Introduction to Blockchain & DLT – 2

Table of contents	
1	Introduction
2	What is Blockchain Technology
3	What are Blockchain Protocols
4	Why are Blockchain Protocols Required
5	Blockchain Architecture
6	Blockchain Consensus
7	Participants of Blockchain Network

Introduction

The present century is all about technology. Today, with the increasing urge for innovation, people are open to accepting various new technologies. Blockchain is one such revolutionary technology that is envisioned to be as impactful as the internet. It is set to revolutionize not just the finance or healthcare industry but many other industries, businesses, government, and even our personal lives.

To assure the accuracy of digital information, Stuart Haber and Scott Stornetta created blockchain technology in 1991. This technology was intended to timestamp digital documents so that they could not be tampered with. They employed cryptographic techniques in a chain of blocks to secure digital documents from data tampering. However, it went unused until it was adopted by Satoshi Nakamoto in 2009 to create a digital cryptocurrency called Bitcoin.

The main hypothesis is that the blockchain establishes a system of creating a distributed consensus in the digital information world. This allows participating entities to know for certain that a digital event happened by creating an immutable record in a distributed ledger. Thus, it has gained a lot of traction in recent years due to its features like transparency, immutability, decentralization, and traceability. From enterprises to startups, banks, and governments, everyone is interested in understanding how blockchain can bring a paradigm shift in their work.

In this chapter, we will cover the basics of Blockchain technology, its origins, its key technological features, and its different potential applications.

What Is a Blockchain Technology?

A blockchain is a secure, decentralized digital database of transactions that is maintained by a network of computers that is responsible for recording transactions and tracking the movement of digital assets inside its network. Each one of these computers called a node, stores a copy of the blockchain database (also called a digital ledger). Any new entries to this digital ledger must be first agreed upon before being added to the blockchain. Each block in the network is securely linked to the one before and after it and remains in place even if the digital asset changes hands. Neither the order of the blocks nor the blocks themselves can be altered, making

the data contained irreversible, unchangeable, and essentially immune to tampering. Once added, a new version of the digital ledger is sent to all nodes.

What are Blockchain Protocols?

Blockchain protocols are the underlying rules, guidelines, and algorithms that define and control the functioning of a blockchain network. These protocols determine how data is stored, transmitted, and validated across the network, ensuring the data's security, consistency, and reliability. Blockchain protocols can vary significantly depending on the specific use case and the desired properties of the network, such as public, private, or permissioned access.

Why are Protocols required?

Blockchain's decentralized nature is the basic tenet of the technology. This implies that there is a lack of centralized control. Protocols are applied to make it function as intended. Peers or nodes must be linked and maintain a copy of the ledger because there is no centralized commodity. The network also employs a consensus technique to verify transactions into blocks. Once constructed, these blocks cannot be altered. The protocols are used for all of this. It serves as a general rule.

Blockchain Architecture

Blockchain gets its name due to its architecture: data is stored in 'blocks' connected in a 'chain'. Blocks are data structures within the blockchain database, where transaction data in a cryptocurrency blockchain are permanently recorded. A block records some or all recent transactions not yet validated by the network. Once the data are validated, the block is closed. Then, a new block is created for new transactions to be entered into and validated. A block is thus a permanent store of records that, once written, cannot be modified, or removed.

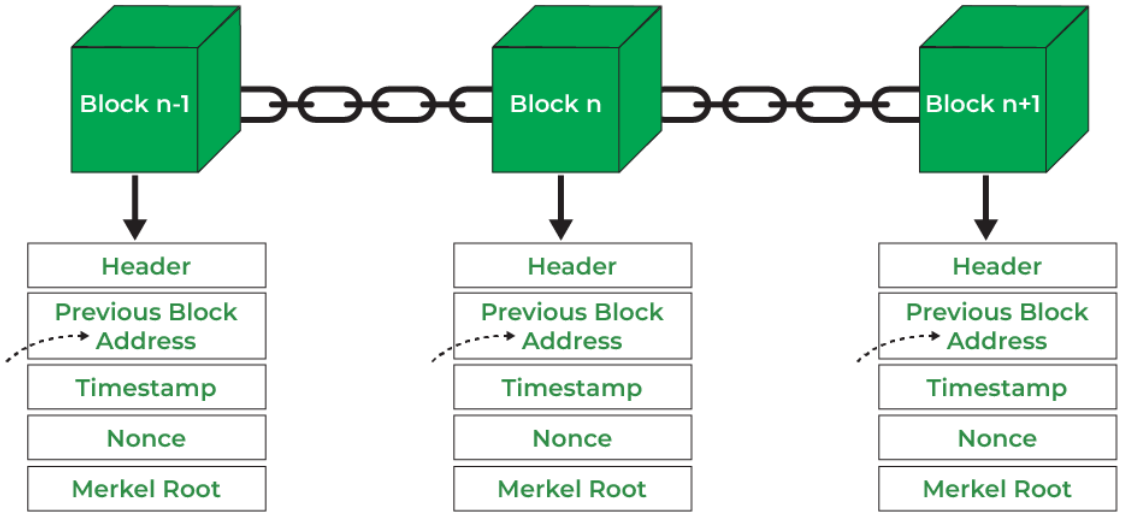


Illustration: Architecture of a Blockchain

Header: It is used to identify the block in the entire blockchain. It handles all blocks in the blockchain. A block header is hashed periodically by miners by changing the nonce value as part of regular mining activity, also Three sets of block metadata are contained in the block header.

Previous Block Address/ Hash: It connects the i+1 block to the" i" block using the hash. In short, it is a reference to the hash of the previous (parent) block in the chain.

Timestamp: It is a system that verifies the data into the block and assigns a time or date of creation for digital documents. The timestamp is a string of characters that uniquely identifies the document or event and indicates when it was created.

Nonce: A nonce number that is used only once. It is a central part of the proof of work in the block. It is compared to the live target if it is smaller or equal to the current target. People who mine, test, and eliminate many Nonce per second until they find that Valuable Nonce is valid.

Merkel Root: It is a type of data structure frame of different blocks of data. A Merkle Tree stores all the transactions in a block by producing a digital fingerprint of the entire transaction. It allows the users to verify whether a transaction can be included in a block or not.

Blockchain Consensus

Consensus is a method of reaching an agreement and it is a form of how nodes on the network can resolve various network-related issues. Consensus is one of the core priorities of a blockchain because, without it, thousands of nodes can never agree. These models exist to create fairness and equality among all the participants. However, there is no one way to reach a consensus within a system. There are lots of algorithms that various blockchain platforms use. Every single one of them works differently and comes with its own set of flaws. The ones that are currently in use are as follows:

- **Proof of Work:** It is one of the popular and first consensus algorithms introduced in the blockchain. Here, nodes are called miners, and they will solve complex mathematical issues with help from their device's computational power to verify the blocks.
- **Proof of Stake:** Proof of stake allows you to take part in the consensus in terms of how many coins you staked in the network. If you have more coins, your possibility of mining a block will increase.
- **Delayed Proof of Work:** Here, some notary nodes will add up data from one blockchain platform to another and secure the power of hashing. Both blockchain networks may use PoS or PoW to reach a consensus.
- **Delegated Proof of Stake:** In this one, there's a concept of delegates and witnesses. Each node is chosen using voting. Witnesses on the platform are responsible for validating the transactions. On the other hand, delegates can change the parameters of the system. Anyhow, all the nodes taking part in consensus will get paid.
- **Leased Proof of Stake:** In leased proof of stake, the smallholders can take part in consensus. As the previous PoS would not let them stake their coins in the network, it creates an unfair environment. That is why LPoS offers more fair ground.

- **Proof of Stake Velocity:** Proof of stake velocity offers an extra incentive to keep the users from staking into the network. Here, one can earn more if somebody maintains an active wallet. This means the users who are not active quite often would not get the extra payment for validating a block.
- **Proof of Elapsed Time:** All the nodes have to wait for a certain amount of time before they can participate in consensus. The time limit is chosen randomly. Thus, one can only create a block when they finish the wait time. There is no way to bypass it, as the system tracks if the node waited or not.
- **Practical Byzantine Fault Tolerance:** Practical Byzantine Fault Tolerance gets rid of the compromised node issue. So, before any node can harm the network, it assumes the possibility of failure. The system gets information from other nodes as soon as a node is compromised to dismiss that node.
- **Simplified Byzantine Fault Tolerance:** Here, the transactions are validated in a batch. More so, the block generator collects all the transactions groups them accordingly, and then gets them into one block. A validator then must validate the whole block to verify the transactions.
- **Delegated Byzantine Fault Tolerance:** Here, the leader of the nodes is called a delegate, and it has limited power. If the leader tries to manipulate the network, another delegate will replace that node. More so, other nodes can disagree with the delegate and can change their leader accordingly.
- **Federated Byzantine Agreement:** Here, all the general nodes get their separate blockchain to run. And before any node can request a transaction, that node needs to be verified and known from the start. Also, here, a node can choose who to trust on the network.
- **Proof of Activity:** It is a combination of PoW and PoS Here, the miner's pre-mine a block template rather than a complete one. Later, a validator validates the remaining block. The more stake a validator has in the network, the more valid his/her validation would be.
- **Proof of Authority:** Here, the nodes participating in consensus will stake their reputation. The validating nodes are selected based on their true identities. Additionally, the validators must invest money and their reputation to earn their place on the platform.
- **Proof of Reputation:** It is quite like Proof of Authority; however, a validator needs to have a good reputation to participate in the consensus. More so, if they try to cheat the network, they will face severe consequences.
- **Proof of History:** Here, the system creates significant events on the network. A node then can validate the transaction based on whether the transaction happened before or after that event.
- **Proof of Importance:** Here, the blockchain works keeping a score of importance. The more coins a user has, the higher his/her score will be. Once they are eligible for participation, they can harvest a block. Additionally, if someone harvests more, their importance score will increase.
- **Proof of Capacity:** Users would use their available hard drive capacity to select mining rights instead of using computational power. So, the larger one's hard drive would be, the more he /she can validate blocks.

- **Proof of Burn:** Here, the blockchain works by burning coins to keep the network stable. So, the users would send some of their coins to an eater address and burn them so that they can participate in consensus.
- **Proof of Weight:** Instead of only relying on how many coins one has staked; the system takes other factors into account to weigh in. So, even if one has fewer coins, he/she may still get to participate in consensus.

Participants of Blockchain Network

Each blockchain network has various participants, who play different roles, in its functioning. They are:

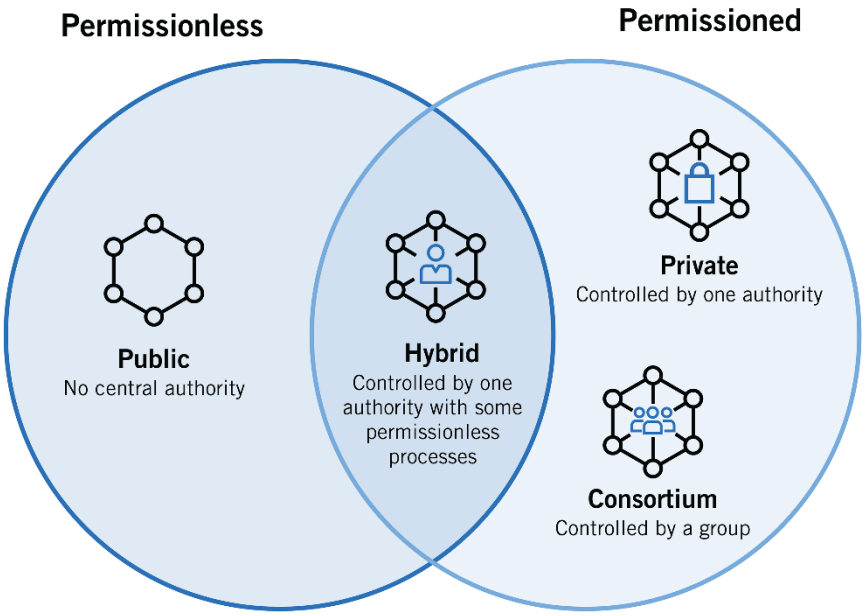
- **Blockchain users**. Participants (typically business users) with permissions to join the blockchain network and conduct transactions with other network participants.
- **Regulators**. Blockchain users with special permissions to oversee the transactions happening within the network.
- **Blockchain network operators**. Individuals who have special permissions and authority to define, create, manage, and monitor the blockchain network.
- **Certificate authorities**. Individuals who issue and manage the different types of certificates required to run a permissioned blockchain.

Types of Blockchain

The evolution of decentralized networks has led to the development of different types of blockchain technology. In this blog post, we are going to explore the different types of blockchains there are, including those listed below:

- Public blockchain
- Private blockchain
- Consortium blockchain or federated blockchain, and;

- Hybrid blockchain



The broader goal of any project creator can also influence the kinds of blockchain technology to adopt. If there is a need to rollout cryptocurrencies, a public blockchain may come in handy and if the ultimate goal is to keep a part of the data open while another part is kept private, then a hybrid blockchain is ideal.

1. Public Blockchain

The first of the different blockchains we would be talking about is the public or permissionless blockchain networks. Public blockchains are one of the most popular and they are the foundational frameworks for digital currencies like Bitcoin, Ethereum, Lite coin, and many other altcoins.

In a public blockchain, anyone can join to make the network operational by conducting transactions and joining the group of validators. Leveraging the web or internet connection, anyone from anywhere can contribute to the management of the network. In a public blockchain, each participant can be a node operator and keeps a copy of the transactions that take place on the network.

Public blockchains have a decentralized form of governance and the verification of transactions follows a predefined consensus. There is a diverse type of consensus that is used for transaction validation in the public blockchain space and these include but are not limited to; Proof of work (PoW), Proof of Stake (PoS), and Proof of space and time. All great towards immutability.

The proof-of-work model involves the solving of complex mathematical computations before transactions are registered within the block, it is energy-intensive and is relatively being replaced by the proof-of-stake method featuring the verification of transactions by validators. These validators usually have a stake in the blockchain network, authorizing them to contribute effectively to the management of the network.

Public blockchain networks usually incentives participation, and guarantee a high level of security due to the spread of the network participants. Should the node operators, miners, or validators not be motivated enough to work, the public blockchain network will become non-functional and can cause network collapse.

- **Advantages of public blockchains**
  A public blockchain network has no restrictive access and is free for anyone to join and participate. While there may be hardware requirements for participants, there are no defined limitations as to who can contribute to the network growth. With all hands on deck in ensuring the optimal functionality of public blockchains, trust becomes a default standard. No one individual can manipulate the entire network.
  The incentivization model based on the consensus protocol as highlighted earlier makes network participants give their all to contributing to the blockchain. This enhances the efficiency of the system. In all, public blockchain networks are very secure as one point of attack cannot lead to the collapse of the entire system.

- **Disadvantages of public blockchains**
  Slower transaction speed and the lack of scalability tops the list of disadvantages public blockchain network suffers. The presence of numerous participants, many of whom must follow the consensus process to validate transactions usually brings about delays. Since there are no restrictions to the number of participants who can join the network, the blockchain may attain a saturation point where the number may begin to work against the platform.
  The energy usage of the PoW blockchain model also makes the entire innovation a source of concern to environmentalists and climate advocates.

- **Use cases of public blockchains**
  The most common use case for public blockchains is mining and exchanging cryptocurrencies like Bitcoin. However, it can also be used for creating a fixed record with an auditable chain of custody, such as electronic notarization of affidavits and public records of property ownership. This type of blockchain is ideal for organizations that are built on transparency and trust, such as social support groups or non-governmental organizations. Because of the public nature of the network, private businesses will likely want to steer clear.

2. Private Blockchain

Private Blockchain is designed to operate in a more restricted or closed manner. Private blockchains thrive under a permissioned model in which access to transactions and validations of entries is restrictive. Private Blockchain is usually more centralized when compared to public blockchain networks.

Private Blockchain is ideal for an organization that wants to leverage the technology to revamp its internal operations. The organization defines the accessibility requirements to the network, who can conduct transactions as well as who can validate the transactions that take place on-chain. Private Blockchain is also ideal for a group of businesses that share similar data in their day-to-day activities. The same way they are used for IoT applications (Internet of Things).

Many may point to the centralization of control as a point of weakness for the private blockchain, however, this does not negate its infrastructural security. Just like others, permissioned blockchain networks are encrypted and feature a high level of data cryptography making them less prone to attacks compared to traditional distributed ledger technologies or digital databases.

Tokenization may or may not be an integral part of running a private blockchain, as incentivization may not be necessary, or typically takes other forms. Some popular examples of a private blockchain network are owned by Ripple Labs and BurstIQ amongst others.

- **Advantages of private blockchains**
  In a private blockchain platform, fewer people managing the system makes the verification of transactions very fast. Public blockchains are known to attain consensus relatively faster than public blockchains. Scalability in a private blockchain network also comes with no hassles as the number of validators does not necessarily have to increase. This implies that the network speed remains the same and the number of validators may remain constant.
  The drudgery in decision-making per ecosystem evolution which always follows a defined process in a public blockchain is eliminated in private blockchains. All these contribute to the increased efficiency of the system.

- **Disadvantages of private blockchains**
  Decentralization is one of the hallmarks of every distributed ledger technology and the fact that a central authority makes the final decision in a private blockchain goes against this fundamental tenet. Based on this, private blockchains are neither as trusted as their public alternatives, neither are they as transparent.
  A bad decision from the controlling authority may adversely impact the entire system. This makes the security provisions of private blockchains not as strong as other types of blockchain networks.
  The same is true for applications from service providers like IBM. Blockchain as a service is completely contrary to the open-source initiative that blockchain is all about.

- **Use cases of private blockchains**
  The speed of private blockchains makes them ideal for cases where the blockchain needs to be cryptographically secure but the controlling entity doesn't want the information to be accessed by the public.
  "For example, companies may choose to take advantage of blockchain technology while not giving up their competitive advantage to third parties. They can use private blockchains for trade secret management, for auditing," Godefroy said.
  Other use cases for private blockchain include supply chain management, asset ownership, and internal voting.

3. Consortium Blockchain/ Federated Blockchain

Just as the name suggests, a consortium blockchain is such that is managed by two or more individuals, associations, companies, or business outfits. Based on its composition, we can say that a consortium blockchain is a semi-decentralized network in which both public and private blockchain features are inherent. This way, certain data are opened to all the participating members while others are restricted.

Consortium blockchains are also known as federated blockchains in which the consensus mechanism is attained based on a predefined number of nodes. It should be noted that the fact that consortium blockchains have a public element does not mean it is less of a decentralized network. No single organizations call the shots as all the participating organizations help maintain the trust upon which the network operates.

In all Federated blockchain networks, every node or participating entity can initiate and receive a transaction, while also being empowered to be able to validate transactions in a broader sense.

Consortium blockchains bring to life the typical features of a private blockchain while leveraging the security infusion of a public blockchain.

Consortium blockchains are majorly seen in Hyperledger Fabric, Corda, and Quorum amongst others.

- **Advantages of Consortium blockchains**
  Consortium blockchains offer several advantages to firms that operate on them. The blockchain attains greater efficiency by combining the features of both private and blockchains. The private parts of the network can easily be taken advantage of to introduce some uniquely tailored features for all participants.
  Just like private blockchains, federated blockchains are highly scalable, and are well secured taking note of the benefits offered by their decentralized nature. Per this latter point, consortium blockchains utilize the combined hash power being supplied by each public node. Access control is enhanced as with a defined consensus or governance model, the network can thrive and work for all.

- **Disadvantages of Consortium blockchains**
  The risk of onboarding different participants can predispose the network. This is of concern as at least one of the key nodes may be the subject of an attack or malicious action, compromising the entire network. The use of Consortium blockchains may also imply working on a fulcrum as government regulations or any form of inconsistency on the part of any of the participating members can offset the system.
  Sharing the features of public blockchains does not imply that it is as secure. Federated blockchain networks still present a few points of weakness for security breaches that is if any can be pulled off.

- **Use cases of Consortium blockchains**
  Banking and payments are two uses for this type of blockchain. Different banks can band together and form a consortium, deciding which nodes will validate the transactions. Research organizations can create a similar model, as can organizations that want to track food. It's ideal for supply chains, particularly food and medicine applications.
  While these are the four main types of blockchain, there are also consensus algorithms to consider. In addition to PoW and PoS, anyone planning to set up a network will also want to consider the other types, available on different platforms like Wave and Burstcoin. For example, leased proof of stake allows users to earn money from mining, without the node needing to mine itself. Proof of importance uses both balance and transactions to assign significance to each user.
  Ultimately, blockchain technology is becoming more popular and rapidly gaining enterprise support. Every one of these types of blockchain has potential applications that can improve trust and transparency and create a better record of transactions.

4. Hybrid Blockchain

A hybrid blockchain also utilizes the combined features of private and public blockchain networks. At first glance, hybrid blockchains maintain a huge similarity with consortium blockchains but the difference between both is striking. Unlike consortium blockchains with multiple participants collectively helping to maintain the network, a hybrid blockchain can have a single entity network administrator.

Hybrid blockchains work best when an organization needs some of its data open access and others kept private for in-house use. The multichain model of hybrid blockchain can give room to a lot of

allowances, as defined by the owner of the system. Transparency can be open or closed depending on how the rules are set.

The decentralization model in hybrid blockchains is partial, as against that of consortium blockchains in which all participants take full control of the network. Hybrid blockchains allow businesses to eat their cakes and have them at the same time. This means they can achieve the transparency they need while also keeping their most important data private.

Incentivization is also another key decision every blockchain project that seeks to utilize the hybrid model must decide on. The decision to roll out incentives depends on the business model and whether such benefits will contribute to the growth of the system.

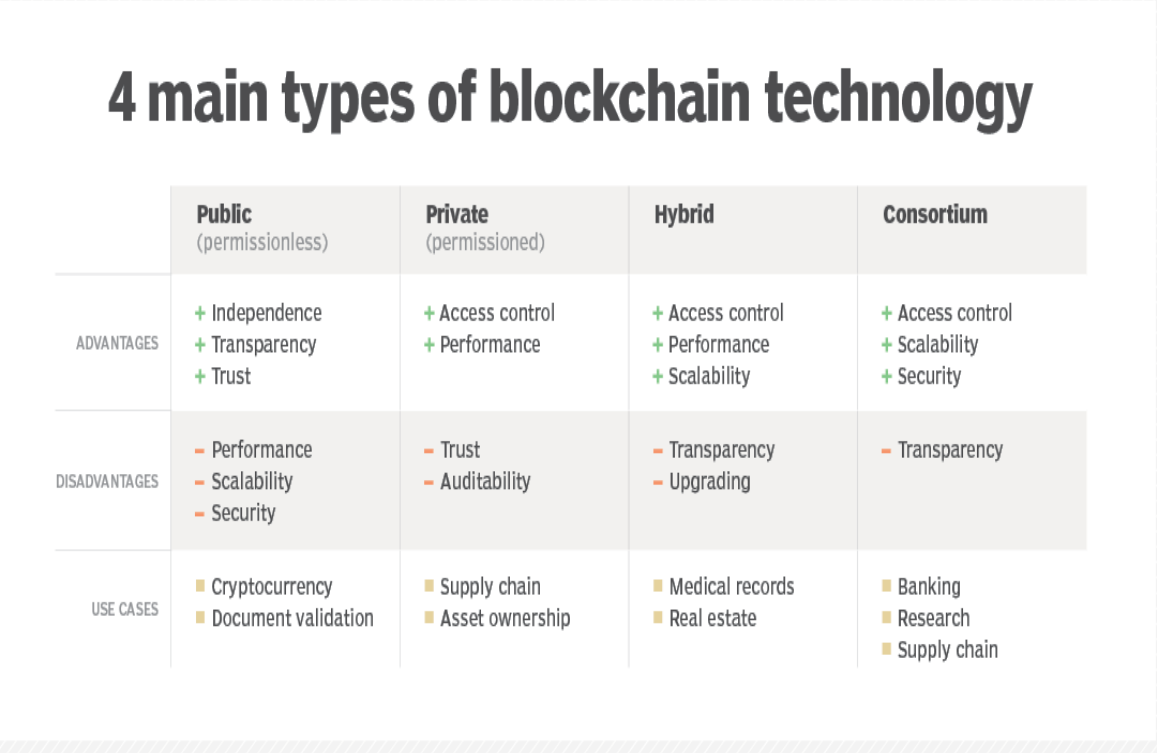
The top examples of hybrid blockchain systems include DragonChain and XinFin's Hybrid blockchain.

- **Advantages of Hybrid blockchains**
  Besides the advantages of hybrid blockchain as described in the features above, these blockchain networks can withstand the popular 51% attacks drawing from their decentralized component. The consensus in hybrid blockchains can be easily modified, or even changed depending on the needs. The ease of scaling a hybrid blockchain is also one of its core benefits.

- **Disadvantages of hybrid blockchains**
  The trust rating is low as control is mostly handled by a central authority. Adopting or switching to a hybrid blockchain system by an organization with a type of distributed ledger system may be a hassle. Should incentives be absent in the system operations, external contributors may not be well motivated to participate in keeping the system operational.

- **Use cases of Hybrid blockchains**
  Hybrid blockchain has several strong use cases, including real estate. Companies can use a hybrid blockchain to run systems privately but show certain information, such as listings, to the public. Retail can also streamline its processes with hybrid blockchain, and highly regulated markets like financial services can also see benefits from using it.
  Medical records can be stored in a hybrid blockchain, according to Godefroy. The record can't be viewed by random third parties, but users can access their information through a smart contract. Governments could also use it to store citizen data privately but share the information securely between institutions.

Comparative Analysis Between Different Types of Blockchain



Criteria to choose types of Blockchain

Choosing the right blockchain platform will not only save you time but also shield you from future business troubles. With the blockchain app development market advancing incredibly, it's crucial to know which one is most suitable for your enterprise. There is a sheer number of blockchain platforms available; this makes it more pressing to make an informed decision while picking one for your business/service/product.

Below is a detailed view of characteristics most innovation leaders and development architects advise considering.

1. **Adoption Rate**
   The adoption rate is nothing but the level of implementation or adoption a particular blockchain technology has received. It is advised to choose technology with a higher adoption rate over one with a poor adoption level. The reason is simple – technology and requirements are changing at a faster pace. This implies that the more embraced a particular technology is, the more assuredly it will be reinforced and advanced shortly.

2. **Programming Language**
   There are multiple variations of programming languages that one can have for blockchain development. Some of the top-picked blockchain programming languages include Solidity, Go, Python, Java, Cadence, and many more.

3. **Transactions per Second**

If a blockchain platform offers a low throughput (transaction speed), the users on the platform will have to pay higher fees to the miners. Considering speed as a parameter is important but it should never be a substitute for low levels of security.

4. **Transaction Cost**
   Cost-effectiveness is another feature to view while selecting a suitable blockchain for your project. While these costs associated are necessary for blockchain, you can take steps to lower the cost or reduce the risk of overpaying as well. You can even select a blockchain that offers a feeless structure.

5. **Consensus Mechanism**
   You will have to choose between Proof of Work (PoW) and Proof of Stack (PoS). Most modern blockchain-based applications are operating on PoS, as it is more energy-efficient. You can look into LPos, DPos, Proof-of-history (PoH), and proof of staked authority (PoSA).

6. **Development Capability**
   You must take into consideration the development know-how of any blockchain platform. Whether you can hire blockchain developers for developing a product/service on the platform? Will it get support from the blockchain community?

7. **Scalability**
   In terms of blockchain, scalability refers to the transaction per second rate of the platform. For instance, bitcoin can perform around 7 transactions in a second, Ethereum (which is more popular among businesses given it offers smart contract support) can handle 20 transactions per second, while Stellar, a payment platform can drive up to 1000 transactions per second.
   So, if you are planning to use blockchain technology for your next product, you must consider the transaction capabilities of the platform before selecting it. For example, a business that is developing a payment gateway utilizing blockchain essentially requires a TPS of more than 7. While those developing an in-house data management platform or something similar would not need a blockchain platform with a higher transaction rate.

8. **Security**
   Security is the aspect of utmost importance especially if the company or organization is dealing with sensitive information. To avoid security breaches and prevent your data from falling into wrong hands, you need to track the security records of all the available platforms and pick the best among them. Platforms such as Bitcoin, Ethereum, Ripple, NEO, EOS, and BUMO are all go-to options with extremely good security records.
9. **Public or Private**
   Blockchain is essentially divided into two categories – centralized and decentralized. In a centralized or private network, a single person controls the network and the access of the information to the users. While, in a decentralized network, anyone can access the information and participate in the network.
   If the system you are planning to develop deals with private information such as sensitive patient data in healthcare systems, then you should go with a private system that is not decentralized. On the other hand, if you want to keep transparency through your platform, then you should put the data on the public blockchain development platform.

10. **Community support**
    You must check how dynamic and available are the developers of the community for the blockchain applications platform of your choice. You can research the same on platforms

like Discord, Reddit, or LinkedIn as well. As you progress along with your blockchain project, you will need a good amount of feedback and support. Also, try and gain an understanding of the availability of supporting developer tools to increase the developer experience.

Notable DLT Platforms:

A. Hyperledger Fabric

What is Hyperledger Fabric?

The Linux Foundation introduced Hyperledger in 2015 to support the growth of the blockchain community. Hyperledger is not just about promoting one standard; it fosters collaboration with multiple efforts.

Hyperledger Fabric, a part of Hyperledger, is an open-source enterprise blockchain project. Like other blockchain networks, it includes smart contracts, ledgers, and protocols to manage transactions.

Unlike typical blockchains, Hyperledger Fabric is permissioned and private. Instead of allowing unknown participants, it has a membership system for permitted ones. This is beneficial for enterprises dealing with privacy issues, helping them maintain integrity and keep competitors out.

Once you understand it, Hyperledger Fabric is flexible, offering options like pluggable features, multiple consensuses, various ledger formats, and Membership Service Providers (MSPs). This flexibility allows users to customize it according to their needs.

It also features channels, allowing participants to create private transactions. This is crucial for companies dealing with sensitive issues, ensuring privacy among participants in the network.

Basic Benefits of Hyperledger Fabric

1. Open-Source:

- Hyperledger Fabric is an open-source platform, meaning anyone can use it freely.
- No need to purchase it, and there are no vendor lock-ins.
- While the source code is free, having programming skills is essential to understand and modify it.
- Allows customization of features to suit specific industry needs.

2. Suitable for Various Industries:

- Hyperledger Fabric is versatile and can be applied to a wide range of industries, including supply chain, banking, Internet of Things, healthcare, government, media, cybersecurity, and more.
- Its permissioned nature makes it adaptable to various environments.

3. Quality Code:

- The Hyperledger Fabric blockchain maintains a focus on quality over quantity.
- All code undergoes careful inspection and rigorous testing before implementation.
- The open-source community actively contributes to refining the codebase, ensuring a high level of quality in Hyperledger Fabric samples.

4. Higher Efficiency:

- Hyperledger Fabric is designed for efficiency compared to other blockchain platforms.
- Its internal structure facilitates high efficiency by assigning different tasks to each node.
- Nodes can process multiple transactions simultaneously without slowing down the system.
- This design minimizes time consumption and accelerates overall functionality.
- Some nodes are dedicated to ledger maintenance or authentication, reducing the burden on transaction processing nodes.

5. Modular Design:

- Hyperledger Fabric boasts a modular structure, enhancing network functionality.
- Users can choose different algorithms for encryption, identity, and consensus, plugging them into the Hyperledger Fabric blockchain.
- This flexibility allows for the use of diverse algorithms, avoiding being limited to a single type.

Hyperledger Fabric Architectural Model Explained

1. **Assets:**
   - In Hyperledger Fabric, assets are things with value, ranging from tangible to intangible items.
   - You can modify assets using chaincode on the network, represented as key-value pairs in JSON or binary form.

2. **Chaincode:**
   - Chaincode is the business logic defining assets and their modifications.
   - It runs separately from transaction orders for enhanced security, enforcing rules for database state changes.
   - Think of chaincode as a smart contract, although the terms are used interchangeably.

3. **Ledger:**
   - The ledger records transaction history in an unchangeable format.
   - Sequenced and tamper-proof; once on the ledger, a transaction's state cannot be altered.
   - Includes read-only queries, access control lists, and configurations for uniform block structures.

4. **Identity:**
   - Hyperledger Fabric is permissioned, requiring identity management.
   - It provides a membership identity service to manage identities, limiting access to the network.
   - Ideal for enterprises safeguarding competitive information.

5. **Confidentiality and Privacy:**
   - Permissioned access ensures confidentiality and privacy.
   - Data restrictions and private transaction facilities are available.
   - While you share the ledger with the network, you can set privileges for specific parties.

6. **Security Protocols:**
   - High-level security protocols protect the network from attacks.
   - Encryption mechanisms safeguard ledger information.
   - Ideal for enterprise companies facing cyber threats.

7. **Consensus:**
   - Hyperledger Fabric's consensus algorithms operate on a Kafka model.
   - Users can set consensus protocols without limitations, allowing multiple consensus mechanisms.
   - Supports BFT-based algorithms, and the new version introduces Raft for crash fault-tolerance.
   - Liveliness ensures non-faulty nodes receive submitted transactions, and safety guarantees consistent state changes for identical transaction sequences.

What's the Process?

Usually, the whole process is split into three parts –

1. **Endorsement**
2. **Ordering**
3. **Validation**

Basically, it follows these steps –

- A client wants to do something.
- The application prepares a request and sends it to specific peers for approval.
- Peers check if the request is valid and if the client is allowed to do it.
- The request, along with details, goes to the smart contract.
- The application checks everything and shares the request with other relevant parties.
- Once everyone agrees, the transaction details go to ordering nodes.
- Ordering nodes organize the transaction details into a block.
- The block is sent to all peers.
- All peers add the block to the chain and update their databases.

Elements of the Ecosystem

1. **Ledger:**
    - The ledger is like a super-organized database where all transactions are stored.
    - Once a transaction is recorded, it can't be changed or tampered with.
    - Everything is in order, making it easy to search for transaction details.
2. **World State:**
    - World state is a database that holds current values of the ledger.
    - You can directly access current values instead of calculating them from logs.
    - Values change frequently based on transactions and smart contract applications.
3. **Block Structure:**
    - Divided into three parts: Block Header, Block Data, and Block Metadata.
    - Block Header has block number, current block hash, and previous block hash.
    - Block Data contains transactions in order.
    - Block Metadata includes time, certification, and more, indicating block validity.
4. **Transaction Structure:**
    - Has five elements: Header, Signature, Proposal, Response, and Endorsement.

- Header includes transaction essentials and chaincode version metadata.
- Signature is crucial for validating the transaction.
- Proposal contains input parameters.
- Response notes before and after states.
- Endorsement includes signs from endorsing peers, based on endorsement policy.

5. **Ordering Service:**
    - Orderer nodes manage the order of transactions.
    - Unlike public blockchains with varied opinions on transaction order, Hyperledger ensures a consistent order through the ordering service.
    - Ledgers don't fork; what peers agree on becomes final after passing through the ordering service.
6. **Private Data:**
    - Organizations can create private channels to keep specific information away from other parties.
    - Only selected members can access information in private channels.
    - Requires an administrative head to manage smart contract versions and policies.
    - Adds an extra layer of security for sensitive information in enterprise settings.

Companies Using Hyperledger Fabric

1. **U.S. Food and Drug Administration (FDA):**
    - Enhances healthcare data security.
    - Empowers patients for independent medical data management.
    - Stores Electronic Medical Records (EMR) and clinical trials securely.
2. **London Stock Exchange Group:**
    - Utilizes Fabric for interoperability, efficiency, and confidentiality in financial services.
    - Promotes secure and private transactions.
3. **Sichuan Hejia Co. Ltd.:**
    - Addresses pharmaceutical sector challenges.

- Collaborates for transparent supply chain management.

4. **ANZ and Westpac:**
    - Digitizes bank guarantee processes.
    - Enhances efficiency, reduces corruption, and ensures proper document verification.
5. **CLS:**
    - Uses Hyperledger Fabric for payment netting solution (CLSNet).
    - Reduces risks, optimizes liquidity, and promotes real-time awareness in foreign exchange.
6. **UBS:**
    - Collaborates for a global trade platform named "Batavia."
    - Empowers organizations, irrespective of size, to enter the trading space transparently.
7. **TenneT Energy Community:**
    - Uses Fabric smart contracts to manage electricity supply insufficiency.
    - Allows households to lend stored electricity for compensation.
8. **Change Healthcare:**
    - Develops "Intelligent Healthcare Network™" using Fabric for claims management.
    - Enhances auditing, development, and tracing of healthcare claims.
9. **Maple Leaf Foods:**
    - Utilizes Fabric for transparent and efficient supply chain management.
    - Aims to reduce losses and enhance transparency in supply chain processes.
10. **Naturipe Farms:**
    - Implements Hyperledger Fabric for tracking blueberries from harvesting to customer hands.
    - Adds QR codes for tracking and ensuring quality of blueberries.
11. **Nestlé:**
    - Works on a food traceability platform with Carrefour using Hyperledger Fabric.
    - Trials for six months to track Mousseline purée production for transparency.

12. **Walmart:**
    - Implements Hyperledger Fabric for tracing food supply chain.
    - Initially tracks mangoes and pork, extends to 25 items, ensuring product authenticity.
13. **Unilever:**
    - Collaborates with IBM to improve digital ad supply chain transparency.
    - Aims to balance ad flows and reduce false advertisements.
14. **Russia's Central Depository:**
    - Sberbank uses Hyperledger Fabric for commercial bond transactions.
    - Enhances transparency and security in large-scale bond transactions.
15. **Banco Bilbao Vizcaya Argentaria and Bank Danamon Indonesia:**
    - IBM collaborates with various financial institutions globally for a transparent payment process.
    - Aims for improved currency flow and transparency in financial transactions.
16. **Rwanda Tantalum Project:**
    - Uses Hyperledger Fabric to ensure purity of tantalum, a rare mineral.
    - Streamlines verification processes, reduces costs, and increases revenue.

B. IOTA (Tangle)

What is IOTA?

The IOTA Tangle stands out as an innovative form of distributed ledger technology (DLT) crafted specifically for the Internet of Things (IoT) landscape. Unlike the traditional blockchain model, IOTA utilizes a novel approach to DLT. Originating from the efforts of the non-profit IOTA Foundation based in Germany, the Tangle addresses the design limitations of conventional blockchain systems, especially concerning applications in the Internet of Things.

The IOTA Tangle caters to the unique demands of an IoT environment, where numerous network-enabled devices, ranging from smart appliances to wearable technology, communicate seamlessly. It was conceived to facilitate micro-transactions within this expanding ecosystem without imposing fees. Offering key features such as high scalability, feeless transactions, and nearly instantaneous transfers, the Tangle serves as a promising solution for the evolving landscape of IoT devices.

Working of IOTA

1. **Directed Acyclic Graph (DAG) Structure:** The IOTA Tangle utilizes a DAG structure rather than a linear blockchain. Each transaction approves two previous transactions, forming a web-like structure. This structure eliminates the need for blocks and miners.

2. **Transaction Validation:** In order to submit a transaction to the Tangle, a user must validate two previous transactions. This validation process adds a level of security and decentralization, as every participant contributes to the network's consensus.

3. **Tip Selection and MCMC:** When a user initiates a transaction, they choose two tips (unconfirmed transactions) to validate. The selection is done through a Markov Chain Monte Carlo (MCMC) algorithm, ensuring a fair and probabilistic choice.

4. **Confirmation:** As more transactions are added to the Tangle, the probability of a transaction being confirmed increases. The network achieves consensus through the cumulative approval of transactions, making the confirmation process more efficient over time.

5. **Removal of Coordinator (Coordinator-Free IOTA):** The IOTA Foundation aims to make the Tangle entirely decentralized by removing the Coordinator. This process involves upgrades and improvements to the network's security and consensus mechanisms.

Advantages of IOTA Tangle:

1. **Scalability:** One of the primary advantages of the IOTA Tangle is its scalability. Traditional blockchain networks face challenges as the number of participants increases, leading to potential congestion. The Tangle, however, becomes more efficient as more participants engage with the network, making it highly scalable.

2. **Feeless Transactions:** Unlike many blockchain networks that involve transaction fees, IOTA Tangle allows feeless transactions. This is particularly advantageous for microtransactions, making it suitable for the Internet of Things (IoT) ecosystem, where countless small transactions may occur.

3. **Decentralization:** IOTA Tangle operates in a decentralized manner. There is no need for miners, and every participant in the network contributes to the validation of transactions. This decentralization enhances security and resilience against attacks.

4. **Fast Confirmation:** Transactions on the Tangle are confirmed at a rapid pace. As more transactions occur, the network's ability to confirm transactions increases, providing near-instantaneous validation.

5. **Quantum-Resistant:** IOTA Tangle has implemented quantum-resistant cryptographic algorithms, making it more robust against potential threats from quantum computers in the future.

Disadvantages of IOTA Tangle:

1. **Security Concerns (in the past):** In the past, there have been security concerns related to IOTA. Vulnerabilities were identified and exploited, leading to the network's temporary shutdown. However, the IOTA Foundation has been actively working to address these issues and enhance the platform's security.

2. **Adoption Challenges:** While IOTA holds great potential, widespread adoption is crucial for its success. Achieving mass adoption can be challenging, especially when dealing with established technologies like traditional blockchains.

3. **Dependency on Coordinator (in the past):** IOTA initially relied on a Coordinator, a centralized entity overseeing the network's security. Critics argued that this contradicted the principles of decentralization. However, the IOTA Foundation has been working on removing the coordinator through network upgrades.

C. Hedera

Until now, we have discussed the closed ecosystem of Hashgraph, its technical workings, and how it claims to be fast, secure, and fair. However, the biggest roadblock to the Hashgraph is its private nature. It is enterprise ready.

Meet Hedera Hashgraph, a Hashgraph network that is public and takes advantage of Hashgraph consensus algorithm. It takes full utilization of asynchronous Byzantine Fault-Tolerant Algorithm(aBFT). It offers guaranteed Byzantine fault-tolerance for replicated state machines.

Hedera Hashgraph establishes its idea on the top of Byzantine-Fault Tolerant (BFT) consensus(aBFT). The improved model will ensure that businesses can bring more value by using Hedera Hashgraph. It is also managed by the Hedera Hashgraph Council. The ultimate goal is to provide public access to Hashgraph capabilities and make the public utilize a secure and fast system for distributed ledger purposes.

Under the hood, both Hashgraph and the Hedera Hashgraph are similar. They both utilize the “gossip about gossip” protocol, which utilizes aBFT agreement to reach consensus. It also uses virtual voting, which means that there is no need for a central authority. It is entirely decentralized and offers a trustless environment for its uses.

The use of aBFT ensures fairness in all conditions — even when the network contains malicious actors. All the properties of Hashgraph are utilized within Hedera Hashgraph. However, to make sure that the Hedera Hashgraph is protected from DDoS attacks, the consensus algorithm doesn’t use the leader format.
With Hedera Hashgraph, you can build on trust. Some of the key applications of Hedera Hashgraph include cryptocurrency, smart contracts, and file services.

Services offered by Hedera Platform

With Hedera platform, you can enable some key services including the following:

- Cryptocurrency: Allows intermediates to use the network for cryptocurrency payments and let them take advantage of lower cost and simple design.
- Smart Contracts: You can also build smart contracts on top of the Hedera platform. To develop smart contracts, you need to use Solidity. As a developer, you can do atomic swaps, create assets, and deploy completely new applications.
- File Services: You can also use the Hedera platform to do file services, i.e., verify files. It is also a GDPR complaint.

Governance

The governance in the Hedera Hashgraph works differently. It can be divided into two tiers – The Governing Board and the Open Consensus.
The Governing Board is a centralized control system which is not an ideal solution for any network that wants to offer its services for the distributed ledger. The community is also not happy with its approach, and it is still one of the most significant criticisms of the Hedera Hashgraph.
The Open Consensus, on the other hand, is the consensus mechanism that we already discussed above. It governs how nodes can join and become part of the network, and also make it more decentralized. To ensure that there is a proper weighted voting model, it utilizes Proof-of-Stake. It ensures that collision is adequately mitigated, and there is also an appropriate incentive for users to run nodes.

Hedra Hashgraph Architecture
Hedra Hashgraph architecture is a three-layered architecture. It consists of the Internet Layer (Bottom), Hashgraph Consensus Layer (Middle), and Services Layer (Top). Let's discuss each layer briefly.

- Internet Layer: The layer takes care of the communication between computers on the internet. It deploys TCP/IP connections with TLS encryption.
- Hashgraph Consensus Layer (Middle): The middle layer contains the nodes which participate in the network. These nodes take part in the consensus method using the Hashgraph consensus algorithm and gossip protocol.
- Services Layer: The topmost layer has their its own subgroups – File Storage, Cryptocurrency, and Hashgraph Smart Contracts.

The nodes earn the cryptocurrency for taking participating in the network. It is a native currency and ensures that the users get their incentive for participating.
The file storage, on the other hand, is Merkle-based. Moreover, if you are a developer, then you can also use Solidity as it is supported by the Hedra. Lastly, it offers smart contract support on the top of the network — giving you the ability to create scalable dApps.

Hedera Hashgraph dApps
There are few top Hedera Hashgraph dApps. They include Sagewise, Hearo.fm, Carbon, Cryptotask and Arbit.

Hedera Hashgraph Tools
There are many awesome Hashgraph tools out there. Few of the notable Hashgraph tools are as follows:

- Hedera Java SDK – SDK in Java for Hedera Hashgraph. It is maintained by Hedera LLC.
- Hedera Rust SDK – SDK in Rust, community-maintained
- Hedera Go SDK – SDK in Go, community-maintained
- Hedera Test – Test Hedera in action
- Hedera Java Keygen tool – A keygen tool used in Hedera Hashgraph for managing ED25519 key pairs. It is a command-line utility.

D. Holochain

What is Holochain?

Holochain is an open-source framework designed for building peer-to-peer networks and applications with a focus on distributed principles. While it shares similarities with blockchain technology, the key distinction lies in their internal workings.

Unlike traditional blockchain systems, which heavily rely on energy-intensive processes like mining, Holochain takes a more sustainable approach. For instance, Bitcoin's Proof-of-Work consensus algorithm demands substantial computational power to solve cryptographic puzzles, leading to significant energy consumption. In contrast, Holochain utilizes the energy-efficient Go programming language, allowing applications to be written in Lisp or JavaScript.

Holochain operates as an agent-centric, energy-efficient ledger system. In this context, each agent possesses a secure ledger copy, enabling independent actions. Agents can interact with other network devices, providing a scalable distributed ledger solution. The technology is overseen by Ceptr, showcasing its commitment to efficiency and sustainability.

Features of Holochain

- **Energy Efficiency:** Holochain addresses the energy consumption issues associated with traditional blockchain platforms, offering a more sustainable and eco-friendly solution.

- **Better Model for Transfer and Storage:** Introduces an improved model for data transfer and storage, enabling edge devices like smartphones to seamlessly integrate into the network, fostering scalability.

- **Holochain Apps:** These distributed applications strike a balance between public and private networks, offering a unique approach within an open-source framework.

- **Uniquely Configurable:** Provides each app with its own network, allowing customization of standards, protocols, consensus algorithms, scalability, latency, throughput, resilience, governance, and privacy.

- **Uniquely Connectable:** Different apps can bridge among themselves using native APIs, ensuring secure and integrated connectivity even when offline or partitioned.

- **Microservices Architecture:** Holochain relies heavily on microservices, making each app a collection of standalone microservices for improved ecosystem and future-proofing.

- **No Need to Learn Different Blockchains:** In an enterprise setup, eliminates the need to learn and use different blockchains, offering an open-source framework for decentralized solutions.

- **Evolvable:** Core dependence on microservices results in an agile and fast development process, allowing for easy evolution of the platform based on changing requirements.

- **Secure:** The architecture ensures app reliability by confining each app to its ecosystem, providing developers with flexibility in setting security restrictions and utilizing cryptography for tamper resistance and data proof-of-authorship.

- **Scalable:** Holochain offers scalability by allowing new apps to join the network and contribute to computing power, leveraging Rust programming language for WebAssembly compilation. The architecture's scalability is also influenced by the local number of peers, ensuring stability with reduced network latency and sensitivity.

How Can You Use Holochain?

Holochain can be used for developing diverse distributed apps. The applications can be created for a wide range of usability. For example, the network is used for social media apps, governance, organization, and so on.

To give you a good idea about its usability, let's go through the list of apps that you can create using Holochain technology.

- Collaborative apps
- Platform-related apps
- Social media apps
- Relationship management apps
- Supply chain-oriented apps
- Resource management apps
- Reputation systems

The wide use-case makes Holochain technology a valid alternative to Ethereum, which is also a dApp platform. It is not the only alternative Distributed Ledger technology (DLT) out there. We also covered Hashgraph which offers a viable alternative DLT solution over the blockchain.

Holochain Architecture

Holochain architecture is interesting — it can be summed up as "shared DHT" where DHT stands for the distributed hash table. It overcomes the blockchain bottlenecks by keeping the key features of blockchain intact.
We can term it as "blockchain without bottlenecks."

It achieves it with the help of Shared Data Integrity. It is a way of handling data in peer-to-peer systems where it is much more challenging to secure data compared to centralized data.

With shared data integrity, it offers robust data security without bringing limitations such as high computation demand.

The key component here is the distributed hash table (DHT), which provides great value to the ecosystem. It offers eventual consistency while ensuring that the data is propagated safely through the network. This way, each peer is accountable for his actions.

The architecture is also efficient as it ensures that the overhead is as feasible as possible. In fact, phones or other devices can join the network and improve computing power.

The Holochain Architecture (dApp architecture) consists of three main sub-systems. They are:

- Shared storage (DHT)
- Application (Nucleus)
- Source Hash Chain