International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 06 | June - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

Hyper Ledger & E-Id Implementation

Harsh Ambaliya
B Tech CSE 8th Sem
Kalinga University
Raipur, Chhattisgarh, India
harshambaliya2334@gmail.com

Khushal Dewangan
B Tech CSE 8th Sem
Kalinga University
Raipur, Chhattisgarh, India
kushaldewangan55665@gmail.com

Abhijeet Singh
B Tech CSE 8th Sem
Kalinga University
Raipur, Chhattisgarh, India
Abhijeettptp5@gmail.com

Omja Shukla
B Tech CSE 8th Sem
Kalinga University
Raipur, Chhattisgarh, India
omja12shukla@gmail.com

Abstract –

Blockchain is a digital ledger used to secure data in a secure manner by chaining encrypted blocks together in a chronological order. Each block in the Blockchain contains a number of transactions, and once a block is added to the Blockchain, it cannot be deleted. Instead of copying or transferring, the digital assests are distributed and decentralized. Blockchain reduces security risks and frauds.Distributed ledger technology, Immutable records, Smart contracts are the key elements of a Blockchain. The most widely known use of Blockchain is in cryptocurrency. These are tokens used as a digital form of cash to buy goods. Bitcoin, Ethereum, Litecoin, Dogecoin are few examples of cryptocurrencies. There are different ways to build a Blockchain network like - Public, Private/Permissioned, Consotrium.The necessary frameworks, standards, tools and libraries to build aBlockchains are provided by Hyper Ledger Fabric. Hyper Ledger Fabric is a permissioned Blockchain platform. It is designed to provide a flexible and modular architecture for building enterprise-grade Blockchain solutions. Fabric uses a unique approach to consensus that allows for greater flexibility and privacy compared to other Blockchain platforms. It also offers a range of features, including smart contract support, permissioned access, and a pluggable architecture that allows for customization and interoperability with other systems. Hyper Ledger Fabric has already been adopted by a number of industry leaders in sectors such as finance, supply chain management, and healthcare. As more companies and organizations see the benefits of using Blockchain technology. There have been discussions about using Blockchain technology to store Aadhaar data. Blockchain can provide a tamper-proof and auditable record of Aadhaar transactions, which can enhance the security and trust of the system. Although, the use of Blockchain for Aadhaar is still in the experimental phase, and further research and development are needed to address the challenges and determine the feasibility of implementing this technology at a larger scale. Implementing an e-ID card system on Hyper Ledger Fabric would require significant technical expertise and resources, but it could provide a secure and efficient way to manage digital identities and enable secure transactions. This would involve several key components and considerations..

Introduction

In the past few years, the world witnessed a clear and significant development in the field of IoT technologies in many different sectors and areas of human activities. Nowadays, technology applications have become the essence of the development and prosperity of peoples and countries across the world and in sensitive services .For example, we find medical doctors rely on advanced technical

Blockchain Technology

Blockchain is a distributed database that is maintained by a network of computers, each of which has a copy of the database. The database is continuously updated with new transactions and each transaction is verified by the network of computers to ensure its authenticity. It stores transactional records of public in several databases in a network connected through peer-to-peer nodes. The database of Blockchain stores data in blocks linked together in a chain. As one cannot modify or delete the chain, the data is chronologically consistent. Blockchain creates a decentralized, temper-proof system to record transactions. The combination of cryptographic algorithms and consensus mechanisms, makes it extremely difficult for an attacker to compromise the network. It is not impossible to hack a Blockchain network, it is highly difficult and requires a significant amount of resources and expertise. In fact, there have been a number of high-profile attacks on Blockchain networks in recent years, including the 51%

attacks on the Ethereum Classic network in 2019 and the Bitcoin Gold network in 2020. A 51% attack, also known as a majority attack, is a type of attack on a Blockchain network where a single entity or group of entities controls the majority of the network's computing power or mining hash rate. This allows them to gain control of the network and potentially execute malicious actions such as double-spending or preventing other transactions from being confirmed. A 51% attack or a majority attack is a type of attack on a Blockchain network where a single entity or group of entities controls the majority of the network's computing power or mining hash rate. This allows them to gain control of the network and potentially execute malicious actions like double-spending or preventing other transactions from being confirmed. Since they control the majority of the network's hash rate, they can mine their own version of the Blockchain faster than the rest of the network, effectively replacing the original version of the Blockchain with their own. This allows them to confirm their own transactions and prevent others from being confirmed, effectively giving them control over the network. These attacks are relatively rare, but they have occurred on several occasions in the past.

The main key features of Blockchain are -

1. Decentralization - The network is made up of a large number of nodes that work together to verify and validate transactions. Every node has the same copy of the ledger. There is no central authority in control.

2. Immutable - To add a transaction to the ledger every node checks the validity of the transaction, without the approval of a majority of nodes no one can add any transaction blocks. Once a transaction is recorded, it cannot be changed or erased.

3. Distributed - All the participants have a copy of the ledger to maintain complete transparency. Public ledger provides all the information about the participants on the network.

4. Secure - Every data on the netwrok has a unique identity that has been hashed cryptographically.

5. Consensus - To reach an agreement quickly and for smooth functioning a decision making algorithm is required. This algorithm is Consensus.

6. Unanimous - It is impossible to add or make any change without the consent of majority of nodes. All the participants have to agree to the validity of the records.
7. Faster Settlement - Blockchain network offers a faster settlement unlike traditional banking system.

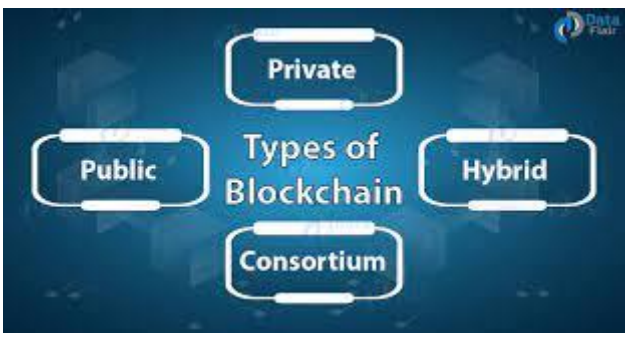
Different types of consensus mechanisms in Blockchain –

1. Proof of Work(PoW)
2. Proof of Stake(PoS)
3. Delegated Proof of Stake(DPoS)
4. Byzantine Fault Tolerance(BFT)
5. Practical Byzantine Fault Tolerance(PBFT)

Application of Blockchain –

Blockchain technology was originally developed for the cryptocurrency Bitcoin, but it has since been applied to a wide range of industries including finance, supply chain management, IoT Mmonitoring, logistics, payments, voting, healthcare etc. The benefits of Blockchain includes increased security, transparency, and efficiency, as well as the ability to reduce costs and eliminate intermediaries.

Types of Blockchain –



Public Blockchain - This is a type of Blockchain that is open to everyone, anyone can join the network and participate in the process. Public Blockchains are typically used for cryptocurrencies and other applications that require transparency and decentralization.

Permissioned Blockchain - This is a type of Blockchain that is used within an organization or a group of organizations. Permissioned Blockchains are typically used for applications that require a high level of security and privacy, such as supply chain management or financial transactions.It usually has additional security measures in place to prevent unauthorized access. They often use consensus mechanisms that are specifically designed to prevent attacks, such as Practical Byzantine Fault Tolerance (PBFT). These consensus mechanisms are designed to prevent malicious activity by requiring nodes to be authorized or by relying on a trusted group of validators.

Consortium Blockchain - This is a type of Blockchain that is controlled by a group of organizations that work together to maintain the network. Consortium Blockchains are typically used for applications that require a high level of trust and collaboration, such as supply chain management or healthcare.

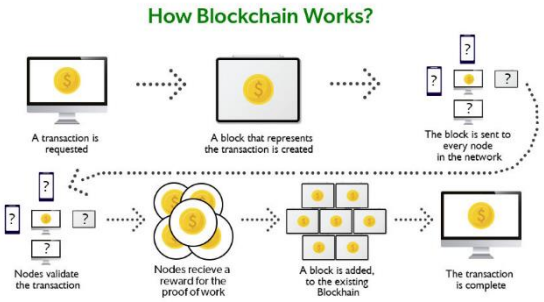
Hyper Ledger Fabric -

Hyper Ledger Fabric is a modular architectural framework that provides confidentiality,validity, adaptability, scalability for distributed ledger applications. It is a permissioned Blockchain platform. Fabric uses a unique approach to consensus that allows for greater flexibility and privacy compared to other Blockchain platforms. It also offers a range of features, including smart contract support, permissioned access, and a pluggable architecture that allows for customization and interoperability with other systems. It is a powerful Blockchain platform that is ideal for enterprise-grade Blockchain solutions.

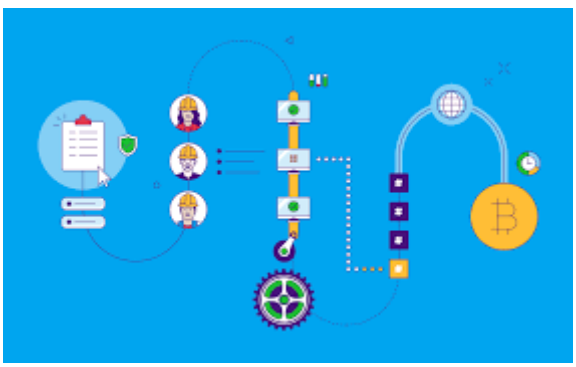
LITERATURE REVIEW -

How does Blockchain work -

There are several types of consensus mechanisms each having different criteria's to reach a global agreement on network. Some of them are -



Proof of Work (PoW) - This is the original consensus mechanism used by Bitcoin and many other cryptocurrencies. It requires miners to solve complex mathematical problems to validate transactions and add new blocks to the Blockchain. The first miner to solve the problem and add the block to the chain is rewarded with newly minted cryptocurrency and transaction fees. This mechanism is highly secure but consumes a lot of energy.These are generally considered to be more secure against attacks, as they require a significant amount of computing power to execute a successful attack. It is currently considered to be the most secure consensus mechanism due to its high computational power requirement and its ability to resist attacks from malicious actors. However, PoW requires a lot of energy consumption to validate transactions and is not environment friendly.



Proof of Stake (PoS) - This is a newer consensus mechanism that requires validators to hold a certain amount of cryptocurrency as a stake to validate

transactions and add new blocks to the Blockchain. This mechanism is more energy-efficient but may be less secure. It may be more vulnerable than PoW to attacks by a malicious actor with a large stake in the network. Due to its ability to reduce energy consumption while maintaining security PoS is becoming increasingly popular.

Delegated Proof of Stake (DPoS) - This is a variant of PoS that allows token holders to delegate their voting rights to other participants who are responsible for validating transactions and adding new blocks to the Blockchain.

Byzantine Fault Tolerance (BFT) - This consensus mechanism is designed for private Blockchains and relies on a predetermined set of validators who are responsible for validating transactions and adding new blocks to the Blockchain. It is highly secure but may be less decentralized than other consensus mechanisms.

Practical Byzantine Fault Tolerance (PBFT) - This consensus mechanism is similar to BFT but is designed for public Blockchains. It requires a predetermined set of validators to reach a consensus on the validity of transactions and blocks.

Versions of Blockchain Technology -

Version 1.0 : Cryptocurrency - The introduction of Cryptocurrency is the first application of Blockchain Technology. It allows two parties to make transactions without the interference of a third party. It was introduced by Hall Finley in 2005.

Version 2.0 : Smart Contract - Due to unscalabity of the first version, new version was introduced in 2008.Smart contract is program that executes, verifies and reduces cost efficiency.

Version 3.0 : DApps - Decentralized Apps(DApps) was introduced after the second version in which the backend code runs on decentralized Peer-To-Peer network and could be called by its frontend which could be written in any language.

New versions and improvements to existing Blockchain technologies are constantly being developed and tested, so the current version of Blockchain technology may vary depending on the specific application and use case.

Hyper Ledger Fabric –

Hyper Ledger Fabric is a modular architectural framework that provides confidentiality,validity, adaptability, scalability for distributed ledger applications. It is a permissioned Blockchain platform. Fabric uses a unique approach to consensus that allows for greater flexibility and privacy compared to other Blockchain platforms. It also offers a range of features, including smart contract support, permissioned access, and a pluggable architecture that allows for customization and interoperability with other systems. It is a powerful Blockchain platform that is ideal for enterprise-grade Blockchain solutions.

Components of Hyper Ledger fabric -

Chaincode - Chaincode in Hyperledger Fabric is the term used to refer to smart contracts or decentralized applications (dApps) that run on the Hyperledger Fabric blockchain network. Chaincode defines the business logic of a blockchain application, enabling it to execute certain actions, access and modify data on the blockchain, and communicate with other applications on the network.

Chaincode is written in programming languages such as Go, JavaScript, or Java, and is deployed onto the Hyperledger Fabric network using Docker containers. Each chaincode has its own unique ID, and multiple chaincodes can be deployed on a single Hyperledger Fabric network.

Once deployed, chaincode can be invoked by other applications on the network, allowing them to access the functionality provided by the chaincode. Chaincode can also interact with other components of the Hyperledger Fabric network, such as the peer nodes, to access and update data on the blockchain.

Hyperledger Fabric uses a modular architecture that allows for the deployment of different types of chaincode, depending on the specific requirements of the application. These include transaction chaincode, which is used to handle transaction processing, and query chaincode, which is used to handle data queries.

Orderer (Ordering service)- In Hyperledger Fabric, the Orderer is a component of the blockchain network responsible for maintaining the order and consistency of transactions. It receives transaction requests from client applications, packages them into blocks, and distributes them to the peers for validation and commitment to the ledger.

The Orderer creates a global sequence of transactions that all participants on the network agree upon, ensuring that transactions are executed in the same order across all nodes. This ensures that the blockchain remains immutable and tamper-proof, as all nodes can agree on the order in which transactions were executed.

Hyperledger Fabric supports multiple types of Orderers, including Solo, Kafka, and Raft. Solo Orderer is a single-node ordering service and is suitable for testing and development purposes only. Kafka and Raft are both distributed ordering services, providing greater scalability, fault tolerance, and availability.

The Orderer is a critical component of the Hyperledger Fabric network, and its failure can lead to significant disruptions in the network's operation. To ensure high availability and fault tolerance, it is recommended to deploy multiple Orderers in the network and use a consensus mechanism such as Raft or Kafka to ensure that the Orderers are always in sync.

Ledger - In Hyperledger Fabric, the ledger is a distributed database that stores all the transactions and state updates that have been validated and committed to the network. The ledger is maintained by the peers in the network and is organized into two main components: the world state and the transaction log.

The world state is a snapshot of the current state of the network, representing the latest values of all assets and variables on the network. It is maintained by the peers using a key-value database, which allows for efficient querying and retrieval of data.

The transaction log, on the other hand, contains a record of all transactions that have been validated and committed to the network. It includes all the data needed to verify the authenticity of the transaction, such as the digital signature of the transaction creator and the hash of the previous block in the chain. The transaction log is maintained by the Orderer, which distributes the transactions to the peers for validation and commitment. Hyperledger Fabric uses a unique approach to maintain the ledger, known as the "separation of duties" model. In this model, the world state is maintained separately from the transaction log, which allows for greater scalability and efficiency. The transaction log only includes the necessary data to validate transactions and ensure their authenticity, while the world state contains the latest state of all assets on the network.

Overall, the ledger is a critical component of the Hyperledger Fabric network, as it provides a tamper-proof record of all transactions and ensures that the network remains transparent and auditable.

Peer Nodes - In Hyperledger Fabric, peer nodes are the nodes that maintain a copy of the ledger and execute transactions on the blockchain network. Peers serve as both clients and servers in the network, enabling them to communicate with other nodes and interact with the ledger.

There are two types of peer nodes in Hyperledger Fabric: endorsing peers and committing peers. Endorsing peers execute the chaincode on incoming transaction proposals and endorse the results. Once a sufficient number of endorsements are obtained, the transaction is considered valid and is passed on to the committing peers for validation and commit to the ledger.

Committing peers receive validated transactions from endorsing peers and update the ledger accordingly. Once the transaction is committed, the new state is added to the world state and propagated to other nodes in the network.
Peers can also participate in the network governance process, such as endorsing new chaincode versions or voting on network configuration changes.

Hyperledger Fabric supports multiple types of peer nodes, including peer nodes with or without chaincode, and anchor peers, which serve as the entry point for other organizations to access the network.

Peers play a critical role in the Hyperledger Fabric network, as they maintain the ledger and execute transactions, ensuring the network's security, transparency, and decentralization.

Clients – In Hyperledger Fabric, clients are the applications or users that interact with the blockchain network to initiate transactions, query data, or monitor the network's activity. Clients interact with the network through APIs provided by the SDKs or command-line tools.

Clients submit transaction proposals to the endorsing peers, which execute the chaincode and return endorsements to the client. The client then collects sufficient endorsements and submits the transaction to the committing peers for validation and commit to the ledger.
Clients can also query the world state of the ledger to retrieve the current value of assets or variables on the network. Querying the world state does not require endorsement from the peers, as the data is already stored in the ledger.

Hyperledger Fabric supports multiple SDKs, including Node.js, Java, and Go, which provide APIs for building client applications. These SDKs abstract the complexity of the underlying blockchain network, enabling developers to focus on building applications that leverage the network's capabilities.

Overall, clients play a critical role in the Hyperledger Fabric network, as they enable users and applications to interact with the network, creating value and driving innovation in various industries.

Membership – Membership in Hyperledger refers to the process of joining the Hyperledger community as a member organization. Hyperledger is an open-source consortium that hosts several blockchain-based projects aimed at developing enterprise-grade distributed ledger technologies. Membership in Hyperledger provides organizations with access to cutting-edge blockchain tools, technologies, and expertise, enabling them to collaborate with other industry players to build robust, secure, and scalable blockchain solutions.

To become a member of Hyperledger, an organization needs to apply and meet certain requirements such as contributing to the community and adhering to the Code of Conduct. There are several levels of membership, each with different benefits and responsibilities. These include General Members, Premier Members, and Associate Members. General members contribute to the development of the projects, Premier members have more influence and access to more resources, and Associate members are typically non-profit organizations that support the Hyperledger community.

Being a member of Hyperledger offers several benefits, including access to educational resources, networking opportunities, and exposure to innovative blockchain projects. Members can also participate in the development of blockchain standards and best practices, helping to shape the future of blockchain technology.

Membership in Hyperledger is the process of joining the open-source consortium that hosts several blockchain-based projects aimed at developing enterprise-grade distributed ledger technologies. To become a member, organizations need to apply and meet certain requirements such as contributing to the community and adhering to the Code of Conduct. Membership offers access to cutting-edge blockchain tools, technologies, and expertise, as well as educational resources, networking opportunities, and exposure to innovative blockchain projects. Members can also participate in the development of blockchain standards and best practices, helping to shape the future of blockchain technology. There are several levels of membership, each with different benefits and responsibilities, including General Members, Premier Members, and Associate Members.

Key features of Hyper Ledger Fabric are – Hyperledger Fabric is an open-source enterprise-grade blockchain platform designed to provide a modular and flexible architecture for building distributed ledger applications. Some of its key features include:

Permissioned Network: Fabric supports a permissioned network model, where only authorized users can access the network and its resources. This ensures confidentiality and security of data.

Modularity: Fabric architecture is modular, which allows developers to customize the platform to meet specific business needs. It provides a pluggable architecture for consensus algorithms, membership services, and smart contract execution engines.

Scalability: Fabric is designed to scale horizontally, which means that new nodes can be added to the network without affecting its performance. It can support a large number of transactions per second and can handle high volumes of data.

Privacy: Fabric supports confidentiality by allowing transactions to be visible only to authorized parties. This is achieved through the use of private channels, where transactions are only visible to the participants of the channel.

Smart Contracts: Fabric supports smart contracts or chaincode, which are programs that can automate business logic and execute on the blockchain. It supports multiple programming languages such as Go, Java, and Node.js.

Endorsement policies: Fabric allows the network to define endorsement policies that govern the approval of transactions. This ensures that only authorized parties can endorse and commit transactions.

Flexibility: Fabric allows the creation of multiple channels, each with its own set of rules and policies. This allows organizations to maintain their privacy while still being part of the larger network.

Consensus: Fabric supports multiple consensus algorithms, including Kafka, Raft, and PBFT. This provides flexibility in choosing the consensus algorithm that best suits the use case.

Modular architecture - Modular architecture is a key feature of Hyperledger, the open-source consortium that hosts several blockchain-based projects aimed at developing enterprise-grade distributed ledger technologies. Modular architecture refers to the ability to break down complex systems into smaller, more manageable components or modules that can be developed, tested, and deployed independently. In the context of Hyperledger, this means that each project is designed to be modular, allowing developers to mix and match different modules to create custom blockchain solutions that meet their specific needs. This modular approach provides greater flexibility, scalability, and interoperability, enabling organizations to build and deploy blockchain-based applications more quickly and efficiently. Furthermore, the modular architecture ensures that each project can be updated, maintained, and improved independently, without affecting other components of the system.

Privacy and confidentiality - Hyperledger Fabric provides privacy and confidentiality through mechanisms such as private data, private channels, endorsement policies, identity management, encryption, and anonymous transactions. These features ensure that sensitive data is kept secure and accessible only to authorized parties.

Scalability – Hyperledger achieves scalability through modular architecture, consensus mechanisms, smart contract frameworks, and sharding. These features allow the network to handle an increasing number of transactions and users while maintaining performance, security, and data privacy.

Permissioned access – Permissioned access control is a key feature of Hyperledger blockchain networks that provides varying levels of access to different network participants. Here are some key points regarding permission access in Hyperledger:

Hyperledger blockchain networks use a permissioned model, meaning that only authorized network participants can access and participate in the network.

Access controls are enforced through a membership service provider (MSP) that manages identity and access for network participants.

MSPs issue digital certificates to network participants, which are used to authenticate and authorize transactions on the network.

Hyperledger also supports role-based access control (RBAC), which allows network administrators to define roles and assign permissions to different participants based on their roles.

With Hyperledger Fabric, access control can be defined at various levels of the network, such as the channel level, the chaincode level, and the transaction level, providing granular control over who can access and participate in different aspects of the network.

Hyperledger Sawtooth also provides access control mechanisms, including transaction family permissions,

which allow for the granular control of permissions for specific transaction types.

Overall, permission access control is a critical feature of Hyperledger blockchain networks that ensures the security and integrity of the network by limiting access to authorized participants only.

Benefits -

Permissioned Network - A permissioned Blockchain is a distributed ledger that is not publicly accessible. It can only be accessed by users with permissions. The users can only perform specific actions granted to them by the ledger administrators and are required to identify themselves through certificates or other digital means.

One might consider the addition of permissioned users as an extra Blockchain security system. Administrators maintain an access control layer to allow certain actions to be performed only by certain identifiable participants. Records are kept within the Blockchain of who is involved in the transactions. This makes permissioned Blockchains different from public Blockchains.

Confidential Transactions - Confidential Transactions keep the amount and type of assets transferred visible only to participants in the transaction, while still cryptographically guaranteeing that no more coins can be spent than are available.

This goes a step beyond the usual privacy offered by Bitcoin's Blockchain, which relies purely on pseudonymous (but public) identities. This matters, because insufficient financial privacy can have serious security and privacy implications for both commercial and personal transactions. Without adequate protection, thieves can focus their efforts on high-value targets, competitors can learn business details, and negotiating positions can be undermined.

Pluggable Architecture - When it comes to Hyper Ledger Fabric or parity, their consensus algorithms are pluggable. What does it mean to be pluggable? When a structure is pluggable, it is simple to add another implementations that does the same kind of work. Thus, Hyper Ledger Fabric supports a variety of consensus algorithms such as Solo, Kafka, and upcoming algorithm, SBFT(Simplified Byzantine Fault Tolerance). Even Parity can operate things, such as PoA, Tendermint, on a private network, excluding the PoW, which is for the public network.

Easy to get started

Hyper Ledger Fabric is a permissioned, open-source Blockchain platform that is designed for enterprises and business use cases. Here are some of the benefits of using Hyper Ledger Fabric:

Privacy and Security: Hyper Ledger Fabric uses a permissioned network, which means that participants need to be authorized to access the network. This ensures that data and transactions are secure and private, and only authorized participants can access them.

Modular Architecture: Hyper ledger Fabric has a modular architecture that allows for flexibility in designing and developing Blockchain solutions. This enables developers to customize the Blockchain to meet specific business requirements.

High Performance: Hyper Ledger Fabric has been designed with high-performance in mind, making it suitable for enterprise use cases. It can handle hundreds of transactions per second, making it much faster than other Blockchain platforms.

Smart Contract Support: Hyper Ledger Fabric supports smart contracts, which are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. Smart contracts can automate complex business processes, reducing the need for intermediaries and increasing efficiency.

Interoperability: Hyper Ledger Fabric is designed to be interoperable with other systems and technologies. This means that it can work with existing enterprise systems, allowing for easy integration with other business processes.

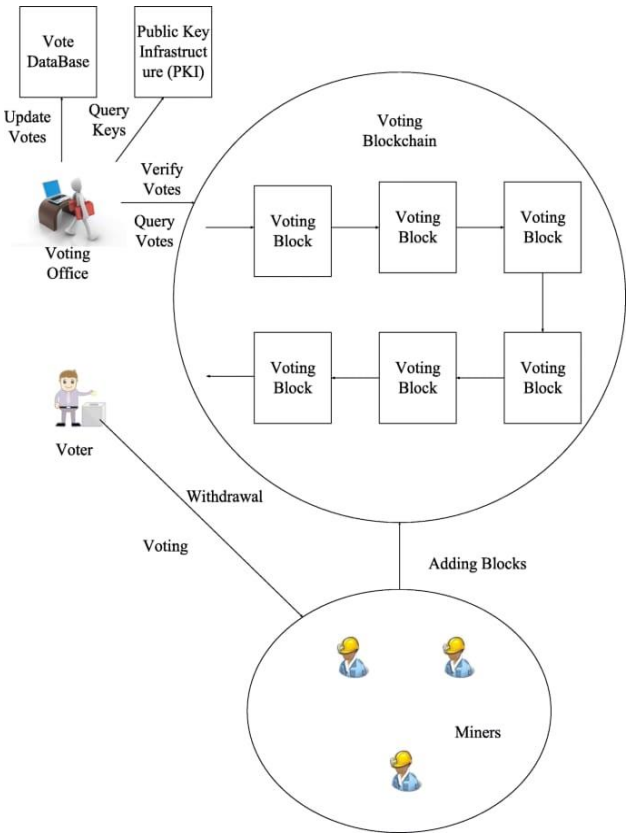
Overall, Hyper Ledger Fabric provides a secure, high-performance, and flexible Blockchain platform that is suitable for enterprise use cases. Its modular architecture and support for smart contracts make it ideal for developing customized Blockchain solutions that meet specific requirments.

There are several factors that suggest Hyper Ledger Fabric will continue to grow and widely adopted in the coming years:

Continuous development and improvement Increased adoption by industry leaders Interoperability with other systems Advancements in related technologies

Aadhar on Blockchain -

Aadhaar is a unique identification number issued by the Indian government to its citizens. Using Blockchain Technology to secure data would be quite benificial as Blockchain provides a secure platform to store data which is highly difficult to hack. Although, there are many challenges in this initiative such as **:**



The issue of privacy- Not every citizen would be comfortaable with sharing their data in a public Blockchain.

Technical feasibility- Transferring all the data to a Blockchain system would require significant technical expertise and infrastructure.

Implementation of e-id card on Hyper Ledger fabric –

White
Implementation of e Id card on Hyper Ledger fabric

Implementing an eID card system on Hyperledger Fabric involves several steps. Hyperledger Fabric is an open-source, permissioned blockchain framework that provides a platform for building distributed applications with a focus on privacy, security, and scalability. Here's an overview of the steps involved in implementing an eID card system on Hyperledger Fabric:

Define the eID Card System Requirements: Begin by defining the requirements of the eID card system, including the data that needs to be stored on the blockchain, the privacy and security requirements, and the user interface for interacting with the system.

Design the Data Model: Next, design the data model that will be used to store the eID card information on the Hyperledger Fabric blockchain. This may include defining the structure of the eID card data, such as personal information, biometric data, and authentication keys.

Create the Smart Contracts: Develop smart contracts using Hyperledger Fabric's Chaincode programming model. Smart contracts define the business logic that governs the behavior of the eID card system, such as how data is stored, verified, and updated on the blockchain.

Set Up the Hyperledger Fabric Network: Set up the Hyperledger Fabric network, which includes creating and configuring the necessary components such as peers, orderers, and channels. Configure the network to meet the privacy and security requirements of the eID card system.

Develop the User Interface: Develop a user interface for interacting with the eID card system. This may include designing and implementing web or mobile applications for users to register, authenticate, and access their eID card information on the Hyperledger Fabric blockchain.

Implement Authentication and Authorization: Implement authentication and authorization

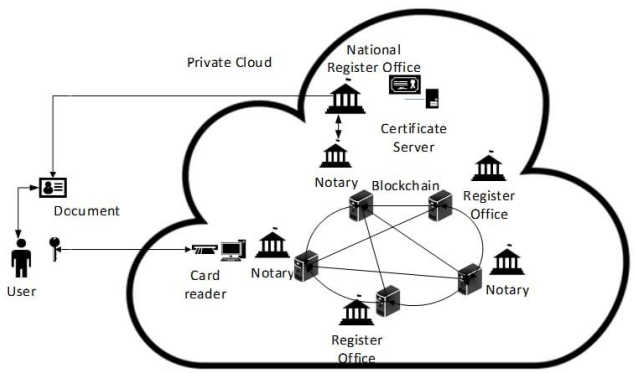
mechanisms to ensure that only authorized users can access and modify the eID card data on the Hyperledger Fabric blockchain. This may involve integrating with external identity providers or implementing custom authentication and authorization logic within the smart contracts.

Test and Deploy the System: Test the eID card system thoroughly to ensure its functionality, security, and performance. Once the system is ready, deploy it on the Hyperledger Fabric network and make it available for production use.

Monitor and Maintain the System: Set up monitoring and maintenance processes to ensure the ongoing operation and security of the eID card system on Hyperledger Fabric. Regularly update and improve the system based on user feedback and changing requirements.

Implementing an eID card system on Hyperledger Fabric requires a solid understanding of blockchain concepts, smart contract development, and system integration. It's important to follow best practices for security, privacy, and data protection to ensure the integrity and confidentiality of the eID card information stored on the blockchain.

The implementation of an e-ID card system on Hyper Ledger Fabric involves following steps –



1. Designing the system
2. Developing smart contracts
3. Building the network
4. Integrating with external systems
5. Testing and deployment

References :-

[1] https://www.investopedia.com/terms/p/permissioned-blockchains.asp (permissioned network)

[2] https://elementsproject.org/features/confidential-transactions (Confidential transaction)

[3] https://medium.com/codechain/codechain-core-pluggable-architecture-network-extension-b29ef51f8b (Pluggable Architecture)

[4] https://data-flair.training/blogs/types-of-blockchain/

[5] https://blogs.iadb.org/caribbean-dev-trends/en/blockchain-technology-explained-and-what-it-could-mean-for-the-caribbean/