INTERNATIONAL JOURNAL
ON INFORMATICS VISUALIZATION

journal homepage : www.joiv.org/index.php/joiv

Prototype of Integrated National Identity Storage Security System in Indonesia using Blockchain Technology

Rana Zaini Fathiyana [a], Syifa Nurgaida Yutia [a,*], Dinda Jaelani Hidayat [b]

[a] *Faculty of Information Technology, Telkom Institute of Technology Jakarta, Jakarta 11710, Indonesia*

[b] *Center of Information and Communication Technology, Indonesian Agency for Meteorology Climatology and Geophysics, Jakarta 10610, Indonesia*

*Corresponding author: *ranazaini@ittelkom-jkt.ac.id*

***Abstract*—Approximately 29 institutions in Indonesia issue were identifying numbers, such as ID cards, driving licenses, BPJS, etcetera. In general, the identity storage system is designed with a centralized system and managed by each government agency. However, this system has some disadvantages, like data replication and redundancy. Furthermore, the Indonesian government is now undertaking a program through the Ministry of Home Affairs to use population data for public services by providing access to organizations cooperating for population data use. With a centralized database managed by a single entity, data abuse can occur and rely on third parties, the sole authority of the national identity data. The blockchain-based solution described in this paper to integrate a national identity system can provide the advantages of a population data utilization program. The system designed can facilitate convenience in sharing and updating population data while also ensuring the security and integrity of the population data. The citizens do not have to worry about the possibility of data misuse by user institutions. Blockchain technology offers decentralization through the participation of members across a distributed network. There is no single point of failure, and no single user may alter the transaction record. Our proposed approach could help the government of Indonesia secure citizens' private information and increase transparency in information management.**

***Keywords*— National identity; integration; blockchain; storage system; security.**

Manuscript received 6 Jan. 2022; revised 16 Feb. 2022; accepted 5 Mar. 2022. Date of publication 31 Mar. 2022.

I. Introduction

National identity is defined as a characteristic that indicates a unique and single citizen, with a citizen identity that is different from one another. Various agencies issue identity in Indonesia for different purposes depending on the agency's interests that issued it [1]. There are personal identification numbers such as ID cards, passports, and some are spatial such as land certificates, etc. The various identity numbers were built by each government agency in its information system, which was not integrated between one agency and another. The current condition is that every citizen is required to register with a different agency when entering the same data. This can lead to replication, unavoidable redundancy, and inefficiency of resource use. Then there could be data inaccuracies, which could lead to the incidence of data misuse for additional crimes.

The Government of Indonesia, through the Ministry of Home Affairs, is currently implementing a program to utilize population data for public services, which are mandated by Government Regulation (PP) Number 40 of 2019 [2] and Minister of Internal Affairs Regulation Number 61 of 2015 [3]. Cooperation in the utilization of population data has been underway since 2013, encompassing government agencies, private sectors, and business participants. The implementation and utilization of population data are designed to encourage the digitization of services to improve the quality of public services, aid in the data verification process, and minimize fraud that can hurt the community. As of September 2021, around 3,904 institutions have collaborated with the Population and Civil Registration Agency of the Ministry of Home Affairs in utilizing population data [4].

Currently, each identity issuing agency still stores its data using a centralized storage architecture or known as a centralized system. The advantages of a centralized system include the ease of managing existing resources [5]. However, its non-transparent characteristics causing the problem of data monopoly [6]. Besides being easier for fraud committed by internal parties, centralized systems are more vulnerable to attacks from outside parties [7], so they are not optimal in providing security, integrity, and privacy in a data storage system.

The lack of integrity in the population data storage system has led to the emergence of information islands, inconsistency of data and information, inadequate security, and the absence of audits are problems in implementing information systems in Indonesia. The government seeks to integrate various existing identities to become a single number known as SIN (Single Identity Number), a solution to this problem. The target of the SIN design is to build a national data warehouse that can integrate government agencies and private sectors have a safe, private, trusted, and integrated nature [8]. Collaboration in the usage and utilization of population data in the delivery of services by government agencies and the private sector demonstrates SIN implementation. The development of the use or exchange of data on information technology-based national identities has developed on a varied architectural basis to date the integration of data storage using blockchain technology.

The conventional system has not accommodated the simultaneous updating of data on a person's identity by government agencies and other identity issuing institutions. Data storage on a decentralized platform can be used to fulfill solutions relating to data transparency, user privacy, data availability, and ease of updating data. Blockchain technology is one such technology that can accommodate. This research could focus on an integrated storage security system of distributed national identity based on blockchain technology to serve the Population and Civil Registration Ministry of Internal Affairs' population data usage program. We have designed a blockchain-based distributed data storage system, especially in integrating national identity data storage security systems, to encourage the implementation of a population data utilization program by user institutions using blockchain technology and carry out testing of the system.

II. Materials and Method

A. Background

The Republic of Indonesia's government is now implementing a national population database center, with an Electronic Identity Card serving as the sole legal reference and data validity for various governmental services. There is an electronic identity card number in Indonesia, a single identity number (ID Number). This ID Number could eventually be used to gain access to all government services. This is consistent with the government's goal toward a single data set based on ID Number.

A previous study on the use or exchange of data on information technology-based population identity with a client-server architecture, such as the research conducted by Amran, *et al.*[9], who has succeeded in designing a distributed system based on the SOAP protocol to handle cross-platform software communication in exchanging population data structures, so that the information on the Electronic Identity Card can be accessed for a variety of purposes. Amin, *et al.* [10] researched the use of data on identity to support e-health services using RESTful Web Services technology. Then, several countries have implemented digital identity systems for their citizens. For example, India has implemented Aadhaar, a loosely coupled approach in which national identity numbers can be used as a general reference or index in every other database. Furthermore, in Pakistan, the government has adopted a single warehouse model approach, which system that adopts a single repository of all identifying information, both basic and functional, with different interfaces for different government agencies [11]. The adoption of blockchain technology is the next breakthrough in data storage integration technology.

Bitcoin transactions were the first to use blockchain technology in the cryptocurrency system[12]. Blockchain is a transparent distributed ledger that consists of several blocks that are related to each other and sequentially so that it could be difficult to change them [13]. It is based on the idea of a decentralized accounting book that cannot be modified or changed, where there needs to be a consensus from all members in the network, and all validated transactions could be recorded in a block[14]. It has potential benefits for the government and society and is the next step in developing e-government[15].

Several studies related to national identity data using blockchain technology, such as the research of Juan *et al* [16]who proposed an electronic identity document model using blockchain technology for document authentication processes combined with biometrics for verifying the authenticity of document owners. Research by Mudliar *et al.* [17] proposed integrating national identity with blockchain technology so that it can be used in other applications such as banking, digitizing health services, digital voting, and others.

Further research Jha *et al* [18] proposed a framework with individuals and government entities as participants. It is the responsibility of government agencies to add citizen entries to the event registration as well as to validate consensus. Citizens have the right to their own data and the ability to provide others access to read their data and execute database modifications. This framework proposes the introduction of a new registration into the system via which citizens who have been confirmed in the system can register or add new citizens who are included as children in agreement with other citizens who serve as witnesses.

Adapting to Indonesian conditions, Fathiyana *et al.* in 2020 [19] proposed a model design for an integrated national identification database system between government agencies by applying the Single Identity Number (SIN) concept using blockchain technology. The blockchain design consists of three peers, namely civil registration, government agencies, and the private sector. Whenever 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. However, this study has not yet reached the design implementation stage. Previous research related to national identity documents and digital identity management became the basis that led to the development of an integrated storage system for national identity data and population data utilization with blockchain technology.

The ID Number is used as the basis for SIN comprises the government's program of population data for public services. The framework in Fathiyana et al [19] was modified and developed on n the role of government agencies issuing national identities or Electronic Identity Card. In this case, Population and Civil Registration Agency were integrated with other institutions issuing another identity numbers. Thus, enabling all relevant institutions aims to work together to fill in citizen identity data in a distributed ledger. The ledger containing integrated population data can then be accessed by user institutions or commercial institutions and industry players with restrictions on access to the use and utilization of population data to ensure the security and privacy of citizens' data.

B. Blockchain

Blockchain is a technology Nakamoto proposed as a back-end cryptocurrency in Bitcoin [20]. The blockchain concept is based on the idea of a decentralized accounting book that cannot be changed or modified, which requires a consensus of all participating nodes in the network to verify each transaction. The characteristics of this technology provide services that are decentralized, integrity, reliable, traceability, and non-repudiation by participants. Blockchain keeps track of a constantly changing and distributed list of records. Each participating entity has the same accounting ledger as all other participants or entities in a network system, ensuring full consensus from all blockchain participants or nodes [21].

Currently, blockchain is a distributed system that outperforms and is more popular than traditional databases. Casino et al demonstrate the findings of examining the potential of blockchain as a solution to traditional databases in four major domain areas. First, in terms of trust, context, performance, the required consensus mechanism [22]. Cachin and Vukolic [23], there are three types of blockchain architecture, namely:

1) Permissionless blockchain: All entities can be users or run a node, change, and participate in consensus in determining a state. Also, the identity or names of participating members are pseudonyms or unknown.

2) Legal blockchain: Managed by a known entity, where only peers or nodes that have permission can operate the blockchain. These blockchain permission systems have the means to identify nodes that can control and update shared data, and often have ways to control who can issue transactions.

3) The Private blockchain is a legal blockchain specifically operated by one entity, where there is only one trust domain.

C. Blockchain Platform Determination

In determining the blockchain architecture used in the system, it could refer to the decision diagram [14]. So first, it is necessary to answer some questions referring to the decision diagram. Several questions could result in a decision whether “You don’t need a blockchain (fast transaction speed)”, “You might need a legal blockchain (medium transaction speed)”, or “You might need public blockchain (slow transaction speed)”.

By answering a few questions and following the arrows, a decision was made that the correct blockchain architecture to be used in the system to be designed is a legal blockchain. A legal blockchain is a blockchain that can only be accessed by participants involved in the network by predetermined access rights. In addition, the use of a legal blockchain can reduce the possibility of hacker attacks and increase privacy because access rights could only be granted to certain nodes with different access rights [18].

Once it has been determined that the architecture used is a legal blockchain. The next step is to choose the platform to be used. The study in [22] compares two blockchain architectures with high popularity and potential for development. Hyperledger Fabric is a Hyperledger framework that implements the legal blockchain system [24].

Hyperledger Fabric was chosen as the blockchain platform to be used. The selection of the Hyperledger Fabric platform is based on only a few entities that could be involved in this blockchain-based integrated storage system or not public. In addition, because Hyperledger Fabric is very suitable for use in developing non-financial systems, it has a modular system architecture, has more features, and can be stored in various formats [25].

III. Results and Discussion

This section provides an overview of the proposed system. Describe the system requirements analysis and an overview of the system being constructed. And evaluate the results of this study.

A. Identification Blockchain Network Component

It has been determined that the Hyperledger Fabric framework could be implemented. Hyperledger Fabric is being developed with the help of Hyperledger Composer and Hyperledger Explorer. Hyperledger Composer supports the Hyperledger Fabric infrastructure and runtime, allowing for easier and faster integration of business network modeling with current applications in a business process [26]. A business network based on Hyperledger Composer has three major components: assets, participants, and transactions [27].

Assets are resources owned by an entity that can be tangible goods such as property and hardware or intangible goods such as contracts and intellectual property rights. Assets, in this case, are registration form documents, such as selected registration documents from four government agencies: Basic Information Data, Driver License Application Registration Data, Passport Application Registration Data, and Health Card Application Registration Data.

TABLE I
LIST OF TRANSACTION IN BUSINESS NETWORK

Code	Transaction Name	Participant
TA.1	Input Basic Information Data	Population and Civil Registration Agency
TA.2	Change Basic Information Data	
TA.3	Delete all records	
TB.1	Input Driver License Application Registration Data	Departmental Police of the Republic of Indonesia
TB.2	Change Driver License Application Registration Data	
TC.1	Input Passport Application Registration Data,	Directorate General of Immigration Republic of Indonesia
TC.2	Change Passport Application Registration Data,	
TD.1	Input Health Card Application Registration Data.	Healthcare and Social Security Agency
TD.2	Change Health Card Application Registration Data.	

Participants are members of a business network who are actors who can own assets and send transactions. Participants involved in the business process come from three different organizational units: Population and Civil Registration Agency, Government Agencies, Private Sector, and Citizen. Transactions are the mechanism by which participants interact with assets. The entire list of transactions can be seen in Table 1.

B. *System Architecture Design*

The architectural model of a blockchain-based integrated national identity data storage system consists of several layers: the Application Layer, Network Layer, and Data Layer. In this section, the system architecture design of the proposed system is carried out as shown in Fig. 1.

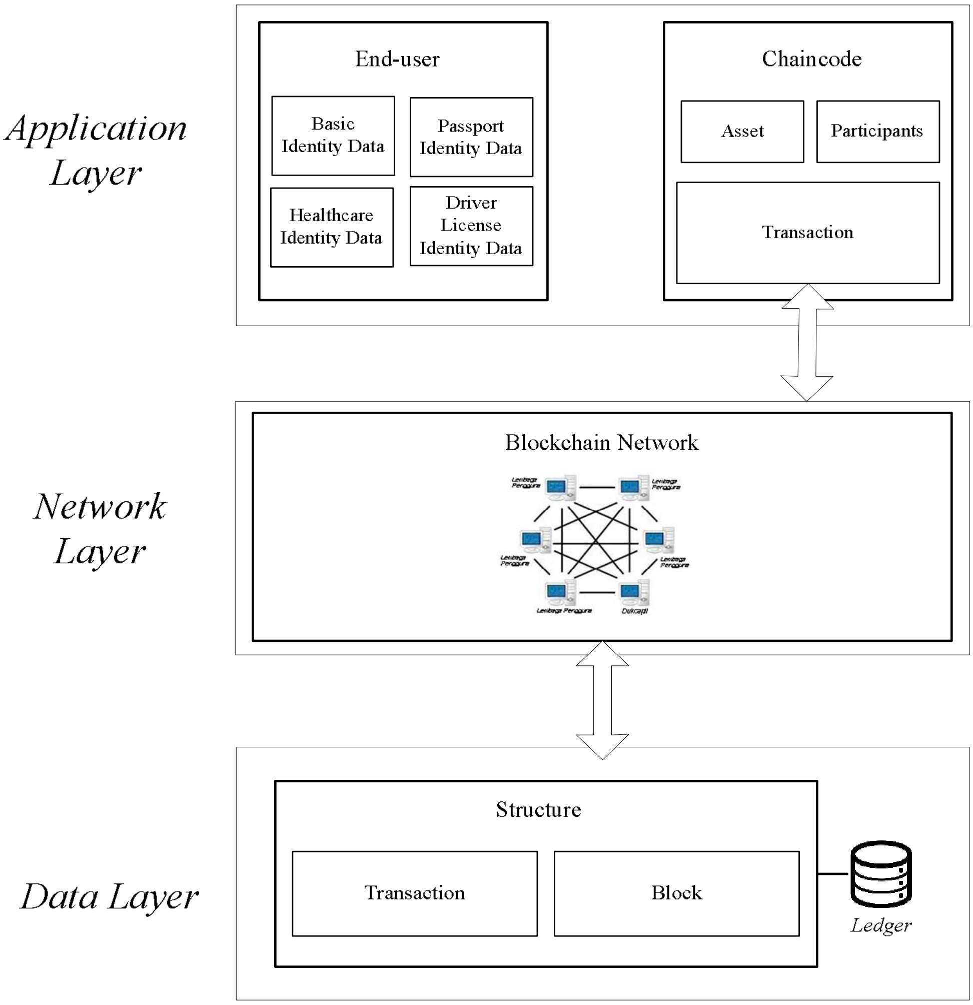


Fig. 1 System Architecture

1) Application layer: Consists of end-user applications and chain code applications. The end-user application could be connected to the blockchain network through the application chain code. First, there is a transaction validation process to Certificate Authentication to check the identity of the authority. If the user data is valid, the chain code could make a transaction request to the blockchain network. The end-user application makes a transaction request to the peer, then the peer could reply to the transaction by sending an approval or rejection of the transaction.

1) Network layer: Represents the blockchain network model of the designed system. The REST Server from Hyperledger Composer is run with the composer rest server tool connected to one of the authenticated peers using a certificate created during the business network creation process. This certificate is used to connect with the ordered in the network. The port that could be used in this research for the REST API uses port 8000. This study used four peers in one organization, as shown in Fig. 2. The organization is intended for the current system of government administration.

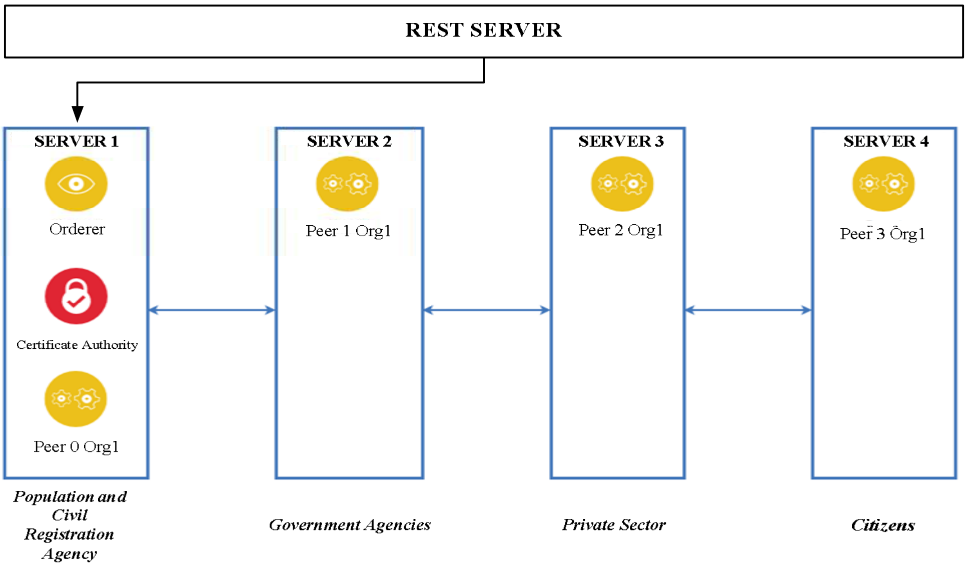


Fig. 2 Network Layer: Blockchain Network Design

TABLE II
PEERS design

Component	Port
Organization	Org1
Peers Name	peer0.org1.example.com peer1.org1.example.com peer2.org1.example.com peer3.org1.example.com
Certificate Authority	7054
Request peer0	7051
Request peer1,2,3	8051
Event hub peer0	7053
Event hub peer1,2,3	8053

The four are peer representing Population and Civil Registration Agency, government agencies consisting of the Director-General of Immigration, Departmental Police, Healthcare and Social Security Agency, the private sector represented by banks, and the last peers for citizens. An explanation of the design of each peer in this study is described in Table II.

2) Data Layer: This layer is responsible for the blockchain data structure and physical storage. The ledger is constructed using a linked list, sometimes known as Merkel trees, of blocks that are encrypted using asymmetric encryption Blockchain structure model of the designed system is as shown as in Fig. 3, the following is an explanation:

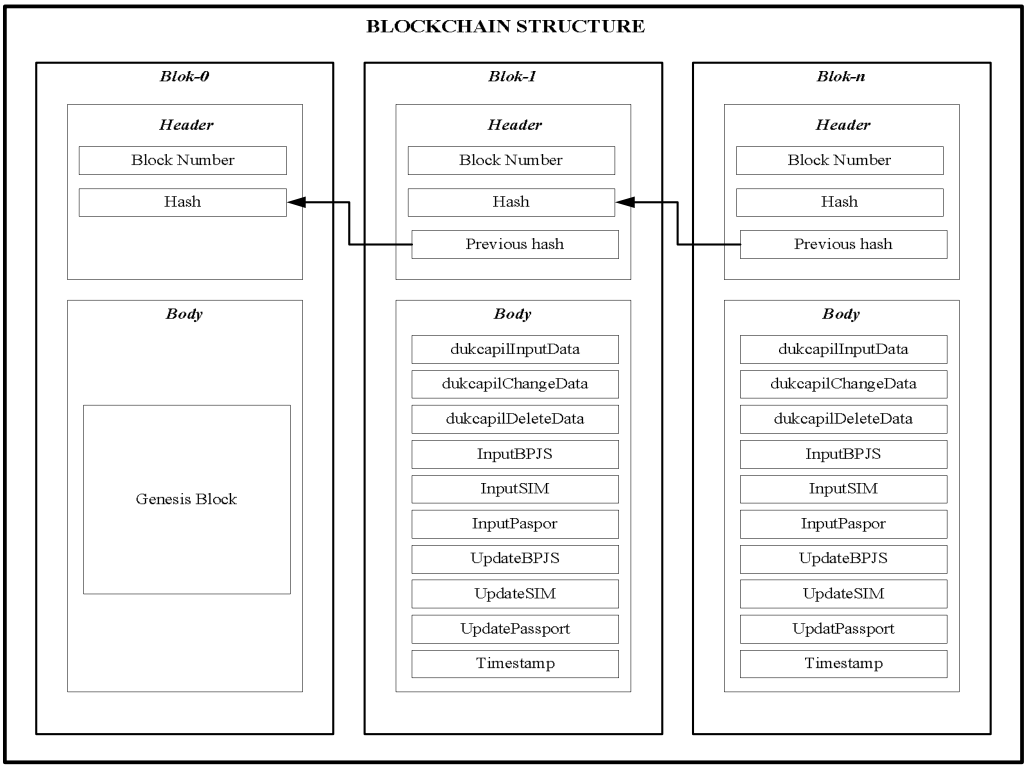


Fig. 3 Data Layer: Blockchain Structure

3) The block header: Consisting of information related to the block, contains three fields, namely the block number which contains the block number in sequence, the current block hash which contains the hash of all transactions from this block, and the previous block hash which is the hash of previous block which is the link between block one and next block.

4) Body block: Consisting of nine transactions occur in the system.

5) Blockchain: Combination of several interrelated blocks, namely the 0, 1st to n-th number of blocks formed. The first block of the blockchain is called the genesis block. In the next block or block 1 there is a header that stores the previous block's hash or block 0. All blocks could be interrelated and difficult to separate or immutability.

C. Transaction Flow

The following are the stages of transaction flow that is designed based on the system design, as described in Fig. 4:

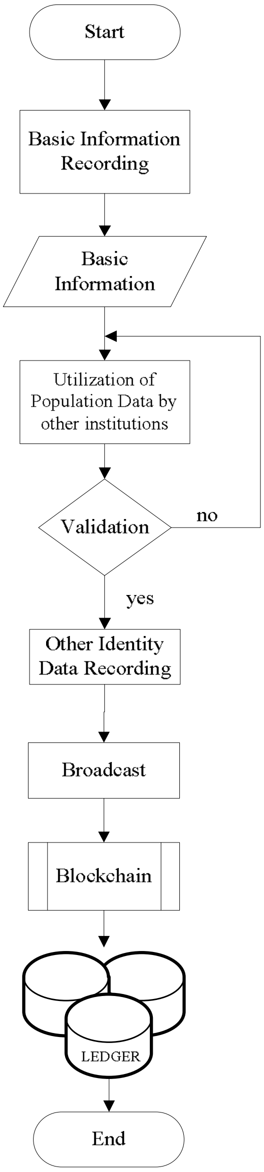

Start
Basic Information Recording
Basic Information
Utilization of Population Data by other institutions
Validation
no
yes
Other Identity Data Recording
Broadcast
Blockchain
LEDGER
End

Fig.4 System Transaction Flow

1) Basic information recording: Population and Civil Registration Agency inputs basic information data from citizens into the ledger so that other institutions can use it.

2) Validation of population data: If the basic information is correct, it could be disseminated or published to the blockchain subprocess for block validation by peer network members before being placed in the ledger.

3) Utilization of population data by other institutions: Basic information data that has been stored in the ledger could be used by other institutions for other identity registration processes or to validate potential customers.

4) Recording other identity data: Other's identity issuing institutions do not need to re-enter basic information data from citizens. They only need to fill in their ID NUMBER.

5) The end of this process is that the national identity data could be integrated in the blockchain system.

D. Implementation

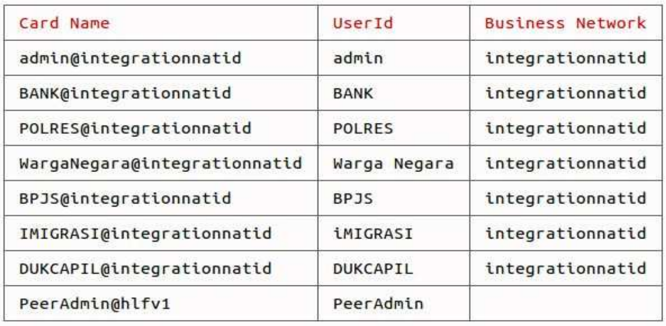
For implementation and system development, we identified the necessary platform and environments, namely Go Language, Python 2.7 x, Docker Engine version 17.03, Docker Compose version 1.8, Node JS version 8.9, NPM version 5. x, which run on a machine with the Linux Ubuntu 16.04, Intel i7- 4600 CPU @2.10 GHz processors and 8 GB of memory. Instead of open blockchain networks, we chose Hyperledger Fabric [28] for our implementation because it is specifically designed for private and performant business networks.

The implementation of the system in this study was carried out in three stages. The first stage is to install Hyperledger Composer. Installation of all software is the first step in installing Hyperledger composer on a virtual computer. These tools are essential for putting the Hyperledger composer into action. The second stage is to put the business network definition into action to create a business network archive (.bna), which is the end product of the design stage. At the identification Blockchain Network Component stage, it has been explained that there are three main components, namely assets, transactions, and participants. The implementation of business network definition uses the help of the Composer Playground tool, which could produce a business network archive (BNA) file. This .bna file could later be used in the Hyperledger Fabric implementation. Finally, implementing a blockchain network consisting of data structure and network artifact implementation.

1) Implementation of the data structure: Data ledger format is used in the blockchain network, while the data structure is a *.bna* file that has been designed at the business network definition stage. It consists of model files, script files, and access control. The model file is a file with. cto format responsible for describing the network structure and defining the participants, assets, and transactions involved in the system. A script file is a file that distinguishes various transaction functions on the network, written in JavaScript in *.js* format, handles transaction logic including the types of participants interacting and what variant of assets are transferred, and access control files are files that describe the scope of access that participants have on the business network.

2) *Implementation of network artifact:* Network artifacts are the result of implementing blockchain networks. It consists of creating a network configuration, creating a digital identity, and deploying the network. At the architectural design stage, it was stated that this research was designed using four peers in one organization. Where the organization has a Certificate Authority (CA) whose communications have been encrypted using TLS [28]. This CA is used as authentication when connecting with an orderer in the network. This orderer functions to validate each transaction and create blocks and distribute them to all peers connected to the orderer. Every peer connected to the orderer must also be in the same channel. In other words, a channel is a connection path between peers and orderers with the configuration stored in the connection profile of each peer. The network configuration implementation is saved in the *configtx.yaml* file, the *docker-compose.yml* file, and the connection profile.

The digital identity consists of a Certificate Authority (CA) and an Admin Card. Every entity in the blockchain network must have both for security in communicating between entities. The admin card is the admin's digital identity in the existing network in each organization. The admin card is an account for administrators on the network, installed in each organization intended for attaching the BNA file. The BNA file is then inserted into the server and installed on the admin card. The implementation for creating the admin card is saved in the file *createPeerAdmin.sh*. To see the cards that have been installed into the business network, you can use *composer card list* command, as shown in Fig. 5.



Card Name	UserId	Business Network
admin@integrationnatid	admin	integrationnatid
BANK@integrationnatid	BANK	integrationnatid
POLRES@integrationnatid	POLRES	integrationnatid
WargaNegara@integrationnatid	Warga Negara	integrationnatid
BPJS@integrationnatid	BPJS	integrationnatid
IMIGRASI@integrationnatid	iMIGRASI	integrationnatid
DUKCAPIL@integrationnatid	DUKCAPIL	integrationnatid
PeerAdmin@hlfv1	PeerAdmin	

Fig. 5 List of Installed Admin Cards

After the blockchain network configuration has been made, the next step is to run or start the network. The implementation for starting the network is saved as a script at the *start.sh* file.

E. Functional Testing

Functional testing is carried out based on testing the suitability of the blockchain network with network artifacts that have been implemented and the suitability of the system with its requirements using the black box method. Functional testing could be carried out based on test scenarios. The transaction is successful as shown in Fig. 6, which shows that one transaction has been successfully added to the ledger.

```
2022-01-02     09:29:12:276     UTC     [kvledger]
CommitwithPvtData     ->     INFO     089     Channel
[mychannel]:  Committed  block  [40]  with  1
transaction(s)
```

Fig. 6 Success Transaction Status

Another functionality test that could be carried out in this research is to disable one of the existing peers on the system. For example, in the scenario where one peer is turned off, and then the other peer makes a transaction issuing the same identity, the status obtained could show Ignoring duplicated identity, the status obtained could show *Ignoring duplicated identity* as shown in Fig. 7.

```
2022-01-02      09:30:21:097      UTC      [vscc]
deduplicateIdentity   ->   WARN   088   Ignoring
Duplicate Identity, Mspid: Org1MSP,
```

Fig. 7 Failed Transaction Status

This research has successfully carried out functional testing in accordance with system design with predetermined scenarios. Based on the results of functional testing of the system, it can be concluded that the prototype of this system can work according to the functional requirements that have been defined. In other words, this research has succeeded in complementing the previous research [19] by developing and implementing the model design proposed in the previous research in Hyperledger Fabric. This research also offers the use of population data by user institutions so that it is equipped with access restrictions that user institutions can carry out.

IV. Conclusion

Based on the results that have been described, we address the issues of the information system developed by the agency responsible for issuing national identity numbers not being integrated and the issue of misuse of data from population data utilization programs by user institutions. According to our implementation and evaluation, this research successfully developed a prototype of an integrated national identity storage security system that was coupled with blockchain technology.

This research proves that blockchain may be used as a solution for system integration, particularly the integration of national data separated across multiple issuing institutions. Because of the blockchain network's decentralization, all data transactions on the network are saved and distributed to all entities on the network. This is also important in the execution of population data usage programs by user institutions, preventing data exploitation. Blockchain technology can optimally realize technology to secure data integrity and immutability. Further work to be done regarding the integrated national identity security system is that the system must be verifiable through test results in real conditions for distributed systems using local area or virtual private networks with device locations physically separated by peers.

Acknowledgment

This research was supported by the grant of PDM (*Penelitian Dana Mandiri*) 2021 of Institut Teknologi Telkom Jakarta (ITTJ). We are grateful to LPPM (*Lembaga Penelitian dan Pengabdian kepada Masyarakat*) of ITTJ.

References

[1] R. D. Lusmiarwan, "The Design Study of Indonesian Single Identity Number Prototype," M.T. thesis, Institut Teknologi Bandung, Indonesia, 2016.

[2] Peraturan Pemerintah, "Peraturan Pemerintah (PP) Nomor 40 Tahun 2019", May 23, 2019.

[3] Menteri Dalam Negeri, "Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 61 Tahun 2015", Agustus 2015.

[4] FPD2K, "Dari 30 Jadi 3.904 Lembaga Pengguna, Integrasi Data Nasional Sudah Berjalan", Sep. 25, 2021. https://dukcapil.kemendagri.go.id/berita/baca/859/dari-30-jadi-3904-lembaga-pengguna-integrasi-data-nasional-sudah-berjalan (accessed Jan. 30, 2021).

[5] D. Schuff and R. St Louis, "Centralization vs. Decentralization of Application Software", *Commun. ACM*, vol. 44, pp. 88–94, Jun. 2001, doi: 10.1145/376134.376177.

[6] R. A. Sarıtekin, E. Karabacak, Z. Durgay, and E. Karaarslan, "Blockchain based secure communication application proposal: Cryptouch", in *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, Mar. 2018, pp. 1–4. doi: 10.1109/ISDFS.2018.8355380.

[7] N. Diallo *et al.*, "eGov-DAO: a Better Government using Blockchain based Decentralized Autonomous Organization", in *2018 International Conference on eDemocracy & eGovernment (ICEDEG)*, Apr. 2018, pp. 166–171. doi: 10.1109/ICEDEG.2018.8372356.

[8] E. Sutanta, "Model Integrasi Database Penduduk Indonesia Dengan Berbagai Sistem Informasi Berbasis Komputer", *Jurnal INFORMATIKA Program Studi Teknik Informatika, Universitas Ahmad Dahlan Yogyakarta, ISSN: 1978-0524*, vol. 5, pp. 542–553, Jul. 2011.

[9] R. Y. Amran, "Interoperabilitas Sistem KTP Elektronik Terdistribusi Berbasis Simple Object Access Protocol (SOAP)", *Jurnal Inspiration*, vol. 2, no. 1, 2012.

[10] M. Amin, A. D. I. Sutrisman, D. Setiawan, E. Ermatita, and A. Maseleno, "Design restful web service of national population database for supporting e-health interoperability service", *Journal of Theoretical and Applied Information Technology*, vol. 96, pp. 4794–4805, 2018.

[11] The World Bank, *ID4D Country Diagnostic: Nigeria*. Washington DC: World Bank Group, 2016. [Online]. Available: http://documents.worldbank.org/curated/en/136541489666581589/pdf/113567-REPL-Nigeria-ID4D-Diagnostics-Web.pdf.

[12] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", *Cryptography Mailing list at https://metzdowd.com*, 2009.

[13] S. Singh and N. Singh, "Blockchain: Future of financial and cyber security", in *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)*, Dec. 2016, pp. 463–467. doi: 10.1109/IC3I.2016.7918009.

[14] M. E. Peck, "Blockchains: How they work and why they'll change the world", *IEEE Spectrum*, vol. 54, pp. 26–35, 2017, doi: 10.1109/MSPEC.2017.8048836.

[15] J. Palfreyman, "Blockchain for Government?", *IBM Tax & Revenue Management*, Oktober 2015. https://www.ibm.com/blogs/insights-on-business/government/blockchain-for-government/.

[16] M. Juan, A. Piñeros, R. V. Páez, R. E. Gustavo, and M. Pérez Cerquera, "A Model for National Electronic Identity Document and Authentication Mechanism Based on Blockchain", *International Journal of Modeling and Optimization*, vol. 8, pp. 160–165, Jun. 2018, doi: 10.7763/IJMO.2018.V8.642.

[17] K. Mudliar, H. Parekh, and P. Bhavathankar, "A comprehensive integration of national identity with blockchain technology", in *2018 International Conference on Communication information and Computing Technology (ICCICT)*, Feb. 2018, pp. 1–6. doi: 10.1109/ICCICT.2018.8325891.

[18] A. Jha, R. Kanti Bhattacharjee, M. Nandi, and F. Barbhuiya, *A Framework for Maintaining Citizenship Record on Blockchain*. 2019. doi: 10.1145/3327960.3332389.

[19] R. Z. Fathiyana, F. Hidayat, and B. Rahardjo, "An Integration of National Identity towards Single Identity Number with Blockchain", Jul. 2020. doi: 10.4108/eai.12-10-2019.2296532.

[20] W. S. Nakamoto, "A Next Generation Smart Contract & Decentralized Application Platform", 2015.

[21] A. R. Rajput, Q. Li, M. Taleby Ahvanooey, and I. Masood, "EACMS: Emergency Access Control Management System for Personal Health Record Based on Blockchain", *IEEE Access*, vol. 7, pp. 84304–84317, 2019, doi: 10.1109/ACCESS.2019.2917976.

[22] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues", *Telematics and Informatics*, vol. 36, pp. 55–81, 2019, doi: https://doi.org/10.1016/j.tele.2018.11.006.

[23] C. Cachin and M. Vukolic, "Blockchain Consensus Protocols in the Wild", *ArXiv*, vol. abs/1707.01873, 2017.

[24] P. Thakkar, S. Nathan, and B. Vishwanathan, "Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform", *arXiv e-prints*, p. arXiv:1805.11390, May 2018.

[25] S. K. Lo *et al.*, "Analysis of Blockchain Solutions for IoT: A Systematic Literature Review", *IEEE Access*, vol. 7, pp. 58822–58835, 2019, doi: 10.1109/ACCESS.2019.2914675.

[26] Hyperledger, "Welcome to Hyperledger Composer", 2018. https://hyperledger.github.io/composer/latest/introduction/.

[27] Hyperledger, "An Introduction to Hyperledger". Jul. 2018. [Online]. Available: https://www.hyperledger.org/wp-content/uploads/2018/07/HL_Whitepaper_IntroductiontoHyperledger.pdf.

[28] Linux Foundation, "Hyperledger Fabric", Dec. 06, 2018. https://www.hyperledger.org/use/fabric (accessed Jan. 30, 2022).