International Journal on Engineering Technology and Infrastructure Development (InJET-InDev)
www.lec.edu.np/journal
Volume 2, Issue no. 1, Page 274-283
Received Date: 5/13/2025
Revised Date: 5/25/2025
Accepted Date: 6/20/2025
ISSN: 3021-999X (Print)

# Streamlining Digital Identity Ecosystem in Nepal: A Private Blockchain Approach

Praches Acharya[1], Binod Sapkota[2]*, Bibat Thokar[3], Babu Ram Dawadi[4]
[1]*Department of Electronics and Computer Engineering, Thapathali Campus, Kathmandu, Nepal*
[2*]*Department of Electronics and Computer Engineering, Thapathali Campus, Kathmandu, Nepal*
[3]*Department of Computer Engineering, Lalitpur Engineering College, Lalitpur, Nepal*
[4]*Department of Electronics and Computer Engineering, Pulchowk Campus, Lalitpur, Nepal*

**Abstract**

As digitization continues to expand into various aspects of human life, the need for ro- bust user authentication becomes crucial to ensure secure online and digital services. However, the process of verifying one's identity has become increasingly complex and burdensome, contradicting the initial intentions of simplifying procedures through digitization. This research paper addresses the challenges associated with digital identity verification and proposes an innovative solution. This solution introduces a digital identity ecosystem powered by a private blockchain network, aiming to revolutionize identity management and authentication processes. By leveraging the decentralized and immutable nature of blockchain technology, this approach simplifies and secures the establishment and verification of digital identities, replacing reliance on physical identification methods. Through an extensive literature review and analysis of existing identity management systems, this research empha- sizes the advantages of utilizing a private blockchain network for identity authentication. It explores the benefits of decentralization, data immutability, and enhanced security provided by blockchain tech- nology, which can alleviate the complexity associated with current authentication methods. The pro- posed solution holds the potential to streamline authentication procedures, unlocking the true potential of digitization by making identity management more efficient, convenient, and secure for both individuals and service providers.

***Keywords:*** Blockchain, Digital Identity, Digitization

## 1. Introduction

The blockchain technology, a decentralized and secure digital ledger, has gained significant attention due to its potential to revolutionize various industries. One area where blockchain shows promise is in identity manage- ment, particularly in the context of secure and decentralized digital identities. This research paper explores the application of blockchain technology in establishing a robust digital identity system for individuals and organiza- tions in Nepal. The primary motivation behind this project is to address the challenges of authenticity, security, and accessibility in identity management. Currently, the authentication process in Nepal relies on physical doc- uments, leading to inefficiencies and risks of fraud. Moreover, centralized storage of digitized information poses vulnerabilities, potentially compromising citizens' data. In light of these issues, a blockchain-based digital identity system can offer tamper-proof and immutable records, mitigate the risks of fraudulent activities and enhance security. The objectives of this research are twofold: to improve the efficiency and speed of identity verification and authentication processes, and to provide individuals with a self-sovereign identity management solution. By leveraging Hyperledger Fabric, a authenticated blockchain network, authorized participants such as government agencies and financial institutions can securely store and manage digital identity information. This research paper assumes the validity and authentication of documents issued by government organizations, as well as the posses- sion of a national identity number by each citizen. It aims to offer a secure and tamper-proof means of storing personal identities and information, enabling individuals to maintain control over their data while enhancing ac-cess to financial services, especially for under-served populations. In this paper, we have structured our content in the following manner. Initially, we try to make the challenges surrounding identity and authentication more conspicuous. Then we provide an extensive review of the existing literature and solutions

* *Corresponding author*

available in this domain. In the subsequent section, we describe the architecture and application model for the proposed digital ecosystem based on blockchain. In the final section of this paper, we offer insights into future research opportunities and share our overall conclusions.

## 2. Related Works

Blockchain technology has gained significant attention in recent years due to its potential to revolutionize various industries, including identity management. Blockchain-based identity management systems offer enhanced security, privacy, and control over personal data. This literature review aims to provide an overview of the research conducted in the field of blockchain-based identity management systems, highlighting key findings, methodology, and challenges identified by researchers.

Kuperberg's survey [4] focuses on the enterprise and ecosystem perspective of blockchain-based identity management. This paper discusses the merits and demerits of different solutions and technologies available in the identity management sector. It provides insights into the use of blockchain and Distributed Ledger Technology (DLT) from an enterprise standpoint, offering valuable information for understanding the application of blockchain in identity management. It also examines the use of government-issued eIDs, such as India's Adharcard and the digital ID issued by the Estonian government.

Sung and Park [6] aim to understand the benefits and challenges associated with the adoption of blockchain-based identity management systems in public services. Through an academic literature review, the authors investigate the factors influencing the adoption of such systems, including organizational, technological, and environmental factors. The study also provides insights into the implementation challenges faced by public sector organizations, highlighting the potential of blockchain technology to increase transparency, efficiency and reliability in public services. Overall, this research offers valuable information for designing and implementing blockchain-based identity management systems in government settings.

Kuperberg takes reference from two prominent government-issued electronic identification (eID) systems: Aadharcard in India and Estonia's Digital ID. Adharcard [8] system utilizes blockchain-like technology for identity management and has been successfully implemented on a large scale. By studying its technology and architecture, the paper gains valuable insights into the principles, design, best practices, and key lessons learned from Aadharcard. Similarly, Estonia's Digital ID, [3] known for its advanced identity management system, offers additional insights and lessons that can be applied in the proposed architecture for the Nepal Government.

The Korean government has also adopted blockchain for identity management, with plans to fully operationalize a blockchain-based digital ID by 2024. As of November 30, 2022, three-quarters of a million South Koreans already have a blockchain-based mobile driver's license (mDL), following the successful piloting of the scheme in January 2022. This implementation serves as a relevant case study for understanding the feasibility and effectiveness of nationwide adoption of blockchain-based digital IDs [5].

By incorporating the findings and insights from these related works and literature, the research paper aims to develop a comprehensive and effective architecture for blockchain-based identity management that combines the positive aspects of existing solutions while addressing the unique requirements of the Nepal Government.

## 3. Methodology

### *3.1. Hyperledger Fabric*

Hyperledger Fabric is an open-source enterprise-grade permissioned distributed ledger technology (DLT) platform, designed for use in enterprise contexts, that delivers some key differentiating capabilities over other popular distributed ledger or blockchain platforms. It has a highly modular and configurable architecture, enabling innovation, versatility and optimization for a broad range of industry use cases. Fabric supports smart contracts authored in general-purpose programming languages such as Java, Go and Node.js, rather than constrained domain-specific languages (DSL). The Fabric platform is also permissioned, meaning that, unlike with a public permissionless network, the participants are known to each other, rather than anonymous and therefore fully untrusted. This means that while the participants may not fully trust one another (they may, for example, be competitors in the same industry), a network can be operated under a governance model that is built off of what trust does exist between participants, such as a legal agreement or framework for handling disputes. One of the

most important of the platform's differentiators is its support for pluggable consensus protocols that enable the platform to be more effectively customized to fit particular use cases and trust models. Fabric can leverage consensus protocols that do not require a native cryptocurrency to incent costly mining or to fuel smart contract execution. Avoidance of a cryptocurrency reduces some significant risk/attack vectors, and absence of cryptographic mining operations means that the platform can be deployed with roughly the same operational cost as any other distributed system. The combination of these differentiating design features makes Fabric one of the better performing platforms available today both in terms of transaction processing and transaction confirmation latency, and it enables privacy and confidentiality of transactions and the smart contracts (what Fabric calls "chaincode") that implement them.

### *3.2. Assets*

Assets can range from the tangible (real estate and hardware) to the intangible (contracts and intellectual property). Hyperledger Fabric provides the ability to modify assets using chaincode transactions. Assets are represented in Hyperledger Fabric as a collection of key-value pairs, with state changes recorded as transactions on a Channel ledger. Assets can be represented in binary and/or JSON form. Digital identity documents, which are stored in JSON format, are the asset in context of this project.

### *3.3. Ledger*

The ledger is the sequenced, tamper-resistant record of all state transitions in the fabric. State transitions are a result of chaincode invocations ('transactions') submitted by participating parties. Each transaction results in a set of asset key-value pairs that are committed to the ledger as create, update, or delete operation is executed. In Hyperledger Fabric, a ledger consists of two distinct, though related, parts – a world state and a blockchain. Firstly, there's a world state – a database that holds current values of a set of ledger states. The world state makes it easy for a program to directly access the current value of a state rather than having to calculate it by traversing the entire transaction log. Ledger states are, by default, expressed as key-value pairs. The world state can change frequently, as states can be created, updated and deleted. Secondly, there's a blockchain – a transaction log that records all the changes that have resulted in the current world state. Transactions are collected inside blocks that are appended to the blockchain – enabling you to understand the history of changes that have resulted in the current world state. The blockchain data structure is very different to the world state because once written, it cannot be modified; it is immutable. It's helpful to think of it as one logical ledger existing for each channel in the network. In reality, each peer in a channel maintains its own copy of the ledger – which is kept consistent with every other peer's copy through a process called consensus. The term Distributed Ledger Technology (DLT) is often associated with this kind of ledger – one that is logically singular, but has many identical copies distributed across a set of network nodes (peers and the ordering service).

### *3.4. Chaincode (Smart Contract)*

Chaincode is software defining an asset or assets, and the transaction instructions for modifying the asset(s). In other words, it's the business logic. Chaincode enforces the rules for reading or altering key-value pairs or other state database information. Chaincode functions execute against the ledger's current state database and are initiated through a transaction proposal. Chaincode execution results in a set of key-value writes (write set) that can be submitted to the network and applied to the ledger on all peers.

### *3.5. Consensus*

Consensus is defined as the full-circle verification of the correctness of a set of transactions comprising a block. Consensus is achieved ultimately when the order and results of a block's transactions have met the explicit policy criteria checks. These checks and balances take place during the lifecycle of a transaction, and include the usage of endorsement policies to dictate which specific members must endorse a certain transaction class, as well as system chaincodes to ensure that these policies are enforced and upheld. It is a broader term overarching the entire transactional flow, which serves to generate an agreement on the order and to confirm the correctness of the set of transactions constituting a block. The consensus mechanism depends on the ordering service used.

### *3.6. Raft*

Raft is the go-to ordering service choice for Hyperledger Fabric. Fabric implementation of the Raft protocol uses

a “leader and follower” model, in which a leader is dynamically elected among the ordering nodes in a channel and that leader replicates messages to the follower nodes. Because the system can sustain the loss of nodes, including leader nodes, as long as there is a majority of ordering nodes (what’s known as a “quorum”) remaining, Raft is said to be “crash fault tolerant” (CFT). In other words, if there are three nodes in a channel, it can withstand the loss of one node (leaving two remaining). If you have five nodes in a channel, you can lose two nodes (leaving three remaining nodes). This feature of a Raft ordering service is a factor in the establishment of a high availability strategy for the ordering service.

### *3.7. Endorsement policy*

Endorsement policy defines the peer nodes on a channel that must execute transactions attached to a specific chaincode application, and the required combination of responses (endorsements). A policy could require that a transaction be endorsed by a minimum number of endorsing peers, a minimum percentage of endorsing peers, or by all endorsing peers that are assigned to a specific chaincode application. Policies can be curated based on the application and the desired level of resilience against misbehavior (deliberate or not) by the endorsing peers. A transaction that is submitted must satisfy the endorsement policy before being marked as valid by committing peers.

### *3.8. Security & Membership Services*

Hyperledger Fabric underpins a transactional network where all participants have known identities. Public Key Infrastructure is used to generate cryptographic certificates which are tied to organizations, network components, and end users or client applications. As a result, data access control can be manipulated and governed on the broader network and on channel levels. This “permissioned” notion of Hyperledger Fabric, coupled with the existence and capabilities of channels, helps address scenarios where privacy and confidentiality are paramount concerns.

### *3.9. MSP*

Certificate Authorities issue identities by generating a public and private key which forms a key-pair that can be used to prove identity. This identity needs a way to be recognized by the network, which is where the MSP comes in. For example, a peer uses its private key to digitally sign, or endorse, a transaction. The MSP is used to check that the peer is allowed to endorse the transaction. The public key from the peer’s certificate is then used to verify that the signature attached to the transaction is valid. Thus, the MSP is the mechanism that allows that identity to be trusted and recognized by the rest of the network.

### *3.10. Private Blockchain Network*

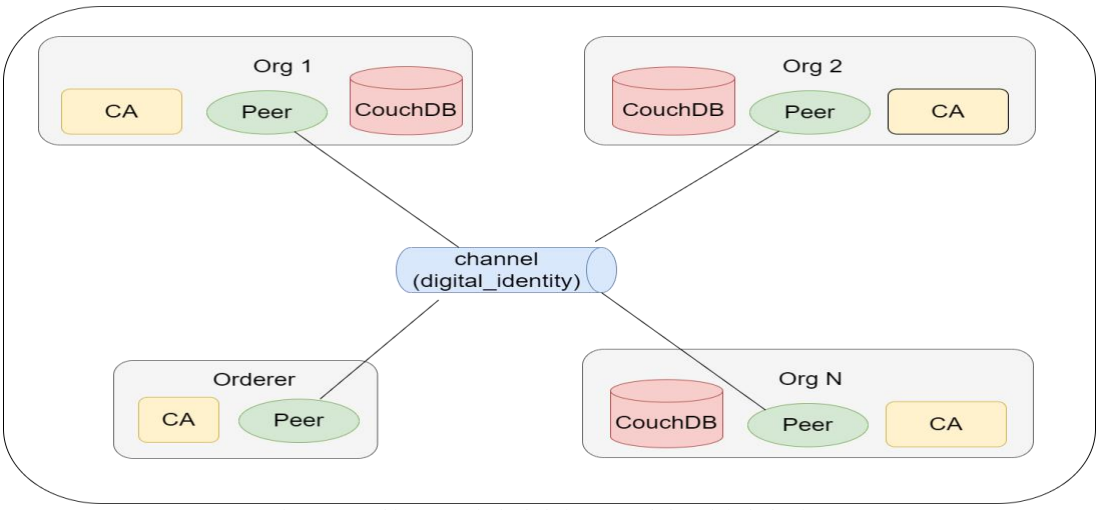


Figure 1. Architecture of Blockchain Network for Digital Identity

Hyperledger Fabric is an ideal framework for establishing a robust and secure private blockchain network, particularly for the purpose of digital identity management. Different trusted governments as well as non-

governmental organizations can host the peer servers to form the private network as shown in figure 1. Government organizations that are responsible for issuing identity documents to the public, like Department of Transport Management, Department of National ID and Civil Registration etc, can participate in the network and maintain

records of identity information in the network. Other trusted organizations and service providers, who can leverage the identity information to provide some services to the public, can also join in the network.

#### *3.10.1. Certificate Authority*

Each organization can have their own certificate authority (CA). They are responsible for dispensing certificates and credentials that can be used by various system and client applications to identify them as belonging to that specific organization. Additionally, it also signs transaction to indicate that an organization endorses the transaction result – a precondition of it being accepted onto the ledger.

#### *3.10.2. Peers and Channels*

Hyperledger has a concept of creating a channel where multiple organizations can collaborate to maintain a shared copy of ledgers to keep record of digital assets. In the proposed architecture, multiple organizations agree on a channel configuration to jointly collaborate on the channel (named "digital identity") to maintain a shared copy of the digital identity records. In this context, all organizations host one peer each and all these peers will be connected to the "digital identity" channel. These peers are a fundamental element of the network: they host ledgers and chaincode(which contain smart contracts), and are therefore one of the physical points at which organizations connect to the channel.

#### *3.10.3. Chaincode*

In Hyperledger Fabric, the business logic that defines how peer organizations interact with the ledger (for example, a transaction that adds a new category in a driving license record), is contained in a smart contract. Chaincode, structure that contains the smart contract, is installed on the relevant peers, approved by the relevant peer organi- zations, and committed to the channel. We can thereby consider a chaincode to be physically hosted on a peer but logically hosted on a channel.

In the proposed system, we will have a smart contract for every unique identity document type and all the functionalities to record a new document, update or access the existing ones will be governed by these smart contracts. For example, a smart contract will be created for Driving License, which will govern all the registrations and modification of the driving license recorded in the blockchain network. Furthermore, an endorsement policy will also be set for these chaincodes, such that all the required authorities must endorse before any transactions takes place in the network through that specific smart contract.

#### *3.10.4. State Database*

Various data update transactions are appended to the distributed ledger on a regular basis. In such a situation, querying the entire ledger to get the latest state of the data is computationally very expensive; so, a global state is maintained to keep the record of the latest state of the data in the ledger and such state is stored in the state database. World state data is stored in a state database for efficient reads and queries from chaincode. All organizations must maintain an instance of a database for this purpose.

#### *3.10.5. Ordering Service*

The ordering service gathers endorsed transactions from applications and orders them into transaction blocks, which are subsequently distributed to every peer node in the channel. At each of these committing peers, transac- tions are recorded and the local copy of the ledger is updated appropriately. A multiple node Raft ordering service will be configured as the ordering service.

### *3.11. Gateway*

Just like peers and orderers, gateway application has an identity that associates it with an organization. So, the gateway applications associated with each organization are connected to the channel. Because Fabric is a permissioned network, blockchain participants need a way to prove their identity to the rest of the network in order to transact on the network. Thus, only after the gateway application has registered and enrolled with its associated

organization's Certificate Authority (CA) and received back necessary cryptographic material, can they use it to authenticate into the blockchain network as shown in figure 2.

Hyperledger Fabric further provides Node SDK with various APIs available to interact with the chaincode. The gateway application will leverage these APIs to create gRPC connection with the blockchain and perform various read/write operations. To create a simple interaction mechanism with the blockchain, we will wrap these SDK APIs with our own set of APIs so that these read-write operations can be performed with a simple set of REST API calls. These REST APIs can be called by other applications to interact with the private blockchain as shown in figure 3.

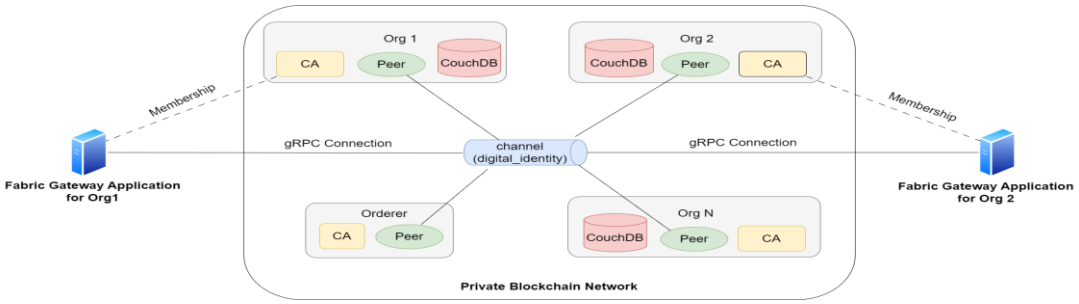


Figure 2. Gateway application's membership and connections in the blockchain network

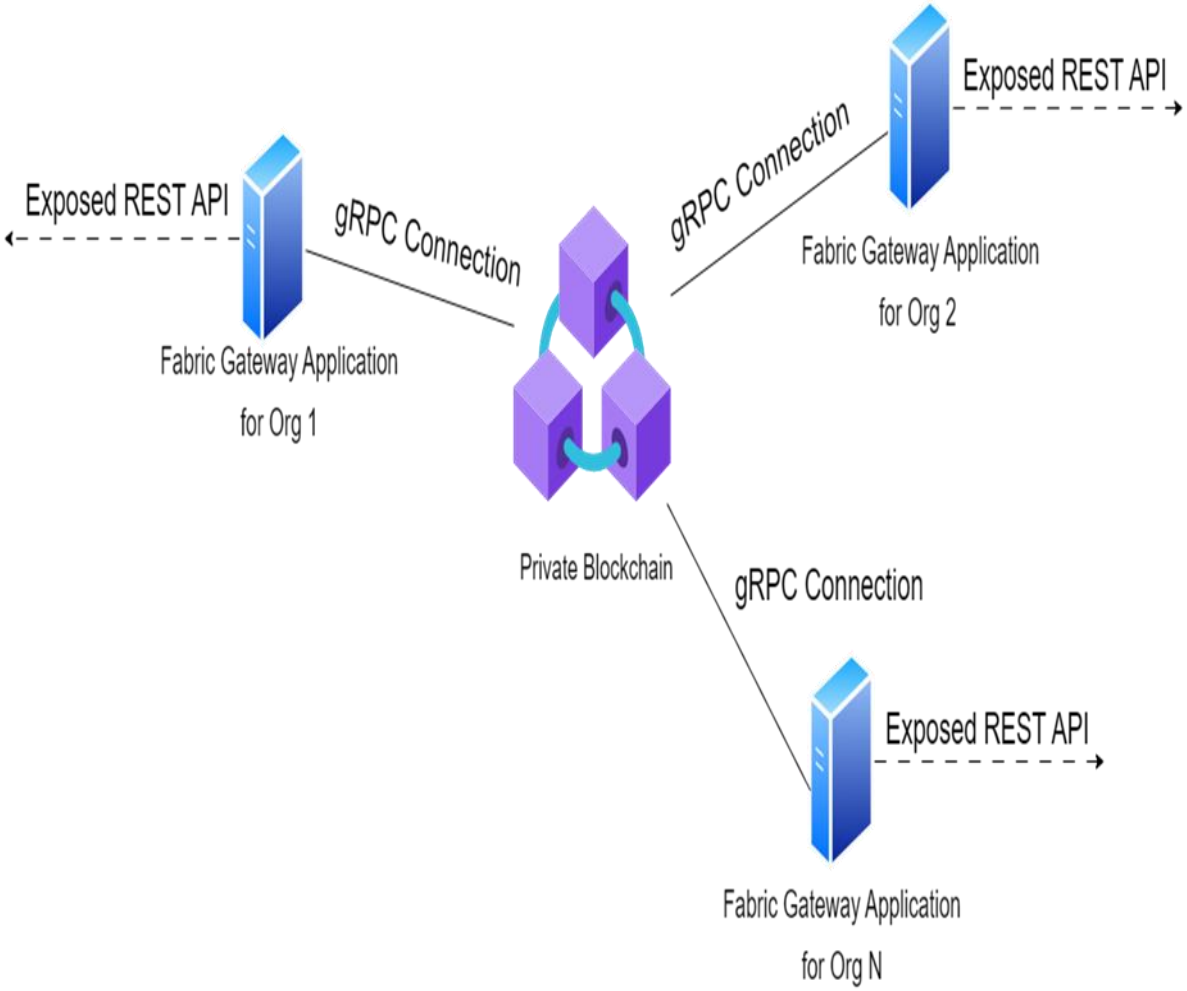


Figure 3. Gateway applications providing proxy connection to the blockchain network.

### *3.12. Client Applications for Government Organizations*

The client application for the government organization will allow government officials to record and update the

required user identity details in the blockchain. A backend server will interact with the blockchain through the gateway to provide the required functionalities to the client application as shown figure 4.

### *3.13. Mobile App*

The mobile app will allow a user to view all their identity documents stored by the government organizations in the blockchain further it can allow a user to share their documents or details with others service providers or users conveniently through means like QR code as shown in the figure 5. All the functionalities for accessing the user data, authenticating and sharing of identity documents/details to other users or service providers will be facilitated by the backend server. This backend server will interact with the private blockchain through the gateway application.

## 4. Proposed Implementation Guidelines

To enhance the user experience within the proposed ecosystem, it is essential to incorporate specific features into the applications and systems, ensuring a seamless and user-friendly interaction.

### *4.1. Unified Identity Access: Nepal's National ID*

Considering the Nepal government's initiative to integrate all identity documents and official records with the National Identity Card, it is crucial for every individual's identity document to be associated with their national ID.

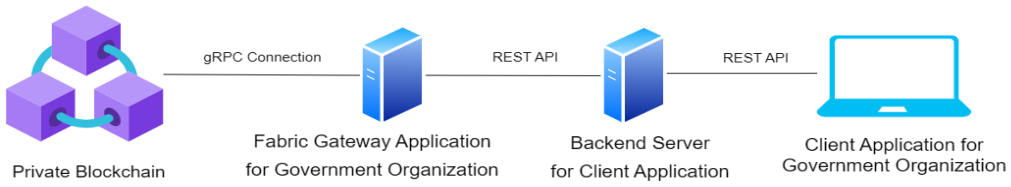


Figure 4. Client applications of government organizations interacting with the blockchain network

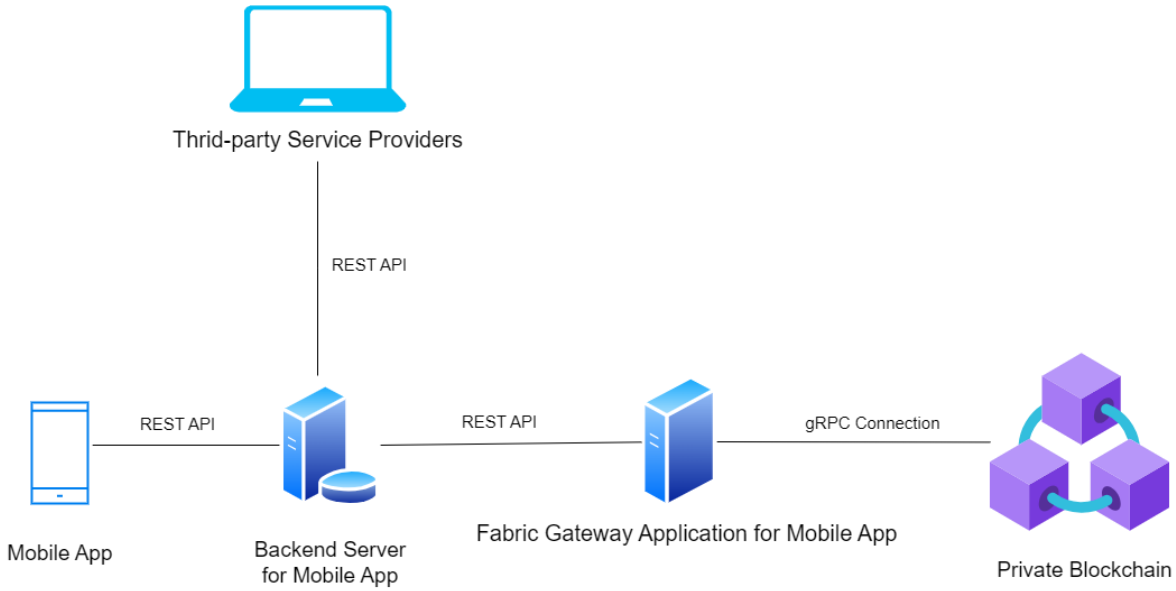


Figure 5. Mobile application interacting with the blockchain network

The storage of identity records should be designed in a manner that enables easy access to all relevant documents through the national ID. The individuals should be able to provide their identity details for any service requiring such information. This system should be implemented across all government services, as well as by other service providers by establishing a single reference point through the national ID.

### *4.2. QR Based Identity Sharing*

In Nepal, more and more people are using digital payments, and they're getting used to using QR codes to make payments easily. Now, we can take this idea further and create a system where you can use QR codes to prove your identity or share information with others. It's like scanning a code with your phone to show who you are or exchange important details. Adopting this feature in the proposed ecosystem can have many advantages. It makes it easier and quicker to prove who you are without remembering multiple passwords or going through complicated verification processes. All you have to do is scan a QR code, and you're good to go. It also makes it safer to share your information with trusted organizations, like banks or government agencies, because you don't have to type everything manually or fill out forms. However,there should be a seamless and consistent method for the users to share their identity details or authenticate in multiple platforms using the QR scan feature in their mobile app.

### *4.3. Data Control and Transparency*

To safeguard user privacy and ensure data control, organizations and service providers in Nepal must obtain explicit approval from the identity owner before accessing their personal information. Users should have the author- ity to approve or reject access to their digital identity, giving them full control over their data. A comprehensive activity history log that records all accesses and updates to identity records should be maintained for transparency. This log enhances accountability, allowing users to monitor data usage and identify any potential misuse or unauthorized access.

## 5. Discussion

### *5.1. Research Objective*

The research aims to investigate the necessity of digital identity over physical documents, the advantages of digital identity in a mobile app, and the problems associated with physical documents such as loss and misuse. Additionally, it seeks to explore the perspectives of the general public and traffic police officers on these topics.

### *5.2. Sampling Method*

#### *5.2.1. General Public*

A random sampling method was used to select 150 respondents from the general population. This approach ensures that the sample represents individuals from various backgrounds, age groups, gender and occupations.

#### *5.2.2.* **Traffic Police Officers on Duty**

The survey was conducted among 50 traffic police officers currently on duty in Kathmandu, Nepal. This sample comprises officers with direct experience in enforcing identification regulations.

### *5.3. Data Collection Method*

The survey was conducted using a structured questionnaire designed to gather information related to the research objectives. The questionnaire consisted of multiple-choice and closed-ended questions, ensuring consistency in responses and facilitating quantitative analysis.

### *5.4. Survey Questions*

The questionnaire consisted of two sections: one for the general public and another for traffic police officers. The questions included in the survey were as follows:

#### *5.4.1. General Public*

- How often do you forget to carry their physical document?
- How often do you lose their physical document?
- Do you prefer carrying a physical document or a digital document?
- Do you own a smartphone?
- Do you citizen have access to internet?

- How long does it take to get verified in banks or other institutes?

#### *5.4.2. Traffic Police Officers on Duty*

- How many people get caught driving without a driving license in Kathmandu, Nepal?

### *5.5. Limitations*

- The convenience sampling technique may introduce bias, as the respondents may not represent the entire population.
- The survey was conducted in a specific geographic location (Kathmandu, Nepal), limiting the generalizabil- ity of the findings.
- The survey primarily focused on public perspectives, and additional research involving other stakeholders may provide a more holistic view.

## 6. Results

The survey results demonstrate that there is a significant need and preference for digital identity solutions over physical documents. The advantages of digital identity in a mobile app, such as convenience, accessibility, and reduced risks associated with physical documents, are recognized by the majority. However, a portion of the popu- lation still prefers physical documents, suggesting the importance of providing options to accommodate individual preferences. Implementing digital identity solutions that are user-friendly, secure, and widely accessible can offer significant benefits to both individuals and organizations. Additionally, streamlining and expediting the verifica- tion process in banks and other institutes could further enhance the benefits of digital identity in various aspects of daily life [11].

## 7. Conclusion and Future Works

In conclusion, this research paper has addressed the challenges surrounding digital identity authentication in the context of increasing digitalization. Through a comprehensive literature review and analysis, the advantages and possibilities of utilizing a private blockchain network for identity authentication have been highlighted. Finally, this research paper has proposed a solution, which is a digital identity ecosystem powered by a private blockchain network. The implementation of a blockchain-powered digital identity ecosystems holds promise for simplifying and streamlining the identity verification processes. This shift from physical identification methods to a digital ecosystem has the potential to alleviate the complexity and burdens associated with current authentication prac- tices. It paves the way for a seamless experience for both individuals and service providers, unlocking the full potential of digitalization in identity management.

However, it is important to acknowledge that the implementation of the proposed system will require collabora- tion and adoption from various stakeholders, including government entities, organizations, and individuals. Real- world testing will be essential to ensure scalability, interoperability, and regulatory compliance. Additionally, the privacy considerations of the blockchain technology used in the system need to be thoroughly addressed to ensure its widespread adoption [9]. The proposed solution presented in this research paper demonstrates the potential of blockchain technology to revolutionize digital identity ecosystem in Nepal further research and development are necessary to refine and expand the use of blockchain technology in digital identity management. With continued development and adoption, it has the potential to reshape the landscape of digital identity authentication, enabling a more efficient and secure digital ecosystem [7].

## References

[1] M. R. Ahmed, A. K. M. Muzahidul Islam, S. Shatabda, and S. Islam, “Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey,” *IEEE Access*, vol. 10, pp. 113436–113481, 2022.

[2] P. Dutta, T.-M. Choi, S. Somani, and R. Butala, “Blockchain technology in supply chain operations:

Applications, challenges and research opportunities," *Transp. Res. Part E: Logist. Transp. Rev.*, vol. 142, p. 102067, 2020.

[3] Enterprise Estonia, "e-Identity in Estonia." [Online]. Available: https://e-estonia.com/solutions/e-identity/id-card/. [Accessed: 30-Jan-2022].

[4] M. Kuperberg, "Blockchain-based identity management: A survey from the enterprise and ecosystem perspective," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1008–1027, 2019.

[5] B. Lindrea, "Koreans to have access to blockchain-powered digital IDs by 2024." [Online]. Available: https://cointelegraph.com/news/koreans-to-have-access-to-blockchain-powered-digital-ids-by-2024. [Accessed: 2022].

[6] C. S. Sung and J. Y. Park, "Understanding of blockchain-based identity management system adoption in the public sector," *J. Enterp. Inf. Manag.*, vol. 34, no. 5, pp. 1481–1505, 2021.

[7] S. Thapa, G. Piras, S. Thapa, P. Rimal, A. Thapa, and K. Adhikari, "Blockchain-based secured traceability system for the agriculture supply chain of ginger in Nepal: A case study," *Arch. Agric. Environ. Sci.*, vol. 6, no. 3, pp. 391–396, 2021.

[8] Unique Identification Authority of India (UIDAI) Technology Center, "Aadhaar technology and architecture: Principles, design, best practices and key lessons." [Online]. Available: https://uidai.gov.in/en/. [Accessed: 2014].

[9] G. Wolfond, "A blockchain ecosystem for digital identity: Improving service delivery in Canada's public and private sectors," *Technol. Innov. Manag. Rev.*, vol. 7, no. 10, 2017.

[10] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," *arXiv preprint arXiv:1906.11078*, 2019.

[11] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology? — A systematic review," *PLoS One*, vol. 11, no. 10, p. e0163477, 2016.

[12] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congress)*, 2017, pp. 557–564.