advances in Technology

Adv. Technol. 2025, 5(2), 106-118

Full Paper

Ensuring Citizen Autonomy through Blockchain: A Single Identity Framework with the Right to Control the Availability of Information

D.M.T.W. Disanayaka, P.K.P.A. Panapitiya, J.A. Aathil, B.N.S. Lankasena*, and H.M.S.C.R. Heenkenda

Department of Information and Communication Technology, Faculty of Technology, University of Sri Jayewardenepura, Homagama, Sri Lanka.

Corresponding Author: nalaka@sjp.ac.lk, nalaka.lankasena@gmail.com; ORCID: 0000-0002-4812-6513

Received: 17 August 2024; Revised: 03 October 2024; Accepted: 09 October 2024; Published: 20 June 2025

Abstract

Centralized electronic national identity systems have emerged as a popular solution to address the inefficiencies and limitations of traditional, hardcopy-based identity management. However, these centralized systems are prone to significant challenges, including single points of failure, data breaches, and restricted citizen control over personal information. These issues highlight the necessity for a more resilient framework that not only provides unique identification but also empowers citizens with control over their data. This study presents a decentralized citizen identity management and verification system built on Hyperledger Fabric and private blockchain technology. The proposed framework addresses critical issues in current systems, such as gas fees, scalability, and operational costs, while enhancing security, privacy, and user autonomy. The system leverages the privacy-preserving features of a private blockchain to ensure that only authorized entities can access and participate in the network, mitigating the risk of unauthorized access. The research involved constructing a Hyperledger Fabric network, defining transaction logic to control the lifecycle of data objects within the ledger using the Hyperledger Fabric SDK for Node.js, and developing a web-based interface for interaction through the MERN (MongoDB, ExpressJS, ReactJS, Node.js) stack. By empowering users to manage and control the information they share with third parties, we ensure their data remains private, secure, and shared only on their terms. The proposed blockchain-based solution offers a robust alternative to existing identity management systems, addressing their key limitations. A distinguishing feature of the system is its network design, which restricts participation to authorized government organizations, safeguarding citizen data's integrity and confidentiality.

Keywords: citizen identification and verification system, hyperledger fabric, national identity, private blockchain, right to citizens

Introduction

In today's digital era, the need for a reliable and secure citizen identification system has become increasingly crucial. The Immigration and Refugee Board of Canada [1] reported several identity fraud incidents resulting from manual identity verification processes in various countries. Centralized electronic identity verification systems have been proposed to address the issues associated with manual verification.

Traditional systems for verifying citizen identity information are plagued by inefficiency, a lack of transparency, and limited control over personal data. Blockchain technology has emerged as a potential solution to these challenges by providing a decentralized and immutable platform for managing sensitive information [2]. Blockchain is a shared database maintained by a network of computers, making it highly resistant to hacking or tampering. It can be used to store various types of data, including citizen identity information [3, 4].

A blockchain-based citizen identification system would offer several advantages over traditional systems. It would provide greater transparency, as all transactions and data would be recorded on the blockchain and visible to all participants. As a result, this system can potentially revolutionize the management of citizen identity information, significantly reducing fraud and identity theft. There are multiple ways to implement a blockchain-based citizen identification system. One option is to use a public blockchain, such as Bitcoin or Ethereum. This approach would enable a decentralized system that is not controlled by any single entity, although it can be slow and expensive [2, 5]. Another option is to use a private blockchain, which is owned and operated by a single entity or group of entities. This method would result in a more efficient and cost-effective system [6].

This paper outlines the development of a citizen identity management and verification system using the Hyperledger Fabric framework, a private and permissioned blockchain. The design and implementation of the blockchain-based system have been customized to meet the specific needs of Sri Lanka. Citizens' identities are managed under a unified identity system by government organizations responsible for handling identity information. Additionally, this study enables public service organizations to request necessary information from citizens, who can then authorize access to their data. Furthermore, smart contracts and distributed applications (DApps) were developed to support the above mentioned processes.

Current National Identity Card System in Sri Lanka

A report by the Immigration and Refugee Board of Canada [1] notes that although Sri Lanka is in the digital age, it still relies on hard-copy documents to validate citizens' identities, leading to numerous incidents involving the creation of counterfeit identity documents. This reliance on physical documentation makes it easier for counterfeit documents to be produced and used for identity theft. The report further highlights that counterfeit documents are most commonly associated with national identity cards, driving licenses, and passports. Smart identity cards, designed with machine-readable barcodes and biometric information, aim to be tamper- and forgery-proof.

However, in Sri Lanka, citizens currently use either an old identity card or an electronic identity card based on a centralized database for electronic identification systems. According to Sin and Naing (2019), current citizen management systems fail to address issues such as human error, challenges in identity recovery, and forgotten identities. Identity management involves several key activities, including registration, updating, confirming, and verifying identities.

Blockchain Technology and its Advantages

Blockchain operates on the advanced technology of electronic ledgers, where data cannot be altered or modified in any way [5]. To make any changes to the blockchain network, the consent of all participating nodes is required, and only approved and confirmed transactions are added. Jha *et al.,* (2019) noted that once consensus is achieved, the distributed ledger is updated to reflect the latest version, thereby preserving the integrity of the blockchain. Its core features, including decentralization, integrity, reliability, and traceability, ensure confidence and trust in the secure storage of digital identity data. Despite maintaining a continuously growing list of blocks, Elisa *et al.,* (2018) explain that blockchain secures data using public key cryptography. Sin and Naing (2019), Elisa *et al.,* (2018), and Jha *et al.,* (2019) all conclude that a decentralized blockchain system offers a superior solution, as it serves as a single point of reference for all records and information [7].

According to *Elisa et al.,* (2018), centralized database systems face numerous challenges, including a single point of failure and a single point of trust, which make them vulnerable to Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. In contrast, blockchain technology offers highly secure and privacy-protected services through decentralized databases. Additionally, data is encrypted and distributed among peers in the blockchain network, further enhancing its security. Blockchain-based systems enhance government legitimacy by providing citizens with reliable information. They also offer advantages such as improved government service delivery, increased transparency in information distribution, cross-organizational information exchange, and enhanced credit systems.

Blockchain-Based Citizen Identity Management and Verification

Due to the significant drawbacks of existing citizen management systems, Elisa *et al.,* (2018) proposed a blockchain-based identity management solution to address these challenges. Blockchain wallets and addresses enable the exchange of information between the government and citizens. Jha *et al.,* (2019) suggested using a decentralized application as an intelligent component to enhance transaction efficiency within blockchain systems, providing a straightforward solution for connecting citizens to the decentralized blockchain-based backend of a smart contract-based government identity management system.

Considering the concerns related to lost, forgotten, or recovering physical identity assets and validations, Sin and Naing's (2021) proposed solution is simple and effective. Moreover, citizens can trace organizations that have verified their identity information within the last six months. Juan *et al.,* (2018) and Paez *et al.,* (2020) have integrated encrypted e-IDs with a blockchain-based citizen management system to mitigate identity fraud and security issues [8, 9]. Additionally, Panchamia and Byrappa (2017) addressed the challenge of integrating the migration process with citizen management [10]. This paper presented a methodology for storing correlated data on the blockchain linked to an individual's identity, along with access control mechanisms enabling authorized organizations to manipulate the data in a smart contract-based blockchain system, while preventing unauthorized access.

The framework presented by Datta *et al.,* (2020) manages citizen information at three levels using blockchain technology [11]. It comprises three interconnected sectors: the central station, sub-station, and rural station, with the mechanism designed to ensure the scalability of the blockchain system. Fathiyana *et al.,* (2022) proposed a Hyperledger Fabric-based citizen identity management system to integrate the blockchain system with existing physical assets [12]. A chain code application connects citizens to the blockchain network and facilitates the coexistence of multiple organizations within the system. With the support of these assets, the chain code validates users. Citizens can view all transaction records but cannot participate in them. The civil registration authority holds significant power to write, update, and delete information. At the same time, third-party organizations or the private sector can access basic citizen information through the system for identity verification. Malik *et al.,* (2019) proposed an approach to maintaining transparency in blockchain transactions. Their method encrypts stored citizen identity information using public key encryption, allowing the government and individual citizens to decrypt it.

We found that Robaitul Islam Bhuiyan *et al.,* (2021), Fathiyana *et al.,* (2022), Malik *et al.,* (2019), and Panchamia and Byrappa (2017) utilized Hyperledger Fabric to develop their citizen identity management and verification systems. Several researchers, including Elisa *et al.,* (2018), Juan *et al.,* (2018), Paez *et al.,* (2020), Tonu *et al.,* (2019), and Datta *et al.,* (2020), have also employed private blockchain technology for their citizen identity management and verification systems [6-14]. Notably, since Hyperledger Fabric is a private blockchain, our literature survey indicates that 56.3% of the studies used a private blockchain to implement Citizen Identity Management Systems. In contrast, Mudliar *et al.,* (2018), Jha *et al.,* (2019), Sin and Naing (2021), Htet *et al.,* (2020), and Amujo *et al.,* (2019) developed citizen identity management and verification systems using Ethereum, which is a public blockchain [15].

Hyperledger Fabric

Hyperledger Fabric is an open-source permissioned blockchain that offers features such as smart contracts, distributed ledgers, client libraries, and a graphical user interface (GUI). It provides flexibility, scalability, and security, with Membership Service Providers (MSPs) managing the blockchain nodes. The logic of the blockchain is established through smart contracts, also known as chaincode. In this framework, the identity of each node is visible to all others, and every node must authenticate to participate in the network and initiate transactions. This transparency allows each node to know who is accessing the data. These features enable us to implement access control privileges for participants in the blockchain at various levels. Utilizing Hyperledger Fabric for document verification facilitates handling high transaction rates while improving overall performance. We can achieve data partitioning on the blockchain by implementing different channels, thereby enhancing data privacy [6].

Unlike public blockchains like Ethereum, which are energy-intensive and open to anyone, Hyperledger Fabric provides a more efficient and secure application environment [2, 5]. Its permissioned nature enables controlled participation within the network, which is critical for managing sensitive citizen data [6]. The consensus algorithm employed by Hyperledger Fabric consumes significantly less energy than Ethereum, making it a more sustainable option for large-scale deployments. This energy efficiency, combined with its ability to manage permissions and data visibility, aligns perfectly with our objectives of privacy and

controlled access [6]. In research conducted by Jamal *et al.,* (2019), the authors defined several features of decentralized applications (DApps). They designed a user interface that allows third parties to submit requests and access user information to interact with the blockchain [16]. The interface includes features such as requesting user details, viewing user details, authority login, and a homepage, as illustrated in the attached screenshots. In this research, we adapted these DApp features to facilitate user interactions within our system.

Research Problem

To address the limitations of traditional manual and centralized citizen identity management systems, blockchain-based solutions are proposed to ensure the confidentiality, integrity, and availability of information [7, 12, 13, 17]. Traditional systems face significant drawbacks, such as a single point of failure [4, 7], the risk of data breaches [2, 7], and, most critically, the lack of citizen authority over the availability of their personal data [7]. Current systems employing single identity management concepts and public blockchain systems fail to grant citizens control over the availability of their information [5, 7, 12, 17].

According to Amujo *et al.,* (2019), a blockchain is an ordered, back-linked list of transactions, where every block refers to the previous one, and a copy of the blockchain is distributed among all peers. This structure makes altering or tampering with information practically impossible, ensuring high security and transparency. Several decentralized blockchain-based identity management systems have been developed using Ethereum blockchain technology for citizen identity management. Ethereum reliance on high energy consumption, such as high gas fees and extensive storage requirements, makes it less efficient for large-scale blockchain systems. Additionally, as a permissionless blockchain, Ethereum allows anyone to join the network anonymously, which limits control and security [2, 5]. Sin and Naing (2021) proved that users must obtain pre-verification from network participants to create validated blocks in a private blockchain system to offer a solution by allowing only restricted users to participate. This approach grants central organizations more control over their operations while maintaining the benefits of a decentralized system. To address the significant research gaps in existing citizen identity management systems, such as the lack of citizen control and the significant risks of centralized failures, we proposed a novel framework with a decentralized, private, and permissioned blockchain system extended with single identity management. The proposed system will prioritize transparency, immutability, integrity, and security, providing a robust solution for managing and verifying citizens through single identity information while empowering citizens with greater control over their identity information.

Materials and Methods

In our system, users include government authorities responsible for maintaining citizenship identity information, such as the Department of Registration of Persons, the Department of Motor Traffic, the Registrar General's Department, and the Department of Immigration and Emigration. It also includes other government and authorized organizations that will utilize citizens' information, citizens, non-government organizations, and foreign immigration and emigration authorities. The government authorities manage

the citizenship identity information by inserting and updating citizen data in the ledger using a single identity. We have regulated the availability of this data, allowing government organizations and foreign immigration and emigration authorities to access information about a citizen only for specific services.

Citizens were also granted the authority to determine what information can be shared with non-governmental organizations. These organizations cannot access a citizen's identity details without their explicit permission. When necessary, a non-governmental organization must request specific information directly from the citizen. The citizen can then accept the request to grant access. A smart contract was created to define the transactions that should be executed on the Hyperledger Fabric network. Distributed applications were developed using NodeJS, the Hyperledger Fabric SDK (Software Development Kit), ReactJS, and MongoDB to enable interaction between users and the smart contract. Figure 1 below illustrates the overall proposed framework architecture of our project.

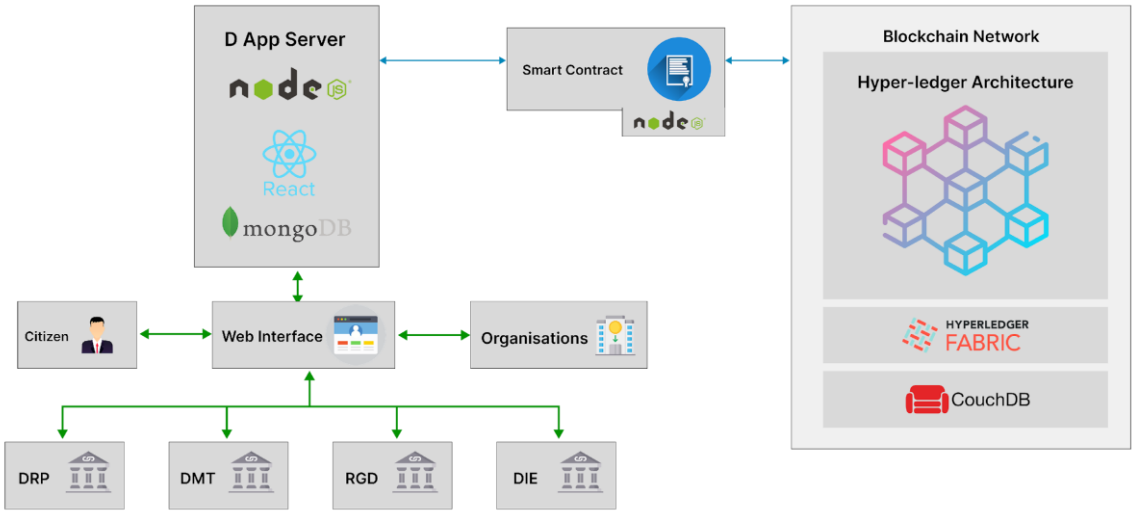

Figure 1. Proposed Framework Architecture

The proposed system uniquely addresses the need for a decentralized identity management solution by utilizing a private blockchain that enables user-governed conditions for data accessibility. The framework integrates a Hyperledger Fabric network to achieve decentralized storage of citizen identity information maintained by four authorized government organizations. Citizens can control access to their information through smart contracts, making the system both transparent and aligned with individual privacy preferences. This approach fulfills the novelty of the study by developing a decentralized blockchain that meets the critical requirement of granting citizens authoritative control over the availability of their data.

To accomplish our research objectives, we created a permission-based private blockchain using Hyperledger Fabric. By implementing Hyperledger Fabric in our proposed solution, we can regulate who can participate in the network, thereby enhancing its governance. For the development of the Hyperledger Fabric blockchain, we utilized Docker, Docker Compose, and CouchDB.

Experimental Setup

The following steps were followed in order to deploy Hyperledger Fabric.

1. Set up an Ubuntu VM and installed Docker, Docker Composer, NodeJS, CouchDB, and NPM (Node Package Manager).
2. Downloaded Fabric CA 1.4.9 and Fabric 2.2.2.
3. Used the Hyperledger Fabric test network to define and set up the network.
4. Developed and deployed a smart contract (chaincode) defining the application's logic and rules.

Hyperledger Fabric Network Creation

Hyperledger Fabric provides a test network to test smart contracts. This network contains two organizations and a peer for each organization. The network.sh bash file can be used to start the network. This was accomplished by running "./network.sh up createChannel -c mychannel -ca -s couchdb" command. In order to run the network, Docker containers were created for Orderer, organizations, peers, certificate authority (CA), and CouchDB.

Chaincode (Smart Contract) Development

Before initiating transactions on Hyperledger Fabric, it is essential to define a common set of contracts that encompass shared terms, rules, concept definitions, and processes. These contracts outline the transaction logic for managing the lifecycle of data objects within the ledger. The contracts are represented as executable code, commonly referred to as smart contracts. Transactions are created on the ledger through the invocation of these functions by the Distributed Applications. The chaincode for this system was developed using the Hyperledger Fabric SDK for Node.js. The chaincode (smart contract) lifecycle on a Hyperledger Fabric network involves five steps: developing the chaincode, packaging it, installing it on all peers, obtaining approval from member organizations, and committing it to the channel. The command "./network.sh deployCC -ccn blockchainid -ccp../chaincode/blockchainid-javascript/ -ccl javascript" is then used to deploy the chaincode to the network.

Application Development (DApp)

1. **Backend Development:** To interact with the chaincode (smart contracts), we developed distributed applications. By having a user identity, we can run smart contracts, receive ledger updates, and add information to the ledger. The application serves as a gateway to the Hyperledger Fabric network and was developed using the Node.js-based Hyperledger Fabric SDK. For our project, we created two Node.js applications: one for citizen identification management (government app) and another for citizens and organizations (public app). Government agencies using the citizen identity management app include the Department of Registration of Persons, the Department of Motor Traffic, the Registrar General's Department, and the Department of Immigration and Emigration.

Through the public app, authorities can verify citizens' information using the blockchain, and citizens have the ability to grant access to non-government organizations to view their information.

As part of the DApp setup, an admin user was initially enrolled, and a user was registered between the application and the certificate authority. Our applications can invoke chaincode functions and execute transactions on the blockchain once all users have been enrolled. Through that identity, we open the gateway to the peer of organization 01 to run the chaincode. This process is illustrated in "Figure 2."

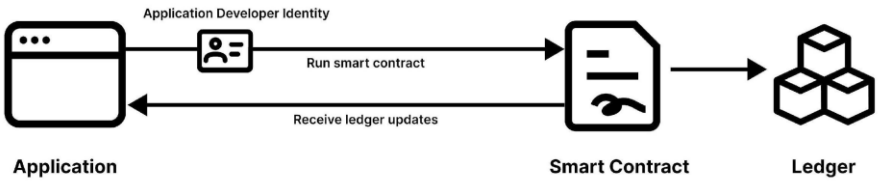

Figure 2. Distributed Application Interaction with Blockchain

The database for registering, logging in, and authenticating users was built using MongoDB.

2. **Frontend Development:** The primary objective of the front-end development of the application was to design a user-friendly and intuitive interface for both the citizen identity management app and the public app. React.js was utilized for this task, along with other complementary libraries such as React Router for navigation management and Axios for sending HTTP requests to the backend.

Main Components

The proposed system consists of a number of main components, which are described below.

1. **Administrative Unit:** The Department of Registration of Persons (DRP) is the main administrator in the system, and the administrative unit is responsible for the following tasks:
    - Create user accounts for the other three departments: the Department of Motor Traffic, the Registrar General's Department, and the Department of Immigration and Emigration.
    - Insert initial citizen identity information into the blockchain.
    - Modify citizen identity-related information in the blockchain.
    - Verify citizen user registration in the Distributed Application.
    - Verify private organization users' registration in the Distributed Application.

2. **Citizen Identity Management Unit:** This unit consists of the users who manage citizen information: the Department of Registration of Persons, the Department of Motor Traffic, the Registrar General's Department, and the Department of Immigration and Emigration. Once the initial information is added to the blockchain by the Department of Registration of Persons, the

other three departments can add information related to citizen identification by mapping it to a national identity card (NIC) number. The Department of Motor Traffic is responsible for adding and updating information about driving licenses, while the Registrar General's Department manages the addition and updating of birth registration information for citizens. The Department of Immigration and Emigration handles the addition and updating of passport information for citizens. We facilitated these tasks in the distributed application to effectively manage citizen information in the ledger.

3. **Hyperledger Fabric Model:**
   The Hyperledger Fabric model is the core of the system, managing the Hyperledger Fabric network, ledger, channel, and smart contracts. The network is created by running the test network available in the Hyperledger Fabric samples. When we define the channel name, the network is deployed on our local computer as a network of Docker containers. After the network is created, the chaincode is installed in the blockchain network. The state databases for this blockchain network are established using CouchDB. Smart contracts enable users to insert information into the blockchain network following these processes. Additionally, they allow users to retrieve information that has been inserted into the blockchain. The blockchain ensures the integrity of the information stored within it.

4. **Citizen User Unit:** Our system enables citizens to create user accounts and view and confirm requests from non-government organizations and third parties to access their information. A citizen account can only be utilized once it has been activated by the Department of Registration of Persons.

5. **Citizen Identity Verification Unit:** Citizens' information is accessible to government organizations, non-governmental organizations, and foreign immigration and emigration authorities through this unit. However, non-governmental organizations must specify the information they need to verify for a given citizen; otherwise, they will not be granted access to the citizen's information. This information is sent as a request to the citizen and stored in the ledger. Once approved by the citizen, the requested information becomes accessible for viewing.

Results and Discussion

Our research successfully addresses the challenges of single identity management and controlled information accessibility through the development of a novel permission-based private blockchain framework using Hyperledger Fabric. This framework integrates the characteristics of private blockchain technology to provide a secure, transparent, and user-controlled environment for citizen identity management and verification.

In this research, we developed a permission-based private blockchain using Hyperledger Fabric for citizen identity management and verification, which consists of an administrative unit, a citizen identity management unit, a Hyperledger Fabric blockchain model, a citizen user unit and a citizen identity

verification unit. Through the use of smart contracts, citizens can control who may access their identity information. Therefore, the framework is capable of empowering citizens with the right to control the availability of their personal information.

The evaluation results demonstrated the successful implementation and functionality of the developed system. Despite initial challenges and the need to switch blockchain platforms, we executed a comprehensive set of test cases to ensure the system's functionalities' effectiveness, accuracy, and reliability across various user roles and scenarios. We tested the functionalities of chain code, such as deploying chain code in the blockchain network, connecting to the blockchain network, and all the functions related to citizen identity information management and verification in the blockchain. We tested functionalities in the two distributed applications, which are the government app and public app. In the government app, we tested 'insert' and 'update' citizen identity information by four government departments, which manage citizen identity information, create user accounts for the other three government departments, and view citizen information changelogs. In the public app, we tested creating requests to view citizen information by third-party organizations, view accepted and pending requests by citizens and third-party organizations, accept requests by citizens, and view citizen information after the acceptance. All of those functionalities were successfully passed. The developed system effectively implements a single identity mechanism, allowing for unified and secure management of citizen identity information across four authorized government organizations. Appendix 1 contains the main user interfaces of the system (Figures S3 to S10).

Comparative Insights

The developed framework for citizen identity management and verification highlights a significant advancement by integrating single identity management, private blockchain features, and controlled information access. The system enhances data security, integrity, and transparency while providing authority to citizens to overcome the limitations of traditional identity management approaches. We have developed a solution tailored to meet the specific needs of managing sensitive citizen data securely and efficiently by utilizing the strengths of Hyperledger Fabric and a Single Identity Management model [6].

Hyperledger Fabric was chosen as the blockchain platform due to its permissioned nature, which ensures controlled participation within the network. This is critical for safeguarding sensitive citizen information [6]. Our comprehensive literature review of various blockchain technologies confirmed that Hyperledger Fabric is the most suitable choice for our system. Unlike public blockchains like Ethereum, which are energy-intensive and open to all, Hyperledger Fabric provides a more energy-efficient, secure, and private environment. Its consensus algorithm consumes significantly less energy than Ethereum, making it more sustainable for large-scale applications. This energy efficiency combined with its ability to manage permissions and data visibility, aligns perfectly with our goals of maintaining privacy and controlled access [2, 5, 6].

Our system draws inspiration from previous research works, including higher-level architecture for government agencies in Fathiyana *et al.,* (2020), the passport authority system in Bhuiyan *et al.,* (2021), and user nodes for different organizations in blockchain network in Elisa *et al.,* (2018). Byrappa (2017)] proposed a system to manage passports, visas, and immigration, and the blockchain network is also open to foreign countries [7]. However, Juan *et al.,* (2018) blockchain network only consisted of government organizations, and Paez *et al.,* (2020) adopted that blockchain network. These researchers proposed blockchain-based architectures for citizen information management with different approaches which involve a combination of government and private organizations. But our framework introduces a more efficient and citizen-focused approach. The features of the unique system proposed for Sri Lanka were influenced by previous studies relevant to citizen information management and verification systems based on Hyperledger Fabric and other private blockchain technologies.

The developed system integrates identity information, including birth certificates, driving licenses, and immigration data, into a single identity record that is centrally managed and verified by authorized government organizations, including the Department of Registration of Persons, the Department of Motor Traffic, the Registrar General's Department, and the Immigration and Emigration Department. This allows our system to address issues of fraud and data inconsistencies, which are prevalent in traditional systems [1]. By effectively utilizing the single identity mechanism in a novel framework, we enhance both data management and accessibility. With the immutable nature of blockchain, we ensure that previously entered information about citizens cannot be modified. When a government authority modifies citizens' identity information, it will add a new block to the blockchain, and the changes to the information can be observed as a version history. One of the most distinguishing features of our framework is its emphasis on citizen authorization. Citizens are granted control over who can access their personal information through the use of smart contracts. Third-party non-government organizations cannot directly access citizen data without explicit permission from the individual citizen. This addresses a critical gap in traditional identity management systems, where citizens often lack control over their personal information. The system was developed in line with software standards for evolution and maintenance concerns [18-20].

Our system provides a user-centered approach, allowing citizens to easily manage data access and ensuring that their privacy preferences are respected at all times [5, 7, 12, 17]. Referring to the need for distributed applications mentioned in the Jamal *et al.,* (2019), we developed two distributed applications as part of our framework: a government app for authorized government organizations to manage and update citizen information (Figure S1 to S4), and a public app for citizen and non-government organization interaction (Figure S5 to S8) [16]. The government app allows for the insertion and updating of various types of identity data while managing user accounts across different government departments. The public app enables citizens to register, view their information, and handle requests from non-government organizations to permit to view requested identity information. Non-government organizations can request access to personal information from citizens through distributed applications. The requested information is only made available once the citizen grants explicit consent. Both applications are web-based and equipped with user-friendly interfaces that facilitate smooth interaction with the blockchain network, ensuring the system remains functional and accessible to all users.

Conclusions

In conclusion, we developed a novel framework utilizing a permissioned private blockchain with Hyperledger Fabric for citizen identity management and verification. Our framework was designed to address the limitations of existing systems by incorporating essential features, including a single identity mechanism, control access, and the availability of citizen identity information. Through a comprehensive literature review, we identified the limitations of existing systems and used Hyperledger Fabric as the blockchain platform due to its suitability for our objectives. We developed a system where government authorities manage citizen identity information using a single identity, and citizens have control over data access through non-government organizations. An individual's citizenship identity information can be inserted and updated using a single identity by government agencies such as the Department of Registration of Persons, the Department of Motor Traffic, the Registrar General's Department, and the Immigration and Emigration Department. Among the main components of the model are the administrative unit, citizen identity management unit, Hyperledger Fabric model, citizen user unit, and citizen identity verification unit. Our system presents an energy-efficient blockchain solution for verifying citizen identity information and empowering citizens with control over their data. This research contributes to ongoing efforts in Sri Lanka to enhance the citizen identification system by leveraging blockchain technology to minimize identity theft and fraud. Further customizations and enhancements will be made to facilitate the engagement of other selected government agencies with the ledger in the future. Further, we may need to modify both the codes and the architecture of the proposed system so that it can be customized for other countries to manage, verify, and control citizen identity information.

Conflicts of Interest

The authors declare no conflict of interest.

Funding

This research did not receive any specific grants from funding agencies.

References

[1] Immigration and Refugee Board of Canada, "Responses to Information Requests - Immigration and Refugee Board of Canada," Irb.gc.ca, Aug. 06, **2020**. https://irb.gc.ca/en/country-information/rir/Pages/index.aspx?doc=458143&pls=1 (accessed Jun. 11, 2025).

[2] Jha, A., Bhattacharjee, R.K., Nandi, M., and Barbhuiya, F.A., *A Framework for Maintaining Citizenship Record on Blockchain*, in *Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure*. **2019**, ACM Press. p. 29-38.

[3] Mudliar, K., Parekh, H., and Bhavathankar, P., *A comprehensive integration of national identity with blockchain technology*, in *2018 International Conference on Communication information and Computing Technology (ICCICT)*. **2018**, IEEE. p. 1-6.

[4] Amujo, O., Ebelogu, C.U., Agu, E.O., and Hammawa, M.B., Development of a national identity management system using blockchain technology. African Journal of Computing & ICT, **2019**. 12, 13-36.

[5] Sin, E.S. and Naing, T.T., *Digital Identity Management System Using Blockchain Technology*, in *International Conference on Innovative Computing and Communications*. **2021**, Springer Singapore: Singapore. pp. 895-906.

[6] Malik, G., Parasrampuria, K., Reddy, S.P., and Shah, S., *Blockchain Based Identity Verification Model*, in *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)*. **2019**, IEEE. p. 1-6.

[7] Elisa, N., Yang, L., Chao, F., and Cao, Y., A framework of blockchain-based secure and privacy-preserving E-government system. Wireless Networks, **2018**. 29*(3)*, 1005-1015. 10.1007/s11276-018-1883-0.

[8] D. Juan, M., P. Andrés, R., M. Rafael, P., E. Gustavo, R., and C. Manuel, P., A Model for National Electronic Identity Document and Authentication Mechanism Based on Blockchain. International Journal of Modeling and Optimization, **2018**. 8*(3)*, 160-165. 10.7763/ijmo.2018.V8.642.

[9] Páez, R., Pérez, M., Ramírez, G., Montes, J., and Bouvarel, L., An Architecture for Biometric Electronic Identification Document System Based on Blockchain †. Future Internet, **2020**. 12*(1)*, 10. 10.3390/fi12010010.

[10] Panchamia, S. and Byrappa, D.K., *Passport, VISA and Immigration Management Using Blockchain*, in *2017 23RD Annual International Conference in Advanced Computing and Communications (ADCOM)*. **2017**, IEEE. p. 8-17.

[11] Datta, P., Bhowmik, A., Shome, A., and Biswas, M., *A Secured Smart National Identity Card Management Design using Blockchain*, in *2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT)*. **2020**, IEEE. p. 291-296.

[12] Fathiyana, R.Z., Yutia, S.N., and Hidayat, D.J., Prototype of Integrated National Identity Storage Security System in Indonesia using Blockchain Technology. JOIV : International Journal on Informatics Visualization, **2022**. 6*(1)*, 109. 10.30630/joiv.6.1.877.

[13] Islam Bhuiyan, M., Wara, T., and Sultana, S., A secured blockchain based integrated framework for national identity and passport. BAIUST Academic Journal, **2021**. 2, 19-32.

[14] Tonu, M.A.R., Hridoy, S., Ali, M.A., and Azad, S.A., *Block - NID: A Conceptual Secure Blockchain Based National Identity Management System Model*, in *2019 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*. **2019**, IEEE. p. 1-7.

[15] Htet, M., Yee, P.T., and Rajasekera, J.R., *Blockchain based Digital Identity Management System: A Case Study of Myanmar*, in *2020 International Conference on Advanced Information Technologies (ICAIT)*. **2020**, IEEE. p. 42-47.

[16] Jamal, A., Helmi, R.A.A., Syahirah, A.S.N., and Fatima, M.-A., *Blockchain-Based Identity Verification System*, in *2019 IEEE 9th International Conference on System Engineering and Technology (ICSET)*. **2019**, IEEE. p. 253-257.

[17] Fathiyana, R., Hidayat, F., and Rahardjo, B., *An Integration of National Identity towards Single Identity Number with Blockchain*, in *Proceedings of the Proceedings of the 7th Mathematics, Science, and Computer Science Education International Seminar, MSCEIS 2019, 12 October 2019, Bandung, West Java, Indonesia*. **2020**, EAI.

[18] Pamunuwa, V.P., Deraniyagala, D.P., Kulasekara, V.T.B., Thennakoon, R.D.A.V., and Lankasena, B.N.S. *Investigating the Impact of Software Maintenance Activities on Software Quality: Case Study*. in *Proceedings of the KDU International Research Conference (KDUIRC)*. **2023**.

[19] Dharmasiri, N.T.D., Kodithuwakku, J.P., Pallawala, P.K.B.T.D., and Lankasena, B.N.S. *The Impact of Agile Practices on Software Evolution in Startup Companies*. in *Proceedings of the KDU International Research Conference (KDUIRC)*. **2023**.

[20] Wisidagama, N.S., Karunarathne, M.L., Paranagama, P.D.C.J., Rathnayake, R.M.D.K.N., and Lankasena, B.N.S. *A Comprehensive Study on Software Evolution in Plan Driven and Agile Methodologies*. in *Proceedings of the KDU International Research Conference (KDUIRC)*. **2023**.