning of the system. Nodes might not trust each other but they can trust the algorithm that runs at the core of the network to make decisions. There are many consensus algorithms available each with its pros and cons. Every blockchain must have a consensus algorithm otherwise it will lose its value.

6. Unanimous

All the network participants agree to the validity of the records before they can be added to the network. When a node wants to add a block to the network then it must get majority voting otherwise the block cannot be added to the network. A node cannot simply add, update, or delete information from the network. Every record is updated simultaneously and the updations propagate quickly in the network. So it is not possible to make any change without consent from the majority of nodes in the network.

7. Faster Settlement

Traditional banking systems are prone to many reasons for fallout like taking days to process a transaction after finalizing all settlements, which can be corrupted easily. On the other hand, blockchain offers a faster settlement compared to traditional banking systems. This blockchain feature helps make life easier. Blockchain technology is increasing and improving day by day and has a really bright future in the upcoming years. The transparency, trust, and temper proof characteristics have led to many applications of it like bitcoin, Ethereum, etc. It is a pillar in making the business and governmental procedures more secure, efficient, and effective.

8. Proof of Work or Transparency

Proof-of-work is a crucial feature and system that Bitcoin uses. It is a piece of information that is very difficult to produce. That means you need to invest a lot of money and effort to produce the information. However, it can be readily verified by others and satisfies specific criteria.

For example, in order to add a block to the Blockchain with bitcoin, miners compete with one another by solving a mathematical puzzle to determine the block's nonce value.If other miners verify a miner's claim after discovering a nonce value, she spreads the word throughout the network and is rewarded with 12.5 bitcoins or some other form of payment. In addition, a block is also added to the Blockchain after a nonce value is discovered.

9. Miners

The act of mining involves rewarding a miner for discovering the correct nonce first. Bitcoins are used to pay miners and can only be added to the network after successful verification. That is the idea behind mining, and a miner receives compensation after completing the proof-of-work consensus.

10. **Public Distributed Ledger**

A public distributed ledger is a collection of digital data that is shared, synchronized, and replicated around the world, across multiple sites, countries, and institutions. Now let's consider a blockchain that can be accessed by anyone in the network around the world. If someone tries to alter data in one of the blocks, everyone in the network can see the alteration, because everyone in the network has a copy of the ledger. In this way, data tampering is prevented.

Benefits of Blockchain Technology :

The following are some of the benefits of blockchain technology:

1. Efficiency
2. Transparency
3. Security
4. Network Distribution
5. Traceability
6. Reduced costs
7. Availability
8. Automation
9. Decentralized
10. Tokenization

1. Efficiency: By simplifying these methods with blockchain, dealings can be achieved quickly and more efficiently.

- Efficiency only indicates that transactions once registered on the blockchain, can't be modified or removed.
- On the blockchain, all transactions are timely and date-wise noted, so there's a permanent chronology.
- Therefore, blockchain can be employed to track information over the short and long term, allowing a secure, trustworthy version of knowledge.
- Blockchain is utilized to digitize genuine estate transactions to keep control of property headers.

2. Transparency: Blockchain produces a track that establishes the origin of an investment at every step of its records. It is achievable to transfer data regarding origin directly with clients.

- Transparency is one of the major difficulties in the IT world.
- To enhance transparency, associations have attempted to execute more rules and protocols.
- The main goal of the blockchain is to make the business model transparent which includes transactions, wallets, etc.

- So that no single individual can make the changes without knowing other participants in the business model.

3. Security: By building a document that can't be changed and is encrypted end to end, blockchain allows for preventing copying and unauthorized movement. Privacy problems can likewise be managed on blockchain by individual data and individual authorizations to maintain access.

- It focuses on the security part also as blockchain is mainly known for its security.
- The security is so tight that it is very difficult to hack the ledger and steal or manipulate the information because of using a consensus algorithm.
- Any trades that are ever registered require to be decided upon according to the agreement approach.
- Furthermore, the individual transaction is encrypted and has a verified connection with the previous transactions with help of hashing algorithms.

4. Network distribution: When users load data into the approach, users cannot modify it and it's hard to eliminate. Even small differences can be traceable, tracked, and registered then distributed on the blockchain ledger for all to view.

- It also concentrates on educating or making awareness regarding network distribution.
- This particular supplies, at the identical moment, various advantages, by having this network distributed, in the foremost example, no one holds the network, permitting various users to consistently have numerous documents of the exact data.
- Moreover, this feature causes it immune and distributed to any kind of defeat as the point that a node dies accomplishes not suggest generalized failures in the P2P network.

5. Traceability: With blockchain technology, users can stop all of the errors. Users' store chains can evolve totally translucent and manageable to track. It allows users to join, outline, and track goods or assets to confirm they are not misapplied or returned during the procedure.

- Participants or members can easily track their business model using blockchain.
- This will increase the growth of businesses as they will get the fault at the right time.
- In blockchain technology, the collection chain evolves better transparently than ever.
- It allows every group to trace the interests and confirm that it is not substituted or misapplied during the collection chain approach.

- Associations can also create the most out of blockchain traceability by executing it in place.

6. Reduced Costs: It delivers protected surroundings where encrypted enterprise transactions between customer and seller can transpire without the requirement for third groups to moderate.

- Associations desire to decrease costs and delay the funds into creating something unique or enhancing existing approaches.
- By operating blockchain, associations can obtain at cheaper costs associated with third-party agents.
- Blockchain includes no inherited centralized performer, there is no necessity to consume on any dealer charges.
- Moreover, there is a minor exchange must when it comes to validating a trade.

7. Availability: Parties of blockchain P2P networks can get shut down from analyzing the shape and correcting it when union producers submit the condition of the design.

- Higher availability, efficiency, confidentiality, and flexibility to adjust any desired solution model.
- The data can be recovered by users from anywhere around the world.
- The availability is higher as productivity increases by using blockchain because it divides each section into each department so that every individual can focus on a particular task or work.

8. Automation: Blockchain transactions can be automated with smart contracts. Using smart contracts increases efficiency and speeds up the process. Once the pre-specified conditions in smart contracts are met then the next steps in the transaction or process are automatically triggered.

- Smart contracts reduce human intervention.
- They also reduce reliance on third parties to verify that the terms of the contracts have been met.

9. Decentralized: Blockchain technology is used to hold data in a decentralized manner so everyone can confirm the accuracy or correctness of the data by using nil understanding evidence via which one group confirms the correctness of data to another group without disclosing anything regarding the information.

- Decentralization indicates the transfer of control and judgment created from a centralized organization to a P2P network.
- These networks attempt to reduce the level of trust that partners should put in individually and prevent their ability over each other.
- It creates blockchain and enhances security for users.
- In demand for someone to meddle with the blockchain, they would have to meddle with all the units of the chain and hack every node, which is unthinkable.

10. Tokenization: Tokenization is the method where the worth of an asset including digital as well as material, is transformed into a digital token that is then registered on and then transmitted through blockchain.

- It has been noticed with digital skills and other virtual support, but tokenization has more general applications that could smooth business transactions.
- It is used to change carbon emission fundings under carbon cap schedules.

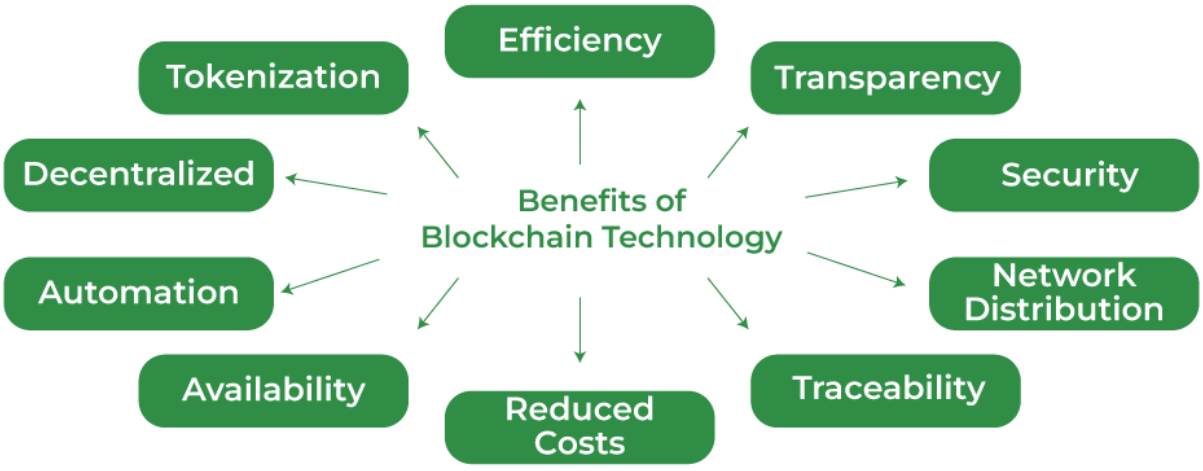


Fig : Benefits of Blockchain Technology

Components / Common terms involved in Blockchain Technology / Network :

The following are the common terms involved in blockchain :

1. Peer to Peer network
2. Distributed Ledger
3. Consensus Mehanism
4. Smart Contracts
5. Cryptography
6. Virtual Machine

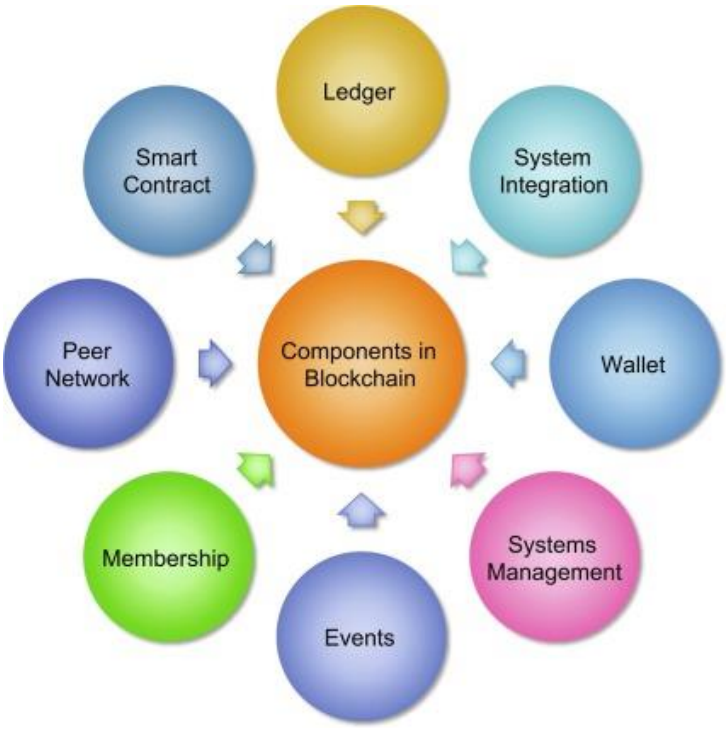


Fig : Components of Blockchain Technology

Peer to Peer Network :

A peer to peer network is a distributed application architecture that consists of computing devices connected to each other, without a central server. In centralised networks, the security is dependent on a single entity. If that central server is attacked, the security of the overall network is compromised. But a peer to peer network is more secure as there is no single point of failure.

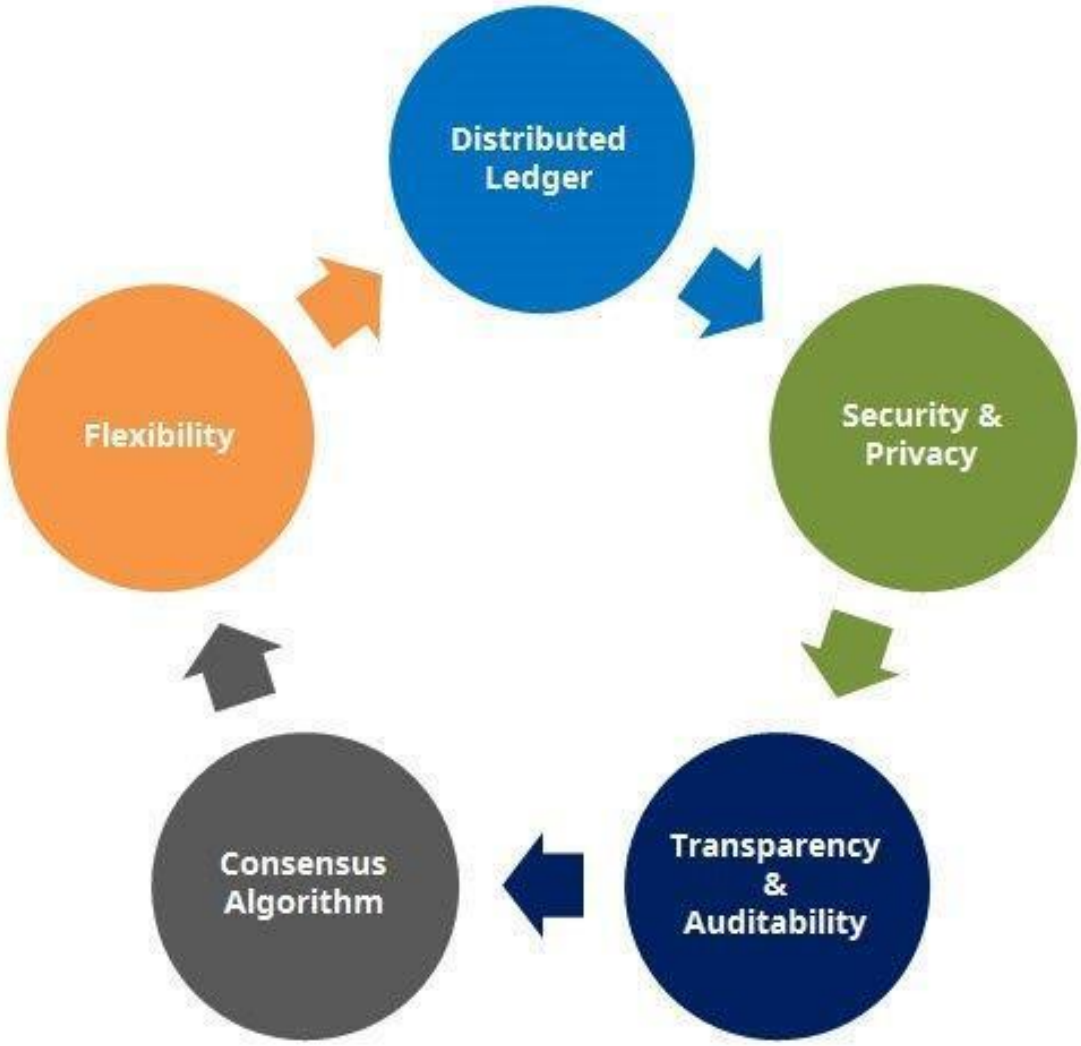


Fig : Peer to Peer dependencies in Blockchain Networks

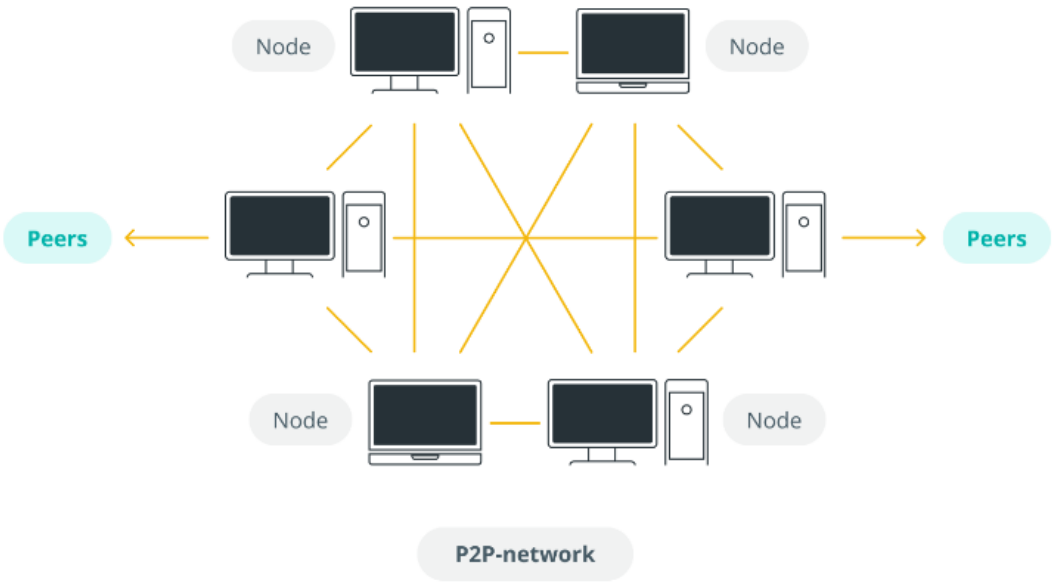


Fig : Peer to Peer network in blockchain

Distributed Ledger :

A ledger is a system containing all the records of a input and output of a process. A distributed ledger is a data structure which is spread across different computing devices.

DLT (Distributed Ledger Technology) is the technology that distribute records across all the users. DLT consists of 3 components – **Data Model** (current state of ledger), **Language of transactions** (which changes ledger state) and **Protocol** (used to build consensus). Blockchain is a type of DLT. This way the data is shared among all its users increasing transparency and avoiding corruption.

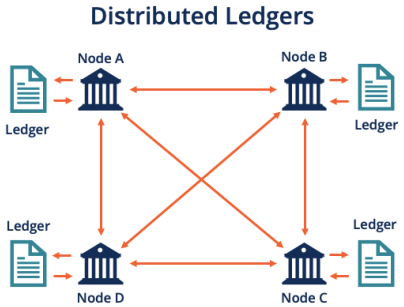


Fig : Distributed Ledgers

Consensus Mechanism :

Consensus is a process of ensuring that all the different users in a blockchain come to an agreement regarding the current state of blockchain. There are several consensus mechanisms that are used by different blockchains to achieve consensus. For example, Bitcoin uses Proof-of-Work while Ethereum is moving from Proof-of-Work to Proof-of-Stake algorithm.

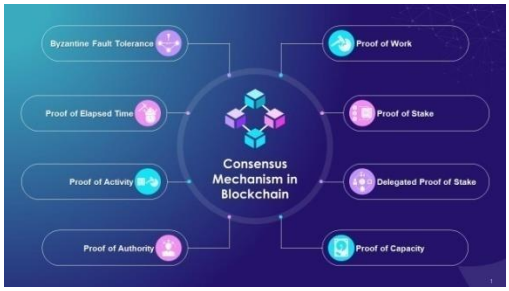


Fig : Consensus Mechanisms in Blockchain

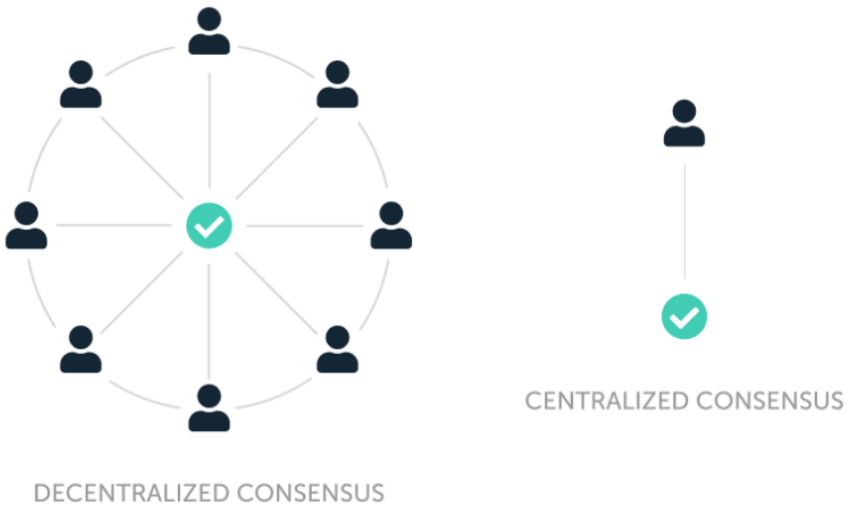


Fig : Distribution of Consensus by using Ledger in Blockchain

Smart Contracts :

Forget smart contract and blockchain for a moment. Think about contracts in general. These contain some conditions which need to be fulfilled in order for some transaction (eg; money exchange) to occur. For example, if you are selling me a laptop, a contract will contain that I will be responsible to pay you only if the laptop works properly. Similarly, smart contracts are pre-requisite conditions which need to be fulfilled for transactions to happen in a blockchain.

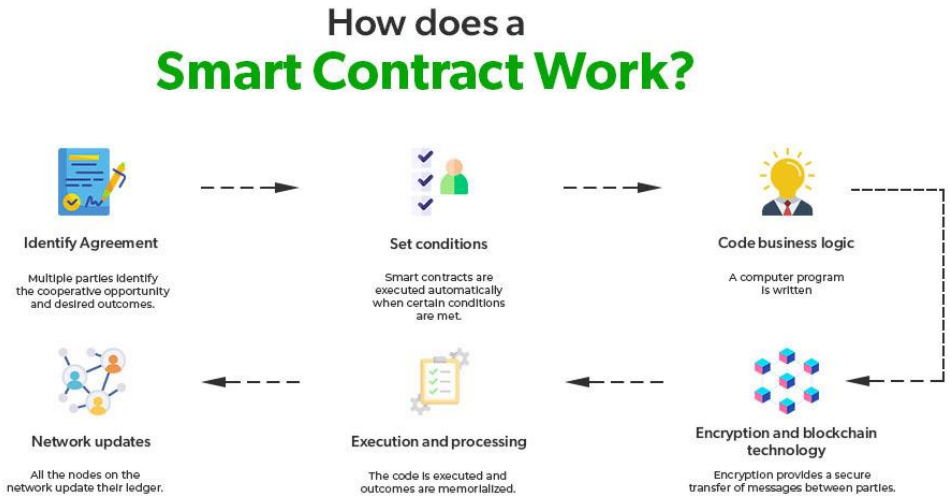


Fig : Working of Smartcontract in Block Chain

Cryptography

This component ensures the security, integrity and verification of the information in the ledger or the information transmitted between the nodes. By building on a foundation of mathematics (especially probability theory) along with knowledge of game theory, cryptography has come up with encryption methods that are impossible to break.

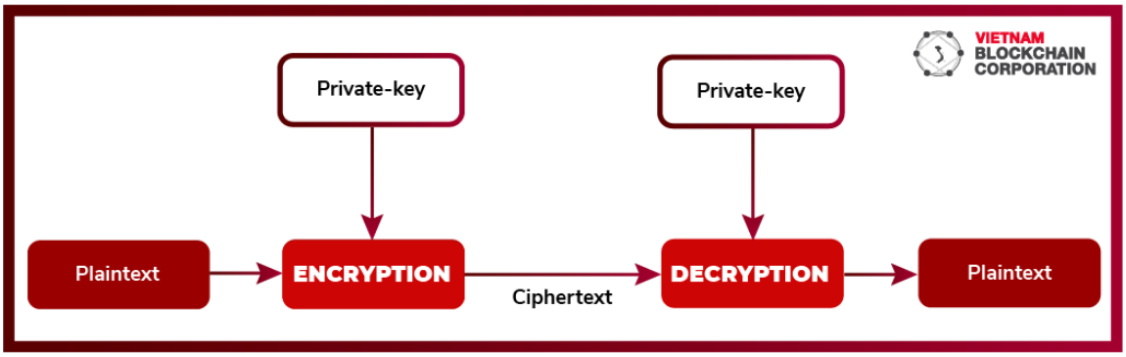
Classification

There are two main types of encryption methods:

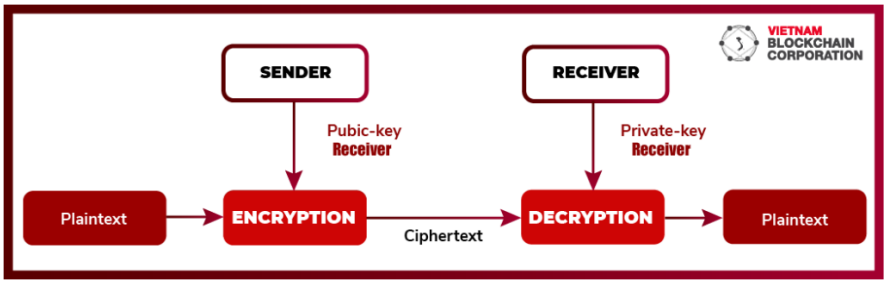
1. Symmetric Encryption

2. Asymmetric Encryption

- ***Symmetric Encryption****:* It is a form of encryption to secure data, in which the encryption and decryption of data use the same key. Since the key is used to decrypt the data, it should be kept secret. Therefore, when using a symmetric key, the sender and receiver need a mechanism to exchange keys before exchanging data



- ***Asymmetric Encryption****:* It is a form of encryption to secure data, in which the encryption and decryption of data uses two different keys. The key used to encrypt data is called a public key, which can be shared widely and seen as a person's identity (or called as a Blockchain address). The key used to decrypt data is called a private key, which is necessary for security to protect the rights of the receiver.



Virtual Machine

A virtual machine is a program that simulates a computer system. It has a CPU, memory and virtual storage. Basically, a virtual machine works like a physical computer, it can be used to store data, run application programs, and exist to jointly operate a Blockchain network with other virtual machines.

Ethereum Virtual Machine (EVM)

The Ethereum virtual machine is used to ensure that transactions processed on completely different environments and computer configurations will always create the same results on the Ethereum platform. Essentially, an EVM is a machine that processes smart contracts running on the Ethereum. Nodes participating in the Ethereum system process transactions received through the EVM. Any transaction that wants to change the status of network must go through the process of the EVM. EVM is just a virtual machine but many copies are made. Each node participating in the execution of the same transactions owns a copy of the EVM to ensure the consistency of the computation.

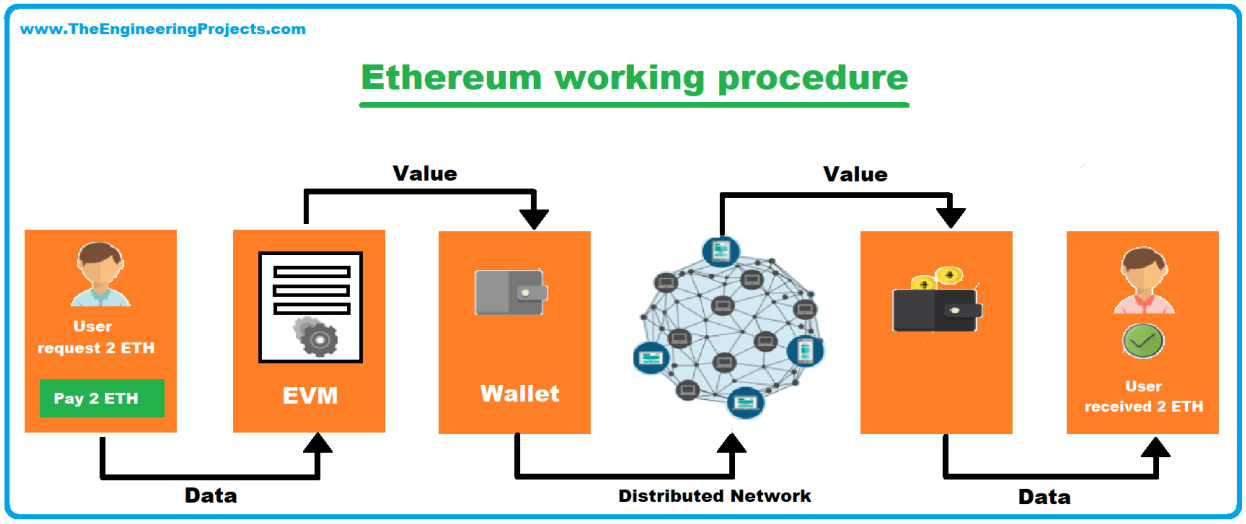


Fig : Etherum Working Process

Types of Blockchain Networks :

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.

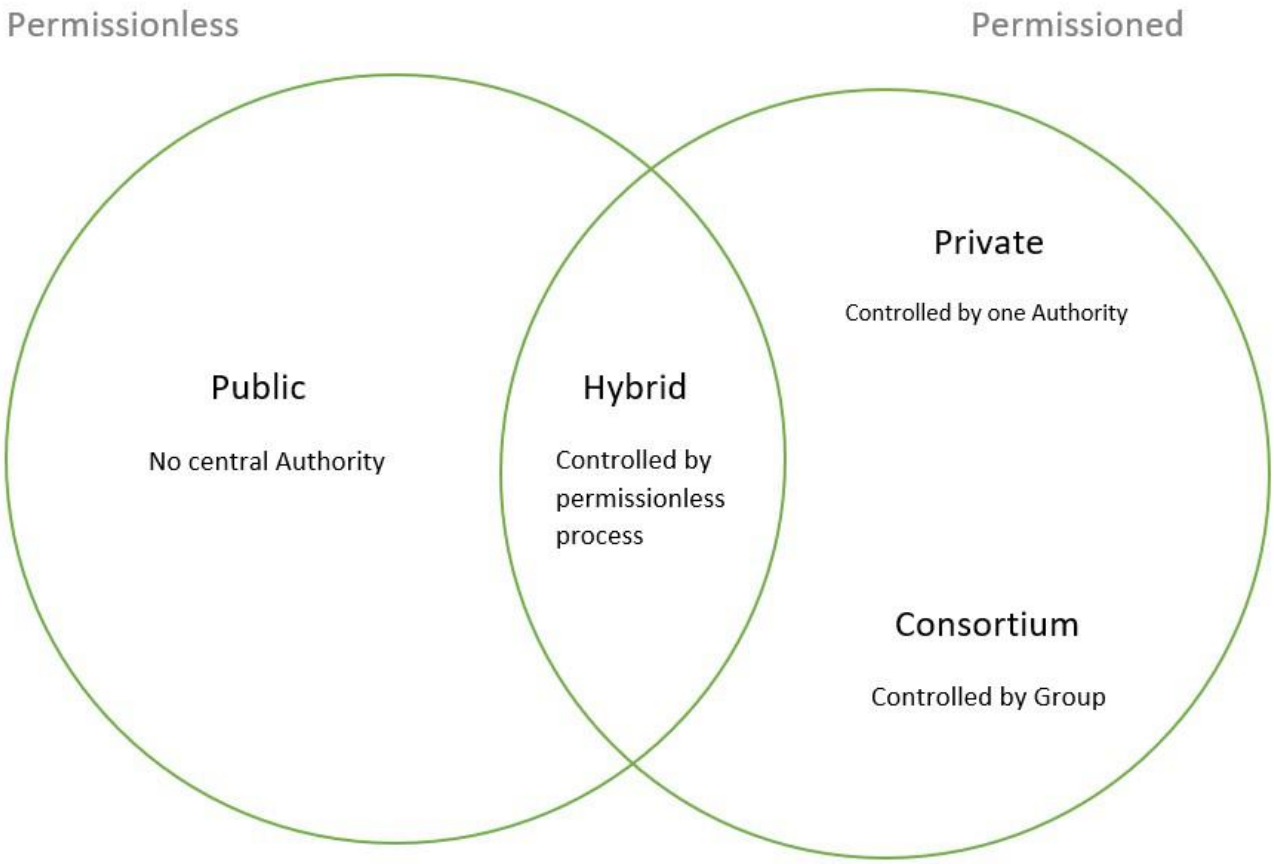


Fig : Permissioned and permissionless blockchain

Permissioned Blockchain :

These are the closed network 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 a 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.

There are 4 types of blockchain:

1. Public Blockchain.
2. Private Blockchain.
3. Hybrid Blockchain.
4. Federated / Consortium 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 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 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 to implement 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. Examples of public blockchain are Bitcoin, 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 user has the 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 a primary entity owns a hybrid blockchain it cannot alter the transaction

Advantages:

- **Ecosystem:** 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 the 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 health care 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 Ripple network and XRP token.

4. Federated / 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 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.

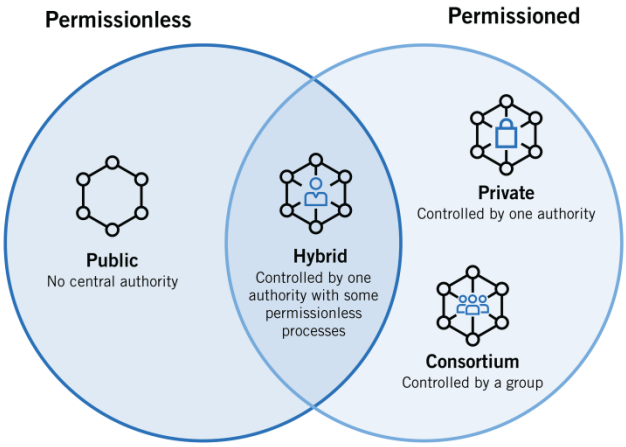


Fig : Types of Blockchain networks

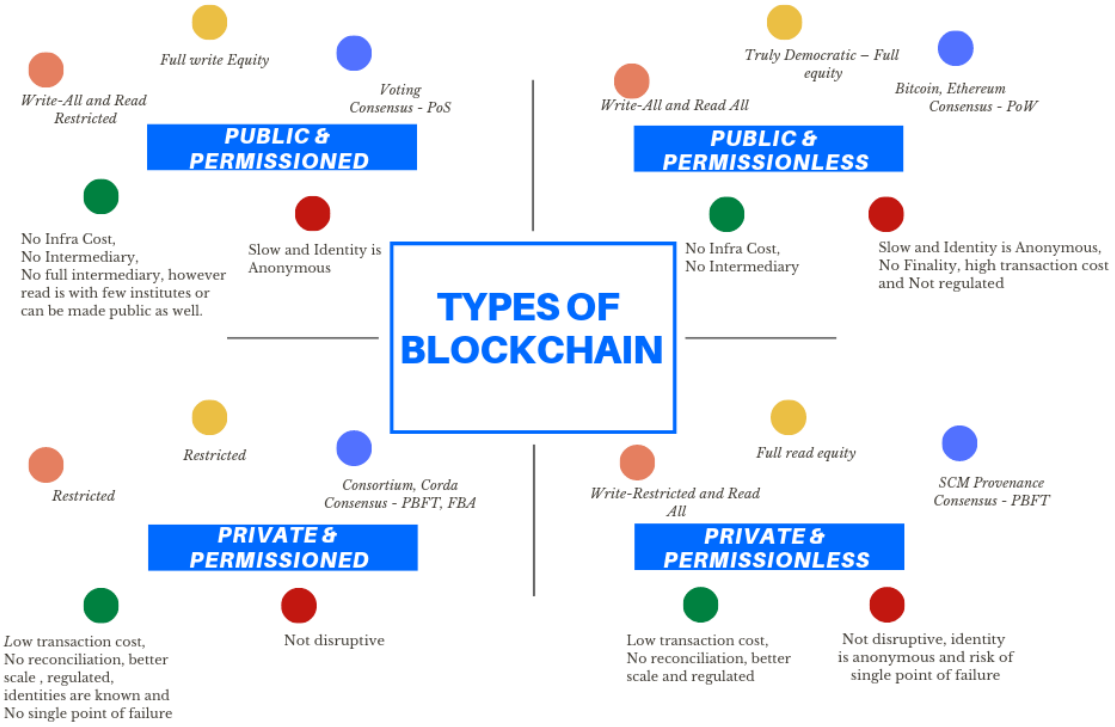


Fig : Permissioned and Permissionless Blockchain networks

Permissioned	Permissionless
Closed; Requires permission to join the network and participate in consensus	**Public**; Does not require permission to join the network and participate in consensus
Incrementally decentralized to fully centralized; A governing authority acts as a gatekeeper	Fully decentralized, no gatekeepers
Transactions are private	Transactions are transparent and accessible
Speed and high performance	Slow transaction speed
Scalable network	Difficult to scale
Energy-efficient	Consumes a lot of energy
Development by private entities; Less mindshare	Development is open-source; More mindshare, as there are more developers
Governing authority provides a certain level of trust in the system	Trustless; The maths provide the proof
Consensus is reached quickly because computations are less complex due to limited users	Consensus takes longer to reach due to network size and complexity of computations

Fig : Differences between Permission and Permissionless

Tools involved in Block chain Technology

Following are the 11 most trending Blockchain Development Tools in 2023:

1.Solidity

2.Hyperledger Fabric

3.Ethereum

4.solc (Solidity Code)

5.Truffle

6.Ganache

7.Metamask

8.Remix

9.Geth

10.web3.js

11.Embark

1.Solidity

Solidity is an open-source high-level object-oriented programming language popularly used for creating smart contracts and decentralized applications (dApps). It got highly inspired by Javascript, C++, and Python, making it easy and relatable for developers to understand.

The language targets Ethereum Virtual Machine (EVM), which executes the code written. Using Solidity, developers write self-executing smart contract code, which executes when the coded conditions are met. Solidity supports several complex user-defined data types, contract inheritance, and various libraries. These features make Solidity easy, robust, and reliable for developers. It is also known as the language of web3 for the future.

2.Hyperledger Fabric

Hyperledger Fabric is an open-source blockchain platform that is maintained by the Linux Foundation. It is designed for enterprise use cases and is intended to be a foundation for building blockchain applications and networks. Hyperledger Fabric has a modular architecture and supports pluggable components, which makes it easy to customize and extend. It also has a flexible consensus model that allows users to choose the consensus algorithm that best fits their needs.

3.Ethereum

Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference. It was developed by VitalikButerin in 2014 and has since become one of the most widely used blockchain platforms.

The Ethereum is based on a blockchain and uses a decentralized virtual machine, called the Ethereum Virtual Machine (EVM), to execute smart contracts. The EVM is a global, open-source computing environment that is designed to be run on a decentralized network of computers. It allows developers to build and deploy decentralized applications (DApps) and write smart contracts in a variety of programming languages.

4.Solc

Solidity Compiler, aka Solc, is a command-line compiler for solidity programs. It aims to convert the solidity code to bytecode for Ethereum Virtual Machine (EVM) to interpret it.

There are 2 types of Solidity compiler (Solc):

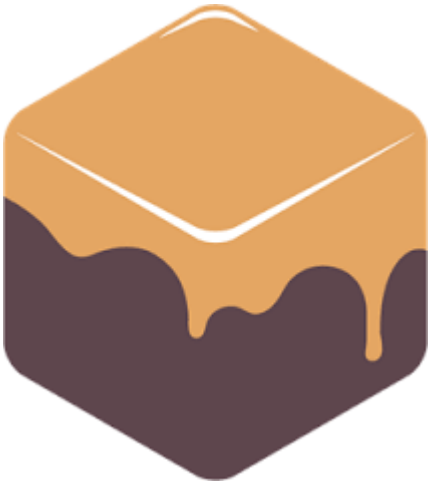
- **Solc** (Written in C++) – It's a command-line compiler that first converts the Solidity code to javascript using emscripten. Then compiles the javascript code to bytecode for EVM.
- **Solcjs** (Nodejs Library) – It's a command-line interpreter which directly compiles solidity code into bytecode for EVM. This JavaScript-based compiler can run in both browser and Node.js environments. The popular Ethereum IDE, Remix also uses Solcjs as a compiler.

5.Truffle

Truffle is a complete blockchain development environment used for compiling, testing, and deploying smart contracts and creating decentralized applications. It enables automated contract testing using Chai and Mocha. Truffle is well-equipped with required libraries and built-in procedures to ease the process of developing and deploying smart contracts.

6.Ganache

Ganache is a Blockchain simulator that can deploy on your local system. It enables a GUI to simulate Blockchain networks without setting up real test networks or an actual remote network. It provides vacant Ethereum addresses with fake 100 ETH in each account, use to test and deploy your smart contracts and decentralized applications.



7.Metamask

Metamask is a software wallet to store, send and receive ETH cryptocurrency and other Ethereum Tokens. It gets added as a web browser (chrome, firefox, brave, etc.) extension and works as an intermediate between the Blockchain and the decentralized applications. In addition, Metamask can connect with Shapeshift and Coinbase to sell and buy ETH cryptocurrency and ERC20 tokens.

8.Remix

One of the most popular and easy-to-use Ethereum IDE is Remix for executing and deploying a Solidity smart contract. It has the compilers compatible with almost all the versions of Solidity. Moreover, it has a simulated Blockchain environment with vacant addresses to test, run and deploy your contract. In addition, Remix can also connect to the Ethereumblockchain using the Metamask wallet.

9.Geth

Geth is an Ethereum node implementation developed using the Go programming language. It's available in three interfaces: the interactive console, JSON-RPC server, and command line. It supports blockchain development on Linux, Windows, and Mac operating systems.

Geth is an ideal and preferred tool for several EthereumBlockchain tasks that include creating smart contracts, token transfer, checking block history, and mining ether tokens. Here, users can also connect to the existing Blockchain or develop their own blockchain network.

10.Web3.js

Web3.js is a collection of libraries that allow users to interact with an Ethereum node remotely or locally. It provides an API to interact with Blockchain easily. Web3.js is a kind of wrapper for JSON RPC to create a connection to a remote or local Ethereum node with either an HTTP or IPC connection.

It usually comes handly while using Nodejs to create decentralized applications.

11.Embark

Embark is a blockchain development and management tool that assists developers while creating decentralized applications. It also provides an environment to develop and deploy a serverless html5 application. Embark follows the contract code directly. So if any changes occur to the contract, it modifies the related dApps.

Working Process of Blockchain Transactions :

- A blockchain is a distributed database that stores information electronically in a digital format and is shared among the nodes of a computer network.
- A typical difference between a blockchain and a database is how data is structured.
- A blockchain is a shared, immutable ledger as the name suggests structures data into chunks or blocks, and a database structures data into tables.
- A blockchain is a chain of blocks. Once a block is filled with data and it is chained to the previous blocks.
- Different types of information can be stored on the blockchain network but the most important is transactions.

How Does a Blockchain Work?

The transaction process in a blockchain can be summarized as follows:

1. Facilitating a transaction: A new transaction enters the blockchain network. All the information that needs to be transmitted is doubly encrypted using public and private keys.

2. Verification of transaction: The transaction is then transmitted to the network of peer-to-peer computers distributed across the world. All the nodes on the network will check for the validity of the transaction like if a sufficient balance is available for carrying out the transaction.

3. Formation of a new block: In a typical blockchain network there are many nodes and many transactions get verified at a time. Once the transaction is verified and declared a legitimate transaction, it will be added to the mempool. All the verified transactions at a particular node form a mempool and such multiple mempools form a block.

4. Consensus Algorithm: The nodes that form a block will try to add the block to the blockchain network to make it permanent. But if every node is allowed to add blocks in this manner then it will disrupt the working of the blockchain network. To solve this problem, the nodes use a consensus mechanism to ensure that every new block that is added to the Blockchain is the one and only version of the truth that is agreed upon by all the nodes in the Blockchain, and only a valid block is securely attached to the blockchain. The node that is selected to add a block to the blockchain will get a reward and hence we call them "miners". The consensus algorithm creates a hash code for that block which is required to add the block to the blockchain.

5. Addition of the new block to the blockchain: After the newly created block has got its hash value and is authenticated, now it is ready to be added to the blockchain. In every block, there is a hash value of the previous block and that is how the blocks are cryptographically linked to each other to form a blockchain. A new block gets added to the open end of the blockchain.

6. Transaction complete: As soon as the block is added to the blockchain the transaction is completed and the details of this transaction are permanently stored in the blockchain. Anyone can fetch the details of the transaction and confirm the transaction.

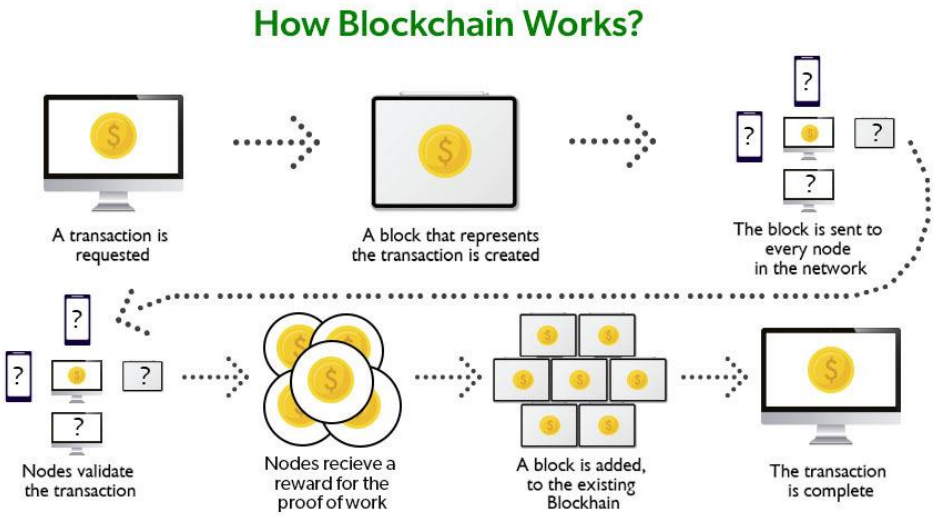


Fig : Working Process of Block Chain Technology

Step 1: Facilitating the transaction: Jack wants to send 20 BTC to Phil via the Blockchain network.

Step 2: Verification of transaction: The message for verification will be sent to all the nodes on the network. All the nodes will check the important parameters related to the transaction like Does Jack has sufficient balance i.e. at least 20BTC to perform the transaction. Is Jack a registered node? Is Phil a registered node? After checking the parameters the transaction is verified.

Step 3: Formation of a new block: A number of verified transactions stack up in mempools and get stored in a block. This verified transaction will also get stored in a block.

Step 4: Consensus algorithm: Since here we are talking about bitcoins so the Proof-of-Work consensus algorithm will be used for block verification. In proof-of-work, the system assigns the target hash value to a node, and according to this, it must come up with a hash for the new block. The node has to calculate the hash value for the new block that is less than the target value. If two or more miners mine the same block at the same time, the block with more difficulty is selected. The others are known as stale blocks. Mining usually rewards miners with blockchain currency. In this case, the blockchain currency is bitcoin.

Step 5: Addition of the new block in the blockchain: After the newly created block has got the hash value and authentication through proof-of-work only then it will be added to the network and the transaction will mark as complete. Phil will receive 20 BTC from Jack. The new block will be linked to the open end of the blockchain.

Step 6: Transaction complete: As soon as the block is added to the blockchain, the transaction will take place and 20 BTCs will get transferred from Jack's wallet to Phil's wallet. The details of the transaction are permanently secured on the blockchain.Anyone on the network can fetch the information and confirm the transaction. This will help to keep track of all the transactions and to verify whether any user is trying to double spend. For example, if Jack tries to carry out a transaction in the future, the rest of the nodes can check Jack's past transaction records to check

whether Jack has enough balance to carry out the current transaction. If there is enough balance then the transaction will be approved.

Is Blockchain Secure?

In the most basic way, one can think of a blockchain as a linked list. Each of the next items in the list is dependent on the previous item, except for the first block, also known as the genesis block, which is hardcoded into the blockchain. In the blockchain, each block contains the hash of the previous block's header and a hash of the transactions in the Merkle tree of the current block. In this way, each block is cryptographically chained to the previous block. Let's understand with an example what happens when someone attempts to change a transaction or block data in a blockchain network.

- Suppose, there is a chain of 10 blocks, where the 10^{th} block depends on the 9^{th} block, the 9^{th} block depends on the 8^{th} block, and so on.
- In this way, the 10^{th} block depends on all the previous blocks and the genesis block as well.
- If someone tries to change data on the 2^{nd} block, then the attacker will have to change data on all the later blocks as well, otherwise, the blockchain will become invalid since the later blocks depend on the hash value present in the 2^{nd} block and the 2^{nd} block has changed, but not the later blocks.
- Thus, as the blocks are added, immutability increases as changing the block is an expensive operation.
- Also, to add/change a block in a blockchain, a consensus algorithm is used by nodes in the blockchain network. In order to compensate for the change in one block, one must have to recalculate the hash of every block to update the hash value of the block header in the next block. This will involve a lot of time and computational resources.
- In order to succeed with such kind of attack, the hacker has to simultaneously control and change 51% or more copies of the blockchain so that their new copy becomes the majority copy and thus the agreed-upon chain.
- Thus, requiring an immense amount of time, money, and computational resources.

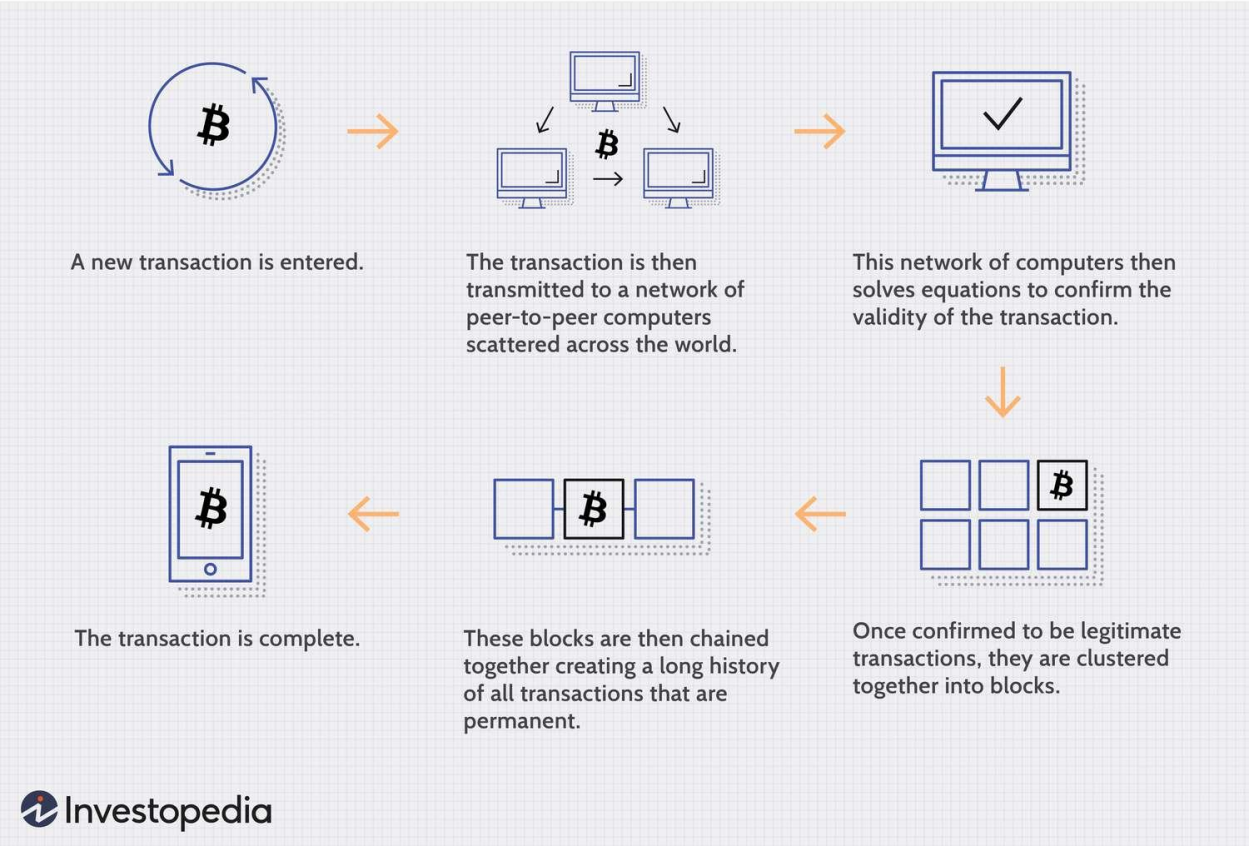


Fig : Working Process of Block chain Technology

Promises of Blockchain ?

The blockchain enables the construction of a vast ledger that is distributed as far and as wide as desired, visible to everyone, updated in accordance with a transactional principle similarly distributed and guaranteed by a community, without the need for a trusted third party as a central authority.

The blockchain makes five promises:

1. Distributed trust.
2. A system of transactions.
3. Guaranteed by an extended community.
4. No trusted third parties
5. The capacity to operate complex protocols.

The blockchain is a genuine innovation: twenty years ago, it was by no means obvious that one day it would be possible for one technology to honour even the first four promises. Having said that, it is very much the combination of the five promises that defines the blockchain's scope of application. If we needed a solution capable of fulfilling only one or two of these promises, other cheaper and more efficient methods would exist (see below).

The fifth promise is crucial, as it lends the blockchain its capacity for disruption: the ability to handle complex protocols (money transfers, banking, validation, and so on) in an automated way, with much lower transaction costs compared with systems that require human input, above all in the form of a trusted third party. In other words, the blockchain not only transports information, but also algorithms, and it does so with the same guarantee of trust as applies to the information itself.

Distributed Trust :

- Distributed trust means that no longer one single party has to be trusted to acgeive the desired result in a process with out unwanted side effects.
- In other words we want to eliminate dependencies from one party or at least reduce them.
- Three examples of such parties today:
    1. If you have money in a savings account , you have to trust your bank , which was not evident at the time of the banking crisis.
    2. If you use face book , you trust that the service is available that is adequately secured and that facebook is dealing with your data in a proper way. We except that abuse, such as by, among others Cambridge Analytical , will not occur .
    3. If you own property, you trust that this has been registered correctly in the land registry and that it is remains registered correctly.
- In syira people are threatened by new law to lose the claim to their home and land .
- In the 3 examples we depend on bank company and a government respectively . So we have to trust them , whether we want to or not.
- Cryptographic techniques allows us to no longer be dependent on that one party , but on a neAs long as the majority of that network is fair , everything runs as it should.
- That is what we mean by distributed trust.

- Everything that can be done with a central authority can also be done without that authority.
- Bitcoin and blockchain have the merit of having popularized this idea.
- This is done not mean , how ever the block chain is the only and perfect solution.
- Blockchain is a specific concept that enables distributed trust.

Protocol :

Protocols are rules which govern the functioning of a blockchain. Since Blockchains are a network of computers which operate on a peer-to-peer basis, protocols define how information is transferred between computers on the network.

Blockchains which note all the transactions of a specific crypto token need to be governed by a set of rules. These rules are essentially the heart of the blockchain. It gives an idea to the miners, stakers and the investing community about how exactly the blockchain functions. The rules also help investors identify if the crypto is worth investing in or not.

Protocols also impact network performance and security measures. These are functional building blocks of the blockchain and hence it becomes imperative for one to stay informed about the same. A detailed blockchain protocol list is mentioned below.

What is Blockchain Protocols?

Blockchain protocols are a set of protocols used to govern the blockchain network. The rules define the interface of the network, interaction between the computers, incentives, kind of data, etc. The protocols aim to address the four principles:

1. Security
2. Decentralization
3. Consistency
4. Scalability

- **Security:** Protocols maintain the security of the whole crypto network. Since the network involves the transfer of money so protocols define the structure of data and also secure data from the malicious users.
- **Decentralization:** Blockchain is a decentralized network. There is no involvement of any central authority. So the protocols authorize the whole network.
- **Consistency:** Whenever a transaction occurs, protocols update the whole database at each step so that each user is well versed with the whole crypto network.
- **Scalability:** Scalability means an increase in the number of transactions. Earlier scalability was an issue in the blockchain. But nowadays most protocols handle the issue of an increasing number of transactions in the network and the addition of nodes to the network.

Each and every transaction is verified by the developers and is stored so that each individual can have access to the transaction and protocols helps to maintain this transparency.

How Does Blockchain Protocol Work?

Suppose there is a transaction between two individuals A and B.

- Individual A makes a request to make a transaction. A block for 'A' is created. This block once created cannot be altered. This is done by the blockchain protocol.
- After this, the block is sent to each and everyone in the network. This distribution of blocks across the network is also done by protocols.
- The nodes verify the transaction.
- After the verification, a reward is sent to each node. The sending of incentives is also managed by protocol. Upon successful transaction, the block is added to the list. Protocols update the database. The updated database is distributed across the network by the protocols so that each user has access to the summary of the whole network.
- After this the transaction is complete.
- So there is the involvement of protocols at each step for a secured transaction. Therefore the whole crypto network is secured, scalable and consistent.

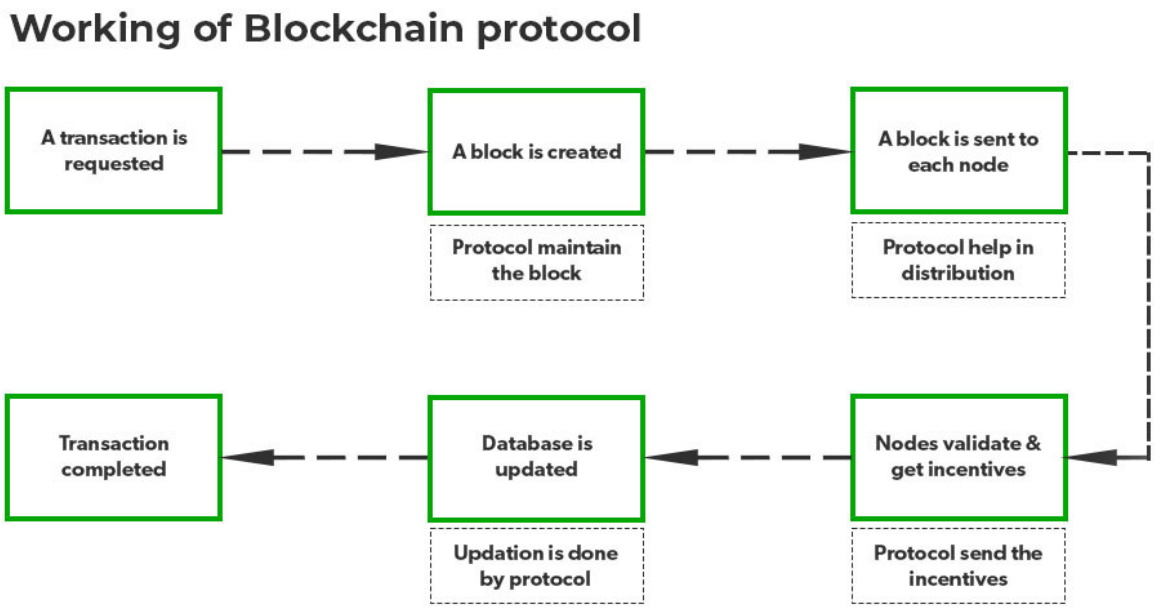


Fig : Working of Block Chain Protocol

Why is blockchain protocol important to crypto?

Blockchain protocols serve as the backbone of cryptocurrency. Cryptocurrency is an encrypted string of data that has some monetary value.

- Protocols are crucial components that facilitate the transfer of data in a secured manner. In the blockchain, there is no involvement of government, central authority, or middleman. So to govern the whole network a set of rules is required.
- Protocols help to establish the whole structure so that the digital money is exchanged securely.
- Blockchain protocols allow users to manage the data. Nowadays many crypto networks allow users to have digital wallets.
- The services such as transactions and payment for all services are handled by protocols.
- Many protocols allow individuals to make financial transactions without the involvement of banks.
- They also allow for preventing double-spending.

Blockchains are evolving day by day and the protocols are also evolving at a rapid rate. Every sector, including supply chain, health, finance, etc, is using a protocol-based blockchain solution.

Main Types of Blockchain Protocols

Below are some of the types of blockchain protocols: Basically , there are 5 types of Block Chain Protocols .

1. Hyper Ledger
2. Quorum
3. Corda
4. Enterprise Etherum
5. MultiChain

1. Hyperledger: Hyperledger is an open-source framework that is developed by Linux. It helps the enterprises to provide blockchain solutions, and how to create a secured blockchain protocol. It was developed in the year 2015. It enables international business transactions. It supports Python and there are many libraries that help in software development. The main aim is to provide universal guidelines for Blockchain implementation.

Advantages:

- It provides enhanced services because of the tools and presence of a large number of libraries.
- It is open-source hence anyone can contribute.
- It helps in international transactions.

Disadvantages:

- There is a lack of use cases as well as skilled programmers.
- It is not a network fault-tolerant.

2. Quorum: Quorum is another enterprise blockchain protocol that aims to address the problems related to finance. It is open source project associated with Ethereum. It was developed by JP Morgan. It can change how financial enterprises function and implement blockchain. It is open-source and nowadays has become one of the best enterprise blockchain frameworks.

Advantages:

- It has the ability to solve any financial query
- It is an open-source framework
- It provides better performance and provides an enhanced experience of transaction

Disadvantages:

- Lack of scalability
- Lack of security and privacy

3. Corda: Corda is an enterprise protocol. It is handled by the R3 banking consortium. This protocol is useful in the field of banking and financial organizations. It utilizes consensus algorithms to maintain transparency and security. It is also an open-source framework. It allows for the building of interoperable blockchain networks with strict privacy.

Advantages:

- It provides enhanced security.
- It is stable and scalable

Disadvantages:

- It is not very flexible as only parties involved in the transaction can take part in the decision.

4. Enterprise Ethereum: Ethereum is one of the public blockchain suite protocols. It defines the platform for decentralized applications. It is the blockchain of choice for developers and enterprises, who are creating technology based upon it to change the way many industries operate. However, for private permissioned networks, enterprise Ethereum is used. It is mostly used for privacy, scalability, and improved performance

Advantages:

- It is an enhanced version of Ethereum and hence supports more privacy.
- It is scalable.

Disadvantages:

- It is volatile and has high transaction fees.
- It is prone to online hacking.

5. Multichain: Multichain is an open-source and was established for private blockchain networks. It was developed to help profit-making corporations. It allows to set up of a private blockchain network. It is a private company that offers API for Blockchain development. It is a cross-chain router protocol. It allows users to swap tokens between different blockchains using a bridge.

Advantages:

- It helps to establish private blockchains that can be used by certain organizations.
- Multichain allows customizing rules for tokens, transaction control, etc.

Disadvantages:

- It does not support smart contracts.

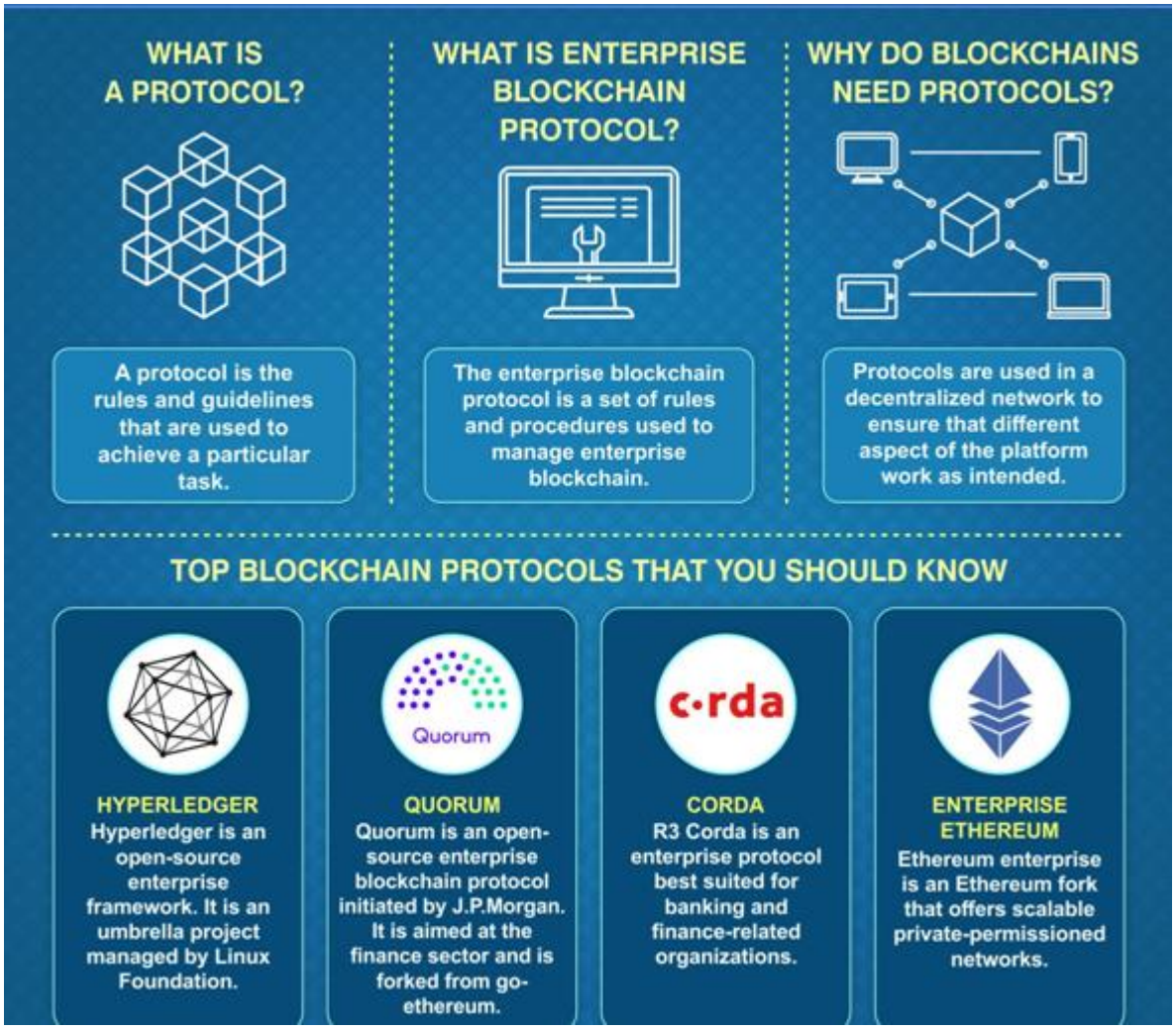


Fig : Classification of Block Chain Protocol

Currency :

Currency is a medium of exchange for goods and services. In short, it's money, in the form of paper and coins, usually issued by a government and generally accepted at its face value as a method of payment.

Currency is the primary medium of exchange in the modern world, having long ago replaced bartering as a means of trading goods and services.

In the 21st century, a new form of currency has entered the vocabulary and realm of exchange: the virtual currency, also known as cryptocurrency. Virtual currencies, such as Bitcoin and Ethereum, have no physical form or government backing in the United States. They are traded and stored electronically.

KEY POINTS

- Currency is a generally accepted form of payment usually issued by a government and circulated within its jurisdiction.
- The value of any currency fluctuates constantly in relation to other currencies.
- Currency is a tangible form of money, which is an intangible system of value.
- Many countries accept the U.S. dollar for payment, while others peg their currency value directly to the U.S. dollar.
- Cryptocurrency is a 21st century innovation and exists only electronically.

Understanding Currency

Currency in some form has been in use for at least 3,000 years. At one time only in the form of coins, currency proved to be crucial to facilitating trade across continents.

A key characteristic of modern currency is that it is worthless in itself. That is, bills are pieces of paper rather than coins made of gold, silver, or bronze.

The concept of using paper as a currency may have been developed in China as early as 1000 BC, but the acceptance of a piece of paper in return for something of real value took a long time to

catch on. Modern currencies are issued on paper in various denominations, with fractional issues in the form of coins.

Money vs. Currency

The terms money and currency are often thought to mean the same thing. However, while related, they have different meanings.

Money is a broader term that refers to an intangible system of value that makes the exchange of goods and services possible, now and in the future. Currency is simply one, tangible form of money.

Money is used in a variety of ways, all related to its future use in some kind of transaction. For example, money is a store of value. This means that it has and maintains a certain value that supports ongoing exchanges. People know that the money they received today essentially will have the same value next week when they need to make a purchase or pay a bill.

Money is also referred to as a unit of account. That means it can be used to account for changes in the value of items over time. Businesses use money as a unit of account when they prepare a budget or give assets a value. Profits and losses are established and relied upon using money as a unit of account.

Money also has certain properties that allow for the smooth exchange of goods:

- It is fungible, or, exchangeable, so that it doesn't need to be re-valued for every transaction.
- It is durable so that it lasts for many exchanges over time.
- It is convenient to carry and divide.
- It is recognizable so that people can trust it and confidently complete their exchanges of goods and services.
- The supply of money should be stable so that its value is reliable.

Understanding what money is clarifies the meaning of currency. It's a form of money used every day by people all over the world. Checks are another form of money (known as money

substitutes). Cigarettes have even been a form of money, as they were for soldiers during the Second World War.

Types of Currency

The United States Mint defines currency as money in the form of paper and coins that's used as a medium of exchange.Currencies are created and distributed by individual countries around the world.

U.S. currency in paper form is issued by the Bureau of Engraving and Printing as $1, $2, $5, $10, $20, $50, and $100 bills. The $500, $1,000, $5,000, and $10,000 bills are no longer issued but those still in circulation are redeemable at full face value. Currency issued in 1861 or earlier is no longer valid and would not be redeemable at full face value.

U.S. currency in the form of coins is issued by the Mint in denominations of 1¢, 5¢, 10¢, 25¢, 50¢, and $1.

There are over 200 national currencies currently in circulation.8 Including the U.S., 42 countries either use the U.S. dollar or peg their currencies directly to the dollar.9 According to the International Monetary Fund (IMF) the dollar makes up 58.8% of the foreign exchange reserves.

Most countries issue their own currencies. For example, Switzerland's official currency is the Swiss franc, and Japan's is the yen.1112 An exception is the euro, which has been adopted by most countries that are members of the European Union.

Some countries accept the U.S. dollar as legal tender in addition to their own currencies, like the Bahamas, Zimbabwe, and Panama.8 For some time after the founding of the U.S. Mint in 1792, Americans continued to use Spanish coins because they were heavier and presumably felt more valuable.

There are also branded currencies, like airline and credit card points and Disney Dollars. These are issued by companies and are used only to pay for the products and services to which they are tied.

Currency Trading

The exchange rate is the current value of any currency relative to another currency. As a result, rates are quoted for currency pairs, such as the EUR/USD (euro to U.S. dollar). Exchange rates fluctuate constantly in response to economic and political events.

These fluctuations create the market for currency trading. The foreign exchange market where these trades are conducted is one of the world's largest markets, based on sheer volume. All trades are in large volumes, with a standard minimum lot of 100,000.15 Most currency traders are professionals investing for themselves or for institutional clients that include banks and large corporations.

The foreign exchange market has no physical address. Trading is entirely electronic and goes on 24 hours a day to accommodate traders in every time zone.

For the rest of us, currency exchange typically is done at an airport kiosk or a bank before we go on a trip or while traveling.

Consumer advocates say that travelers get the best value by exchanging cash at a bank or at an in-network ATM. Other options may have higher fees and unattractive exchange rates.

What Does Currency Mean?

The term currency refers to the tangible form of money that is paper bills and coins. It's used as a medium of exchange that's accepted at face value for products and services as well as for savings and the payment of debt.

What's an Example of Currency?

One example of currency is any of the U.S. paper bills you may have on hand. It is any of the coins the U.S. issues, such as the penny, nickel, and quarter. Currency can also be the paper bills and coins issued by the governments of other countries across the globe.

What's the Difference Between Money and Currency?

Money is an intangible system of value that provides the means for the ongoing exchange of goods and services in a society. Money has taken many forms since it overtook the system of bartering. Currency is a tangible form of it. So, instead of, say, bartering agricultural produce for the clothing you may need, you can use currency (paper notes and coins) to obtain it.

Cryptocurrency

A cryptocurrency is not a type of currency that can be used in the real world. It can be used to perform transactions only in the digital world. So in order to buy/sell using a cryptocurrency, it has to be converted from a digital form to some existing currency that is used in the real world. For example, Dollars, Rupees, etc. Cryptocurrencies don't have a central issuing authority instead using a decentralized system to record transactions and issue new units.

What is Cryptocurrency?

Cryptocurrency is a digital payment system that does not rely on banks to verify transactions. Cryptocurrency payments exist purely as digital entries to an online database. When cryptocurrency funds are transferred, the transactions are recorded in a public ledger.

- In cryptocurrency, "coins" (which are publicly agreed on records of ownership) are generated or produced by "miners".
- These miners are people who run programs on ASIC (Application Specific Integrated Circuit) devices made specifically to solve proof-of-work puzzles.
- The work behind mining coins gives them value, while the scarcity of coins and demand for them causes their value to fluctuate.
- Cryptocurrencies can be used for buying goods just like fiat currency.
- Cryptocurrencies use encryption to verify and protect transactions.
- It does not exist in physical form and is not typically issued by any central authority.
- They use decentralized control in contrast to central bank digital currency.

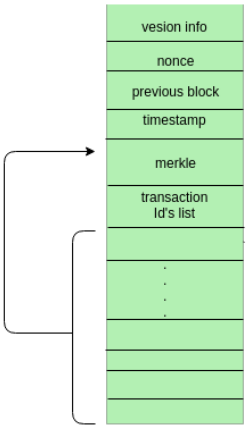
Cryptocurrency Examples

Some of the best-known cryptocurrencies are:

1. **Bitcoin:** Bitcoin is the most widely accepted cryptocurrency. Founded in 2009 by Satoshi Nakamoto, it is still the most commonly traded. It is a decentralized digital currency that can be transferred on a peer-to-peer bitcoin network.
2. **Ether:** Ether is the native cryptocurrency of the Ethereum blockchain network. Each Ethereum account has an ETH balance and may send ETH to any other account. The smallest subunit of Ether is known as Wei.
3. **Litecoin:** Litecoin is a peer-to-peer cryptocurrency and in technical terms, Litecoin is nearly identical to Bitcoin. It uses scrypt in its proof-of-work algorithm. It is an adaptation of Bitcoin that is intended to make payment easier.
4. **Stablecoins:** These are the class of cryptocurrencies whose values are designed to stay stable relative to real-world assets like the U.S. Dollar.
5. **Solana:** Solana is a competitor of Ethereum whose main emphasis is on speed and cost-effectiveness.

Cryptocurrency Working vs Fiat Currency Working

There are two things that make cryptocurrency working and fiat currency working different: Transactions and the Consensus protocol. A block in a Blockchain has the following structure:



As we can see, a block contains multiple transactions at a time in the transaction's id_list.

1. Transactions: The transactions performed in the crypto world are very different than those that of which are performed in the real world. Let's consider that Alice wants to buy a Bicycle.

- **Real-world:** In the real world Alice can pay in any available currency. The seller will return the change if any to Alice.
- **Crypto world:** Suppose the bicycle costs 0.6 BTC and Alice has 0.7 BTC in the Bitcoin Wallet. Alice has to consider the whole amount i.e 0.7 BTC
    - **Transaction 1:** Transfer only 0.6 BTC from Bitcoin wallet to the seller's wallet. Now, Alice has already exhausted 0.6 out of 0.7 BTC. The remaining 0.1 BTC has to be transferred back to Alice's wallet. There is no change in BTC being offered by the seller to Alice.
    - **Transaction 2:** Alice offers 0.1 BTC back to herself. So 0.1 BTC is an unspent transaction amount in Alice's wallet.

2. Consensus protocol: Consensus decision-making is a group decision-making process in which group members develop, and agree to support a decision in the best interest of the whole. Basically, it states that the longest valid chain in the Blockchain network should exist on every node in the Network.

How Does Cryptocurrency Works?

Cryptocurrencies are not regulated or controlled by any central authority hence cryptocurrency works outside the banking system using different types of coins.

1. Mining: Cryptocurrencies are generated through the process called Mining. In this process, the miners are required to solve a mathematical puzzle over a specially equipped computer system to be rewarded with bitcoins in exchange.

2. Buying, selling, and storing: Users can buy cryptocurrencies from central exchanges, brokers, or individual currency owners and sell crypto to them. Cryptocurrencies can be stored in wallets.

3. Investing: Cryptocurrencies can be transferred from one digital wallet to another. Cryptocurrencies can be used for the following purposes:

- Buying goods and services.
- Trade-in them.
- Exchange them for cash.

How To Buy Cryptocurrency?

There are three steps involved in buying a cryptocurrency:

1. Choosing a platform: There are two platforms available to choose from:

- **Traditional Brokers:** There are online brokers who offer to buy and sell cryptocurrencies along with stocks, bonds, etc, but they offer lower trading costs and fewer crypto features.
- **Cryptocurrency exchanges:** Different types of cryptocurrency exchanges are available to choose from with different cryptocurrencies, wallet storage, etc.

2. Funding your account: After choosing the platform, the next step is to fund the account. Most crypto exchanges allow users to purchase cryptocurrencies using fiat currency like U.S. Dollar, the Euro, or using Credit and Debit cards, but this varies from platform to platform. An important factor to consider here is the fees that include the potential deposit and withdrawal transaction fees plus the trading fees.

3. Placing an order: The order can be placed via exchanges or broker's web or mobile platform.

- Select the Buy option.
- Choose the order type.
- Enter the amount of cryptocurrencies.
- Confirm the order.

A similar process needs to be followed for selling cryptocurrencies.

There are also other ways to invest in crypto : These include payment services like PayPal, Cash App, and Venmo, which allow users to buy, sell, or hold cryptocurrencies. In addition, there are the following investment vehicles:

- **Bitcoin trusts:** You can buy shares of Bitcoin trusts with a regular brokerage account. These vehicles give retail investors exposure to crypto through the stock market.
- **Bitcoin mutual funds:** There are Bitcoin ETFs and Bitcoin mutual funds to choose from.

- **Blockchain stocks or ETFs:** You can also indirectly invest in crypto through blockchain companies that specialize in the technology behind crypto and crypto transactions. Alternatively, you can buy stocks or ETFs of companies that use blockchain technology.

How To Store Cryptocurrency

Once the cryptocurrency is purchased, it needs to be stored safely to protect it from hackers. The usual place to store cryptocurrency is crypto wallets which can be physical devices or online software. Not all exchanges or brokers provide crypto wallet services. The cryptocurrencies can be stored in these four places:

1. **Custodial Wallet:** In this approach, a third party such as a crypto exchange stores the cryptocurrency either through cold storage or hot storage, or a combination of the two. This is the most simplest and convenient method for the users as it requires less work on the user part.
2. **Cold Wallet:** These are also known as Hardware wallets. It is an offline wallet in which hardware connects to the computer and stores the cryptocurrency. The device connects to the internet at the time of sending and receiving cryptocurrency but other than that the cryptos are safely stored offline.
3. **Hot Wallet:** These are the applications that store cryptocurrencies online. These are available as desktop or mobile apps.
4. **Paper Wallet:** This is also known as a physical wallet. It is a printout of the public and private keys available as a string of characters or scannable QR codes. To send crypto scan the public and private keys and crypto will be received using the public keys.

Overall, cryptocurrencies offer a range of features that make them a unique and innovative form of digital currency. However, they also come with potential risks and challenges that users must be aware of before investing in or using them.

	Custodial Wallet	Cold Wallet	Hot Wallet	Paper Wallet
Definition	Third-party such as the crypto exchange store the cryptocurrency.	The hardware connects to the computer and stores the cryptocurrency.	Applications that store cryptocurrencies online	Physical storage of public and private keys.
Advantage	• Simple and convenient method. • Easy to access. • No worry about losing your crypto wallet.	• Highest level of security.	• Gives control over crypto. • Almost always free. • Easy to use.	• Maximum security at the lowest possible cost.
Disadvantage	The security risk of leaving crypto in third-party's possession.	• The process is slower compared to when storing crypto online. • Cost of device.	Risk of being hacked.	• Less user-friendly. • Risk of losing a wallet.

What Can You Do With Cryptocurrency

Here are some of the examples:

- **Shopping:** Some luxury retailers like Rolex and Patek Philippe accept cryptocurrency as a form of payment.
- **Insurance:** Some insurance companies like Premier Shield insurance accept Bitcoin for premium payments.
- **Gift:** Cryptocurrency can be a great gift for persons who want to learn and invest in new technology.
- **Travel:** As crypto is not tied to a specific country, thus traveling with crypto can save a lot on money exchange fees.

Advantages of Cryptocurrencies

The following are some of the advantages of cryptocurrencies:

1. **Private and Secure: Blockchain** technology ensures user anonymity and at the same time the use of cryptography in blockchain makes the network secure for working with cryptocurrencies.
2. **Decentralized, Immutable, and Transparent:** The entire blockchain network works on the principle of shared ownership where there is no single regulating authority and the data is available to all the permissioned members on the network and is tamper-proof.

3. **Inflation Hedge:** Cryptocurrencies are a good means of investing in times of inflation as they are limited in supply and there is a cap on mining any type of cryptocurrency.
4. **Faster Settlement:** Payments for most cryptocurrencies settle in seconds or minutes. Wire transfers at banks can cost more and often take three to five business days to settle.
5. **Easy Transactions:** Crypto transactions can be done more easily, in a private manner in comparison to bank transactions. using a simple smartphone and a cryptocurrency wallet, anyone can send or receive a variety of cryptocurrencies.

Disadvantages of Cryptocurrencies

The following are some of the drawbacks of cryptocurrencies:

1. **Cybersecurity issues:** Cryptocurrencies will be subject to cyber security breaches and may fall into the hands of hackers. Mitigating this will require continuous maintenance of security infrastructure.
2. **Price Volatility:** Cryptocurrencies are highly volatile in terms of price as they have no underlying value and there is a supply-demand-like equation that is used to determine the price of cryptocurrencies.
3. **Scalability:** Scalability is one of the major concerns with cryptocurrencies. Digital coins and tokens adoption is increasing rapidly but owing to the sluggish nature of the blockchain makes cryptocurrencies prone to transaction delays. Cryptocurrencies cannot compete with the number of transactions that payment giants like VISA, and Mastercard processes in a day.
4. **Less awareness:** Cryptocurrency is still a new concept for the people and the long-term sustainability of cryptocurrencies remains to be seen.

Features of cryptocurrencies:

Decentralization: Cryptocurrencies are decentralized, meaning they operate on a peer-to-peer network and are not controlled by a central authority or government.

Security: Cryptocurrencies use cryptographic techniques to ensure the security and integrity of transactions and to protect against fraud and hacking.

Transparency: Most cryptocurrencies operate on a public ledger called a blockchain, which allows anyone to see all transactions that have occurred on the network.

Anonymity: While most cryptocurrencies are not completely anonymous, they do offer a high degree of privacy and can allow users to transact without revealing their identity.

Limited Supply: Cryptocurrencies are designed with a limited supply to maintain their value and prevent inflation.

Global Accessibility: Cryptocurrencies can be accessed and used from anywhere in the world, as long as there is an internet connection.

Low Transaction Fees: Compared to traditional banking and financial institutions, cryptocurrencies generally have lower transaction fees, making them an attractive option for international transactions.

Programmability: Some cryptocurrencies allow for programmable transactions, meaning that they can be programmed to execute automatically based on certain conditions.

However, there are also some potential drawbacks to cryptocurrencies, including:

Volatility: Cryptocurrencies can be highly volatile, with prices fluctuating rapidly and unpredictably.

Lack of Regulation: Cryptocurrencies are not yet fully regulated by governments, which can lead to uncertainty and potential risk for users.

Limited Acceptance: While the number of merchants accepting cryptocurrencies is growing, they are still not widely accepted as a form of payment.

Hacking and Fraud: Cryptocurrencies are vulnerable to hacking and fraud, and there have been numerous high-profile incidents of theft and scams in the cryptocurrency world.

Crowdfunding

The Crowdfunding platform in block-chain makes different possibilities for the startups by raising the funds to create their own digital currency and it is peer-to-peer fund raising model some of the famous crowdfunding cryptocurrencies are coinspace, swarm, judobaby etc. Crowdfunding has offers for creators and other consumers. Anyone can participate in this crowdfunding if they have invented any new cryptocurrency (e.g., Ethereum) and also can contribute as much as they want.

How does BlockChain support Crowdfunding ?

There are several areas where block-chain supports and improves crowdfunding, crowdfunding platforms powered by blockchain technology removes the need for intermediate third party.

- **Decentralization:** Since block-chain is decentralized it doesn't rely on any other platforms to create funds. for starters, no longer to be obliged to any rules and any project can get visibility and funded if the investors think to invest, eliminates fees which makes crowdfunding less expensive for the creators.
- **Access Equity:** To provide investors equity or ownership block-chain relies on asset tokenization. For example, a person who plans to create multiple new products with the incoming funds and grant small ownerships stake in the company.This could potentially open whole new world of opportunity.
- **Universal Opportunity:** Any project using a block-chain-based crowdfunding model can get funded. Any person with an internet connection can contribute projects.
- **Flexible Options:** Using block-chain as asset tokenization grants creators and entrepreneurs more liberties.usually asset tokens have their own currency to enable organizations to hire professionals and advertisers.
- **Peer-to-Peer:** The cryptocurrencies are exchangeable on a peer to peer network.This usually help the people for their investment which even generates more interest in the entire process.