Journal of Engineering and Science Research 2 (5): 13-17, 2018
e-ISSN: 2289-7127

DOI: 10.26666/rmp.jesr.2018.5.3

Block-Chain Based E-Voting For Indonesia

Agus Winarno, Javalina Harsari, and Bayu Ardianto
National Cyber and Crypto Agency
Jl. Harsono RM No 70, Ragunan, Pasar Minggu, Jakarta Selatan, Indonesia

Abstract: Indonesia is the third largest democracy in the world. Election is a means for Indonesians to deliver votes to elect leaders and representatives of the people. Existing elections still use traditional methods. Watch the development of blockchain technology being the favorite in the world of research and development, blockchain will be designed based on e-voting for Indonesia. Based on the design created, the benefits of the blockchain can fulfill the principles in Indonesia which were introduced in Law No. 7 of 2017. The principles of the election include direct, public, free, confidential, honest and fair can be fulfilled with the nature of blockchain which consists of anonymity, autonomy, fairness, secrecy, and transparency. Other things that become the advantages of blockchain are distributed and auditable.
Key words: *blockchain, e-voting, public key*

INTRODUCTION

Indonesia is a country with democratic governance based on Pancasila and 1945 Constitution of the Republic of Indonesia. One of the implementation of people sovereignty so as to produce a democratic government is by the existence of general elections to elect government leaders that carried out directly by the people.

According to the Law of the Republic of Indonesia Number 15 of 2011[1] concerning General Election Organizers, it is explained that the definition of General Election, hereinafter referred to as Election means of implementing people sovereignty held directly, publicly, freely, confidentially, honestly and fairly in the Unitary State The Republic of Indonesia is based on Pancasila and the 1945 Constitution of the Republic of Indonesia. Based on the provisions of Article 22E of the 1945 [2] Constitution of the Republic of Indonesia which explains that the General Election is held to elect the President and Vice President, DPR members, DPD members, and DPRD members who held according to the principle of direct, public, free, confidential, honest and fair.

Explanations regarding election principles are as follows[3]:

a. Direct
   People who have the right to vote have the right to vote directly in accordance with their beliefs without an intermediary.
b. Public
   Voters have guaranteed opportunities that apply to all citizens, without discrimination based on ethnicity, religion, race, class, gender, and social status.
c. Free
   Every voter has the freedom to determine his choice without coercion from other parties.
d. Confidential
   Citizens who have chosen guaranteed his choices are unknown to anyone through any means.
e. Honest
   In holding elections, election organizers, officials, election participants, election supervisors, monitors and all involved must be honest in accordance with the laws and regulations.
f. Fair
   Every election participant gets the same treatment, and is free from cheating any party.

Corresponding Author: Agus Winarno, National Cyber and Crypto Agency, Jl. Harsono RM No 70, Ragunan, Pasar Minggu, Jakarta Selatan, Indonesia, agus.winarno@bssn.go.id

Bitcoin is a digital currency that is a means of payment that is point to point from one person to another without need assistance from financial institutions. As a substitute for the function of financial institutions in maintaining the existence of double spanding in remittances, bitcoin utilizes the function of digital signatures. Transactions recognized by the system are transactions that have been signed with the digital signature of the token owner and are first recognized in the bitcoin network[4]. There are several components used in bitcoin, namely[5]:

a. Node
   Bitcoin nodes are computer devices that run bitcoin cores that are connected to the internet. Bitcoin nodes play an important role in providing blockchain copies and providing information related to transactions that have been stored on the blockchain.
b. Bitcoin Network
   The bitcoin network is a network that connects the entire bitcoin system. The bitcoin network has two main network types (mainnet) and a test network (testnet). All transactions that are running at this time are located and operate on the mainnet network, while the network used to develop the bitcoin system is found on the testnet network.
c. Bitcoin Address
   A bitcoin address is a user address that can be used as an address to send bitcoin.
d. Transaction
   Transaction is a process of transferring coins from one user to another using the digital signature chain mechanism.

Blockchain can be interpreted as a data structure that allows us to create digital books from a data and share data in a network. Each block contained in blockchain technology is always linked to one block before and one block afterwards.

There are several types of blockchain that exist today, namely [6]:

a. Public Blockchains
   Public blockchains, such as Bitcoin, are large distributed networks that are run through a native token. They're open for anyone to participate at any level and have open-source code that their community maintains.
b. Permissioned Blockchains
   Permissioned blockchains, such as Ripple, control roles that individuals can play within the network. They're still large and distributed systems that use a native token. Their core code may or may not be open source.
c. Private Blockchains
   Private blockchains tend to be smaller and do not utilize a token. Their membership is closely controlled. These types of blockchains are favored by consortiums that have trusted members and trade confidential information.

All three types of blockchains use cryptography to allow each participant on any given network to manage the ledger in a secure way without the need for a central authority to enforce the rules. In addition, there are benefits that blockchain has that can be used in system design[7] :

a. Security
   Cryptography in the system Follow My Vote is asymmetric encryption. The resulting key is in the form of two pairs of public keys that are mathematically related. Public keys will be published in the system and private keys are only accessed by users. Only people who have private keys can use the account..
b. Accuracy
   In the selection of each user used will be verified by the verifier and registar so that the user who can choose is the verified user. These users can only make direct and can't delegate.
c. Transparency
   All ballots in the system are stored in the blockchain so that the user can see how many votes each of the objects has. In addition the system is auditable.
d. Autonomy
   The big thing that the follow my vote system has is that it has advantages in the field of decentralized systems. This system also runs according to what was initiated by software developers.
e. Anonymity
   The voting system used is anonymous so the user feels safe but can still check that the selected sound entered the system.
f. Forgiveness
   Every user who has made a vote is possible to make changes during the election period.
g. Fairness
   Each user can choose each wish they want.
h. Efficiency

The expected target of this system is to maximize revenue and minimize operating costs..

Blockchain is a technology that is widely used in research and development in various fields of technology. Blockchain became famous as a cryptocurrency that has fantastic value. Blockchain has advantages that provide distributed, safe, anonymized, transparent, auditable systems. The blockchain nature is expected to help create an e-voting system that can fulfill the principles of elections in Indonesia (Article 22E of the 1945 Constitution), namely Direct, General, Free, Secret, Honest, and Fair.

BLOCKCHAIN DESIGN

Based on Law No. 7 of 2017 concerning General Election article 2, it is stated that the principles that must be fulfilled in elections are direct, free, confidential, honest and fair. These principles are also contained in the 1945 Constitution in article 22E paragraph 1. In this paper will be explained These election principles mapped in the blockchain function as follows:

NO	Election Principle	Explanation	Blockchain Feature	Information
1	Direct	The elections must be carried out directly, not allowed to be represented	*Acuracy,*	Only the owner of the token (private key) can use their voting rights
2	General	Elections can be followed by all citizens who have the right to use votes without exception	*Acuracy, Transparency*	Voters can use their right to vote if they fulfill demographic rules in Indonesia (over 17 years of age) and everyone can see the tabulation and audit the system.
3	Free	Elections are carried out without coercion from any party.	*Autonomy,*	Each voter can make a choice without coercion from any party and is not changed by another party.
4	Secret	Voters are confidential and closed and ballots cannot be known by any party except the voters themselves	*Anonymity, secrecy*	The election process is confidential and only those who know.
5	Honest	Honest principles in elections mean that good and democratic elections are carried out in accordance with the rules that have been determined.	*Fairness*	Each voters can only vote once.
6	Fair	Fair principles in elections are the same treatment for election participants and voters.	*Fairness*	Each voter has the same token value for each selection process.

E-VOTING DESIGN AND ANALYSIS

To facilitate the implementation of elections in Indonesia, it is necessary to carry out blockchain-based evoting design, the design consists of the issuance of permanent voter lists and the selection and tabulation process.

Issuance of Permanent Voters List

The process of determining the voter list is still done by verifying population data based on KTP (National ID Card) so that only citizens who meet the requirements can become voters in the election. The conditions that must be fulfilled contained in article 1 paragraph 34 are voters who are Indonesian citizens aged 17 years or over, are married, or have been married. Here are voter registration schemes in blockchain-based e-voting schemes:

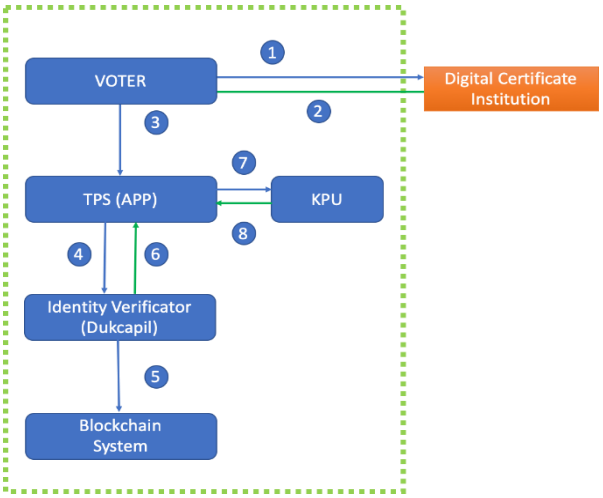

Figure 1 Registration for voting process

The voter registration process is carried out with the following 8 stages:

1. Voters submit a request for a key partner of Digital Certificate Institution by attaching a National ID Card (NIC).
2. Digital Certificate Institution checks identity, whether the NIC is connected to a particular key pair, if it already has a key pair, the system will provide notification (with 2FA) for revocation or keep using the same key and if it will not degenerate 2 key pairs given to voters (identity key pair and vote key pair).
3. Voters enters the TPS application using the given key pair, the public key1 (Vote ID) will be submitted to the entire system and the private key is attached to the voters.
4. The application will ask the voter to upload photos and identity cards. Along with the public key (Vote ID), TPS (APP) will send the information to the ID verificator to verify that the voter has fulfilled the requirements of 17 years old, is married, or has ever married.
5. The ID verifier will verify the voter has fulfilled the legal requirements and the public key (Vote ID) used is unique. If the conditions are met, the ID verifier will register the public key (Vote ID) into the blockchain system.
6. ID verificator gives access to the public key (Vote ID) of the voter to be able to access certain ballots by giving a certificate of approval.
7. APP will send an approval certificate from ID verificator and blinded token to KPU, KPU will sign the blinded token and send it back to APP. The APP then sends an unblinded token signed with the Vote key to request the ballot.
8. KPU approves that vote keys can access certain ballots.
9. The APP can request to make certain ballots to vote.

The next process is the voting process that will be carried out using the following mechanism (Figure 2):

1. Voters login in the application by having two key pairs of Digital Certificate Institution.
2. The application verify the identity of the ID Verificator and KPU that voters are entitled to vote.
3. Voters make an election by signing a ballot with a private key from the Vote key to the Blockchain Ballot Box anonymously and confidentially.
4. The system calculate the ballot based on the tokens received during the election and participants can check whether the votes given are entered into the system.

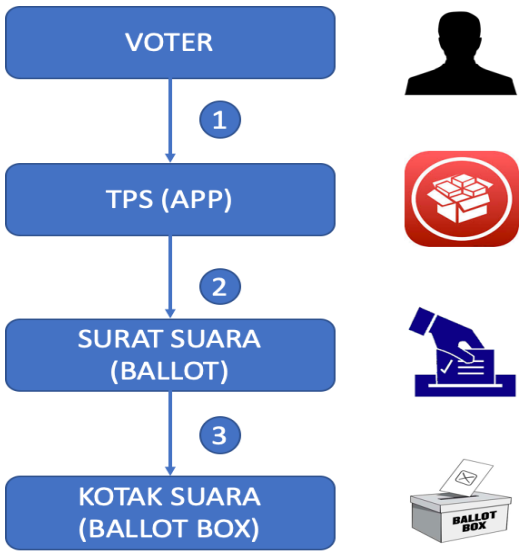

Figure 2 Blockchain Votin

The advantages of e-voting design with blockchain are as follows:

1. Voter can make a selection directly anywhere.
2. Voter's identities are anonymous and confidential.
3. Voters can verify that their ballot has entered.
4. The sound system is distributed so the system has good backups.

CONCLUSION

The conclusions of this paper are as follows:

1. The principles of elections in Indonesia can be fulfilled by the blockchain system.
2. Blockchain makes it easy to conduct elections based on the internet

ACKNOWLEDGMENTS

The authors acknowledge the financial support from National Cyber and Crypto Agency

REFERENCES

[1] Republic of Indonesia.2011. Undang-Undang No 15 Tahun 2011. Sekretariat Negara, Jakarta
[2] Republic of Indonesia.1945. Undang-Undang Dasar Tahun 1945. MPR, Jakarta
[3] Republic of Indonesia.2008. Undang-Undang No 10 tahun 2008. Sekretariat Negara, Jakarta
[4] Nakamoto, Satoshi.2008. Bitcoin: A Peer-to Peer Electronic Cash System**. www.**Bitcoin.org
[5] Ankaa Wijaya, Dimaz.2017. Blockchain Dari Bitcoin untuk Dunia. Jasakom. Jakarta
[6] Laurence, Tiana.2017. 2009. Blockchain For Dummies. John Wiley & Sons, New Jersey.
[7] Ernest, Adam Kaleb.2014. The Key To Unlocking The Black Box: Why The World Needs A Transparent Voting DAC.Follow My Vote.