A

Project Report On

“Hyperledger for Public Data Management: Connecting Identities and Streamlining Updates”

Submitted in Partial Fulfilment of the Requirements for the Degree of

### Bachelor of Technology

### in

### **Computer Science and Information Technology**

*by*

Mr . Chinmay Pawar 2010005

Mr . Malik Mujawar 2010008

Mr . Swaroop Mane 2010015

Mr . Samrat Mali 2010018

Under The Guidance Of

### **Prof. A. C. Adamuthe**



### Department of Information Technology

K.E. Society’s

Rajarambapu Institute of Technology, Rajaramnagar

(An Empowered Autonomous Institute, Affiliated to Shivaji University, Kolhapur)

2023-2024

**CERTIFICATE**

This is to certify that Mr. Chinmay Pawar, Mr. Malik Mujawar, Mr. Swaroop Mane, Mr. Samrat Mali has successfully completed the project work and submitted project report on “Hyperledger for Public Data Management: Connecting Identities and Streamlining Updates” for the partial fulfillment of the requirement for the degree of **Bachelor of Technology** in **Computer Science & Information Technology** at **Rajarambapu Institute of Technology, Rajaramnagar, Dist: Sangli**. This final report is the record of the students work carried out under my supervision and guidance.

Prof. P. N. Jadhav Dr. A. C. Adamuthe Dr. P.V. Kadole

### **Project Guide Head IT Dept. Director**

### **Name and Sign of External Examiner: -**

Date:

Place: RIT, Rajaramnagar.

**DECLARATION**

We declare that this report reflects our thoughts about the subject in our own words. We have sufficiently cited and referenced the original sources, referred or considered in this work. We have not misrepresented or fabricated or falsified any idea/data/fact/source in this submission. We understand that any violation of the above will be cause for disciplinary action by the Institute.

| Sr. No. | Student Name | Roll No | Signature |
| --- | --- | --- | --- |
|  | Chinmay Pawar | 2010005 |  |
| 2. | Malik Mujawar | 2010008 |  |
| 3. | Swaroop Mane | 2010015 |  |
| 4. | Samrat Mali | 2010018 |  |

Date:

Place: RIT, Rajaramnagar.

**ACKNOWLEDGEMENT**

We take this opportunity to express our gratitude to the people who have been instrumental in the successful completion of this project. We would like to show our highest appreciation to **Dr. A. C. Adamuthe**. We can't say thank you enough for his tremendous support and help. We feel motivated and encouraged, without whose guidance this project would not have been materialized.

The guidance and support received from all the members who contributed and who are contributing to this project were vital for the success of the project. We are grateful for their constant support and help. We are also thankful to **Dr. A. C. Adamuthe (Head of Department) and Prof. Mrs. P. N. Jadhav (Project Coordinator) and** Mr. Pranav Shinde (Blockchain Researcher B.Tech IT) for providing us facilities to work in, without which this work would not have been possible.

In addition, the very energetic and competitive atmosphere of the Information Technology Department had much to do with this work. We acknowledge with thanks to the faculty, teaching and non-teaching staff of the department, Central library, and colleagues.

Place: RIT, Rajaramnagar

Date:

**ABSTRACT**

Traditional government document management systems often suffer from several shortcomings such as lack of transparency, data inconsistency, and limited accessibility. These shortcomings can cause significant problems, such as fraudulent activities, inefficient and slow processes, and difficulty in ensuring the accuracy of the data. In traditional document management systems, there are multiple copies of the same document maintained by different departments, which can lead to inconsistencies and errors. Updating the information on these documents can also be a slow and time-consuming process. This is where Hyperledger blockchain technology can come in handy. By using a decentralized, immutable ledger, the data on the government documents can be stored securely, and any changes made to them can be replicated across all other copies of other documents in real-time. This ensures that the data is accurate and consistent across all departments. The Hyperledger blockchain can provide an audit trail of all changes made to the documents, making it easier to track and detect any fraudulent activities. The use of smart contracts can also automate the process of document verification and validation, ensuring that only authorized parties have access to the data. Overall, Hyperledger blockchain technology in the government sector can lead to more efficient, secure, and transparent document management systems. It can help to reduce the likelihood of fraudulent activities, ensure the accuracy and consistency of the data, and improve the accessibility of the documents to authorized parties.

**CONTENTS**

*CERTIFICATE*  2

*DECLARATION*  3

*ACKNOWLEDGEMENT* 4

*ABSTRACT* 5

*CONTENTS* 6

*LIST OF FIGURES*  8

*LIST OF TABLES* 8

1. **Introduction**

1.1 Background of Government bodies 9

1.2 Introduction of Digital technology 10

1.3 Problems in current scenario 12

1.4 Motivation 14

1.5 Objective 15

1.6 Problem statement 15

1.7 Layout of work 16

1. **Literature survey 18**
2. **Blockchain Technology 26**
3. **Problem definition**

4.1 Benchmark 30

4.2 Defining problem 30

4.3 Parameters consideration 31

4.4 Challenges 32

1. **Implementation & Results**

5.1 Blockchain structure 33

5.2 Organization Structure 35

5.3 Process identification 37

5.4 Transcation Workflow 38

5.5 Algorithm 43

5.6 Smart contract 44

1. **Conclusion**  47

**References 49**

**1. LIST OF FIGURES\_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_**

Figure 1. Government Current Working System

Figure 2. Proposed Hyperledger Fabric Blockchain

Figure 3. Blockchain Structure

Figure 4. Transaction workflow

Figure 5. Framework Architecture

**2. LIST OF TABLES\_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_**

Table 1. Organization Entities

Table 2. Process Identification

**Chapter 1**

**Introduction**

**1.1 Background of Government bodies**

Over the years, government departments have experienced a significant evolution and transformation in their approaches to data management and documentation. The advent of digital systems has revolutionized how government agencies handle data, leading to increased efficiency, accuracy, and accessibility. Let's delve into a comprehensive explanation of the evolution and background of government departments' data management.

In the past, government departments relied on manual record-keeping systems, wherein documents and information were stored in physical files. This process involved labor-intensive tasks such as filing, sorting, and retrieving records. However, the manual approach was time-consuming, prone to errors, and presented challenges in efficiently managing large volumes of data.

The introduction of computers and technology marked a pivotal shift as government departments began adopting computerized systems for data management. This involved the digitization of paper records and the creation of databases to store and manage information. Computerization brought about faster data processing, improved searchability, and reduced physical storage requirements.

As technology progressed, government departments embraced more sophisticated database management systems (DBMS) to store and organize their data. DBMS offered structured storage, ensuring data integrity, and advanced querying capabilities, enabling efficient retrieval and manipulation of information. This transition facilitated the implementation of standardized data formats and enhanced data integration across different departments.

Recognizing the need for seamless data sharing and collaboration, government departments established networked systems. Local and wide-area networks connected various departments, allowing for the exchange of data and information. This interdepartmental data sharing enhanced coordination, facilitated the flow of information, and supported integrated service delivery.

The rise of e-government initiatives brought about a significant transformation in how government departments interacted with citizens and managed data. Online portals and systems were developed, enabling citizens to access government services, submit applications, and retrieve information remotely. This digital transformation aimed to improve convenience, transparency, and efficiency in public service delivery.

To enhance data interoperability and facilitate information exchange between departments, governments emphasized data standardization and integration efforts. They established standardized data formats, metadata frameworks, and data exchange protocols to ensure consistency, compatibility, and effective sharing of data across different government systems.

With the expansion of the digital landscape, data security and privacy became paramount concerns for government departments. Robust security measures were implemented to protect sensitive citizen information from unauthorized access, breaches, and cyber threats. Compliance with data protection regulations and frameworks became a crucial aspect of government data management.

The emergence of blockchain technology introduced new possibilities for government departments. Blockchain's distributed ledger offers tamper-proof data storage, transparency, and decentralization. It enables secure and verifiable transactions, simplifies auditing and verification processes, and enhances trust in government data management.

Government departments have evolved significantly in their approaches to data management and documentation. The transition from manual record-keeping to digital systems, databases, networked environments, e-government initiatives, and data standardization has revolutionized the efficiency, transparency, and security of government data. The introduction of blockchain technology further holds the potential to transform government data management by ensuring integrity, trust, and decentralization.

**1.2 Introduction of Digital Documentation**

The transition from physical to digital data management within government departments has brought about significant changes in how information is stored, accessed, and processed. This shift has revolutionized the efficiency, effectiveness, and security of government data.

One of the key advantages of digital data storage is its accessibility and scalability. Moving away from physical records allows government departments to store vast amounts of information in a compact and easily accessible format. Through the use of databases, cloud storage, and server systems, government agencies can efficiently store, organize, and retrieve data, leading to faster and more accurate information access.

Digital data management systems have also improved the overall management of government data. Database management systems (DBMS) provide advanced tools and functionalities that enhance data organization, simplifying data retrieval and enabling better analysis and reporting. This leads to improved decision-making and streamlined processes within government departments.

The digitization of government data has resulted in enhanced efficiency and productivity. Manual paperwork and physical file management have been replaced by automated and streamlined processes. Tasks such as data entry, record updates, and information sharing can now be performed more efficiently, allowing employees to focus on higher-value tasks and services.

Digital data management systems offer enhanced security measures compared to physical records. Government departments can implement encryption, access controls, user authentication, and backup mechanisms to protect sensitive data from unauthorized access, loss, or destruction. Digital records can also be replicated and stored in multiple locations, ensuring data preservation and disaster recovery capabilities.

Collaboration and information sharing have been significantly improved through digital data management. Shared databases, secure networks, and online platforms enable authorized personnel from different government departments and agencies to access and exchange data in real-time. This promotes better coordination, decision-making, and service delivery across various government entities.

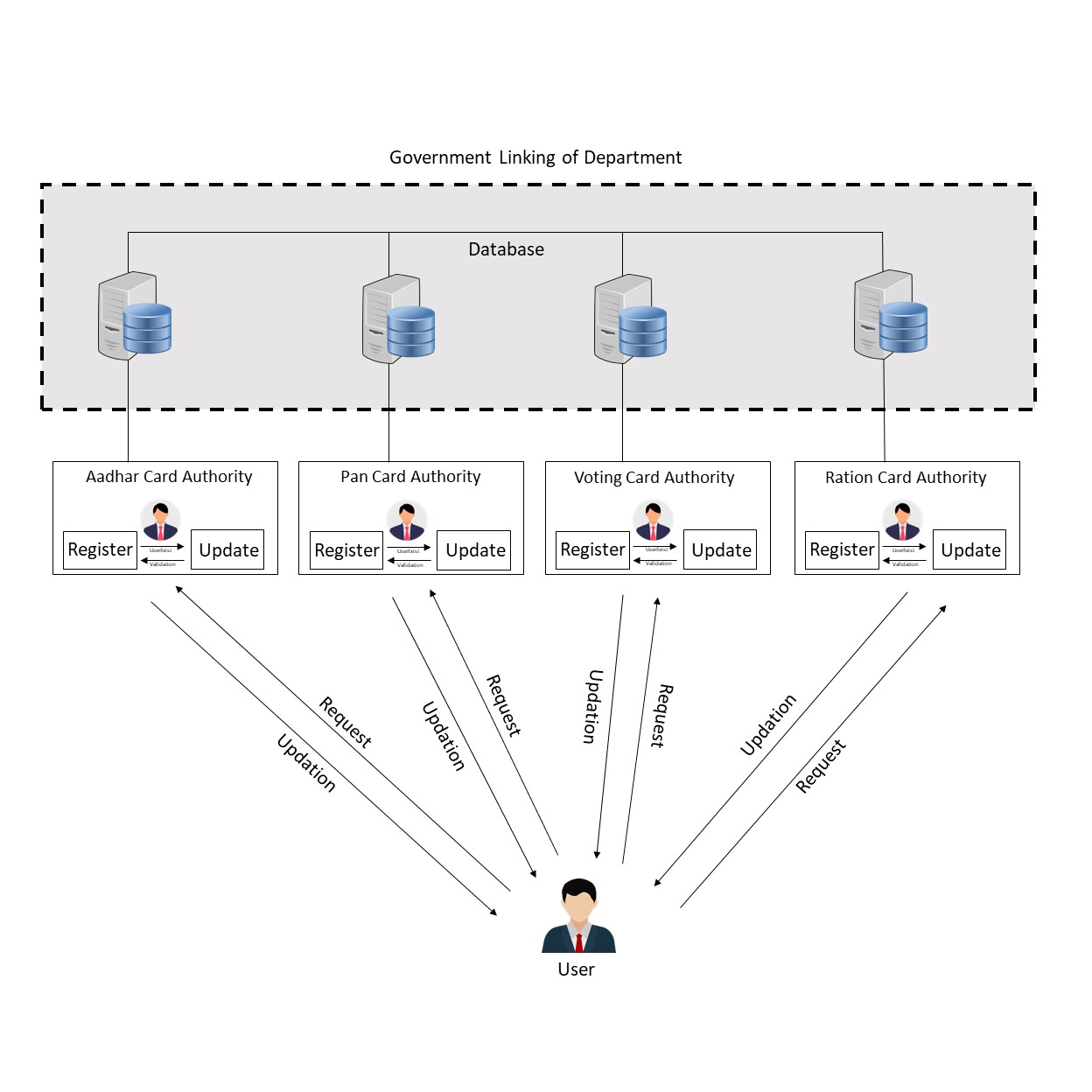
The use of digital data management systems also ensures data integrity and auditability. Changes made to digital records can be tracked, logged, and audited, providing transparency and accountability. This is particularly important for government departments dealing with sensitive information, legal compliance, and regulatory requirements.

The transition to digital data management brings about cost savings and environmental benefits. By eliminating the need for physical storage infrastructure, paper-based documentation, and manual processes, government departments can reduce operational costs, optimize resource utilization, and contribute to environmental sustainability.

Ultimately, the digitization of government data enables the delivery of citizen-centric services. Online portals, digital platforms, and self-service options empower citizens to access government information, submit applications, and interact with government departments conveniently and efficiently. This improves citizen satisfaction, reduces administrative burdens, and enhances the overall citizen experience.

The transition from physical to digital data management within government departments has revolutionized the way information is stored, accessed, and processed. It has improved efficiency, data security, collaboration, and service delivery, while also providing cost savings and environmental benefits. The digital transformation of government data management ultimately benefits both government agencies and citizens alike.

**1.3 Problems in current scenario**

****

***Figure 1. Government Current Working System***

The traditional way of managing government documents such as Aadhaar Card, PAN Card, Driving License, and Voter ID Card is inefficient and prone to errors. The updates made in one document are not automatically reflected in other documents, leading to inconsistencies and discrepancies in the information stored in different databases. This can cause delays and errors in processing applications and can also lead to fraud.

In the current scenario, there are several problems with the traditional system of public document updation. Firstly, there is a lack of transparency in the process, making it difficult for the public to verify the authenticity and integrity of the updated information. This lack of transparency undermines trust and can lead to disputes or doubts regarding the accuracy of the data.

The responsibility for document updation is usually centralized in a government agency or authority. This centralized control can result in delays, inefficiencies, and potential risks of corruption or manipulation. The process of updating documents involves multiple steps, paperwork, and interactions with various stakeholders, leading to complexity and redundancy. This can be time-consuming, cumbersome, and prone to errors or duplication of efforts.

There are concerns regarding the security and privacy of public data in the current system. Unauthorized access, data breaches, or misuse of personal information are potential risks that can compromise the confidentiality and integrity of the data.

Hyperledger for Public Data Management offers a promising solution to these problems. Hyperledger technology utilizes a distributed ledger system where data updates and transactions are recorded transparently and immutably. This ensures that all updates to public documents are visible and traceable, enhancing trust and accountability. The decentralized nature of Hyperledger allows the authority for document updation to be distributed among multiple participants or nodes, reducing dependency on a single central authority. This decentralization leads to a more efficient and secure update process.

Hyperledger employs cryptographic techniques and access controls to ensure the security and privacy of public data. Users can have confidence that their information is protected and accessed only by authorized parties, mitigating the risks associated with data security and privacy. Hyperledger also streamlines the process of document updation by providing a decentralized and automated mechanism. Updates can be verified, recorded, and propagated seamlessly across the network, reducing paperwork, delays, and redundancy. This automation simplifies the process and improves efficiency, saving time and effort for both the authorities responsible for managing public data and the individuals seeking to update their documents.

Hyperledger for Public Data Management offers significant advantages over the traditional system of public document updation. It improves transparency, efficiency, and security, addressing the challenges faced in the current scenario. By leveraging distributed ledger technology, decentralization, and cryptographic techniques, Hyperledger enhances trust, simplifies processes, and ensures the accuracy and integrity of public data, benefiting both the authorities and the general public.

**1.4 Motivation**

The motivation behind developing a Hyperledger blockchain for government documents is to create a robust and efficient system for updating and managing crucial information. Traditional methods of document management often suffer from inefficiencies, delays, and potential for errors. By leveraging blockchain technology, we aim to address these challenges and revolutionize the way government documents are handled.

One of the key benefits of using Hyperledger blockchain is its inherent immutability. Once data is recorded on the blockchain, it becomes tamper-proof and resistant to unauthorized modifications. This ensures the integrity and authenticity of government documents, enhancing trust among all stakeholders involved. Additionally, the decentralized nature of the blockchain ensures that no single entity has complete control over the system, reducing the risk of data manipulation or corruption.

By implementing a hierarchical structure with primary and secondary authorities, we establish a clear chain of command for document updates. The primary authority, in this case the Aadhaar Card Authority, acts as the central point for initiating and validating update requests. This ensures that all updates undergo a thorough verification process, preventing unauthorized changes and maintaining data accuracy. Furthermore, the replication of data across secondary authorities ensures that updates are seamlessly propagated throughout the system. This eliminates the need for redundant data entry and significantly reduces the chances of inconsistencies or discrepancies in the information stored across different departments.

From a technical standpoint, Hyperledger blockchain offers high transaction throughput and scalability, making it suitable for handling a large volume of government documents and user requests. Its permissioned nature ensures that only authorized entities can participate in the network, safeguarding the privacy and security of sensitive information.

The development of a Hyperledger blockchain for government documents aims to streamline document management processes, enhance data integrity, and promote transparency and efficiency in government operations. By leveraging the power of blockchain technology, we aspire to create a secure and reliable platform that simplifies document updates and ultimately benefits both government entities and citizens alike.

**1.5 Objective**

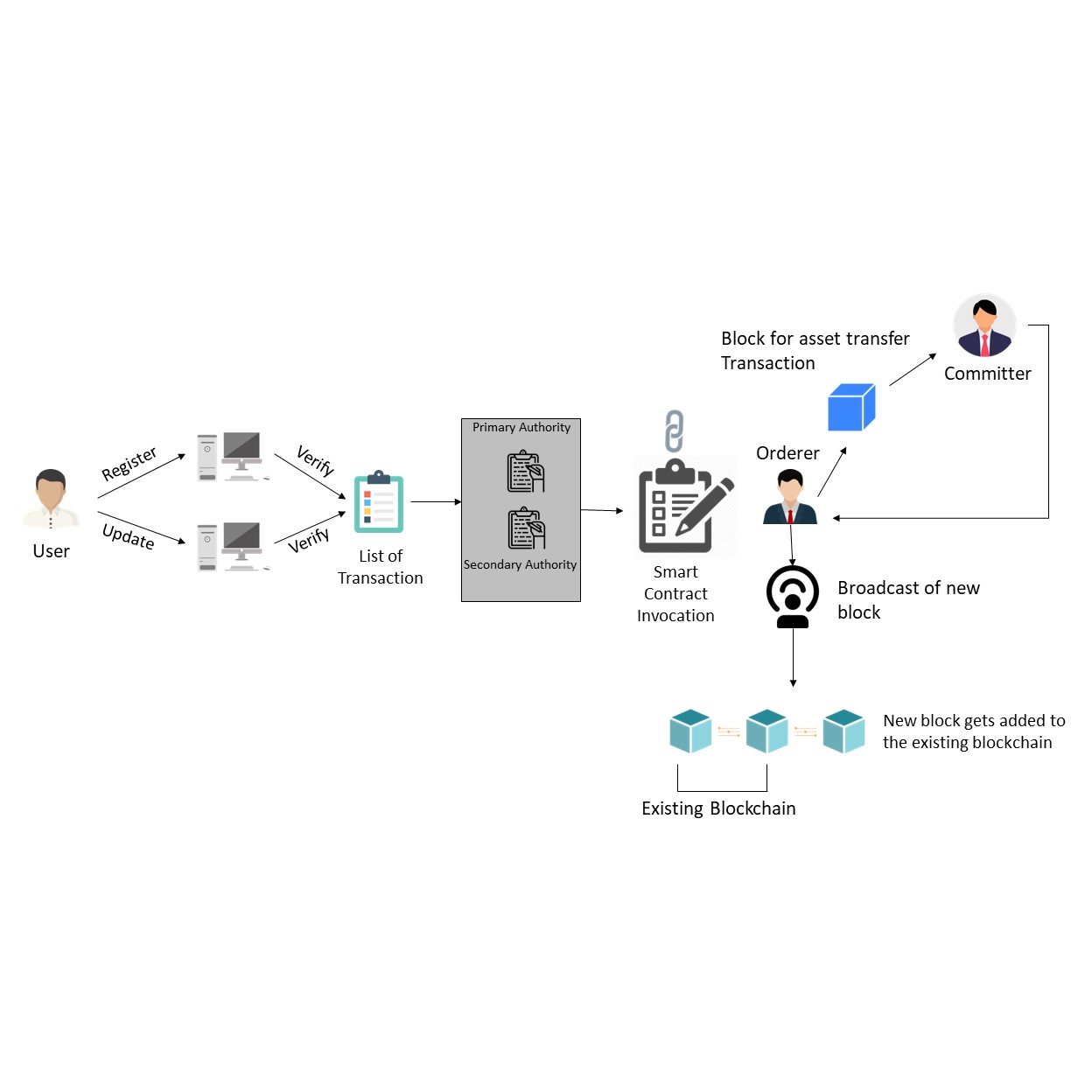
The objective of this research paper is to investigate the inadequacies of conventional approaches employed by the government sector for managing critical documents such as Aadhaar Card, PAN Card, Driving License, and Voter ID Card. The conventional method involves a centralized database system that is vulnerable to cyberattacks and data breaches, posing a significant risk to the privacy and security of sensitive information.

* To study the current scenario of public document/data management and implementing Hyperledger for Public Data Management.
* To analyze and to find how methodologies for blockchain technology can be used and implemented in Public Data Management.
* To improve the process of government document updation increasing the efficiency and making it more secure and accessible to authorized part/user.

**1.6 Problem Statement**

The traditional way of managing government documents such as Aadhaar Card, PAN Card, Driving License, and Voter ID Card is inefficient and prone to errors. The updates made in one document are not automatically reflected in other documents, leading to inconsistencies and discrepancies in the information stored in different databases. This can cause delays and errors in processing applications and can also lead to fraud.

**1.7 Layout of work**



***Figure 2. Proposed Hyperledger Fabric Blockchain***

The use of blockchain in the development of a government document management system brings numerous benefits to the table. Blockchain technology offers a decentralized and immutable ledger that enhances the security, transparency, and efficiency of managing government documents. In the layout of work, the blockchain serves as the foundational technology for storing and updating government documents. It provides a secure and tamper-proof environment where data can be recorded and verified. By leveraging the blockchain's immutability, the integrity of government documents is ensured, preventing unauthorized modifications or tampering.

The primary advantage of blockchain lies in its decentralized nature. Unlike traditional centralized systems, blockchain eliminates the need for a single governing authority, distributing control and validation across a network of participants. This decentralized architecture fosters trust among stakeholders and minimizes the risk of data manipulation or corruption.

Additionally, blockchain technology enables transparent and auditable transactions. Each update or modification to a government document is recorded on the blockchain, creating an immutable audit trail. This enhances accountability and facilitates easy verification of document history. Furthermore, the use of blockchain streamlines document updates. Once a user requests an update to their document attributes, the primary authority initiates the process by sending requests to secondary authorities for replication. The blockchain's distributed nature allows for seamless and efficient replication, eliminating the need for redundant data entry.

The implementation of a blockchain-based government document management system simplifies the process of updating and managing crucial information. It ensures the security, transparency, and integrity of government documents, promoting trust among users and authorities. By leveraging the decentralized and immutable nature of blockchain technology, this system brings efficiency and accountability to document management in the government sector.

**Chapter 2**

**Literature survey**

The paper highlights the potential of blockchain technology in transforming e-governance in smart cities. It explores the benefits of blockchain integration in addressing challenges and improving transparency, efficiency, and citizen trust. The research identifies key areas of e-governance where blockchain can have significant advantages and discusses various urban applications. The paper emphasizes the decentralized and secure nature of blockchain, its ability to enable smart transactions, and its impact on industries such as agriculture and food supply chains. It also mentions the growth of blockchain technology in cities worldwide and its potential to reduce effort and save time. The paper provides insights into the systematic review of blockchain technology, application examples, and bibliometric analysis. It discusses the relevance and architecture of smart cities, types of blockchain implementations, citizen participation, government initiatives, and the benefits of blockchain integration in creating and sustaining smart cities. The research suggests that combining blockchain with other technologies like AI, IoT, and cloud computing can contribute to sustainable smart cities. It emphasizes the need for policymakers to understand blockchain and its applicability in e-governance. The paper concludes by discussing future research directions, including scalable transactions, energy consumption optimization, DeFi applications, and supply chain management for perishable goods. Overall, blockchain technology is expected to enhance trust, transparency, and security in the relationship between citizens and governments in smart cities [1].

The paper discusses the limitations of existing e-Governance systems, such as lack of transparency and susceptibility to corruption. It proposes the use of blockchain technology as a solution to these challenges, focusing on the specific use case of land registration. By leveraging blockchain's immutability and distributed ledger, the paper suggests that corruption can be eliminated, transparency can be enhanced, and citizen trust can be improved. We get the benefits of blockchain technology in e-Governance, including secure data storage, reduction in bureaucracy, elimination of paperwork, and cost reduction. It also addresses the barriers to e-Governance in India and suggests ways to improve adoption, such as increasing internet penetration and providing training to officials. The paper concludes by emphasizing the potential of blockchain technology in revolutionizing e-Governance and increasing citizen trust in the government [2].

Blockchain technology is gaining popularity as it has the potential to eliminate the need for third-party validation in peer-to-peer transactions. It offers features like smart contracts, consensus mechanisms, and secure and efficient transaction completion. This technology has applications in various fields such as medicine, IoT, e-Governance services, smart cities, taxation, supply chain, and banking. This paper provides an in-depth discussion of blockchain technology, including its data structure, open-source platforms like Ethereum and Hyperledger, technical aspects, potential applications, and challenges and limitations in its adoption. Blockchain technology is disruptive and has the potential to transform ICT services by eliminating the need for third-party validation and ensuring data integrity through its decentralized and. It originated with the proposal of Bitcoin in 2009, where transactions are validated by peer members without the need for a controlling authority. Each transaction is recorded in blocks, which are linked together in a chain. Blockchain technology combines various elements such as mathematics, cryptography, consensus algorithms, peer-to-peer networks, and decentralized databases. It utilizes the Public Key Infrastructure (PKI) for the identification and authentication of peer members and ensures the immutability of the blockchain. After its success in the realm of cryptocurrencies, blockchain technology is now being adopted in other sectors such as medical treatment, IoT, e-Governance services, smart cities, taxation, supply chain, and e-vehicles, promising significant growth and advancements in these areas [3].

The text discusses the potential of blockchain technology in addressing the challenges faced by Electronic Property Registration (EPR) systems in e-Governance. It proposes a Smart Contract-based blockchain framework to improve the security, transparency, and efficiency of property registration processes. The framework aims to address issues such as data security, integrity, single-point-of-failure, and data interoperability among different government agencies. It highlights the benefits of blockchain, such as tamper-proof records, decentralized data storage, and trust among stakeholders. The proposed framework demonstrates scalability and performance in handling transaction loads. Overall, it concludes that the framework offers practical solutions for enhancing EPR systems and can be implemented within the existing e-Governance ecosystem [4].

The text highlights the security challenges faced by e-governments, such as cyberattacks and data breaches, and explores the potential of blockchain technology, specifically the Hyperledger Fabric platform, in enhancing security and transparency. The study conducted performance evaluations and analyses of the platform in multi-organization and multi-client scenarios, focusing on parameters like latency, throughput, and scalability. The results show that increasing the number of organizations and clients negatively affected the platform's performance, leading to reduced throughput and increased latency. Additionally, the impact of transaction rates and block sizes was examined, with a block size of approximately 100 transactions per block showing better results. The study concludes that the performance of the Hyperledger Fabric platform is influenced by various factors, including hardware and software configuration, smart contract complexity, user and organization volume, and network architecture. It suggests that a moderate number of organizations and clients can have a positive impact on performance while increasing their numbers can degrade system performance [5].

The paper discusses the adoption of blockchain technology in supply chain management (SCM) to address issues faced by traditional SCM systems. The traditional SCM is described as centralized, time-consuming, and lacking transparency and traceability. The paper gives me the benefits of blockchain in improving security, transparency, traceability, stakeholder involvement, and countering issues like product counterfeiting, delays, fraud, and instabilities. The study provides a comprehensive analysis of existing literature on blockchain characteristics, implementations, and business consequences in various SCM contexts. It identifies transparency, traceability, information sharing, and product anti-counterfeiting as key drivers for adopting blockchain in SCM. The paper also discusses the challenges and open research questions in implementing blockchain in SCM. It emphasizes the need for decentralized infrastructure, a trust layer for business logic, tamper-proof tracking, and cryptographic security. It highlights advantages such as real-time data handling, reduced paperwork, increased efficiency, improved supply chain visibility, and reduced risks of SCM attacks with blockchain adoption. The motivation behind the survey is to address SCM challenges and explore the potential of blockchain technology. It compares existing surveys on blockchain and SCM integration and provides insights for researchers interested in this field. The study aims to provide an understanding of blockchain technology in SCM, its current adoption status, and future research directions. Overall, the paper presents a comprehensive overview of blockchain adoption in SCM, discussing benefits, challenges, and potential applications. It serves as a valuable resource for researchers, engineers, educators, and readers interested in understanding the intersection of blockchain technology and supply chain management [6].

Two models are proposed: the blockchain certification traceability model (BTM) for offline business scenarios and the blockchain-based e-commerce model (BEM) for online business scenarios. The BTM allows consumers to check product information by scanning barcodes in offline stores, while the BEM enables consumers to verify and purchase products online. The paper highlights the need for quantitative methods to confirm the benefits of blockchain adoption in OASCs and presents a comparative analysis using the Stackelberg game to evaluate supply chain profit and consumer surplus. The study extends the analysis by using the case of Red Beauty oranges to demonstrate the effectiveness of the blockchain e-commerce model in scenarios with high shopping convenience and low operating costs of the blockchain platform. The findings suggest that the BEM is a favorable supply chain model that improves the performance of OASCs. The paper emphasizes the nutritional and health benefits of organic products, the growing consumer preference for organic agriculture, and the potential of blockchain technology to enhance the credibility, efficiency, and transparency of supply chains.However, the benefits of blockchain adoption in OASCs and the existence of divergent views regarding the economic impact of blockchain technology. It identifies the need to compare the benefits of offline and online business scenarios and explores potential trade-offs between the two. The paper contributes by providing a conceptualization of the BTM and BEM models, a quantitative analysis of their benefits, and guidance for implementing blockchain traceability in online and offline businesses. In conclusion, the paper tells us that the adoption of blockchain technology in OASCs can increase the profit of the supply chain, enhance consumer surplus, and promote the growth of organic agriculture. It emphasizes the importance of improving service quality in traditional supply chain models, setting reasonable certification costs for the blockchain platform, and considering the BEM as an optimal decision-making approach [7].

The provided text discusses the potential impact of blockchain technology and management accounting on the efficiency of supply chains in Jordanian Manufacturing Companies (JMC). The study conducted a survey with 258 respondents from JMC and found that both blockchain technology characteristics and management accounting have a positive and significant impact on the efficiency of supply chains in JMC. Blockchain technology offers advantages such as lower costs, avoidance of human errors, and enhanced control of information integrity. It can improve transparency, trust, cooperation, and coordination among supply chain parties. The adoption of modern information technology, including blockchain, can reduce transaction costs and improve supply chain operations. The paper acknowledges the need for more research in developing countries and highlights the obstacles to implementing blockchain in supply chains. The findings of the study support the use of blockchain technology and management accounting to increase the efficiency of supply chains in JMC, helping them survive and thrive in competitive business environments [8].

The document discusses the challenges of information sharing within supply chains and explores the potential impact of blockchain technology on addressing these challenges. Supply chains are complex and fragmented due to globalization and market competition, resulting in a lack of trust and transparency in information sharing. The paper aims to understand how blockchain technology can improve information sharing within supply chains. The text explains that blockchain technology, with its decentralized and transparent nature, offers a solution for trustable information sharing. Through a systematic literature review, the authors identify potential benefits, challenges, and gaps in blockchain-enabled information sharing within supply chains. The findings suggest that blockchain technology can enhance collaborative work in various types of supply chains, including health, construction, and smart cities. By providing verified information to all members, blockchain strengthens collaborative partnerships. The use of blockchain-based platforms with smart contracts enables secure information sharing between trusted and non-trusted institutions.However, the paper also highlights barriers to blockchain adoption, such as the lack of understanding among businesses and conflicts of interest. The authors recommend further research in areas like information hiding and understanding different supply chain dynamics to better deploy blockchain technology. In summary, the document emphasizes the potential of blockchain technology in improving information sharing within supply chains, while acknowledging the challenges that need to be addressed for successful implementation [9].

The implications of blockchain smart contracts in modern e-commerce. the shift of business challenges to online platforms and the need for secure and transparent solutions. Smart contracts are identified as a potential solution to enhance security, accountability, inclusiveness, cost-effectiveness, and transparency in e-commerce various domains of e-commerce, including financial transfer, record-keeping, real estate, insurance, supply chain management, and more. The widespread adoption of smart contracts offers benefits such as decentralization, efficacy, cost-effectiveness, transparency, speed, autonomy, privacy, and security, etc. The technology faces challenges related to security, transparency, cost-effectiveness, and regulatory frameworks. Organizational and technical challenges, such as compatibility with legacy systems, scalability, bugs, speed, and lack of talent and understanding, hinder the deployment of smart contracts. The need for policymakers, developers, researchers, practitioners, and stakeholders to invest time and effort in addressing these challenges and fostering the global adoption of smart contracts in small and big businesses pharma, mechanical engineering, healthcare, insurance, tourism, construction, and public administration. In this paper the increasing interest and investments in blockchain technology, as well as the potential transformational impact it can have on traditional business models blockchain technology, particularly smart contracts, holds significant potential for e-commerce, but there are still challenges to overcome before its widespread adoption [10].

The research paper focuses on the challenges of tracking data provenance and maintaining traceability in modern supply chains, specifically in the context of Agriculture and Food (Agri-Food) supply chains. It highlights the limitations of centralized systems in terms of transparency, accountability, and auditability, which affect credibility and traceability. The proposed solution leverages the immutability and transparency of the blockchain to ensure traceability and trust throughout the supply chain. Transactions are recorded on the blockchain and data is stored on the Interplanetary File Storage System (IPFS) for secure and reliable storage. Smart contracts facilitate interactions between supply chain entities. The paper emphasizes the importance of maintaining quality, transparency, and security in supply chain systems, as enforced by regulatory authorities. It identifies limitations in existing solutions and research works.

The proposed solution aims to achieve accountability, credibility, auditability, autonomy, and authenticity in the Agri-Food supply chain. It addresses challenges related to information asymmetry, decentralized payment mechanisms, and dispute resolution. A reputation system is introduced to ensure entity credibility and product quality ratings. Detailed explanations are provided regarding traceability mechanisms, trading and delivery processes, the reputation system, and autonomous transactions. The performance of smart contracts is evaluated to ensure efficiency and robustness. The authors acknowledge the practical implementation challenges of blockchain-based systems and discuss future plans for integrating refund and return mechanisms and detecting fake reviews. In summary, the research paper presents a comprehensive blockchain-based solution for managing Agri-Food supply chains, focusing on traceability, trust, and transparency. It offers insights into the proposed solution's components and evaluates its performance, contributing to the advancement of supply chain management in the Agri-Food industry [11].

The research paper explores the application of blockchain technology in supply chain management to address challenges related to transparency, trust, and efficiency. It surveys existing blockchain frameworks designed for supply chains and discusses their components, operation, advantages, and disadvantages. It also outlines the properties required for a successful blockchain framework in supply chain management and identifies remaining challenges and future research opportunities. Overall, the paper provides insights into the use of blockchain in improving supply chain processes and highlights areas for further exploration [12].

The research paper addresses the challenges in tracking and ensuring the safety and quality of agricultural food supply chains. It highlights the problems of numerous participants, communication inefficiencies, data distrust, and centralized systems. The paper proposes a framework based on consortium and smart contracts, leveraging blockchain technology to enhance traceability and shareability in the supply chains. The framework aims to eliminate the need for central institutions, improve transaction record integrity, reliability, and security. It incorporates the use of the InterPlanetary File System (IPFS) for storing environmental and crop growth data, enhancing data security while alleviating blockchain storage concerns. The framework has been applied in a real-world case study, demonstrating disintermediation and QR code-based tracing of agricultural product information. The paper emphasizes the significance and reference value of the proposed framework for enterprises to ensure product quality and safety traceability. However, it acknowledges the existing challenges related to scalability, privacy, and regulation in blockchain and suggests further research to address these issues and enhance the reliability and auditability of data transactions and payments in the agricultural food supply chain [13].

This research paper explores the application of blockchain technology in the fresh agricultural product supply chain to address the challenges of maintaining freshness and greenness during delivery, particularly in the context of increased demand on e-commerce platforms during the COVID-19 pandemic. The traditional cold chain delivery system is effective in preserving freshness but lacks transparency, leading to potential compromises in freshness-keeping efforts by supply chain members. The paper investigates whether blockchain can effectively solve these problems by discussing the dynamic optimization of freshness-keeping effort, advertising effort, and blockchain adoption degree. The findings suggest that in the traditional supply chain, suppliers tend to give up freshness-keeping efforts after receiving wholesale funds, which negatively impacts the quality of agricultural products. However, when blockchain technology is adopted, suppliers continue to prioritize freshness-keeping during delivery. The paper identifies five specific settings in which blockchain is effective in maintaining freshness, while two other settings are deemed unsuitable for blockchain adoption. The decision to adopt blockchain is influenced by the profit margin of the retailer and the supplier's freshness-keeping effort. The research highlights that blockchain adoption does not affect the supplier's greenness investment decision and can reduce advertising effort and goodwill required to achieve the same profit margin. Additionally, the retailer's increased profit margin leads to higher advertising effort and goodwill. The study emphasizes the need for active cooperation between retailers and suppliers in implementing blockchain technology. The paper acknowledges certain limitations, such as the assumption that wholesale funds are transferred earlier than the delivery time, and suggests that future research should consider alternative scenarios. Furthermore, the specific impact of blockchain adoption on other aspects of the supply chain could be explored in future studies. Overall, this research provides insights into the management of cold chain logistics in the context of fresh agricultural products and offers guidance on the adoption of blockchain technology [14].

This research paper provides a systematic review and analysis of blockchain technology in supply chain management. The study explores the current status, potential applications, and future directions of blockchain in the supply chain. The authors conducted a literature survey and analyzed review articles to understand the use of blockchain and smart contracts in supply chain management. They highlight four major issues: traceability and transparency, stakeholder involvement and collaboration, supply chain integration and digitalization, and common frameworks on blockchain-based platforms. The paper emphasizes the potential of blockchain to disrupt supply chain operations for better performance, distributed governance, and process automation. It also identifies technical issues and research gaps related to blockchain's scalability, security, and interoperability. The study provides insights into blockchain applications in supply chain management and suggests promising areas for future research [15].

**Chapter 3**

**Blockchain Technology**

The government sector in India plays a critical role in providing essential services to its citizens and driving economic growth. However, traditional bureaucratic processes often suffer from inefficiency, lack of transparency, and concerns related to data manipulation. Blockchain technology has become a viable answer to these problems in recent years. A permissioned blockchain system called Hyperledger Fabric has a lot of potential for modernizing India's public sector. This paper explores the technology requirements, components, working principles, and potential use cases of Hyperledger Fabric in the government sector

**3.1 Technology Requirements of Hyperledger Fabric**

Implementing Hyperledger Fabric in the government sector requires specific technology requirements. Firstly, a robust infrastructure capable of supporting the distributed nature of the blockchain is essential. This includes reliable network connectivity, adequate computing resources, and storage capacity. Additionally, organizations need to establish a network of participating nodes to ensure decentralized governance and consensus mechanisms. These nodes form a consortium, where each member maintains a copy of the ledger and participates in the consensus process.

**3.2 Components of Hyperledger Fabric**

1. Participants: Hyperledger Fabric involves multiple participants, including organizations or government entities that form a consortium. Each participant in the network maintains a copy of the ledger, ensuring decentralized governance and consensus. Participants can be divided into two types: peers and ordering service nodes.

2. Peers: Peers are the nodes within the network that maintain copies of the ledger and execute chaincode (also known as smart contracts). Types of Peers in Hyperledger Fabric are as follows

* Endorsing Peers: These peers receive transaction proposals and execute the chaincode, endorsing the results by signing them. They simulate the transaction to determine its validity and update the ledger's state. Multiple endorsing peers are required for consensus on the transaction results.
* Committing Peers: Once the transaction is endorsed, committing peers validate the endorsements and update the ledger's state accordingly. These peers ensure the transaction's integrity and maintain a copy of the complete ledger.

3. Ordering Service: Receiving endorsed transactions from endorsing peers, ordering them into a block, and distributing the block to committed peers are the responsibilities of the ordering service. It ensures a consistent order of transactions across the network and guarantees the immutability of the ledger. The ordering service can be implemented using various consensus algorithms, such as Kafka, Raft, or Solo.

4. Ledger: Hyperledger Fabric utilizes a distributed ledger to record all transactions and maintain the state of the network. The ledger consists of two components:

* World State: The world state represents the current state of assets and their values. It is typically stored in a database, enabling efficient querying and retrieval of asset information.
* Transaction Log: The transaction log records all the transactions that have occurred in the network. It maintains an immutable history of transactions, ensuring transparency and auditability.

5. Chaincode (Smart Contracts): Chaincode, also known as smart contracts, contains the business logic of the applications running on the Hyperledger Fabric network. Chaincode defines the rules and conditions for executing transactions and updating the ledger's state. It is written in programming languages such as Go, JavaScript, or Java and is installed and instantiated on endorsing peers.

**3.4 Working Principles of Hyperledger Fabric**

The working of Hyperledger Fabric involves the following steps:

1. Transaction Proposal: A client initiates a transaction by sending a proposal to endorsing peers. The proposal includes the necessary inputs and parameters for the transaction. Endorsing peers simulate the transaction based on the chaincode's logic and return the endorsement results.

2. Transaction Endorsement: Endorsing peers validate and execute the transaction based on the chaincode's rules. They endorse the transaction by signing the results, confirming its validity. Multiple endorsements are required for consensus.

3. Ordering: Endorsed transactions are sent to the ordering service, which orders them into a block. The ordering service uses a consensus algorithm to ensure a consistent order of transactions across the network.

4. Transaction Commitment: Committing peers receive the ordered block from the ordering service. They validate the endorsements, ensure the transaction's integrity, and update the world state and transaction log accordingly. The transaction is committed to the ledger, making it immutable and tamper-proof.

5. Consensus: Hyperledger Fabric employs a consensus mechanism to ensure agreement on the transaction order and validity. The consensus algorithm can be chosen based on the network's requirements and can be replaced or upgraded as needed.

**3.5 Potential Use Cases in the Government Sector**

Hyperledger Fabric offers numerous use cases in the government sector, enabling efficient and transparent processes. Some potential use cases in India include:

1. Identity Management: Hyperledger Fabric can provide a secure platform for managing and verifying identities. This can be beneficial in areas such as e-governance services, passport issuance, and voter registration systems, ensuring secure and tamper-proof identity records.

2. Land Registration: Implementing Hyperledger Fabric for land registration can help reduce fraud, eliminate multiple claims on properties, and streamline the process of land transfer and registration. The transparency and immutability of the blockchain ensure the integrity of land records.

3. Supply Chain Management: Hyperledger Fabric can be utilized for supply chain management in government sectors such as agriculture, ensuring traceability and transparency in the supply chain. This can help eliminate counterfeit products, improve quality control, and facilitate efficient logistics.

4. Government Benefits and Subsidies Distribution: Blockchain technology can enhance the distribution of government benefits and subsidies by ensuring transparency, reducing fraud, and improving accountability. Hyperledger Fabric can provide a secure and auditable platform for managing and distributing social welfare schemes.

Hyperledger Fabric provides a secure and transparent platform for modernizing the government sector in India. By leveraging the advantages of blockchain technology, such as increased efficiency, enhanced data security, and improved transparency, Hyperledger Fabric can streamline processes, reduce fraud, and enhance citizen trust. While challenges exist, addressing them and seizing future opportunities can lead to a more efficient, accountable, and citizen-centric government sector in India.

**Chapter 4**

**Problem definition**

**4.1 Benchmark of Current Existing System**

The existing literature on blockchain technology has primarily focused on its application in financial systems and supply chain management. While these areas have seen significant advancements and adoption of blockchain solutions, there is a noticeable research gap when it comes to exploring the potential of blockchain for government document management. Specifically, there is a lack of studies addressing the design and implementation of a blockchain system for updating government documents in a hierarchical structure involving multiple authorities.

Government documents play a crucial role in various administrative processes, such as identity verification, taxation, voting, and social welfare distribution. However, the current paper-based or centralized digital systems often suffer from inefficiencies, lack of transparency, and potential data manipulation. Blockchain technology has the potential to address these issues by providing a decentralized and immutable ledger for storing and updating government documents.

Therefore, it is essential to conduct research that focuses on developing a robust blockchain framework specifically tailored for government document management. This research should aim to address the unique challenges and requirements associated with updating government documents, such as data integrity, privacy, hierarchical authority structure, and regulatory compliance. By filling this research gap, we can unlock the potential of blockchain technology to revolutionize the way government documents are managed, leading to enhanced efficiency, transparency, and trust in administrative processes.

**4.2 Defining Problem**

The problem we aim to address is the inefficiency and lack of transparency in the current process of updating government documents. The manual handling of document updates across multiple authorities often leads to errors, delays, and potential data discrepancies. Moreover, the lack of a standardized and secure system for document updates poses significant challenges in maintaining the integrity and accuracy of the information.

By developing a blockchain-based solution for government document management, we seek to streamline the process of updating documents while ensuring data integrity, accessibility, and security. The hierarchical structure of authorities involved in managing different types of documents adds complexity to the problem. Therefore, our solution will focus on designing a system that allows for seamless updates, replication of changes across relevant authorities, and efficient validation mechanisms.

The proposed blockchain system will facilitate the secure transfer and storage of document updates, reducing the dependency on manual processes and minimizing the risk of errors or data manipulation. By establishing a transparent and auditable record of document updates, the solution will enhance trust, accountability, and traceability in government document management. Ultimately, our goal is to provide a scalable and efficient framework that improves the efficiency and reliability of document updates, benefiting both the authorities responsible for managing the documents and the users who rely on them.

**4.3 Parameters Consideration**

1. Data Integrity: Ensuring the integrity of government documents is of utmost importance. The blockchain system should provide immutability and tamper-proof features, ensuring that any updates or changes made to the documents are securely recorded and verifiable.
2. Accessibility and Transparency: The blockchain system should allow authorized entities, such as government authorities and users, to access and verify the documents easily. The transparency of the blockchain ensures that all updates and changes are visible to relevant parties, promoting trust and accountability.
3. Hierarchical Structure: Considering the hierarchical structure of authorities involved in managing different types of documents, the blockchain system should support replication and validation of document updates. The primary authority should have the ability to request updates and replicate changes to secondary authorities, ensuring consistency and uniformity across all entities.
4. Security and Privacy: The blockchain system must employ robust security measures to protect sensitive user information and ensure privacy. User data should be encrypted and accessible only to authorized parties, complying with data protection regulations and privacy standards.
5. Scalability and Performance: As the number of government documents and users increases, the blockchain system should be capable of handling a large volume of document updates efficiently. It should have high transaction throughput and low latency to meet the demands of government document management, ensuring a seamless user experience and system performance.

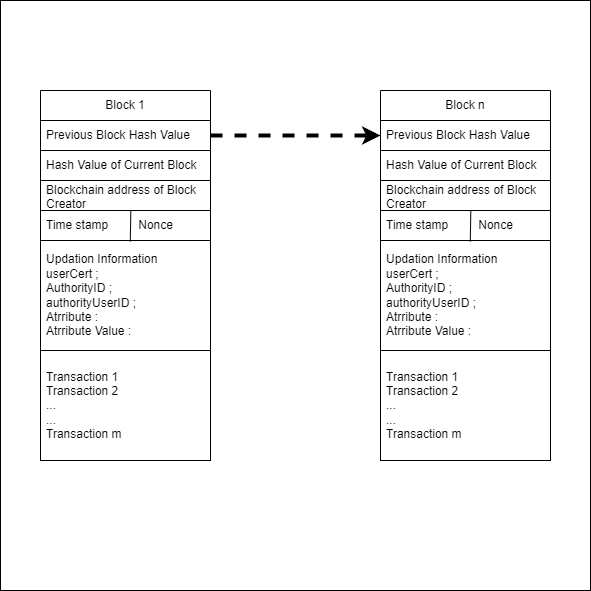
**4.4 Challenges for the Problem We Solve**

1. Interoperability: Ensuring interoperability between different government systems and authorities can be challenging. Integrating existing systems with the blockchain solution and enabling smooth data exchange is crucial for seamless document updates.
2. Governance and Consensus: Establishing governance models and consensus mechanisms among authorities to validate and approve document updates can be complex. Designing an efficient consensus algorithm that accounts for the hierarchical structure is crucial for maintaining trust and accountability.
3. Legal and Regulatory Compliance: Adhering to legal and regulatory frameworks for government document management is essential. Ensuring compliance with data protection laws, privacy regulations, and identity verification requirements adds complexity to the solution.
4. User Adoption: Encouraging user adoption and trust in the blockchain system may pose a challenge. Educating users about the benefits, security measures, and privacy protections offered by the blockchain solution is vital for widespread acceptance.
5. Scalability and Performance: As the number of government documents and users grows, ensuring scalability and maintaining optimal performance of the blockchain system can be a significant challenge. Efforts should be made to optimize the system's architecture and transaction processing capabilities.

**Chapter 5**

**Implementation & Results**

**5.1 blockchain structure**

****

***Figure 3. Blockchain Structure***

Hyperledger Fabric Blockchain Technology offers a robust framework for managing government documents by providing a secure and efficient system for updates and verifications. With its decentralized and tamper-resistant approach, it ensures data integrity and transparency in the document management process.

The blockchain structure in Hyperledger Fabric consists of a series of blocks, each encompassing a set of transactions or updates related to government documents. These updates primarily involve modifications to attributes such as name, date of birth, pin code, and mobile number. By employing this structure, the system ensures the reliability and security of document-related information.

A fundamental element of the blockchain structure is the inclusion of the previous block hash value. Every block in the chain contains a reference to the hash value of the preceding block. This linking mechanism establishes an interconnected chain of blocks, assuring that any unauthorized modification or tampering with a previous block would be immediately detectable. Altering the contents of a block leads to a change in its hash value, providing a robust mechanism for tamper detection.

Each block possesses a unique hash value, computed based on the data contained within. This hash value acts as a digital fingerprint, offering data integrity and immutability. Even the slightest modification to a block's data would result in a completely different hash value, making it virtually impossible to tamper with the block unnoticed.

The blockchain structure incorporates the blockchain address of the block creator. In the context of government documents, this address represents the organization or authority responsible for managing and updating the documents. By including the blockchain address, the system ensures transparency and accountability, enabling participants to trace the origin of transactions and updates.

To maintain chronological order, each block is assigned a timestamp indicating the precise time of its creation. This timestamp enables efficient organization of blocks and establishes a reliable record of transaction occurrence and update timings.

Lastly, the blockchain structure utilizes a nonce, a randomly generated value utilized during the block creation process. The nonce plays a crucial role in finding a hash value that meets specific criteria, such as predefined difficulty levels or proof requirements. This mining process adds an additional layer of security, as it necessitates computational effort to create new blocks, making it difficult for malicious actors to manipulate the blockchain.

By leveraging the blockchain structure in Hyperledger Fabric, government authorities can establish a secure and transparent system for managing document updates. The decentralized nature, immutability, and cryptographic integrity of the blockchain provide a reliable platform to ensure accuracy and authenticity throughout the document management process.

**5.2 Organization Structure**

In Hyperledger Fabric, an organization refers to a group of entities or participants that collaborate and interact within a specific blockchain network. Each organization in Hyperledger Fabric has its own identity, roles, and responsibilities.

Organizations play a crucial role in governing the network and managing the shared ledger. They have control over their own set of peers, endorsing policies, and membership access control. Each organization typically represents a distinct entity, such as a company, government agency, or consortium member. Within an organization, entities can include users, authorities, or other stakeholders who engage in transactions and interact with the blockchain network. These entities have specific roles and permissions assigned to them, dictating their level of access and actions they can perform within the network. Entities within an organization can define and manage their own channels, which enable private and secure communication with specific network participants. Organizations can establish trust relationships by endorsing transactions, verifying identities, and participating in the consensus mechanism.

The overall goal of organizations in Hyperledger Fabric is to enable collaboration, transparency, and accountability within a decentralized network. By utilizing permissioned blockchain technology, organizations can securely share and update information, enforce governance rules, and ensure data integrity and confidentiality. In the context of the specific use case mentioned earlier, the entities (User, Aadhaar Card Authority, PAN Card Authority, Voting Card Authority, and Ration Card Authority) represent different organizations collaborating within the Hyperledger Fabric network to manage government documents efficiently and securely. Each organization plays a crucial role in maintaining and updating the relevant document information, ensuring accuracy, consistency, and integrity throughout the network.

In this Hyperledger Fabric blockchain implementation for government documents, the organization consists of various entities with distinct roles. The primary authority is the Aadhaar Card Authority, responsible for maintaining Aadhaar card information, including attributes like name, date of birth, pin code, and mobile number. Users interact with the system and can register their information and request updates to their attributes. Secondary authorities include the PAN Card Authority, Voting Card Authority, and Ration Card Authority. These entities maintain information related to PAN card, voting card, and ration card, respectively. They receive updates from the primary authority and replicate the changes made to their specific documents.

The primary authority acts as the source of truth and validates update requests from users. It ensures the authenticity and integrity of the updates by verifying the proof provided by users. Upon successful validation, the primary authority replicates the changes to the secondary authorities. Users have the permission to request updates to their attributes in the primary authority, while only the primary authority has the authority to request the replication of updates to the secondary authorities. This design ensures that updates are securely and accurately propagated throughout the network, maintaining consistency and synchronization of data across the organization. The organization can create a transparent, immutable, and decentralized system for handling government documents by utilizing Hyperledger Fabric's blockchain technology. This would make modifications simple while preserving data security and integrity.

***Table 1. Organization Entities***

| Entity | Role | Description |
| --- | --- | --- |
| User | Document Holder | Represents individuals who hold government documents such as Aadhaar card, PAN card, voting card, and ration card. Users can request updates to their information. |
| Aadhaar Card Authority | Primary Authority | The primary authority responsible for maintaining Aadhaar card information. It stores attributes like name, date of birth (DOB), pin code, and mobile number. Users can request updates to their Aadhaar card, and the authority validates and replicates the changes to secondary authorities. |
| PAN Card Authority | Secondary Authority | A secondary authority responsible for maintaining PAN card information. It stores attributes like name, Aadhaar number, DOB, and mobile number. The authority receives updates from the primary authority and replicates them accordingly. |
| Voting Card Authority | Secondary Authority | A secondary authority responsible for maintaining voting card information. It stores attributes like name, DOB, pin code, and Aadhaar number. The authority receives updates from the primary authority and replicates them accordingly. |
| Ration Card Authority | Secondary Authority | A secondary authority responsible for maintaining ration card information. It stores attributes like name, Aadhaar number, and pin code. The authority receives updates from the primary authority and replicates them accordingly. |

**5.3 Process Identification**

***Table 2. Process Identification***

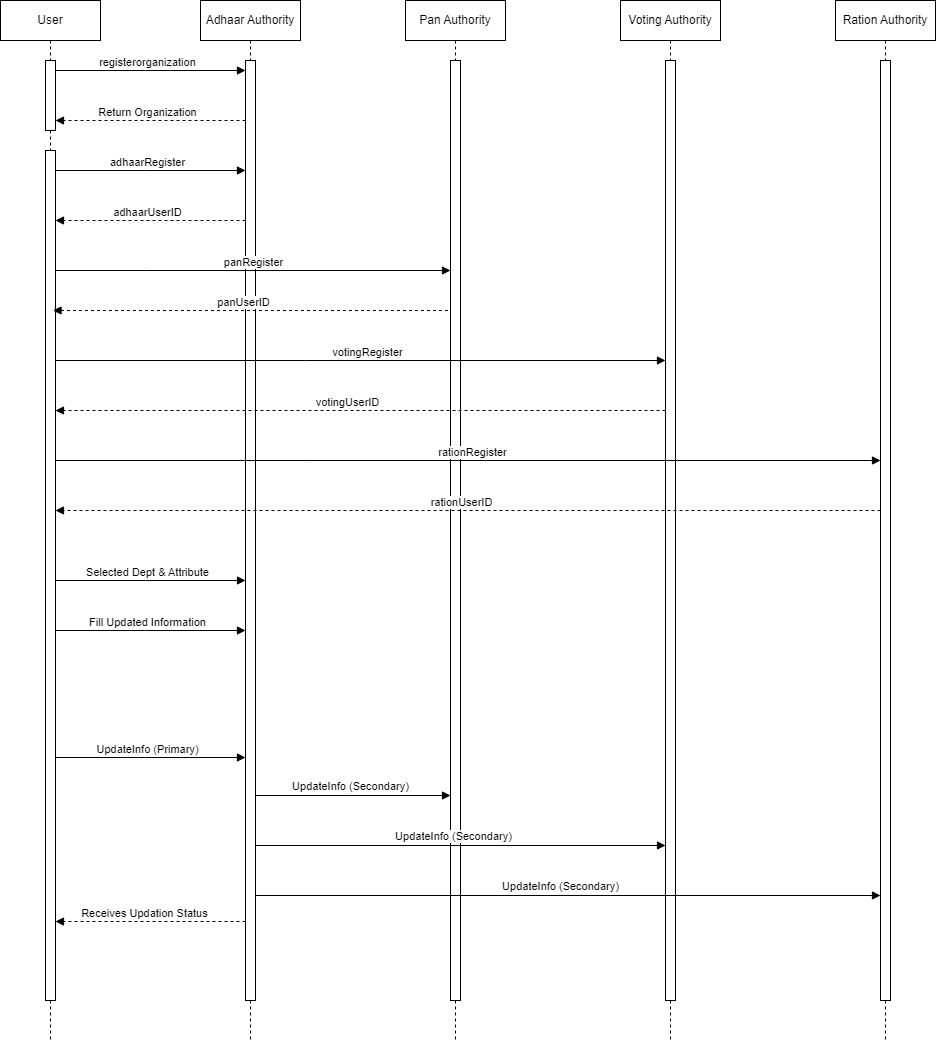
| Process | Description | Role/Entity Involved | Access Level |
| --- | --- | --- | --- |
| Register-  Organization | Assigns hierarchy keys (hKey) to the authorities. Primary authorities have hKey = 1, secondary authorities have hKey = 2, and users have hKey = 3. Creates authority objects if they don't exist. | Aadhaar Card Authority, PAN Card Authority, Voting Card Authority, Ration Card Authority | Admin/Network Operator |
| Adhaar-  Register | Allows users to register their Aadhaar card information. Generates a unique user ID based on name and date of birth. Creates a new user object in the buffer. Validates user existence. | User | User |
| panRegister | Enables users to register their PAN card information. Generates a unique user ID based on name, date of birth, and Aadhaar ID. Creates a new user object in the buffer. Validates user existence. | User, Aadhaar Card Authority | User |
| votingRegister | Facilitates user registration for voting card information. Generates a unique user ID based on name, date of birth, and Aadhaar ID. Creates a new user object in the buffer. Validates user existence. | User, Aadhaar Card Authority | User |
| rationRegister | Allows users to register their ration card information. Generates a unique user ID based on name and Aadhaar ID. Creates a new user object in the buffer. Validates user existence. | User, Aadhaar Card Authority | User |
| UpdateInfo (Primary Authority) | Allows users to update their information. Validates user existence and access permissions. Changes data in the primary authority. | User, Aadhaar Card Authority | User (invoke access) |
| UpdateInfo (Secondary Authority) | Transfers changes made in the primary authority to the secondary authorities if the hierarchy key is equal to the primary authority's hierarchy key + 1. | User, Aadhaar Card Authority, PAN Card Authority, Voting Card Authority, Ration Card Authority | Aadhaar Card Authority (Primary Authority Access) |

**5.4 Transaction Workflow**

The proposed transaction flow in the Hyperledger blockchain for government documents begins with user registration, where users provide their personal information to the primary authority, the Aadhaar card authority. Following the registration, a unique user ID for Aadhaar is generated based on the user's name, date of birth, and the identifier "ADHAAR." This unique ID serves as a reference for subsequent interactions. After successful registration, users can proceed to register with secondary authorities such as the PAN card authority, voting card authority, and ration card authority. During registration with each authority, users provide the required attributes, including their unique user ID from Aadhaar.

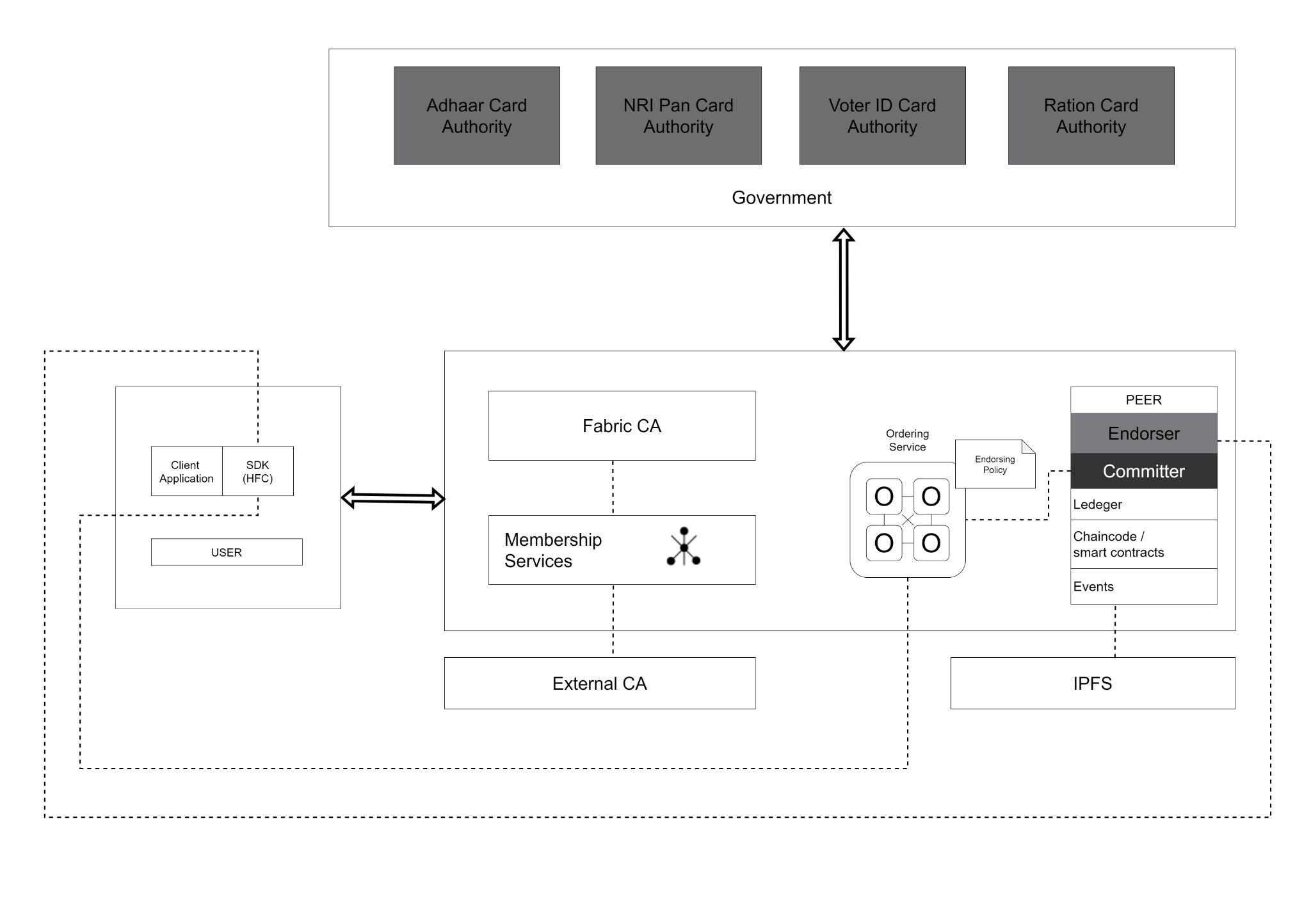
To initiate updates, users invoke the "UpdateInfo" function, which allows them to modify specific attributes. The function first creates an update key using the unique user ID of Aadhaar. By utilizing the "gatestate" function, the function verifies the existence of the user in the buffer and retrieves the user's data for further processing. Only the primary authority, i.e., the Aadhaar card authority, has permission to request updates. Once changes are made in the primary authority, the "UpdateInfo" function triggers the replication of updates to the secondary authorities. The function ensures that the hierarchy key of a secondary authority is one greater than the hierarchy key of the primary authority. This verification process ensures that updates propagate accurately, maintaining the integrity of the data.

The transaction flow involves sequential steps, including user registration with the primary authority, generation of unique user IDs, subsequent registration with secondary authorities, and the initiation of updates through the primary authority, leading to the replication of changes in the secondary authorities. These steps carried for the specified permissions and hierarchy within the blockchain system, providing an efficient and secure mechanism for updating government documents.



***Figure 4. Transaction workflow***

**5.4 Framework Architecture**

***Figure 5. Framework Architecture***

The proposed system utilizes various components and concepts from the enterprise resource planning (ERP) domain to facilitate the management of government documents on a Hyperledger blockchain as follows:

1. Fabric CA (Certificate Authority): Fabric CA is used to manage the digital certificates and identities of participants in the blockchain network. It ensures secure authentication and access control for the entities involved in the system, such as the authorities and users.

2. Ordering Services: Ordering services handle the ordering and sequencing of transactions within the blockchain network. They ensure that the transactions are processed in a consistent and agreed-upon order across all network nodes.

3. Membership Services: Membership services enable the registration, authentication, and management of network members, including the authorities and users. It verifies the identity of participants and grants them appropriate access permissions to the blockchain network.

4. IPFS (InterPlanetary File System): IPFS is a distributed file system that can be used to store and retrieve large files or documents. It provides a decentralized and resilient storage solution for storing the government documents associated with the system.

5. External CA (Certificate Authority): An external CA can be integrated into the system to provide additional security and trust for the digital certificates used by the participants. It ensures that the certificates issued by the authorities are valid and trustworthy.

6. Peer Node Structure: The blockchain network consists of peer nodes, which maintain a copy of the shared ledger and participate in the consensus process. The peer nodes communicate with each other to validate transactions, maintain the integrity of the blockchain, and replicate data across the network.

7. Endorsers: Endorsers are responsible for executing and validating transactions proposed by users. They apply the necessary business logic to verify the correctness of the transaction before endorsing it and forwarding it to the ordering service.

8. Committer: The committer is responsible for committing endorsed transactions to the blockchain ledger. It ensures that the transactions are permanently recorded and distributed to all participating nodes in the network.

9. User SDK and Application: Users interact with the system through a user software development kit (SDK) and application. The SDK provides a set of libraries and tools that allow users to interact with the blockchain network, submit transactions, and query the documents' status. The application provides a user-friendly interface for users to access and update their government documents.

**5.5 Algorithm**

**1. `beforeTransaction(ctx)`**

```

function beforeTransaction(ctx)

{

if (client is not from the authorized organization) then

throw "Access denied. Only authorized organizations can invoke this contract."

end if

}

```

**2. `registerOrganization(ctx)`**

```

function registerOrganization(ctx)

{

for each authority in authorities do

if (authority does not exist) then

create and store the authority

end if

end for

}

```

**3. `adhaarRegister(ctx, name, dob, pinCode, mobileNo)`**

```

function adhaarRegister(ctx, name, dob, pinCode, mobileNo)

{

if (user with Aadhaar details already exists) then

throw "User with the provided Aadhaar details already exists."

end if

create and store a new user with Aadhaar details

return the unique ID of the registered user

}

```

**4. `panRegister(ctx, name, adharUserID, dob, mobileNo)**`

```

function panRegister(ctx, name, adharUserID, dob, mobileNo)

{

if (user with PAN details already exists) then

throw "User with the provided PAN details already exists."

end if

if (user with the provided Aadhaar details does not exist) then

throw "User with the provided Aadhaar details does not exist."

end if

create and store a new user with PAN details

return the unique ID of the registered user

}

```

**5. `votingRegister(ctx, name, adharUserID, dob, pinCode)`**

```

function votingRegister(ctx, name, adharUserID, dob, pinCode)

{

if (user with voting card details already exists) then

throw "User with the provided voting card details already exists."

end if

if (user with the provided Aadhaar details does not exist) then

throw "User with the provided Aadhaar details does not exist."

end if

create and store a new user with voting card details

return the unique ID of the registered user

}

```

**5.6 Smart Contract**

The given smart contract is named "GovernmentDocumentsContract" and is implemented in JavaScript using the Fabric Contract API. It defines a contract for managing government documents and their registration process on a Hyperledger Fabric blockchain network. Let's analyze its technical aspects:

1. Dependencies:

`fabric-contract-api`: The `Contract` class is imported from this dependency, which provides the base class for creating smart contracts in Hyperledger Fabric.

`fabric-shim`: The `ClientIdentity` class is imported from this dependency, which allows access to client identity information and certificate-related operations.

2. Class Structure:

The contract class `GovernmentDocumentsContract` extends the `Contract` class provided by the `fabric-contract-api`.

It overrides the `beforeTransaction` method to implement access control based on the client's membership service provider (MSP) ID.

The contract defines several transaction functions for registering different types of government documents and updating user information.

3. Access Control:

The `beforeTransaction` method checks the client's MSP ID against a predefined `networkName` (in this case, 'org.gov-network.govnet.com'). If the MSP ID does not match, an error is thrown, denying access to unauthorized organizations.

4. Registration Process:

The contract provides functions for registering different types of government documents: Aadhaar, PAN, voting card, and ration card.

Each registration function checks the existence of the user and validates input parameters before registering the document.

The functions create a unique user ID based on the user's name, date of birth (DOB), and the corresponding authority ID. The generated ID is used as the key for storing user information in the ledger.

5. Updating User Information:

The `updateInfo` function allows users to update their information, such as name, DOB, pin code, and mobile number.

It first checks the existence of the Aadhaar user and updates the user's information.

Then, it iterates over the secondary authorities (PAN, voting, ration) and updates their corresponding user information if it exists.

6. Data Storage:

User information and authority details are stored in the ledger using unique composite keys.

User data is serialized as JSON and stored as a buffer in the ledger using the generated user ID as the key.

7. Helper Functions:

The contract includes helper functions like `authorityExists` and `userExists` to check the existence of authorities and users, respectively.

The `generateUniqueUserID` function creates a unique user ID based on the user's name, DOB, and authority ID.

This smart contract provides a basic framework for registering and managing government documents on a Hyperledger Fabric blockchain network. It enforces access control based on the client's MSP ID and ensures data consistency and integrity by validating inputs and maintaining unique user IDs. However, additional considerations such as data privacy, authorization rules, and more complex business logic may need to be implemented depending on the specific requirements of the government document management system.

**Chapter 6**

**Conclusion**

We have designed a Hyperledger blockchain solution to facilitate the efficient and secure updating of government documents. This system involves five entities: the user, Aadhaar Card Authority (primary authority), PAN Card Authority, Voting Card Authority, and Ration Card Authority (secondary authorities). The Aadhaar Card Authority holds a primary position, while the other authorities serve as secondary entities. Each authority stores specific attributes related to the respective document types. The registration process begins with the user submitting their information to the primary authority, which is then replicated to all secondary authorities. The user can request updates to their attributes by contacting the primary authority, who subsequently sends update requests to all relevant departments. The secondary authorities then request validation proof from the primary authority, which verifies the proof provided by the user. Upon validation, the secondary authorities replicate the updated changes.

To facilitate these operations, we have defined several functions. The "registerOrganization" function assigns hierarchy keys (hkeys) to the authorities based on their primary or secondary status. It also creates authority objects for each entity, ensuring they exist in the system. The "adhaarRegister" function enables users to register their Aadhaar Card information, generating a unique user ID based on their name, date of birth, and the document type. Similarly, the "panRegister," "votingRegister," and "rationRegister" functions allow users to register their PAN Card, Voting Card, and Ration Card details, respectively. The "UpdateInfo" function enables users to request updates to their attributes. It generates an update key based on the unique user ID of the Aadhaar Card and checks if the user exists in the buffer. The function allows changes to be made in the primary authority and subsequently transfers these updates to the secondary authorities based on the hierarchy key of each entity.

This blockchain-based system provides several advantages for government document management. It ensures the integrity and immutability of records, prevents unauthorized access, and facilitates seamless updates across multiple authorities. The use of a distributed ledger technology like Hyperledger ensures transparency, auditability, and trust in the system, enhancing the overall efficiency of government document management processes.

In conclusion, our Hyperledger blockchain solution offers a robust framework for managing government documents, streamlining the update process, and ensuring data consistency and security across multiple authorities. By leveraging the power of blockchain technology, we can create a transparent, tamper-proof, and efficient system that meets the evolving needs of government document management in the digital age.

**References**

1. Khanna, A., Sah, A., Bolshev, V., Jasinski, M., Vinogradov, A., Leonowicz, Z., & Jasiński, M. (2021). Blockchain: Future of e-governance in smart cities. *Sustainability, 13(21), 11840.*
2. Veeramani, K., & Jaganathan, S. (2020). Land registration: Use-case of e-Governance using blockchain technology. *KSII Transactions on Internet and Information Systems (TIIS), 14(9), 3693-3711.*
3. Pal, O., & Singh, S. (2019). Blockchain technology and it’s applications in e-governance services. *International Journal of Recent Technology and Engineering (IJRTE)*, *8*(4), 5795-5802.
4. Sen, S., Mukhopadhyay, S., & Karforma, S. (2021). A Blockchain based Framework for Property Registration System in E-Governance. *International Journal of Information Engineering & Electronic Business*, *13*(4).
5. Kadhum, O. I., & Hamad, A. H. (2023). Performance Evaluation of Multi-Organization E-Government Based on Hyperledger Fabric Blockchain Platform. *Journal homepage: http://iieta. org/journals/isi*, *28*(2), 499-507.
6. Agarwal, U., Rishiwal, V., Tanwar, S., Chaudhary, R., Sharma, G., Bokoro, P. N., & Sharma, R. (2022). Blockchain technology for secure supply chain management: A comprehensive review. *IEEE Access*.
7. Hu, S., Huang, S., & Qin, X. (2022). Exploring blockchain-supported authentication based on online and offline business in organic agricultural supply chain. *Computers & Industrial Engineering*, *173*, 108738.
8. Murad Ali Ahmad Al-Zaqebaa, Baker Akram Falah Jaraha, Nehad Ibrahim Ineizeha, Zeyad Almatarneha and Mufleh Amin AL Jarraha(2022) The effect of management accounting and blockchain technology characteristics on supply chains efficiency *https://growingscience.com/uscm/uscm.html*
9. Wan, P. K., Huang, L., & Holtskog, H. (2020). Blockchain-enabled information sharing within a supply chain: A systematic literature review. *IEEE access*, *8*, 49645-49656.
10. Singh, K. K. (2022). Application of Blockchain Smart Contracts in E-Commerce and Government. *arXiv preprint arXiv:2208.01350*.
11. Affaf Shahid, Ahmad Almogren, (Senior Member, IEEE), Nadeem Javaid1, (Senior Member,IEEE), Fahad Ahmad Al-Zahrani, Mansour Zuair, and Masoom Alam. (2022)Blockchain-Based Agri-Food Supply Chain: A Complete Solution How Blockchain Enhances Supply Chain Management *IEEE*
12. Shakhbulatov, D., Medina, J., Dong, Z., & Rojas-Cessa, R. (2020). How blockchain enhances supply chain management: A survey. *IEEE Open Journal of the Computer Society*, *1*, 230-249.
13. Wang, L., Xu, L., Zheng, Z., Liu, S., Li, X., Cao, L., ... & Sun, C. (2021). Smart contract-based agricultural food supply chain traceability. *IEEE Access*, *9*, 9296-9307.
14. Li, Y., Tan, C., Ip, W. H., & Wu, C. H. (2023). Dynamic blockchain adoption for freshness-keeping in the fresh agricultural product supply chain. *Expert Systems with Applications*, *217*, 119494.
15. Chang, S. E., & Chen, Y. (2020). When blockchain meets supply chain: A systematic literature review on current development and potential applications. *Ieee Access*, *8*, 62478-62494.