ISSN 2347 - 3983
Volume 8. No. 7, July 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter83872020.pdf
https://doi.org/10.30534/ijeter/2020/83872020

Identity Management Technology Using Blockchain in Indonesia

Lutfi Januar Widayanto[1], Ahmad Nurul Fajar[2]
[1]Information Systems Management Department, Binus Graduate Program – Master of Information System Management, Bina Nusantara University, Jakarta, Indonesia 11480, lutfi.widayanto@binus.ac.id
[2] Information Systems Management Department, Binus Graduate Program – Master of Information System Management, Bina Nusantara University, Jakarta, Indonesia 11480, Indonesia, afajar@binus.edu

ABSTRACT

The underlying technology behind blockchain can provide a significant benefit for various industries in term of transparency, security and many features. Blockchain technology also believed to transform the existing identity management in a highly secure manner. Indonesia is one of the largest archipelagic country in the world, extending 5,120 km from east to west and 1,760 km from north to south with 237.6 million population, the fourth largest in the world. It will be very difficult to implement identity management for its citizen. There are multiple ID cards being used and accepted in Indonesia, from student card, driver license, tax id, etc. Blockchain technology is expected to simplify the existing identity management problems in Indonesia. This paper will try to describe the implementation, advantages and disadvantage of blockchain technology when applied to identity management in Indonesia.

Key words : blockchain, identity management, Indonesia, smart contract.

1. INTRODUCTION

The existing identity management system implemented in Indonesia is neither secure or reliable. At every point, we are being asked to identify ourselves through multiple government issued cards, such as student card, passport, tax id, driver license, id card and so on.

Today many peoples in Indonesia can not formally prove their identity or has invalid identity due to several reasons, such as address change, change in marital status, etc. Invalid identity may lead in various issues, such as fraud, unable to enjoy public facility, up to government incentive may be received by invalid person.

In banking industry, the current identity system also caused several issues. Bank is required by regulation to do KYC – *Know Your Customer* process, however in the same time, Bank is unable to validate whether the identity card presented by its clients is valid. The current identity management ecosystem is archaic and inefficient, we see today some person has multiple eKTP with different information, some person identification card also not recorded in Government database, hence a new authentication and identity management framework is required.

Digital identity may increase the speed of processes between organization, by allowing for greater interoperability between department or organization. But if digital identity is stored in central sever, like we have today in Indonesia for eKTP, it becomes a honeypot for hackers.

In principal identity need to be portable and verifiable by other parties, any time, everywhere and digitization can help to overcome this requirement, however being digital only is not enough, identity should also be private and secure to be able to fully replace the existing digital identity management that is archaic, fragmented and inefficient.

Government, across the globe are continue to strengthen their identity management strategies to fight criminal in stealing or forging identity up to fight terrorism as well as money laundering activity.

Blockchain technology come as an answer, it allows the control of identity data to move from government to the citizen, [1] securely and efficiently. It would enable citizens to view their public service identity via an identity app on their smartphone and share relevant data with government agents or any other parties in a secure manner.

The identity management system supported by blockchain technology also may also provide a benefit for its citizen and any other parties to use the identity management system for online services. The solutions may provide a convenient, efficient and accountable online service delivery. This also provide benefit for government in term of law enforcement and national security where government can easily and accurately track an individual or linking the individual data with any third-party data to help any criminal investigation.

2. LITERATURE REVIEW

2.1 Blockchain Technology Overview

Blockchain technology can be described as a distributed database that records transactions that are shared with people who are members of a distributed database network [2]. Every transaction that occurs must always be in accordance with the agreed consensus in the distributed database network which ultimately makes the possibility of fraud to be minimized. The system was created for Bitcoin as it is the first application of this network [3].

In general, blockchain is a collection of blocks that are interconnected (linked) and contain information about the transactions that occur. The key in blockchain technology is the ability to trace back in a distributed database network.

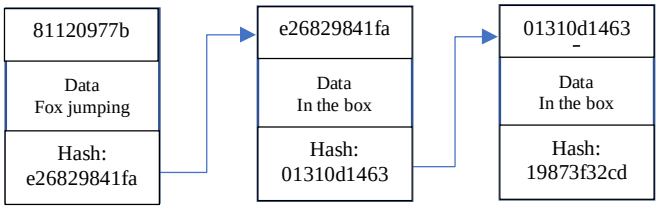


Figure 1: Structure of Blockchain [4]

2.2 Benefit of Blockchain Technology

a) Decentralized
This is one of the main benefits of Blockchain Technology. Blockchain technology require no middle man to verify the data. Each participant will verify any new block added to ensure the validity of the block and further make a consensus.

b) Transparency
Any records added to the blockchain will be shared with any other participant and it can't be changed or deleted due to the unique hashing method. When a new block is created a relevant hash is calculated. The hash will also contain the hash value of previous block. This technique makes it safer, because if someone successfully tamper one block, in the chain then hash will change and it will also make the next block to become invalid because it does not store the valid hash from previous block. These recordings technique provide Blockchain transparency, eternity and trust [5]

c) Immutable
When a data or transaction added to the chain, it will not be possible to change it as the data will be replicated to all participant system unless, someone has a sufficient computer power to overwrite or delete the information in all participant system.

d) Security
Blockchain security is a reliable chain of cryptographic hash. When a new block or transaction is created a relevant has for this block/transaction is calculated. The hash will also contain the hash value of previous block. This technique makes it very difficult to change any information without changing the hash value.

2.3 Individual Case Study

2.3.1 The Republic of Georgia Land Title Registry

The Republic of Georgia uses blockchain technology to provide digital certificate for its citizen land title. The National Agency of Public Registry (NAPR) of Republic of Georgia in partnership with Bitfuri Group, adding the cryptographical proof of the transaction in public Bitcoin blockchain [6].

The project was started in April 2016 [6] and the solution is proven to help Georgia to fight corruption and resolve property claims dispute. This project may also help to increase trust in citizen in the way how government do record keeping of their property as now everyone can check whether their land title is legitimate or not and everyone can ensure that nobody can tamper the record.

The Land Title registration process can be described in the below figure:

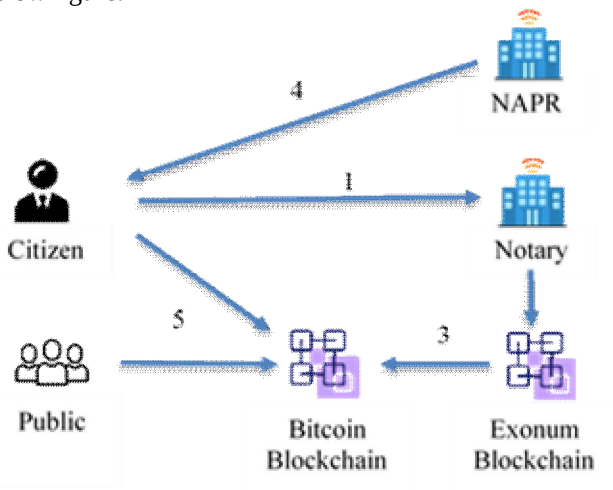


Figure 2: NAPR Land Title Registration Process [6]

Process flow can be described as follow:

1. Citizen initiate a land title registration or verification request to notary, similar like traditional system;
2. The notary performs registration of land title in exonum blockchain;
3. The hashes generated by private exonum blockchain are further anchored on public bitcoin blockchain. This is to ensure the integrity of transaction data in private exonum blockchain. Private data, such as land title registration information, are not stored in the public blockchain but it

is stored in the private exonum blockchain where both Notary and NAPR has an actual copy of the data;
4. Citizen will receive a digital certificate of their land from NAPR. The digital certificate is also supported by cryptographical proof of the originality of the extract that were published on the public bitcoin blockchain;
5. Any Gergoarian citizen can now check if the land title certificate is legitimate or not;

Key Takeaway

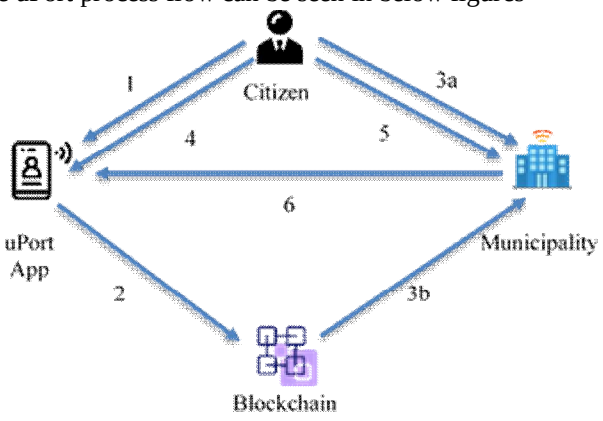
a) The main advantage of blockchain technology in this use case is increased security and reliability of digital certificates issued by NAPR;
b) The implementation of blockchain technology does not replacing the existing system, however it provides a new functionality and benefit on top of existing system hence the integration with existing system is relatively easy;
c) Verification of NAPR digital certificate is done via public blockchain, which is no participant has control on it. This provide independency and incorruptible layer that help government to combat frauds and minimize land title disputes.

2.3.2 City of Zug decentralized identity (uPort)

The City of Zug, Switzerland launched a project that aim to provide a trusted blockchain based identity that can be used to authenticate for any government service as well as to share the personal data with third parties. The project has commenced on 15 November 2017. It was called uPort and build on the Ethereum blockchain [7].

uPort allow citizen to selectively disclose their personal data to certain third parties or government institution hence it gives citizen a full control and ownership of their personal data.

The uPort process flow can be seen in below figures



Figures 3: uPort process overview [7]

Process flow can be described as follow:

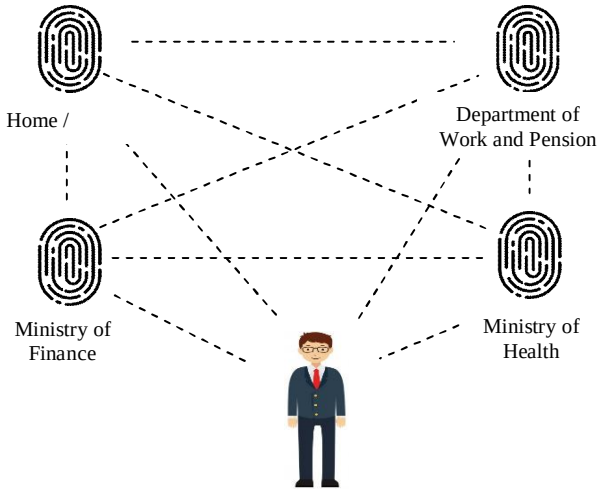
1. Citizen download the uPort app on their mobile phone;
2. The application will automatically generate a uPort ID. The uPort ID is a public address of a smart contract and this registered in Ethereum blockchain;
3. The citizen registers the uPort ID, their city of Zug ID Number and date of birth on the municipality website. Municipality system will further automatically link the uPort ID to the citizen personal ID as registered in Zug citizen registry system;
4. The citizen uses the uPort App to sign the registration request which is further send to the municipality;
5. Citizen is required to visit the municipality office in person to validate the request;
6. Once request is validated, municipality will digitally sign the request and automatically send the verification to uPort.

Key Takeaway

a) The uPort identity is a smart contract address, which can interact with other smart contracts and users;
b) Citizen, by using the uPort App, can selectively release the information to other parties. They can also choose what data, to whom and when to disclose. This ensure citizen has full control of their data;
c) Personal data is stored in a secured and encrypted form.

3. RESEARCH METHODOLOGY

3.1 Current Identity Management in Indonesia

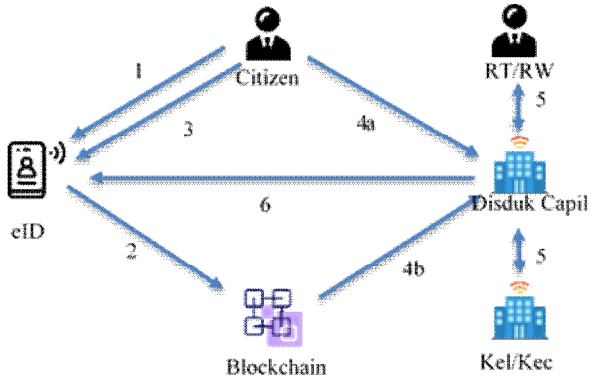


Figures 4: Today's world: multiple identity

- Indonesia identity card is called eKTP;
- eKTP was introduced by Ministry of Home Affair to replace the previous identity card;
- eKTP is issued by Department of Civil Registration, it will keep the individual person data in eKTP as well as in the central storage;
- The eKTP data is protected by cryptography and hence to authenticate whether the eKTP is valid or not, it will require a registration to Ministry of Home Affair to obtain the cryptography key;

- eKTP is not linked to any other individual data, such as student certificate, driver license, etc.
- Any personal data change, citizen need to visit multiple government office only to update their data, hence take a lot of effort and time.

3.2 Blockchain based identity management



Figures 5: Blockchain: Single, secure identity

The process can be described as follow:

1. Citizen download the government eID application on their mobile phone;
2. The application will automatically generate a smart contract ID. The ID is act as public address of smart contract and this is registered in public blockchain;
3. Citizen can enter their personal data in the eID application, including their existing eKTP ID. The eID application will encrypt and sign the data and send it to Department of Civil Registration;
4. Citizen is required to visit any government offices in person to validate the request including to record their biometric information. The information will then send to Department of Civil Registration for recording;
5. Department of Civil Registration will send signing request to local government official, such as Neighborhood Association (RT/RW), village head (Lurah), and sub-district head (Camat) where the citizen is living to verify the citizen;
6. Once all local government official digitally signed the request, Department of Civil Registration will digitally sign the request and push the verification to eID application

4. RESULT AND DISCUSSION

This paper tries to investigate the possibility to use blockchain for identity management in Indonesia. This section will describe the benefit of using blockchain for identity management as follow:

1. Efficiency gain for citizen. Any further ID changes, such as change in address, education, work, can be done directly by citizen at anytime and anywhere. Citizen only require other competent party, such as office, school, Neighborhood Association (RT/RW), village head (Lurah), and sub-district head (Camat) to digitally signed the request and their data will be updated;
2. Reduce risk of cyberattacks as most of citizen data is stored by citizen.
3. All party can easily verify citizen identification and on any data update, it will be distributed to all government official;
4. Reduce fake Government ID as every Indonesian can now ensure the citizen ID is legitimate or not;
5. Any other government institution and/or other party can link their own attestation to any citizen ID and citizen can either accept or reject such attestation.

While shifting the identity record from government to citizen may provide a huge benefit, this also introduce several risks associated with this implementation, for example citizen might:

1. suffer significant financial or non-financial loss by interacting with fraudulent entity;
2. experience major life disruption due to the loss of his/her identity credential such as stolen/missing device, missuses of their identity credential by unknown party, etc;
3. discriminated by society due to the trail left in their identity management.

5. CONCLUSION

The identity management system supported by blockchain technology may given huge benefit for either government, citizen and also third party, however there are also known risk associated with this. To minimize the risks there are several mechanisms in place, such as user level control, etc but none of them are likely be sufficient. Another key factor that must be in place are:

1. Education: Government must educate their citizen on how they should deal with their ID, including who they can share their ID with;
2. Law: Relevant law must be issued to ensure government is there to protect their citizen;
3. Technology: Choosing the right technology may also help to increase security, minimize risks and increase control

Despite the benefit offered by blockchain for identity management system, as of now only few countries adopting blockchain technology for identity management due to several consideration such as, the evolving nature of the technology itself, and the lack of standardization of data exchanges.

Many institutions and government agencies are now invested in the technology and continuous efforts to make blockchain-based systems fool proof. While no mechanism can be completely foolproof and devoid of vulnerabilities,

continuous technical innovation and awareness can help to bringing down the risk significantly and help us to move towards a safer world.

REFERENCES

[1] G. Zyskind, O. Nathan, and A. S. Pentland, "**Decentralizing privacy: Using blockchain to protect personal data**," in *Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015*, Jul. 2015, pp. 180–184, doi: 10.1109/SPW.2015.27.

[2] D. Efanov and P. Roschin, "**The all-pervasiveness of the blockchain technology**," 2018, doi: 10.1016/j.procs.2018.01.019.

[3] S. Nakamoto, "**Bitcoin: A Peer-to-Peer Electronic Cash System** | Satoshi Nakamoto Institute," 2008.

[4] A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, and J. Clark, **Bitcoin and Cryptocurrency Technologies Introduction to the book**. 2016.

[5] A. Bahga and V. K. Madisetti, "**Blockchain Platform for Industrial Internet of Things**," *J. Softw. Eng. Appl.*, 2016, doi: 10.4236/jsea.2016.910036.

[6] Q. Shang and A. Price, "**A Blockchain-Based Land Titling Project in the Republic of Georgia: Rebuilding Public Trust and Lessons for Future Pilot Projects**," *Innov. Technol. Governance, Glob.*, 2019, doi: 10.1162/inov_a_00276.

[7] P. Kohlhaas, "**Zug ID: Exploring the First Publicly Verified Blockchain Identity**," 2017. https://medium.com/uport/zug-id-exploring-the-first-publicly-verified-blockchain-identity-38bd0ee3702.