International Journal of Technology and Engineering Studies
volume 4 issue 2 pp. 50-56 doi: https://dx.doi.org/10.20469/ijtes.4.10002-2

# Ethereum Blockchain and Smart Contract Modelling For Presidential E-Voting System in Indonesia

**Alvin Julian Tjahajadi** *
Department of Informatics,
Surya University, Banten, Indonesia

**Vivian**
Department of Informatics,
Surya University, Banten, Indonesia

**Theresia Herlina Rochadiani**
Head of Informatics Department,
Surya University, Banten, Indonesia

***Abstract:*** This paper discusses the modeling of an e-voting system for the Indonesian Presidential Election using Ethereum Blockchain and Smart Contract technology. In Indonesia, the election in which the people elect a presidential candidate directly took place in 2004. However, the voting procedure has never changed since then. The Indonesian Parliament has discussed using e-voting in early 2008 to minimize fraud and accelerate counting and data recapitulation. In the current system, Ethereum blockchain is used as the solution to minimize fraud in the election process. Ethereum blockchain is a distributed ledger where every vote accepted must be validated and verified by every node. There is a smart contract feature in Ethereum, which functions as a public notary in the system that records and proves the credibility of each vote. For supporting of government's seriousness in developing the e-voting system in Indonesia, this study successfully designed the e-voting system by using Ethereum blockchain technology and smart contract as a security benchmark and utilizing the data of E-KTP as voter's unique identification. However, further enhancement in the supporting technology would be needed in order to be able to implement the proposed design system.

***Keywords:*** *Ethereum blockchain, smart contract, Indonesia, presidential election*

***Received:*** 20 November 2017; ***Accepted:*** 23 February 2018; ***Published:*** 13 April 2018

## I. INTRODUCTION

The democratic history of Indonesia started in 1955. It was the year when election was first held in Indonesia. The first election held was to elect the members of Parliament and the Constitutional Council. In 1998, the first Indonesian Presidential Election took place after President Soeharto's New Order Era. However, only in 2004, Indonesia held its first general election when citizens were the people who had the rights to elect President and Vice-President. Every citizens element in Indonesia has the same voting weight, that is, one man only has one vote [1].

The election system in Indonesia has been held since 2004 and it did not have any alteration. One of the factors why there is no change is because the election system in Indonesia is one of the best in the world and it has been acknowledged by other countries [2].Therefore, to be able to change the election system in Indonesia, it requires the public's trust in the new system that it will not create unconducive election environment. Hence, the system developed must have tabulation system and clear voting record while maintaining the privacy of voters [3].

Indonesian General Election Council has planned on implementing e-voting in 2014; however, it has yet to be done [4]. The chief of SIAK, Husni Fahmi stated that e-voting system will give more budget efficiency in Indonesian election because there will be faster vote counting, printing of the ballot cards will be unnecessary,

*Correspondence concerning this article should be addressed to Alvin Julian Tjahajadi, Department of Informatics, Surya University, Banten, Indonesia. E-mail: alvin.julian14@student.surya.ac.id

easier voting procedure, and the equipment are reusable in the next election [5].

Ministry of Home Affairs, Tjahjo Kumolo is very supportive towards the implementation of e-voting in 2019 Indonesian Election [6]. For supporting of government's seriousness in developing the e-voting system in Indonesia, we attempt on designing the e-voting system by using Ethereum Blockchain technology and Smart Contract as a security benchmark and utilizing the data of E-KTP as voter's unique identification.

## II. SUPPORTING TECHNOLOGY

### A. *Ethereum Blockchain*

Blockchain, also known as distributed ledger, has become an increasingly popular technology in the world. Blockchain technology became well-known from one of their end products, a digital cryptocurrency known as Bitcoin.

Blockchain began to become popular during the global economy crisis. Satoshi Nakamoto used the peer-to-peer protocol, which is used in download and file sharing process, and developed it into a protocol for electronic cash system named Bitcoin [7]. He developed cryptography-based electronic cash system with no government issues and other factor that will obstruct the currency's growth.

The main key from digital-based currency is that there is no centralized record. In the conventional process, a bank client is bound to the bank they use. Bank will record all the transactions including debit or credit from the client. In digital-based currency, all the records are implemented in a distributed ledger or a big distributed book which requires "volunteers" to verify and validate a transaction and accept it as a transaction in Blockchain [7].

Then how about transaction verification and acceptance in the Blockchain system? Blockchain is designed to have a set of rules regarding it. Blockchain system consists of a set of distributed computers connected to a global network. Then who is the owner of these computers? The computers connected to this distributed network are the volunteers who will verify and validate every single transaction in the Blockchain system [8]. Each computer which verifies and validates these transactions is known as miner. Miners will verify and validate by performing complex calculation algorithm which requires high-level computational capabilities. Therefore, miners usually use a computer with several Graphical Processing Unit (GPUs) as the main computing device to perform the calculation. Several considerations of using GPU instead of Central Processing Unit (CPU) are because GPU is cheaper and has higher computational capabilities compared to CPU [9].

Every miner is also called as a node. Every transaction that has been verified and validated by each node will be duplicated to another node [10]. This will make Blockchain system far more secured than the centralized system. Database used in Blockchain system is also distributed where database is stored in every node assigned as a miner. Transactions recorded in Blockchain are public and can be verified easily. However, Blockchain can be set as private consortium where only authorized users can get into the system.

In daily implementation, Blockchain can be analogized as Google Docs [11]. Google Docs has a feature, that is, if someone made changes in the document, everyone will have the updated version of the document right at that instance. This is the simple example of Blockchain that data will always be updated, and storage is distributed. Blockchain has encryption feature with high-level security. Without encryption, data stored in Blockchain are already secured. It is said to be secured because data are not stored centrally. With distributed network, data are stored in several nodes. However, only distributed ledger will not guarantee the security. Therefore, Blockchain uses encryption with public and private keys [7]. Not only using key as a security measure, Blockchain adds two additional features to enhance security. The two features are hash and blocks. Hash is a mathematical function that changes data into the fingerprint of the data named hash [12]. The formula or algorithm in hash will turn data into a different data with the same length. There are many hash functions, however one of the most well-known and secured is SHA-256 that the number 256 indicates how many bits are used.

Beside hash, one of the other security features in Blockchain is blocks. Blocks is one of the key features highlighted in Blockchain [12]. Blocks can be analogized as a big book that holds all the transaction records. Every transaction done in a firm is recorded into the big book. These recorded transactions are easily manipulated. In Blockchain system, transactions are not recorded per line, but per page. Every transaction done per page is added to the previous transaction. Previous transaction's data recorded on next transaction are data that have been hashed. This becomes the validator whether a transaction is valid to be stored in the Blockchain system [13].

The transaction that has been validated will not be recorded directly in the system; it will be gathered as a block or a book that will be inserted to the Blockchain system. The more blocks are validated and inserted into the system, the harder it is to alter the records [10]. However, this doesn't mean that data alteration is not possible. An admin can alter the transactions recorded in the system. But, the alteration must be verified and validated by the nodes which verified the record previously. This process makes data alteration harder for irresponsible parties. Blockchain is the technology behind Bitcoin. Blockchain proves that with database system and distributed ledger, a system can live without data centralization. Blockchain brings forth a new platform named Ethereum. Ethereum is a Blockchain platform that is available where this platform gives access to everyone who wants to create and use decentralized application that runs on Blockchain platform. Ethereum serves as a Blockchain system that uses programming language that fulfills the Turing-complete requirement [14]. This programming language can be used to create 'contracts' that will perform encoding against transition state function, create digital contract, digital currency and other things by writing a few code lines. Ethereum is a Blockchain development that Blockchain does not have the feature to write contracts or other things beside cryptocurrency and cryptocurrency exchange. It is developed by Vitalik Buterin, Gavin Wood, and Jeffrey Wilcke [15]. With the support from Microsoft and ConsenSys as decentralized application software creator service, Ethereum develops into one of the most used platforms for Blockchain-based application [16].

Ethereum has contract features named Smart Contract. The difference between Smart Contract and Blockchain in the Bitcoin system is that Smart Contract has more extensive features which can be applied in various applications. Every Smart Contract will be translated into bytecode that will be stored in Ethereum's distributed ledger. For every executed transaction, executor will receive some rewards from the node that requested it to be executed. The rewards received are called gas. Gas is the counting currency in Ethereum that shows the amount of power required to perform algorithm calculation from each transaction [10]. To execute each contract, the gas needed varies depending on the content of the contract that will be executed. If a contract that will be executed for the first time contains 2 characters, and the second contains 4 characters, there will be a difference between the amount of gas needed to record the transaction into distributed ledger. For the first contract, it will consume 26,587 gas (0.00053174 ether), and the second contract will consume 26,587 gas (0.00053302 ether). Gas is obtained by performing transaction verification and validation [10]. However, a computer could not complete verification and validation all the time. When a computer reaches the time that it could not perform verification and validation, gas can be obtained by purchasing it using digital Ether currency. The amount of gas equals to one Ether which varies depending on the level of difficulties of each block in the network [10]. There are four key technologies implemented in order to decentralize application to perform, Cryptographic tokens and addresses, Peer-to-peer networking, Consensus formation algorithm, and Turing complete virtual machine [17]. Not only these key technologies become the foundation to perform, Ethereum also uses hash function named KECCAK-256 [18]. This hash algorithm is similar to SHA-3 which becomes one of the most popular hash algorithms which reaches a high security level.

### *B. Smart Contract*

Smart Contract is one of the features in Ethereum Blockchain. Smart Contract becomes the primary bridge to store data or private counting. Analogized as contract, Smart Contract will also perform validation from each of the transactions. Currently, Smart Contract can be customized and built by ourselves using Solidity programming language that is developed by one of the Blockchain developers. This facilitates a way to make a contract which will be used by transactions in need.

Smart Contract is an account that holds the object in Ethereum Blockchain. Smart Contract contains a code that holds functions and it can interact with other contracts, make decision, store data, and send ether to the others [19]. Contracts are made and defined by the creator of contract; however, while performing execution, it depends on running the network service. They will keep existing and can be executed as long as the network is running, and it can vanish only when it is programmed to destroy itself.

The based concept for Smart Contract has been researched since 1997 by two scientists, Szabo and Miller [10]. In early 1990, everything became clearer that the agreement recorded by algorithm can be stronger and have legal certainty. Algorithm-based record concept was discussed in 1990s; however, during that period, there was no specific system that could be proposed to fulfill the concept. Smart Contract implementation in Ethereum Blockchain could be one of the main implementations in crypto-law [10].

There are several things that Smart Contract can do. One of them is to become a multi-signature account. In this case, an agreement can only be executed when a few percent of participants have agreed. Make buying and selling transactions between users, provide utilities for other contracts, and store several things, such as membership data, etc. [20]. The main purpose of Smart Contract is to enable two people or more to perform trading and finish business purpose through internet without the need of third party as mediator. Right now, Smart Contract has been implemented in lots of production-stage system. Until October 2017, there are 790 projects that have been developed or are in development using Smart Contract and Ethereum Blockchain [21]. The projects under development are not limited to cryptocurrency exchange or token exchange, but also games, copyrights record, social media platform, academic publishing, etc. Many kinds of project have been developed using Smart Contract and Ethereum Blockchain. This creates the opportunity for voting system that will be designed using Smart Contract. Smart Contract implementation into voting system is considered ideal enough because it provides high-level security (in this case, distributed system) and high availability (consensus). With the support of Smart Contract, e-voting system will be more secure and harder to be hacked by irresponsible parties.

### C. E-KTP (Electronic Resident Identity Card)

E-KTP is the individual identity card in Indonesia which consists of security system or control in administration or information technology based on national population database. One resident only will be able to have one E-KTP with National Identification Number. Thus, this identification number is sole identity for every Indonesian resident and it applies for a lifetime. There is a chip in E-KTP that stores fingerprints, the right thumb, and index finger which serve as unique identification.

## III. DESIGN OF E-VOTING SYSTEM

### A. Proposed E-Voting System Design

After performing a check on National Identification Number and current election system in Indonesia, the proposed design implementation is performed by inputting National Identification Number as unique identifier, and the vote for candidate will be stored in the counting container. The e-voting system design that we proposed is using National Identification Number as unique identifier and Fingerprint as voters' identity verification. Voters do not have to come to voting booth where their National Identification Number is especially assigned to. Because the e-voting system is global which means access is not limited to one location based on their address.

Fingerprint verification method will not be discussed further in this paper. In the Presidential Voting in Indonesia, voters do not only choose the President, but also the Vice-President. So, one vote means vote for President and Vice-President.

The e-voting implemented with Blockchain and Smart Contract will not be saved in public network, but private network. Thus, only people with authorities can access into the Blockchain system.

E-KTP data will serve as the key of the proposed e-voting system. E-KTP stored details about individual data that consist of personal information, even his fingerprint and retina. Not only personal data and biometric information, E-KTP is equipped with National Identification Number as unique identifier. By using the existing and recorded data in the E-KTP system, e-voting system will be easier to design and implement.

One of the most concerning issues in e-voting system is to keep data about the individual who votes and the candidate whom he voted secretly. This could create chaos and smudge the democracy. To ensure this confidentiality, every vote accepted is not allowed to be mapped against who voted. Every voter only will be checked whether he or she had voted. A Smart Contract must be designed separately for every election. For example, 2014 and 2019 Presidential Election. This will ensure everyone to have the rights to vote in every Presidential election as long as he or she still has the voting rights. For confidentiality, every transaction will only store the voter's National Identification Number and which candidate is voted without mapping or knowing who voted that candidate.

To verify the right voters, system will use fingerprint verification. The fingerprint data were recorded previously when the voters sign up for E-KTP. Not only fingerprint, resident's retina data are also recorded in the E-KTP system. Fingerprint verification is preferred than retina because the device is more affordable and faster. Because Presidential voting in Indonesia does not only choose the President, but also the Vice-President, the proposed design system will facilitate it by providing the candidate who will be voted, consisting of President candidates name and Vice-President candidates name. So, when a voter votes, it means he chooses the President and Vice-President at once.

The proposed e-voting system will be connected to Ethereum Blockchain. Every time voters cast a vote, the data will be recorded in two different storages. The first storage is the database of the e-voting system itself. This database will support the system by providing data for National Identification Number checking and fingerprint verification. Beside the database connected to e-voting system, Ethereum Blockchain will record the voters and selected candidate separately. Every vote and voters identity will be saved in different tables; so, it will not be mapped to one another. All the transactions that e-voting performs against a contract will be done in private consortium network. This will prevent irresponsible parties from accessing and making a change in the blockchain system. Private consortium concept will provide access only to authorized users. Ethereum Blockchain implementation in Private Consortium Network will not reduce the security level and the features of Ethereum Blockchain. But the restrictions in writing access on ledgers make the transactions unable to be written by unauthorized users.

### *B. The Election Process of Voters*

For the election process, every voter comes to the voting booth nearest to their home or it could be in public area. Voters are required to bring their E-KTP as a requirement to vote. When the voter has arrived at the voting booth, voter must input the 16 digits of National Identification Number into the system to access the e-voting system. After voters input their National Identification Number, voter is required to scan their fingerprint. This process is done to ensure that the voter is the rightful owner of the E-KTP.

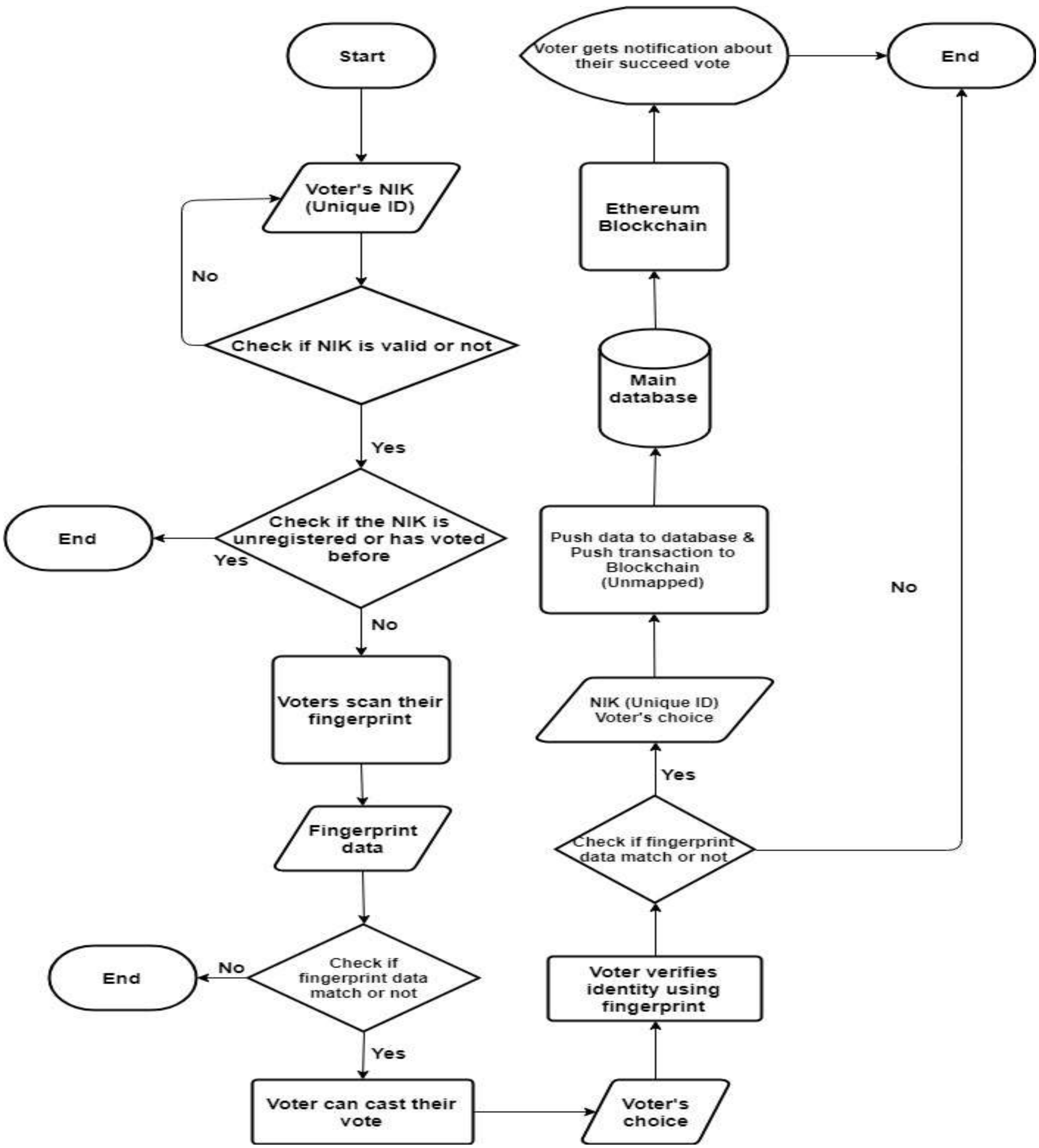


Fig. 1. E-voting flowchart

The purpose of the first fingerprint scan is to prevent fraud. This will determine whether someone is eligible to vote. If the scanned result does not match the recorded data, system will refuse that voter to vote. On the contrary, if the scanned fingerprint matches the data, voter can proceed to vote for the desired candidate.

After voting for the desired candidate, voter is required to scan their fingerprint once again as verification and confirmation of their choice. This is to avoid the possibility of fraud caused by irresponsible parties to vote using other's identity. Fingerprint verification is performed by checking the E-KTP data. While the scanned fingerprint does not match, the vote for candidate is invalid until voters succeed the verification.

After voter finishes the voting process, the vote will be recorded at two locations as explained in the previous section. The recording done in Ethereum Blockchain consists of two types of data, voter's National Identification and the candidate they voted without mapping. For National Identification Number, verification will be handled by main database. This main database can be made as decentralized and distributed database depending on the available infrastructure. National Identification Number verification is performed on the main database to reduce the gas needed for every transaction performed on Ethereum Blockchain.

Every voter can vote while still in election period. After the election period, the election will be closed, and voters cannot vote for any candidate anymore. Apart from that, every vote received for each candidate will not be shown live. This is to avoid the possibility of bias against the candidate voted for by every voter. The election result will be shown by the end of election period where vote cannot be done anymore.

To count the received votes, system will call the function from Contracts used during election. Every vote will be calculated directly and the exact number of votes for each candidate will be shown. The election result will be shown on the website to be easily accessed by various parties.

Not only the election result will be shown, each voter can check their own voting status. Voters can perform search using their National Identification Number and check whether they have vote and also the timestamp if they have voted.

### C. *Ethereum Blockchain Dataflow*

As shown in Figure 2, the voting result's data which contain result from web application will be sent using Web3Js. Web3Js is Ethereum's library provided to communicate between web applications and Ethereum RPC. Our web application will create transactions using web3js, web3js will trigger Ethereum RPC to communicate with the Ethereum Network and record the transactions. Ethereum RPC is the entrance for transaction processes in the Ethereum Network. Transactions will proceed in the Ethereum Private Consortium Network.

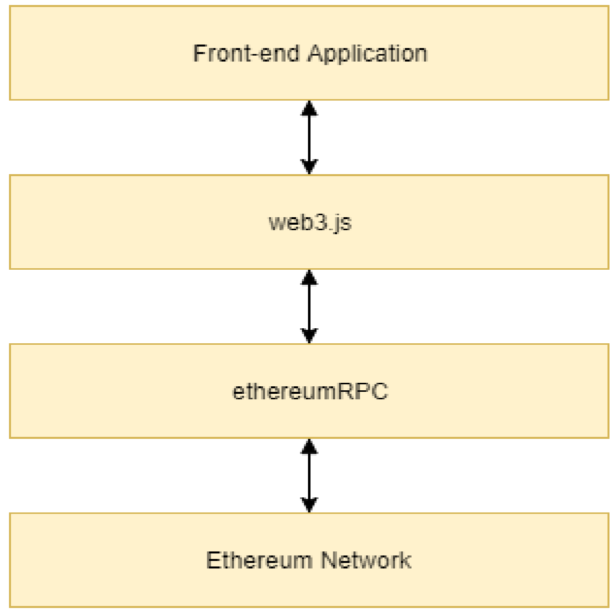


Fig. 2. Ethereum dataflow

## IV. DISCUSSION

From the discussion of the E-voting system above, the implementation of Blockchain and Smart Contract in Indonesian E-voting system can enhance the systems security. However, the system that we designed currently is not optimal enough to be implemented yet because of several circumstances.

First, Vitalik Buterin stated that public Ethereum Network is still slow for mainstream application. "Bitcoin is processing a bit less than 3 transactions per second," he said. "Ethereum is doing five a second. Uber gives 12 rides a second. It will take a couple of years for the blockchain to have Visa-scale TX capacity" [22]. The experiment was conducted on public consortium. This will disrupt the stability of e-voting System because of piled up transactions and it could not be completed in a short period of time. If the election period starts from 7 A.M. until 1 P.M. [23], which means the voting duration is 6-hour long, the number of voters who will vote is 190 million citizens [23], the Blockchain system must process roughly around 8797 transactions per second. Ethereum Blockchain networks need to improve their capabilities to handle transactions per second. It will need further research and time to grow the network. So, it will be better if the contract is deployed on Ethereum Private Consortium. Another reason is, Indonesia has their own geographic challenge. Indonesia consists of many islands, and the uneven infrastructure development will cause e-voting system hard to implement. Indonesian Government must consider the areas that have yet to be reached by technology and development. An evenly spread development will make e-voting easier to be implemented in wider areas.

Furthermore, there are inland people who are yet to be recorded. E-KTP data collection is still unfinished and tends to be undirected which can obstruct e-voting implementation. There is no other unique identifier that could substitute E-KTPs National Identification Number as an identifier in election. Government must give the eye and accelerate E-KTP registration, not only as citizens identity data but also to support e-voting implementation.

## V. CONCLUSION AND RECOMMENDATIONS

The designed E-voting system can minimize frauds because it implements Blockchain and Smart Contract in it. Blockchain system that records transactions per page supports anti-fraud and vote manipulation. Also, voters do not have to come to voting booth where their National Identification Number is especially assigned to. Because the e-voting system is global which means access is not limited to one location based on their address.

### Declaration of Conflicting Interests

There are no conflicts of interest.

## REFERENCES

[1] KPU RI, "Election commission of the Republic of Indonesia, KPU, Jakarta, Indonesia," 2008. [Online]. Available: http://www.kpu.go.id/

[2] D. Tapscott and A. Tapscott, "Realizing the potential of blockchain: A multistakeholder approach to the stewardship of blockchain and cryptocurrencies," in *World Economic Forum White Paper*, Geneva, Switzerland, 2017.

[3] D. Tapscott and T. Alex, *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. London, UK: Penguin, 2016.

[4] Ahmadi, "The feasibility study on trapping experiments with lights in Barito river of Indonesia," *Journal of Advances in Technology and Engineering Research*, vol. 3, no. 6, pp. 235–243, 2017. doi: https://doi.org/10.20474/jater-3.6.3

[5] Bitcoin Wiki, "Why a GPU mines faster than a CPU," 2013. [Online]. Available: https://bit.ly/KebBar

[6] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, 2014.

[7] A. Rosic, "What is blockchain technology? A step-by-step guide for beginners," 2018. [Online]. Available: https://bit.ly/2nna7Ac

[8] A. Lewis, "A gentle introduction to immutability of blockchains," 2016. [Online]. Available: https://bit.ly/2a91owv

[9] A. Berke, "How safe are blockchains? It depends," *Harvard Business Review*, 2017. [Online]. Available: https://bit.ly/2naCjoO

[10] V. Buterin, "A next-generation smart contract and decentralized application platform," 2014. [Online]. Available: https://bit.ly/2lH1ZtG

[11] A. Hertig, "Who created ethereum?" 2017. [Online]. Available: https://bit.ly/2JgL7o2

[12] A. Rosic, "What is ethereum? A step-by-step beginners guide," 2016. [Online]. Available: https://bit.ly/2pdR4L5

[13] ConsenSys, "Ethereum is how the internet was supposed to work," 2017. [Online]. Available: https://bit.ly/2LU1UmL

[14] J. Manning, "SHA-1 may be broken but ethereum is still secure," 2017. [Online]. Available: https://bit.ly/2n9Q1Ko

[15] Ethereum, "Building a smart contract using the command line," 2017. [Online]. Available: https://bit.ly/2OLr3Oi

[16] A. Hertig, "How do ethereum smart contracts work?" 2017. [Online]. Available: https://bit.ly/2xqOhQU

[17] State of the DApps Community, "A curated collection of 790 decentralized apps," 2017. [Online]. Available: https://bit.ly/2lbbZv7

[18] B. Hermawan, "Bawaslu: Elections in Indonesia best in the world," 2015. [Online]. Available: https://bit.ly/2n8yTER

[19] BPPT, "E democracy voting at the fingertip (I)," 2013. [Online]. Available: https://bit.ly/2MhiWr2

[20] BPPT, "Information technology, energy & material technology," 2010. [Online]. Available: https://bit.ly/2LO1AWq

[21] BPPT, "Minister of home affairs Tjahjo: We are ready to apply 2019 election voting," 2015. [Online]. Available: https://bit.ly/2KpUhyw

[22] J. Biggs, "Ethereum will match visa in scale in a couple of years says founder," 2017. [Online]. Available: https://tcrn.ch/2hdGtLd

[23] Ronald, "Pay attention, this is the clock & the rules for the people of DKI who want to vote," 2017. [Online]. Available: https://bit.ly/2LQpv7U