IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 12, December 2021

DOI: 10.17148/IARJSET.2021.81253

E-VOTING USING BLOCKCHAIN TECHNOLOGY

Abhishek Nikat[1], Abhishek Kadam[2]

Dr D Y Patil School Of Engineering Academy, Ambi.

Abstract: Blockchain technology could be implemented not only in digital currency, but also in other fields. One such implementationis in democratic life, namely voting. This research focuses on designing a blockchain-based electronic voting system for medium to large-scale usage that complies with law, specifically voting principles in Indonesia. In this research, we proposed the following: a ballot design as block transaction employing UUID version 4, a modified block structure using SHA3-256 hash algorithm, and a votingprotocol. The minimum length of a ballot is 43 bytes (excluding ECDSA signature) if one character is used as candidate's identifier and timestamp is stored as integer. We built a simulation program using Pythonbased Django web framework to cast 2000 votes andmine them into blocks. Tampered transactions in each block could be detected and restored by synchronizing data with another node. We also evaluated the proposed system. By using this system, voters can exercise voting principles in Indonesia: direct, public, free, confidential, honest, and fair.

IndexTerms: Blockchain, voting, design, simulation, Python

I. INTRODUCTION

Information and communication technology is advancing rapidly. The performance and efficiency of Central Processing Unit(CPU) as the heart of a computer have continued to improve in the last few decades. Moore's Law, based on Gordon Moore's observation in 1965 and later adjustment in 1975, stated that the size of transistors was shrinking so fast that every two years, twiceas many could fit onto a single computer chip.

This advancement has revolutionized many aspects in our social life and government. One such case that is going to be discussed in this study is voting. Democratic countries, such as the Republic of Indonesia, guarantee the rights of their citizens toparticipate in decisionmaking, for example, to choose leaders by the mean of voting. By definition, voting (to vote) is "a formal indication of a choice between two or more candidates or courses of action, expressed typically through a ballot or a show of handsor by voice". In Indonesia, this right is listed on the state's constitution, namely Undang-undang Dasar Negara Republic Indonesia1945 (UUD NRI 1945) article 28J paragraph 3: "everyone has the right to freedom of association, assembly, and issuing opinions".Nowadays, voting process may be done electronically. Several electronic voting systems had been developed such asVOTAN (Votes Analyzer) for conducting electronic elections through the Internet securely. It is ideal for small communities such as organizations, universities and ——chambers.

It uses a centralized database, just like many other similar systems. Centralized systems have common weaknesses. The dataare stored centrally, so they have central point of failure, which can be exploited by computer crackers. Those systems are usuallyhandled by single organization, so the data can be manipulated secretly by those who have administrative access to the database .

The recent development of blockchain technology can solve this problem. The first work on cryptographically secured chainof blocks was published in 1991 in order to implement a system where documents' timestamps could not be modified. In 2008, Satoshi Nakamoto, whose identity is still unknown, wrote about a "purely peer-to-peer version of electronic cash" known as Bitcoin . Since then, blockchain made its public debut. Over time, people started to realize that blockchain could be usedbeyond cryptocurrency and they started to explore how blockchain could enhance many existing systems, including in voting process. This study focuses on the design of several important components of the blockchain-based electronic voting system, anddiscusses the implementation of the proposed system for secure electronic voting to guarantee the rights of people, especially Indonesian citizens. The proposed system must follow the rules and principles recognized by the state.

II. REQUIRED MATERIAL AND METHODOLOGY

1. ELECTRONIC VOTING AND ELECTION LAW

Electronic voting refers to voting process that utilizes electronic devices and other modern technologies to cast and count the votes. Electronic voting can be held via internet, which the voters submit their votes to the voting organizer, from any location [9]. Organizers must employ any means necessary to ensure authentication and authorization for every cast ballot. Specifically in Indonesia, Law (Undang-undang) number 7-year 2017 states in Article 2 that general election must comply with the following principles:

1) Direct: Each voter must cast his/her vote directly and not represented by other person or party.
2) Public: Every eligible member of society may participate in the voting, to cast his/her vote.
3) Free: A voter chooses candidate by his own will, not under threat or forced.
4) Confidential: Only the respective voter knows a voter's choice.
5) Honest: Every election and voting must comply with the regulation to guarantee the right of the voters, and that each vote cast has the same value.
6) Fair: All voters have equal right to vote, without any special privilege or discrimination. Those principles formally apply to national election (such as electing president or regional representatives), although there is no reason not to use it as basis for any other type of voting in a democratic country such as Republic of Indonesia.

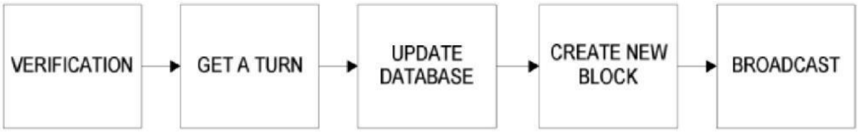


Fig.1(Flow Chart)

2. BLOCKCHAIN

Blockchain is a shared ledger of transactions. The transactions are ordered and grouped into blocks. Currently, the real-worldmodel is based on private databases that each organization maintains, whereas the distributed ledger can serve as a single source of truth for all member organizations that are using the blockchain. Blockchain is also a data structure, a linked list that uses hashpointers instead of normal pointers. Hash pointers are used to point to the previous block [10]. Bitcoin cryptocurrency with chainof blocks as its basis was proposed by [5]. Blockchain employs consensus algorithm to achieve decentralization of control. Consensus provides a way for all peers to agree and accept a single version of truth on the blockchain network. Bitcoin itself usesproof-of-work consensus to prove that enough computational resources have been spent before proposing a truth to be accepted by peers, therefore solving the double spending problem and Byzantine General's problem.

3. SECURE HASH ALGORITHM 3 (SHA-3)

SHA-3 is a latest member of secure hash algorithm standards. A cryptographic hash function is a one-way function that usesmathematical algorithm to map data of any size (message) to a fixed size bit string (hash). SHA-3 is meant to be an alternative toSHA-2, after successful attacks were proven on MD5 and SHA-1. SHA-3 uses Keccak algorithm. It is based on un-keyed permutations as opposed to other usual hash functions' constructions that used keyed permutations. A new approach called spongeand squeeze construction is used in Keccak, which is a random permutation model. The draft of SHA-3 (FIPS 202) was approved on 2015 by US National Institute of Standards and Technology [11]. SHA-3 is considered safe against quantum attack [12]. The performance is in par with SHA-2 [13]. The variant used in this study is SHA-3 with 256-bit of output (SHA3-256).

4. UNIVERSALLY UNIQUE IDENTIFIER (UUID) VERSION 4

A UUID is 128 bits value that is used to identify a piece of data or information in computer systems. Every UUID is unique.The uniqueness of each value is guaranteed when it is generated using standard methods, and it does not depend on the parties thatgenerate it. The protocol to generate UUID is specified in RFC 4122 [14]. UUID version 4 (UUID4) is generated randomly, not timebased or name-based like previous versions of UUID. Its probability of collision is so small that it can be safely ignored. It leaves 122 of its 128 bits available for random data. The probability to find a duplicate within 103 trillion UUID4s is one in a billion.

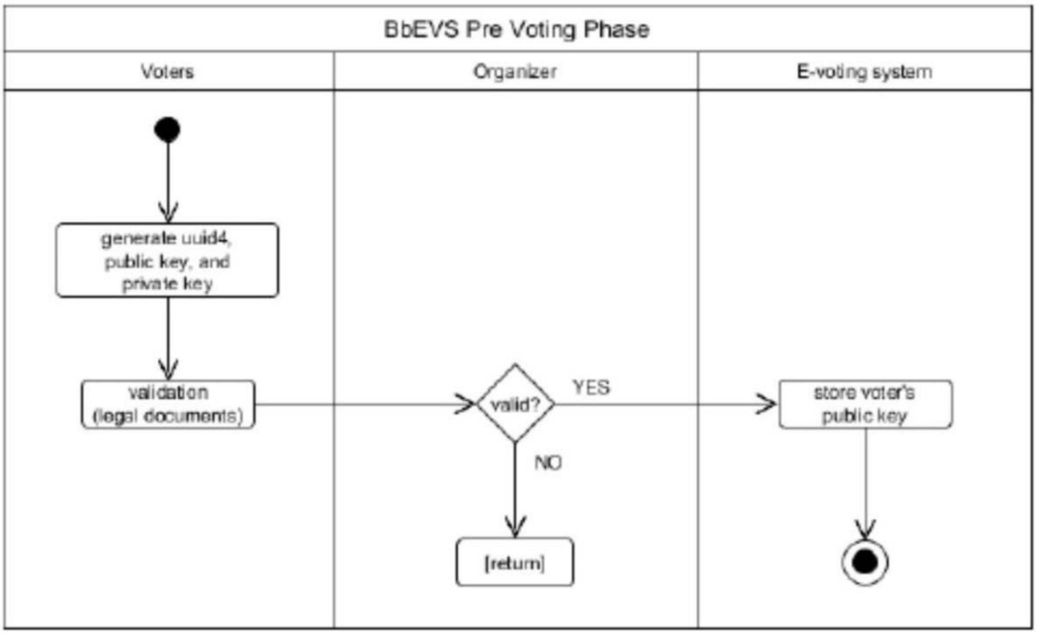


Fig. 2 Pre-voting Phase

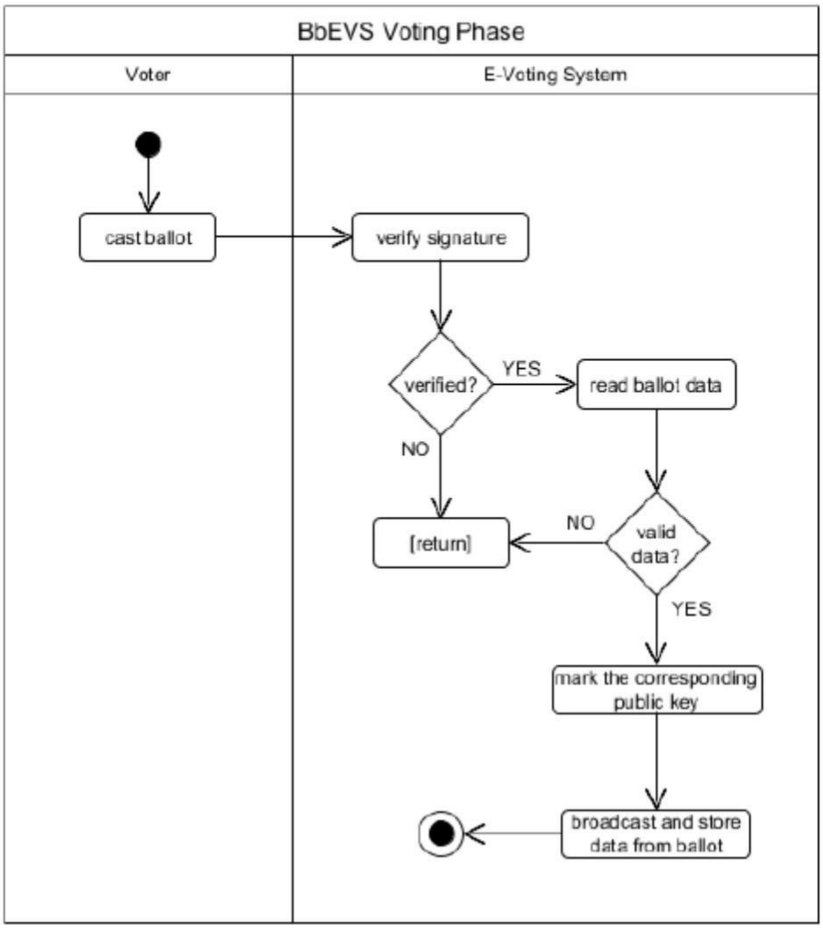


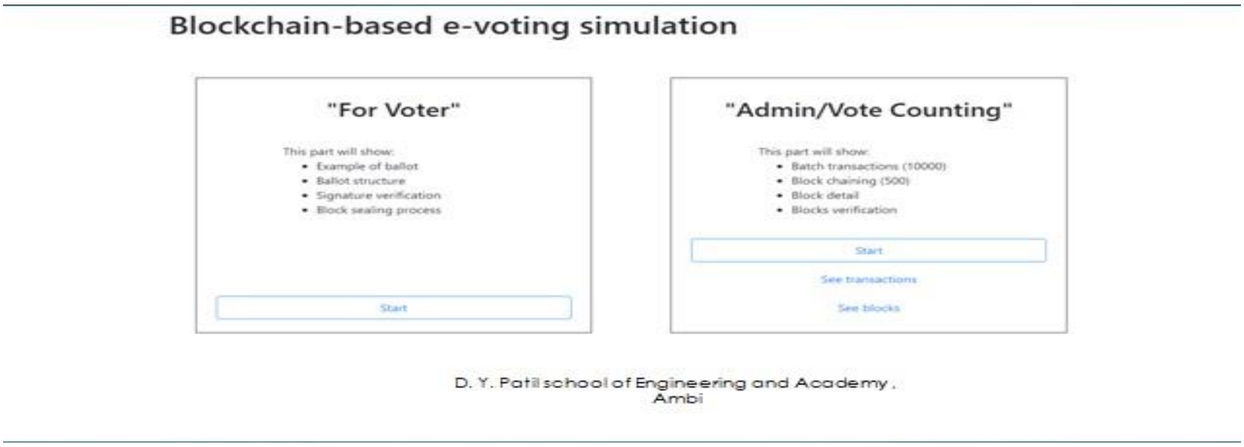
Fig. 3 Vote Casting Phase

DOI: 10.17148/IARJSET.2021.81253

Fig. shows the diagram of vote casting phase. In this phase, each voter casts his/her own ballot after signing it. Once accepted byserver, the ballot will be verified for authenticity and integrity before being relayed to all nodes. Data from a verified ballot are considered valid if the pseudonym is unique, candidate identifier is valid, and (optionally) the timestamp is considered reasonable.Now we discuss the recording and counting phase. Ideally, a block is created when certain numbers of transactions (ballots) havebeen relayed to all nodes, and then that block is broadcasted. Finally, the voting result can be counted. The counted votes Vcountedshould be less than or equal to the total votes cast, shown in (2).
Vcounted = Vtotal □Vunmarked (2)
The vote is 'unmarked' if the corresponding public key is never used for verification, or the data in the ballot are invalid. In the proposed system, the ballot has the following structure:
bv_id + bc_id + t,
where bv_id is the UUID as voter's ID (32 bytes), bc_id is the candidate ID (length may vary), and t as timestamp (can be either integer or float value). Timestamp value may be either the ballot creation time or the time the ballot is received by electronicvoting system. Thus, the minimum length of a ballot is 43 bytes. One or more fields may be added or modified depending on voting requirements. The following is an example of valid ballot:
ae19033a1d9a4f6cbaed53c6d2de1f730011540300734.584385.
As comparison, the size of a Bitcoin transaction is approximately 267 bytes. The structure of the block used in this study doesnot contain block version and difficulty target.

III. SIMULATION OF SYSTEM(RESULTS OF SYSTEM)

In this simulation, transactions are broadcasted to two nodes. One of the nodes acts as an always-honest node so all blocks and transactions can be compared later. The number of transactions, transactions per block, and puzzle difficulty can be adjusted to compensate the performance of the computer that runs the simulation.
The simulation comprises two sections:



Blockchain-based e-voting simulation

"For Voter"

This part will show:
- Example of ballot
- Ballot structure
- Signature verification
- Block sealing process

"Admin/Vote Counting"

This part will show:
- Batch transactions (10000)
- Block chaining (500)
- Block detail
- Blocks verification

D. Y. Patil school of Engineering and Academy ,
Ambi

Fig. 4 FrontPage of Simulation Program

1) "For Voter": This section shows the example of ballot and demonstrates signature verification and mining processes.
2) "Admin/Vote Counting": This section demonstrates the batch generation of transactions, sealing (mining) process, detail of each block, verification, and data synchronization process.
Some tests must be run to ensure the proposed system meets the following requirements. First, each user can examine their cast ballots after voting is over. Second, users can examine the detail of each block (hashes, nonce, number of transactions it contains, total number of blocks, etc.). Third, in case a node gets corrupted, it must be able to sync with majority of nodes aka "theagreed truth". A reasonably great number of dummy, valid ballots must be generated to run this test, i.e., 10,000. In our study, theyare generated programmatically. The built-in user interface, i.e., web UI, is used to confirm the result.

The simulation was run and benchmarked on the computer with the following specifications:
- CPU: 4 Cores, up to 3.6 GHz,
- RAM: 8 (2x4) GB, 1,600 MHz,
- Hard drive: 466 GB capacity, Read 74.45 MB/s, Write 64.18 MB/s,
- Operating system: Windows 8.1 Pro, 64-bit.

DOI: 10.17148/IARJSET.2021.81253

KEY ADVANTAGES OPPOSED TO EVM AND PAPER BALLOTS

Having the simplest voting process and best accessibility. The voter can determine the vote at anywhere and anytime with only a few clicks (Elections Canada Online | A Comparative Assessment of Electronic Voting, 2018). Moreover, apart from disability,people who are out of the area, impatient, and others so-called absentee will be turn out to determine their vote.

Embrace affordability. No paper and EVM require which highly increase the cost-effective (Elections Canada Online | A Comparative Assessment of Electronic Voting, 2018).

With I-voting, the voter has been fully guided by the system UI to prevent human error (i.e. incorrect choice, invalid vote). In paper ballots, the voter would be committing mistakes when marking or the issued ballot paper was invalid. Moreover, while use EVM,the voter may press the wrong button.

Encourage youth generations to cast vote (comfortable with technology).

KEY DISADVANTAGES

- It may good for just as an online voting system but not for the “national.” There is no flawless security while using the Internet, compare to the other types of the voting system, it has the greatest and fatal security vulnerabilities.
- For a national election, once there is something so-called defects or bugs happen, even it is a minor issue, that can highly discouragevoters to "believe" the system.

According to the foregoing facts and researches, even though I-voting system has overcome limitations of the other types of the voting system but security represent another story. Security represents the most significant challenge for the I-voting system, and there is research or implementation by some of the countries about the “architecture” that could possible to lower the problems but turned out the unideal solution, that is one the reasons that blockchain technology began followed by the public. In this case, Blockchainrepresents the technology that most suitable to fulfill both "transparency" and “security,” thus, the idea behind the proposed system.

IV. REFERENCES

[1] J. L. Hennessy and D. A. Patterson, Computer Architecture: A Quantitative Approach, Burlington: Morgan Kaufmann, 2017.

[2] S. Valsamidis, S. Kontogiannis, T. Theodosiou and I. Petasakis, "A Web e-voting system with a data analysis component," Journalof Systems and Information Technology, vol. 20, no. 1, pp. 33-53, 2018.

[3] The Economist, "The great chain of being sure about things," 31 October 2015. [Online]. Available:https://www.economist.com/briefing/2015 /10/31/the-great-chain-of-being-sure-about-things. [Accessed 8 October 2018].

[4] A. Narayanan, J. Bonneau, E. Felten, A. Miller and S. Goldfeder, Bitcoin and Cryptocurrency Technologies: A ComprehensiveIntroduction, Princeton: Princeton University Press, 2016.

[5] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[6] R. Hanifatunnisa, "Design and Implementation of Blockchain Based EVoting Recording System," Master’s Program Thesis, InstitutTeknologi Bandung, Bandung, 2017.

[7] Y. Liu and Q. Wang, "An e-voting protocol based on blockchain," IACR Cryptol. ePrint Arch., vol. 1043, p. 2017, 2017.

[8] J. Hsiao, R. Tso, C. Chen and M. Wu, "Decentralized E-Voting Systems Based on the Blockchain Technology," in Advances in Computer Science and Ubiquitous Computing, Singapore, Springer, 2017, pp. 305- 309.

[9] D. Zissis and D. Lekkas, "Securing e-Government and e-Voting with an open cloud computing architecture," Government Information Quarterly, vol. 28, no. 2, pp. 239-251, 2011.

[10] I. Bashir, Mastering Blockchain, Birmingham: Packt Publishing Ltd., 2017.

[11] NIST, "Announcing Approval of Federal Information Processing Standard (FIPS) 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, and Revision of the Applicability Clause of FIPS 180-4, Secure Hash Standard," 5 August 2015. [Online]. Available: https://www.gpo.gov/fdsys/pkg/FR-2015-08-05/pdf/2015- 19181.pdf. [Accessed 26 October 2018].

[12] M. Amy, O. Di Matteo, V. Gheorghiu, M. Mosca, A. Parent and J. Schanck, "Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3," in International Conference on Selected Areas in Cryptography, Cham, 2016.

[13] G. Bertoni, J. Daemen, M. Peeters, G. Assche and R. Keer, "Is SHA-3 slow?," 12 June 2017. [Online]. Available: https://keccak.team/2017/ is_sha3_slow.html. [Accessed 15 November 2018].

[14] P. Leach, M. Mealling and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace," Internet Engineering Task Force, July 2005. [Online]. Available: https://tools.ietf.org/html/rfc4122.html#section-4.1. [Accessed 15 November 2018].