An Integration of National Identity towards Single Identity Number with Blockchain

Rana Zaini Fathiyana[1], Fadhil Hidayat[2], Budi Rahardjo[3]
{ranazainifathiyana@students.itb.ac.id[1], fadhil@stei.itb.a.id[2], rahard@gmail.com[3]}

Bandung Institute of Technology, Bandung, Indonesia[1,2,3]

Abstract. The lack of coordination in the integration of information systems between government agencies that issue identity numbers causes replication and redundancy of population information data. Another problem is the emergence of citizens' concerns over data integrity and security due to national identification records is also used by the private sector. In this paper, one of the solutions offered to overcome the above problem is to build an integrated national identification database system between government agencies by applying the concept of Single Identity Number (SIN) using blockchain technology. Blockchain is a secure and robust system for keeping a record of the identities of all citizens and also able to facilitate data integration between institutions. This paper uses the strengths of blockchain to possess characteristics of immutability that it is possible to store national identification records.

Keywords: National Identity, Single Identity, Blockchain

1 Introduction

Nationality means a group of people who have a common language and culture that they have entitled to self-government as a country [1]. In general, identity is any set of characters that defines a person and can be used to identify that person uniquely [2]. National identity means a unique identity provided by the government for their citizen. Nowadays, at least there is 29 national identity document issued by 24 different agencies in Indonesia including driver’s license, tax identification number, passport, and insurance that stored in a database owned by agencies [3]. Each identity number is different, depending on the interests of the issuing agency.

The lack of coordination between government agencies and the unrelated information system to each other has made population data ineffective. Citizens must register at different agencies with different methods, while the data provided is the same. Replication, redundancy, and inefficient use of population data and information are inevitable. In addition, separate databases for each agency cause difficulties to share information and result in duplication, overlap, and contradiction in the information held [4].

Several countries have established policies in the development of digital identity. Digital identity serves as the basis for authenticating or verifying someone's identity, due to it contains very sensitive personal information. Government store this type of information in the centralized database. Personal data stored on a centralized platform is the main target for information breaches because it makes it relatively easier for hackers to break into large systems at once and reach their malicious targets [5].

MSCEIS 2019, October 12, Bandung, Indonesia

DOI 10.4108/eai.12-10-2019.2296532

Much of this effort will be taken by national governments and supported by development partners to improve the quality of public services, plan development, and also enforce the law and prevent crime. A number of governments propose or implement national digital identity programs. Through this government-managed or coordinated program, the government aims to provide a single digital identity to the citizen. In Indonesia, a single digital identity well knows as Single Identity Number (SIN) is a unique identification number that is integrated with combined data from various government and private sectors.

The role of the private sector in the digital identity ecosystem proves the emergence of evolving models of a public-private partnership to build and strengthen the identification system in developing countries. Recently, the government established a policy in registering SIM cards for mobile users, there are conditions for accessing digital services and communications are by making user identification. Connecting a digital or biometrics-linked identity to a SIM card is not only a digital security concern, but there are also problems of trust and the ownership of access rights to personal data. With this potential come important challenges, and both public and private stakeholders must work together to ensure that digital identity systems are effective, safe, inclusive, and trustworthy [6].

The relationship between digital identity and blockchain begins with the role of blockchain as an open database service for each transaction, and the global identity system is distributed through a decentralized mechanism. One identity will be used for an individual and shared on the blockchain system and functions for many systems and applications. Blockchain is a distributed ledger that allows many entities to write entries into information records, and the user community can control how information records are changed and updated [7]. Blockchain technology stores the same information at different nodes, and the information will only be added when the nodes have reached consensus. Able to track the history due to the previous information cannot be removed when the new transactions added.

The implementation of the blockchain means the next step for the development of e-government, it has the potential benefits for government and community in reducing costs and complexity, sharing trusted processes, increasing audit trial findings and ensuring reliable [8]. The superior characteristics of the blockchain network are transparency and trust. However, there are times when in business situations when data privacy is still needed.

The aim of this paper is to resolve technological constraints in the implementation of SIN. We propose an integrated population database system between agencies for citizenship by applying the concept of SIN. As data is shared, security factors are very important to consider when exchanging data. Blockchain provides the security system because the data is distributed to each node that makes the attacker hard to change the data. Government agencies related to citizens' identities can write entries into one large ledger that is integrated together. The available attributes of the national identity database can be used effectively by the private sector to improve their services. The rest of the paper is organized as follows: Section II provides a background of digital identity. Section III reviews the existing national digital identity with blockchain technology systems. The proposed system is defined in Section IV. Finally, Section V presents future work and conclusion.

2 Digital Identity

2.1 The Identity Lifecycle

There are three fundamental stages of digital identities lifecycle [9]:

a. *Registration:* In creating a digital identity, the most important step is registration. In enrollment, there is process capturing and recording key identity attributes from a person who claims a certain identity, include biographical data (e.g., name, date of birth, address, gender), biometrics (e.g., fingerprint, iris scan), and other related attributes. In validation process establishes whether or not the claimed identity has one or more of the following properties: existence, uniqueness, and linkages.

b. *Issuance of document or credentials:* Traditionally, ID issuers provided documents (e.g., a birth certificate) or eID, ePassports. The types of electronic credentials include Smartcards, 2D Bar code card, Mobile identity, and ID in the cloud.

c. *Authentication*: Authentication is the process to verify and validate the relationship between the document and its owner. The user must be authenticated using one or more factor that generally falls into one of four categories: something that the person is, something that the person has, something that the person knows, and something that the person does [10].

Lifecycle Management: Provide ease to manage and organize the identity system, such as updating the status and content of digital identities. Sometimes the user may need to update various identity attributes, such as marital status, address, profession. On the other side, the identity provider may need to revoke invalidating the digital identity to security reasons, and terminate an identity in the case of the individual's death.

2.1 Evolution of Identities

The model for identity has evolved through four stages: centralized identity, federated identity, user-centric identity, and self-sovereign identity[11]. We give a comparison of the identity category and it is summarized in Table I.

a. *Centralized Identity:* Administrative control by a single authority or hierarchy. For example, in the case of a national ID card when allowing the personal data and the administration of the identification process is managed and held by the government in one central database.

b. *Federated Identity:* Administrative control by multiple, enable the sharing of identifiers and attributes amongst organizations that participate in a defined circle of trust, such as provide access to citizens using national identity provider, for example in Emirates ID [12].

c. *User-centric Identity:* This method focused on providing decentralization of identity and enhancing user privacy and control over identifiers and personal data.

d. *Self-sovereign Identity:* Individual has sole ownership over the ability to control their account and personal data. With self-sovereign identity, they can be independent without having to rely on central authority and they can store their data to their devices and provide it for verification and transactions. Moreover, also they have complete control over how their personal information is kept and used.

Table 1. A Comparison of Identity Category.

	Centralized Identity	Category Federated Identity	User-centric Identity
Centralized	Centralized	Centralized combine with partly distributed	Centralized combine with distributed
Trust Domain	Sole Centralized	Mutiple	Mutiple
Storage of ID		Distributed	Individual
Authentication	Single Method	Support for many centralized and few distributed methods	Support centralized and distributed methods
Advantages	Simplify the management of digital identities, Lower administrative cost	Single-Sign On, Increased Organizational Productivity	User can choose appropiate credentials flexibly
Disadvantages	Lack of transparency and control to identify the owner	Vulnerable to security and privacy attack	Users are expected to be more responsible for identity usage

From the comparison in Table I it can be seen that the current national identity system is in the category of centralized identity. However, in the system that will be designed, we will propose the use of the hybrid category, which is a category between federated identity and user-centric. That is, the system to be designed will allow the government and related institutions to have access to writing data about individual identities into the system. By using blockchain technology, data storage will not be centralized. While the user-centric system is a plan for further development. Citizens can regulate which institutions their data can be accessed or utilized.

3 Review of Existing National Digital Identity with Blockchain Technology

The results of a systematic literature review on [13] reveal that the use of blockchain for digital identity is mostly still conceptual. The number of high-quality papers related to this merger technology meager. The following is a literature review relating to identity with blockchain technology, especially regarding national identity.

N. Buchmann *et al.* [14] present a conceptual system architecture with cost-efficient to enhance the long-term security of breeder documents by utilizing blockchain technology. The most suitable blockchain for the described breeder scenario is using the Bitcoin blockchain. Shah and Kumar [15] complete the result from [14] with requiring an efficient technology to store birth records which cannot be tampered as well as easy to maintain, well secured and easily shareable using blockchain technology along with Cryptography algorithms and IPFS protocol.

A security model for a national electronic Identity Document (e-ID) based on blockchain network concept using smart card and taking the advantages of the traditional authentication methods as biometry (citizen authentication) and physical security (document authentication) in order to reduce the security issues of the currently used identity document proposed by [16].

K. Mudliar *et al*. [17] proposed a model that allows people to carry their national identity on their phones by utilizing blockchain technology. National identity can be checked by regime officials by scanning a barcode or QR code, which can be automatically generated by utilizing the regime portal. The main advantage of this system is that there is transparency between the regime and the citizens.

N. Chalaemwongwan and W. Kurutach [18] submit a framework to help improve digital identity government service to simple sign-on and kept preserving privacy by providing personal information to service only when users grant permission for each service. This framework is composed of five-phase: 1. Identity and Services Provider registration phase, 2. User privacy creation phase, 3. User registration phase, 4. User authentication phase, 5. More information request phase.

Table 2 summarizes the features of some (proposed) method of national digital identity with blockchain technology, with the methodologies used, their strengths and weaknesses. The current review of the national digital identity system with blockchain technology reveals several gaps to achieve the objectives of this study.

Table 2. Summary of Characteristics of Existing National Digital Identity with Blockchain Technology.

No.	Author(s) and system year	Methodology	Strength of Method	Limitation
1	Nicolas Buchmann, Christian Rathgeb, Harald Baier, Christoph Busch, and Marian Margraf, 2017 [14]	Uses a Bitcoin blockchain to enhance the long- term security of breeder document	• It uses cryptographic building blocks regarding long-term security and post-quantum security. • Uses 2D barcode to save the biometric information.	• Only presented a conceptual system architecture . • Create data has not been integrated with other institutions, also no share of data.
2	Maharshi Shah and Priyanka Kumar, 2019 [15]	They use an Inter Planetary File System (IPFS) protocol and blockchain technology for issue of birth certificate and verification of genuine birth records.	• They are sharing digital birth certificate with other related institutions (shared of data). • They are using blockchain technology along with Cryptography algorithms and IPFS protocols to secure birth records.	• This work is still in progress — difficulty accessing birth records because of there no output physical documents by the system. • Possible attacks on the device (phone) which registered on the blockchain. • Create data has not been integrated with other institutions

No.	Author(s) and system year	Methodology	Strength of Method	Limitation
3	Montes D. Juan, Rincón P. Andrés, Páez M. Rafael, Ramírez E. Gustavo, and Pérez C. Manuel, 2018 [16]	Use of a PIN and biometric authentication (iris recognition and fingerprints) combined with the blockchain network.	• Combining three factors for generating a secure user authentication: something that the user has (e-ID), something the user knows (PIN), something the user is (Biometrics).	• The network would be necessary to lease computing capacity due to the number of transaction. • Population data has not been integrated with other institutions
4	Kumaresan Mudliar, Harshal Parekh, Dr. Prasenjit Bhavathankar, 2018 [17]	Make the utilization of e-ID card along with Blockchain technology and everyone can carry their national identity on their phone.	• Uses a barcode or QR code to replace physical national identity which could be checked by regime officials. • It provides transparency between the regime and the citizen. • Open the possibilities to endless application in the field of healthcare, voting (shared of data).	• Only presented a conceptual system architecture. • Possible attacks on the device. • The only share of data does not share control of data.
5	Nutthakorn Chalaemwongwan and Werasak Kurutach, 2018 [18]	National digital ID Framework on Blockchain (NIDBC) consists of three-part: smart contracts, libraries, and application	• They are sharing data informatiion blockchain with other related institutions. • Easy login regularly promotes citizens to access government services regularly.	• The only share of data does not share control of data. • It is the misuse of the provider user information at the service provider.

4 Proposed Solution

In this section, we describe the high-level architecture of an integrated national identity with blockchain technology and then provide its detailed design of assets and transactions. Figure 1 shows the network architecture in a distributed and decentralized way including all the nodes of the network.

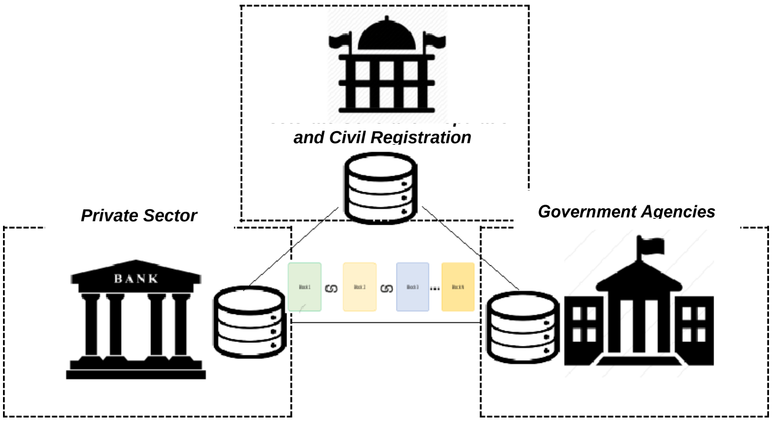

Fig. 1. Blockchain Architecture of an integrated national identity system

4.1 Participants and Assets

Participants: The members of a business network. They may own assets and submit the transaction. Participants of the integration national identity system are divided into three groups, there are Directorate General of Population and Civil Registration, Government Agencies, and Private Sector. The Citizens are also included in the participant in the system but in the currently developed system, citizens can only see all transaction records, do not have full control over their information, and allow anyone who can access their personal information.

a. *Directorate General of Population and Civil Registration:* Who has access to write or enter data related to basic information from citizens. They can delete all records from citizens who have died
b. *Government agencies:* In the system designed it is modeled by three groups namely the Directorate General of Immigration, the Ministry of Religion and the Ministry of Health. It is the person who writes or changes the data, including health records, marital status records, and immigration records (passport numbers).
c. *Private sector:* Who only has access to view basic information data from citizens. Used to verify potential customers that the data used is data following the data in the Directorate General of Population and Civil Registration. Examples of the private sector are banks, insurance, and telephone operators.

Assets: Assets are the key value of a business network. This is a resource that in business will be used can be tangible or intangible. In the national population records, there are identity attributes that can be filled out by several related institutions. Such as marital status can be written by the Ministry of Religion, medical record by the Ministry of Public Health, passport number by the Director-General of Immigration. So, the asset will be classified into four types, including basic information, medical record, immigration records, and religion records.

a. *Basic information:* Basic information is a record of citizens consisting of the full name, address, place of birth, and gender.
b. *Medical Records:* Medical record is a record of citizen consisting of blood type, medical conditions, and information of abnormalities that will be owned by the Ministry of Health.
c. *Immigration Records:* Immigration record is a record of citizen consisting of passport numbers and passport issuance dates that will be owned by the Director-General of Immigration
d. *Religion Records:* Religion record is a record of citizen consisting of religion data, marital status, date of marriage or divorce to be owned by the Ministry of Religion.

4.2 Blockchain Transaction

Transaction means a mechanism through which participants interact with assets. It does contain the t*ransaction ID* and *timestamp* properties.

a. *Register citizen:* This transaction will keep a record of citizen population data by the Directorate General of Population and Civil Registration. After citizens register themselves with the relevant government agency to obtain an identity, the government institution will write it in this transaction and submit it to the system.
b. *Update data:* This transaction will change the population record data of citizens by institutions whose identity needs to be updated, such as marital status by the Ministry of Religion node, passport number by Director-General of Immigration node, and others.
c. *Verify Data:* This transaction will see and match data between data owned by citizens and data stored in the blockchain that is filled out by relevant government agencies.
d. *Delete citizen:* This transaction has been thought for the ones of dead citizens.

Blockchain works based on the principle of assets (basic information, medical records, immigration records, religion records), participants (Directorate General of Population and Civil Registration, Government agencies, Private sector), and transactions (registering citizen, update data of citizen's records, verify data, and delete citizen). Every time an asset, participant, or transaction is created, updated, or deleted, the blockchain records the event and adds it to the audit trail that cannot be changed in the distributed ledger.

5 Conclusion and Future Work

Blockchain answer technical constraints in implementing SIN. With blockchain, it is possible to record data/identity of a person by several institutions. Facilitate the integration of data between institutions by considering the security aspects. Then it can realize the restriction of access rights to private institutions over the use of population data. In the future, so the citizen has full control over their information and also controls who access to their personal information. Platforms built upon blockchain make it so one’s digital identity cannot be controlled by a central institution but instead only by the individual itself. However, in order blockchain to develop to deploy its full potential, technological, organizational, and regulatory changes must be done.

References

[1] Arora, S.: National eID card schemes: A European overview, Inf. Secure. Tech. Rep., vol. 13, pp. 46– 53 (2008)

[2] Enriquez, A. M. and Domingo, A. I. S.: Digital Identity: the current state of affairs, BBVA Research.

[3] Lusmiarwan, R. D.: The Design Study of Indonesian Single Identity Number Prototype, Institut Teknologi Bandung, Indonesia (2016)

[4] Aggarwal, N. M., Ben Hassine, W. and Chima, R. J. S.: National Digital Identity Programmes: What's Next? (2018)

[5] Ferreira, M. B. and Alonso, K. C.: Identity management for the requirements of the information securitym, in 2013 IEEE International Conference on Industrial Engineering and Engineering Management, pp. 53–57, (2013).

[6] Digital Identity.: Towards Shared Principles for Public and Private Sector Cooperation, International Bank for Reconstruction and Development / The World Bank, Washington DC (2016).

[7] Kikitamara, S.: Digital Identity Management on Blockchain for Open Energy System, Radboud University, (2017).

[8] Palfreyman, J.: Blockchain for Government ?, IBM Tax & Revenue Management (2015)

[9] Technical Standards for Digital Identity, International Bank for Reconstruction and Development / The World Bank, Washington DC, (2017)

[10] Haque, M. A., Khan, N. Z. and Khatoon, G.: Authentication through keystrokes: What you type and how you type, in 2015 IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN) pp. 257–261, (2015)

[11] Allen, C.: The Path to Self-Sovereign Identity, Life with Alacrity (2016)

[12] Nallathamby, J.: What is Federated Identity Management? (2018)

[13] Rivera, R., Robledo, J. G., Larios, V. M., and Avalos, J. M.: How digital identity on blockchain can contribute in a smart city environment, in 2017 International Smart Cities Conference (ISC2), pp. 1–4 (2017)

[14] Buchmann, N., Rathgeb, C., Baier, H., Busch, C., and Margraf, M.: Enhancing Breeder Document Long-Term Security Using Blockchain Technology,” in 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), vol. 2, pp. 744–748 (2017)

[15] Shah, M. and Kumar, P.: Tamper proof Birth certificate using Blockchain Technology, Int. J. Recent Technol. Eng. IJRTE (2019)

[16] Juan, M., Piñeros, A., Páez, R. V., Gustavo, R. E., and Pérez Cerquera, M.: A Model for National Electronic Identity Document and Authentication Mechanism Based on Blockchain, Int. J. Model. Optim., vol. 8, pp. 160–165 (2018)

[17] 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) pp. 1–6 (2018)

[18] Chalaemwongwan, N. and Kurutach, W.: A Practical National Digital ID Framework on Blockchain (NIDBC), in 2018 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), pp. 497–500 (2018)