International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 11 | Nov 2024 www.irjet.net p-ISSN: 2395-0072

Reimagining Identity: A Decentralized Approach to Document Verification

Atharva Kumtakar[1], Nishant Khandagale[2], Amrish Karpe[3], Narhari Joglekar[4], Dr. Pramila Chawan[5]

[1] *B. Tech Student, Dept of Computer Engineering and IT, VJTI College, Mumbai, Maharashtra, India*
[2] *B. Tech Student, Dept of Computer Engineering and IT, VJTI College, Mumbai, Maharashtra, India*
[3] *B. Tech Student, Dept of Computer Engineering and IT, VJTI College, Mumbai, Maharashtra, India*
[4] *B. Tech Student, Dept of Computer Engineering and IT, VJTI College, Mumbai, Maharashtra, India*
[5] *Associate Professor, Dept of Computer Engineering and IT, VJTI College, Mumbai, Maharashtra, India*

Abstract - *The process of obtaining government-issued documents in India, such as Aadhar, PAN, and voter ID, often necessitates that citizens submit their personal information multiple times, resulting in redundant data entry, delays, and inefficiencies. This paper introduces a blockchain-based decentralized document issuance system designed to optimize this procedure. By securely storing verified personal details during the initial document application, citizens can access their pre-verified information via password authentication in subsequent applications, thereby eliminating redundancy and significantly reducing processing times. Upon the issuance of their first government document, such as an Aadhar card, a citizen's personal information—including address, age, gender, and family details—will be securely recorded on the blockchain. For future applications (e.g., PAN card, voter ID), citizens will simply need to provide a password to retrieve their pre-verified data, streamlining the process. Blockchain technology offers a promising way to address inefficiencies in the current system. Its decentralized and unchangeable nature provides a safe method for storing personal information that has been verified, ensuring security and transparency. By leveraging blockchain, the government can improve operational efficiency and security through a trustless system that safeguards privacy, maintains data integrity, and enhances transparency.*

Key Words: Blockchain, Decentralization, Data verification, Redundancy, Government documents

1.INTRODUCTION

The current system for issuing government documents in India often leads to inefficiencies and potential errors due to redundant data entry. Citizens must repeatedly provide personal information for each document application, wasting time and increasing the risk of data breaches and inconsistencies.

To address these challenges, this paper proposes a decentralized document issuance system based on blockchain technology. By storing verified citizen data on a distributed ledger, this system aims to streamline the process of obtaining government documents, improve data security, and enhance transparency.

The proposed system comprises the following components:

Blockchain Network: A decentralized network of nodes that maintains a shared ledger of citizen data.

Smart Contracts: Self-executing contracts deployed on the blockchain that automate the document issuance process and ensure data integrity.

Citizen Portal: A user-friendly interface for citizens to access their stored data and initiate document applications.

Additionally, this paper surveys various blockchain technologies to identify the most suitable framework for implementing this decentralized document is- suance system.

2.BLOCKCHAIN TECHNOLOGIES FOR DOCUMENT ISSUANCE

2.1 HLF

Hyperledger Fabric (HLF) serves as a permissioned blockchain platform, making it particularly advantageous for government scenarios that involve various authorized stakeholders such as government agencies, which need to verify and issue documents while maintaining data privacy and control. It facilitates private transactions and data sharing across networks, enabling the government to manage access levels for different institutions regarding

citizen data. Key features include permissioned access, where participation in the document issuance process is restricted to authorized entities, and private channels are employed to share sensitive information solely among relevant institutions. Its modular architecture supports integration with existing government databases, easing the migration from legacy systems. Smart contracts, or chain code, automate document verification and issuance, ensuring that when citizens apply for new documents, their pre-verified data is securely retrieved. The consensus mechanism used by Hyperledger Fabric, Practical Byzantine Fault Tolerance (PBFT), is efficient in environments where trust is established among participants.

2.2 PoA

Proof of Authority (PoA) is a consensus mechanism that assigns the responsibility of validating transactions to a select number of trusted nodes, or authorities. This model works exceptionally well in government contexts where specific trusted government agencies act as validators for citizen data. Key characteristics of Proof of Authority (PoA) include its capacity to establish centralized trust while still harnessing the advantages of decentralization, guaranteeing that only verified data is entered into the blockchain. PoA's efficiency facilitates quicker transaction processing than Proof of Work (PoW) systems, making it well-suited for extensive applications such as document issuance. Since the validators are recognized and trusted entities, the system can attain a high degree of security while utilizing fewer computational resources, rendering it a viable option for governmental operations.

2.3 ZKP

Zero-knowledge proofs enable someone to prove their knowledge of a value with- out disclosing the value to anyone. This feature is especially significant in government document issuance systems, where validating a citizen's personal in- formation—such as age or address—must be done without disclosing sensitive details. Key advantages of ZKP include its ability to protect personal information while still allowing for efficient verification processes. Even if parts of the blockchain are compromised, ZKP ensures that the actual data remains secure, thus enhancing overall system integrity. By employing ZKP, the government can maintain privacy and security in citizen data verification while streamlining the document issuance process.

2.4 Ethereum

Ethereum is a prominent decentralized platform that allows users to create smart contracts and build decentralized applications (dApps) in a public environment. While it offers a large developer community and a plethora of tools, Ethereum may face scalability challenges, particularly for applications that require a high volume of transactions, such as government document issuance. However, its established infrastructure and ability to support complex interactions make it a viable option for pilot implementations and proofs of concept in the development of a decentralized document issuance system.

2.5 Corda

Corda is a distributed ledger platform designed primarily for business use, with a strong emphasis on privacy and interoperability among different parties. Originally developed for the financial services sector, Corda allows only the necessary parties to access transaction data, ensuring confidentiality. This feature is beneficial in the context of government documents, where personal information should be accessible only to authorized entities. Corda also supports smart contracts, making it a suitable choice for automating document issuance processes.

2.6 EOSIO

EOSIO is a blockchain platform known for its scalability and flexibility, aimed at the development of decentralized applications. With its high transaction throughput and ability to manage complex smart contracts, EOSIO stands out as a promising technology for large-scale applications like government document issuance. The platform's emphasis on speed and efficiency can help streamline the process, reducing wait times for citizens seeking access to government ser- vices.

2.7 Algorand

Algorand utilizes a method known as Pure Proof of Stake, allowing for rapid transactions at minimal costs. This scalable blockchain platform is designed for rapid transaction finality, making it particularly well-suited for applications re- quiring quick responses, such as issuing government documents. By minimizing transaction fees and maximizing throughput, Algorand can enhance the efficiency of the decentralized document issuance system, ultimately benefiting citizens through faster access to their verified information.

2.8 Tezos

Tezos is a self-amending blockchain that supports smart contracts and aims to provide more secure and upgradable protocols. Its governance model allows for community-led updates, ensuring that the platform remains adaptable and sustainable over time. This feature is beneficial for a government document is- suance system, as it may need to evolve in response to changing regulations and technological advancements. Tezos combines a robust infrastructure with a commitment to

long-term viability, making it an attractive option for implementing a decentralized system for issuing government documents.

Here, 2.1, 2.2 and 2.3 are deemed suitable for usage. An overall view of the schema is shown below(see Fig. 1).

3 Proposed System

3.1 Problem Statement

The current centralized system for issuing government documents in India faces significant challenges, including redundant data entry, data security risks, and a lack of transparency. Citizens are forced to repeatedly provide personal information for each document application, leading to time-consuming processes and potential errors. Centralized systems are vulnerable to data breaches, compromising sensitive personal information. Additionally, the lack of transparency in the traditional system hinders the tracking of document processing and identification of potential bottlenecks.

Our solution is a blockchain-based decentralized document issuance system to mitigate the challenges and improve the overall efficiency and security of the document issuance process.

3.2 Problem Elaboration

The existing system for issuing government documents such as Aadhar cards, PAN cards, and Voter IDs is characterized by significant inefficiencies and security vulnerabilities. Citizens often face the cumbersome requirement of providing the same personal information repeatedly for different applications. This redundancy not only causes frustration but also raises the chances of errors during data entry, potentially resulting in delays in receiving important documents. These inefficiencies obstruct individuals from accessing essential services and fully engaging in civic activities. In addition to the challenges faced by citizens, the administrative burden on government agencies is substantial. The need to maintain multiple records for the same individual complicates data management and consumes valuable resources. Inconsistencies among various databases can create obstacles in verifying an individual's identity and eligibility for services, ultimately diminishing public trust in the system. Moreover, the risk of data breaches poses a critical threat to citizens' sensitive information. Storing personal data in multiple locations increases the chances of unauthorized access, making the entire system more vulnerable to attacks. A single breach can com- promise sensitive information across various platforms, leading to identity theft, fraud, and a broader erosion of trust in the government's capacity to protect personal data. To effectively tackle these issues, a blockchain-based decentralized document issuance system is proposed. By securely storing verified citizen data on a distributed ledger, this solution can eliminate the need for repeated data entry. Citizens would only need to provide their information once during the initial application, allowing subsequent applications for various documents to leverage pre-verified data. This simplification of the application process not only saves citizens time but also greatly minimizes the effort needed to manage and verify their information. Smart contracts will be integral to this system, automating the issuance and verification processes to ensure data integrity and reduce the potential for human error. By facilitating real-time updates and en- forcing predefined rules, smart contracts can enhance operational efficiency and reduce administrative overhead. Additionally, adopting a blockchain-based approach will improve transparency and security. Citizens will have greater control over their personal information, allowing them to manage who has access to their data. This empowerment builds trust and confidence in the government's capacity to protect sensitive information. Adopting a decentralized document is- suance system based on blockchain technology offers a transformative solution to address the inefficiencies and security risks inherent in the existing government document issuance process. By leveraging advanced technologies, the proposed system aims to create a more efficient, secure, and user-friendly experience for individuals seeking essential government services.

3.3 Problem Methodology

1] Requirement Analysis:

A] Identify the necessary personal details required for various government documents (e.g., Aadhar, PAN, voter ID).

B] Understand the current processes for document issuance and the challenges citizens face, such as redundancy and lengthy verification times.

2] Blockchain Design:

A] Create a blockchain framework designed to securely store and manage citizen data, guaranteeing that the information remains immutable and protected from tampering.

B] Establish access control measures to ensure that only authorized govern- ment officials can access and validate this data.

3] User Registration and Verification:

A] Develop a process for citizens to register for their first document (e.g., Aadhar) by filling out a comprehensive form.

B] Implement a secure method for verifying the details provided by citizens, utilizing government databases and manual checks if necessary.

4] Data Storage:

A] Use a decentralized ledger technology (DLT) to store the verified details on the blockchain.

B] Assign a unique password to citizens, allowing them to access their data for future applications.

5] Subsequent Document Applications:

A] Create a streamlined process for citizens applying for additional documents (e.g., PAN or voter ID) to retrieve their existing data from the blockchain using the provided password.

B] Ensure that the application process is simple and user-friendly. – Interoperability with Government Systems:

C] Design the system to be compatible with existing government databases and processes to facilitate smooth transitions and data sharing.

D] Train government officials on using the new system for efficient document issuance.

6] Testing and Validation:

A] Conduct thorough testing of the entire system, including user interfaces, blockchain functionalities, and data retrieval processes.

B] Validate the system against security, efficiency, and usability bench- marks.

7] Deployment and User Training:

A] Deploy the system in a phased manner, starting with pilot programs in select regions.

B] Provide training sessions for citizens and government officials to ensure effective use of the new system.

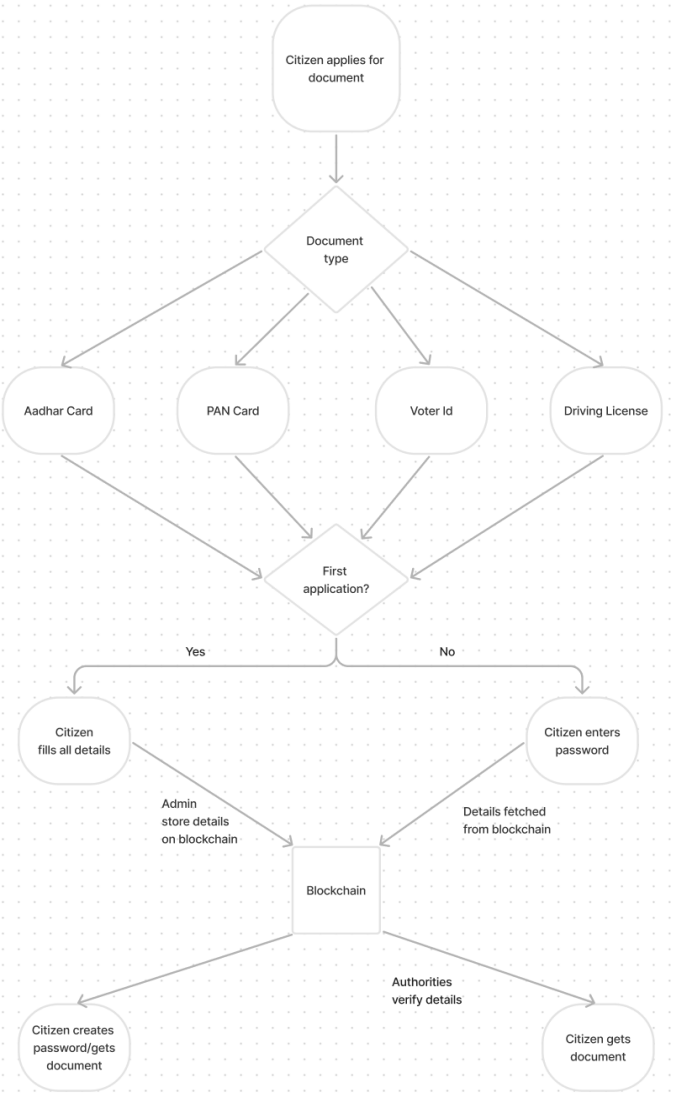

Fig -1: Flow of the system

4. CONCLUSIONS

The conventional system for issuing government documents in India is marred by inefficiencies, security vulnerabilities, and a lack of transparency. Citizens are frequently burdened with the repetitive task of providing personal information for numerous document applications, resulting in time-consuming processes and potential errors. Centralized systems are susceptible to data breaches, compromising sensitive personal information. Moreover, the opacity of the traditional system hinders the tracking of document processing and identification of potential bottlenecks. To address these challenges and enhance the overall efficiency and security of the document issuance process, this paper proposes a blockchain-based decentralized document issuance system using hyper ledger fabric. By securely storing verified citizen data on a distributed ledger, this system aims to streamline the document issuance process,