Blockchain Based E-Voting Recording System Design

Rifa Hanifatunnisa (Author)
School of Electrical Engineering and Informatics
Bandung Institute of Technology
Bandung, West Java, Indonesia
rifahani@students.itb.ac.id

Budi Rahardjo
School of Electrical Engineering and Informatics
Bandung Institute of Technology
Bandung, West Java, Indonesia
rahard@gmail.com

Abstract — **Increasingly digital technology in the present helped many people lives. Unlike the electoral system, there are many conventional uses of paper in its implementation. The aspect of security and transparency is a threat from still widespread election with the conventional system (offline). General elections still use a centralized system, there is one organization that manages it. Some of the problems that can occur in traditional electoral systems is with an organization that has full control over the database and system, it is possible to tamper with the database of considerable opportunities.**

Blockchain technology is one of solutions, because it embraces a decentralized system and the entire database are owned by many users. Blockchain itself has been used in the Bitcoin system known as the decentralized Bank system. By adopting blockchain in the distribution of databases on e-voting systems can reduce one of the cheating sources of database manipulation. This research discusses the recording of voting result using blockchain algorithm from every place of election. Unlike Bitcoin with its Proof of Work, this thesis proposed a method based on a predetermined turn on the system for each node in the built of blockchain.

Keywords — e-voting; blockchain; database; security

I. INTRODUCTION

The use of technology has become commonplace at this point in helping to meet human needs. The increasing use of technology has brought new challenges in the process of democracy as most people today don't trust their governments, making elections very important in modern democracy [1]. Elections have a great power in determining the fate of a nation or an organization.

Simple purpose of the election is the channeling of popular sovereignty as a representative democracy. Every voter who likes to come to polling stations and shows voter cards to the committee and election supervisors to indicate whether the choice is valid or not, after the disaster as a legitimate option then the committee provides a vote for the choice of botanical sound votes made by voting in the choice of letter sound, then fold the ballot and put it in the ballot box.

The vote count in conventional elections can take 3 to 7 working days depending on the speed of sending the sound to a higher level [2]. At each stage of the vote count that is in the total series of votes or not. The most frequent problem in elections is the issue of data manipulation, security, and transparency.

With the development of technology, the use of technology in overcoming the problems that occur becomes important, as well as the intricacies of the collection process [3]. Security is always the biggest concern for an e-voting system. There should be no e-voting system to secure data and should be able to withstand potential attacks.

Blockchain technology is one solution that can be used to reduce the problems that occur in voting. Blockchain has been used in Bitcoin transaction database systems [4]. Blockchain is distributed, unchangeable and transparent ledger who can't deny the truth [5]. Consists of several blocks that are linked to each other and in sequence. The block is related because from the previous hash used in the next block making process, the attempt to change the information will be more difficult as it has to change the next blocks [6]. The database was made public, acquired by many users. The circumstances of cheating, the database owned by users who do the cheating will be different from the database owned by other users. Then the existing database on the user is not valid.

In the Bitcoin system, a mining process is required. In this research, a method that use turn rules for each node in blockchain creation, with the assured importance of each node joining the blockchain. This research is on the recording of the results of e-voting conducted after the election process is completed. The data corresponding to the results on each node distributed under the blockchain permission protocol.

978-1-5386-3546-9/17/$31.00 ©2017 IEEE

II. RELATED WORK

A. Blockchain and Its Use

Blockchain is a distributed database that stores data records that continue to grow, controlled by multiple entities. Blockchain (distributed ledger) is a trustworthy service system to a group of nodes or non-trusting parties, generally blockchain acts as a reliable and reliable third party to keep things together, mediate exchanges, and provide secure computing machines [7]. There are several types of Blockchain [7] ie.

1. *Permissionless Blockchain*, like Bitcoin or Ethereum, all can be a user or run a node, anyone can "write", and anyone can participate in a consensus in determining the state's validity.

2. *Permission Blockchain* inversely proportional to the previous type, operated by known entities such as consortium blockchains, where consortium members or stakeholders in a particular business context operate a Blockchain permission network. This Blockchain permission system has means to identify nodes that can control and update data together, and often has ways to control who can issue transactions.

3. *Private blockchain* is a special blockchain permitted by one entity, where there is only one domain trust.

The widely known Blockchain technology currently exists in the Bitcoin system which is the public ledger of all transactions. Bitcoin is a decentralized, peer-to-peer digital payments system based on the first public key cryptography proposed by Satoshi Nakamoto in 2008 [4]. Bitcoin uses a consensus protocol called PoW (Proof of Work) based on cryptocurrency to ensure only legitimate transactions are allowed within the system. Where each transaction is calculated its hash value and entered into a database called Blockchain as described in fig.1. To connect between one block with another block, the hash value of the previous block inserted into the next block then calculated its hash value. The hash value must meet certain requirements called difficulty in order to be considered a legitimate block. Searching for hash values that match those requirements is called Proof Of Work.

Bitcoin stores all transaction information in a database called blockchain in the internet network. Blockchain consists of several blocks associated with each other and in sequence as shown in fig.1 The blocks are related because the hash values of the previous block are used in the next block creation process. The effort to change the information will be more difficult because it must change the next blocks. The first block is called the genesis block.

In creating new blocks, miner required in the mining process using hash computing equipment. Miner compete against each other to create a new legitimate block in accordance with the specified difficulty. A new block is generally generated by a miner but there are times when more than one new block is generated by multiple miners that both meet the criteria even though the odds are small, making blockchain a fork. If this case occurs, then the voting process conducted by the miners.

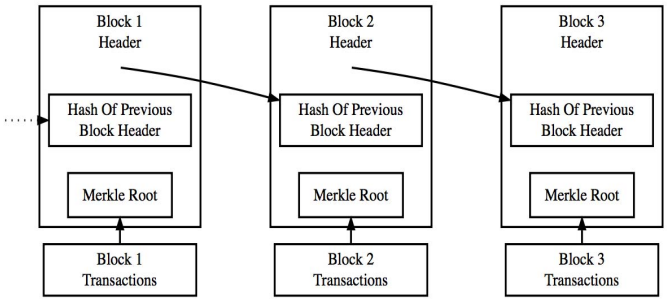

Figure 1. Blockchain Illustration

Source : www.blockchain.org

The voting process is done by way of the miner choosing one of several new blocks and then producing the discovery of a longer chain branch. Then the entire Bitcoin system uses the longest branch and deletes all other branches. Unused blocks are called block orphans and become invalid, also all transactions that have been recorded in the block orphan will be inserted into the new block. Blockchain comes with a variety of different types, but has several common elements :

• Blockchain is distributed digitally to a number of computers in almost real time.

• Blockchain is decentralized, the entire recording is available for all users and peer to peer network users. This eliminates the need for central authorities, such as banks, as well as trusted intermediaries.

• Blockchain uses many participants in the network to reach consensus.

Participants use their computers to authenticate and verify every new block. For example, to ensure that transactions not occur more than once, new blocks are only adopted by the network after the majority of its members agree that they are valid.

• Blockchain uses cryptography and digital signatures to prove identity.

Transactions can be traced back to the cryptographic identity, which is theoretically anonymous, but can be re-linked with real-life identity using reverse engineering techniques.

• Blockchain has a difficult (but possibly) mechanism for altering stored records.

Although all data can be read and new data can be written, previously existing data on blockcahin can't be changed theoretically unless the rules embedded in the protocol allow such changes by requiring more than 50 percent of the network to approve the change.

• A Blockchain is time-stamped.
Transactions in blockchain are timed, so they are useful for tracking and verifying information
• Blockchain is programmable.
Instructions embedded in blocks, such as "if" this "then" do that "else do this, allow transactions or other actions to be performed only if certain conditions are met, and may be accompanied by additional digital data.
Blockchain has several advantages, which makes it a powerful and secure alternative to distributed databases [8]:
• High Availability: Distributed completely to all nodes and stored in the database completely.
• Verifiability and Integrity: Each block is verified and added to the blockchain. Therefore, it will be difficult to change the data in it because all the blocks have to be changed value.
• Easy in determining a common starting point, where to store data - which is always added to the last block in the longest chain.
These advantages make the blockchain attractive for use in recording systems on e-voting.

B. Election and Blockchain Technology

E-voting currently widely used by some countries in the world, for example in Estonia. The country has been using the e-voting system since 2005 and in 2007 conducted online voting and was the first country in the world to conduct online voting [9]. Since then, a legally binding online voting system has been implemented in various other organizations and countries such as the Austrian Federation of Students, Switzerland, the Netherlands, Norway, and so on [10]. But it still has considerable security issues and the selection is often canceled [8]. Although getting a lot of attention, online voting system is still not widely done in various countries around the world. The traditional voting system has several problems encountered when managed by an organization that has full control over the system and database, therefore the organization can tamper with the database, and when the database changes the traces can be easily eliminated [11].
The solution is to make the database public, the database owned by many users, which is useful to compare if there are any discrepancies. The solution to the e-voting system is compatible with using blockchain technology. Blockchain technology allows in support of e-voting applications. Each voter's vote serves as a transaction that can be created into blockchain that can work to track voice counting. In this way, everyone can approve the final calculation because of the open blockchain audit trail, the vote count can be verified that no data is altered or deleted nor is there any unauthorized data entered in the blockchain.

III. DESIGN

This research proposed a database recording system on e-voting using blockchain technology. The blockchain technology used mostly works the same as the blockchain technology contained in the Bitcoin system and focuses on database recording. The nodes involved in Blockchain that have been used by Bitcoin are independently random and not counted [12]. However, in this e-voting system a blockchain permission is used, for nodes to be made the opposite of the Bitcoin system and the Node in question is a place of general election because the place of elections must be registered before the commencement of implementation, it must be clear the amount and the identity. This method aims to maintain data integrity, which is protected from manipulations that should not happen in the election process.

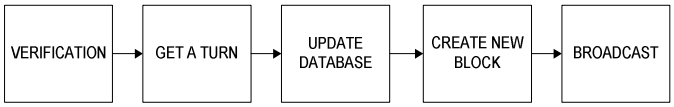

Figure 2. Flow Chart Design

This process begins when the voting process at each node has been completed. Before the election process begins, each node generates a private key and a public key. Public key of each node sent to all nodes listed in the election process, so each node has a public key list of all nodes. When the election occurs, each node gathers the election results from each voter. When the selection process is completed, the nodes will wait their turn to create the block. Upon arrival of the block on each node, then done verification to determine whether the block is valid.
Once valid, then the database added with the data in the block. After the database update, the node will check whether the node ID that was brought as a token is his or not. If the node gets a turn, it will create and submit a block that has been filled in digital signature to broadcast to all nodes by using turn rules in blockchain creation to avoid collision and ensure that all nodes into blockchain. The submitted block contains the id node, the next id node as used as the token, timestamp, voting result, hash of the previous node, and the digital signature of the node.

A. Verification and Update

The verification process starts from the acquisition of a block containing the voting result, the previous hash of the hash value originating from the previously valid block, and the digital signature. Then separated between electronic documents (result of voting and previous hash) and digital signature. The electronic document is calculated its hash value. As for the digital signature is done by decryption process using the public key of the node that makes the

electronic document. These two hash values are then compared, if the value is the same then the digital signature is valid and the process continues, but if the value is not equal it is considered invalid and the system will refuse the block to continue the process.

After the digital signature verified and proven to be valid, further verification of the previous hash begins with the capture of the voting result, and the previous hash contained in the most recent in database, and searched hash values with the SHA-256 algorithm. Then compare it with the previous hash carried by the block being done verification.

If the value is the same, then the hash value is valid and the whole block is verified as a valid block and sent by the node contained in the system, but if the value is not the same considered invalid and the system will reject the block. The verification process has proven to be valid, so the next process is update the database by adding the existing data on the block.

Refer to the Bitcoin system using the Blockchain system, the ECDSA (Elliptic Curve Digital Signature Algorithm) method is used in digital signature techniques, the small key size in this method can support the desired security. In other words, the key size of less than or more than 160 bits in the ECDSA algorithm is equivalent to security using RSA algorithm with a key of 1024 bits, the performance on the signature using any ECDSA algorithm component and its security level is always faster than the RSA algorithm [13]. The ECDSA (Elliptic Curve Digital Signature Algorithm) algorithm is the most widely used elliptic curve-based digital signature scheme [14]. The algorithm was proposed by Scott Vanstone in 1992 [15], which is the analog elliptic curve of the Digital Signature Algorithm (DSA). The main advantage of ECDSA is the same level of security as DSA but with a smaller key length, allowing for faster calculation. This algorithm is a development of generalized digital signature algorithm using ECC algorithm in digital signature generation process and its verification.

Breaking ECDSA is tantamount to solving the Elliptic Curve Discrete Logarithm Problem (ECDLP) problem. Means, if one manages to complete ECDLP, he will get Bitcoin access equivalent to 4.5 billion USD [16]. Selection of Kobiltz curves can have a real impact on ECDSA performance. The Kobiltz curve belongs to the NIST Digital Signature Standard [17] and also recommended for government since 2000 [18]. This indicates that the curve provides adequate security in the use of ECDSA.

B. Get A Turn

The voting time will begin and end simultaneously. When the voting time has been completed, each node will wait its turn to create a block. The system will always broadcast the database followed by the ID of a given node. The node ID serves as a token, if a node detects that the broadcast ID belongs to it, then it is the node's turn to create a new block. But to create a new block it is necessary to clarify that the sender of the block is a valid sender and part of the election, then the verification process is done.

If the verification was successful, then the node (the node that is in turn) starts creating a new block which will then be broadcast to all nodes in the system. In a condition where the node that gets the turn is problematic either down in the network or so the system will not stop. In each node it has its own counter time according to the length of time the block is added with the broadcast time then multiplied by the order of the nodes getting the turn. Node that get counter time = 0, then it can be interpreted that turn to make new block even though not get node ID as token because there is node or some number of previous node has trouble. After the destination node knows that its turn has arrived, it is verified to ensure that the previously received block is from the legitimate node in the system. Using get a turn method can minimize collisions that can occur in a data transmission network. This method can also facilitate the required audit process after the voting process takes place.

C. Create New Block and Broadcast

Nodes collect votes from each selector, then calculated and combined with the previous hash as an electronic document in the system. The electronic document is processed with a hash function to generate a message digest. It encrypts the hash value using the private key ECC. The proposed block refers to the research referred to [19] consisting of an id node, a timestamp, and three validation sections also in this study plus an id node of the node that earned a next turn.

The validation section consists of the results of the general election in the node, followed by the hash of the previous block in the database, lastly inserted with a digital signature which means the node uses the private key to encrypt the message digest of the block, which then broadcasts to the entire node. After the nodes that get the turn finished creating a new block, then the block is broadcast to all nodes. This process generates a new block performed by each node. The hash function is one of the cryptographic techniques in calculating the unique value that can be likened to the fingerprint of a data. Two different documents will have different hash values. A document of any length will produce a hash value of a certain length according to hash function algorithm used.

SHA-256 is a standard hash function by NIST in 2002 as a second-generation SHA and its description details can be

found in NIST standard documents [20]. SHA-256 will produce 256 bits output. The hash function used in the research is SHA-256, has been used by U.S. Government Applications and is strongly recommended to use because it has been set under the law, with its algorithm has been proven safe including used with cryptographic algorithms and other protocols that serve to secure documents containing information [21].

In terms of security can be searched for possible attacks that can be done on SHA-256. The possibility of brute force attack work is 2^L where L is the number of bits in Message Digest and Collision attack with possibly $2^L / 2$, in case of document signing even the attacker is difficult to make a fake digital signature even though the attacker makes it from the original document, the attacker must pair from Documents by working on each one for the complete document and the corrupted document to obtain the private key holder [21]. The possibility of a meet in the middle attack whose research has been done for the complexity of the time in one round is $2^{253.3}$ and requires $2^{10}.10$ words of memory then for now this hash method is still considered safe [22].

IV. Experiment Results

In this research simulation is done by using Python programming using PyCharms Community software. Tested using small number of nodes for implementation using visualization, and large scale without using visualization with reference the number of election places in Indonesia. Data storage designs of e-voting systems play a very important role in real-world implementation, because how to think of storing election data is key to protecting the privacy and integrity of the data.

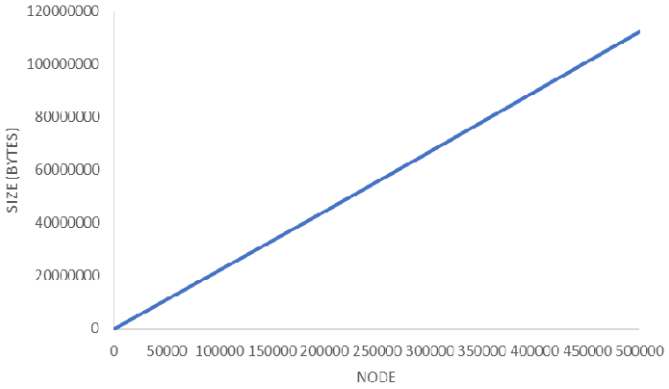

Figure 3. Possible Database Storage

In the functional testing of the proposed method, it is possible to implement this method for e-voting records system because the required storage is adequate for present-day computer capacity with the results shown in the graph of Fig.3.

Reliability testing is performed with the required capacity parameters on each number of nodes. With the number of nodes tested ranging from 1 to 500,000 many nodes assuming the number of nodes is the number of places of election then the resulting data as in fig.3. More number of nodes is directly proportional to the capacity required in the process of recording this e-voting. It is seen in fig.4 that more number of nodes needed, it takes longer time for this e-voting record system to work.

In the database stored data block of all nodes that each block contains the Node ID, Next ID Node, List of Votes, Previous Hash, Digital Signature, and timestamp. In this simulation, if the node is down on the network or any other disturbance that causes the node can't broadcast block and then the node is disabled and the system has succeeded in continuing the sequence to the next node because there is counter time for each node which when the time has expired counter, Then the node knows that its turn has arrived "My Turn = TRUE".

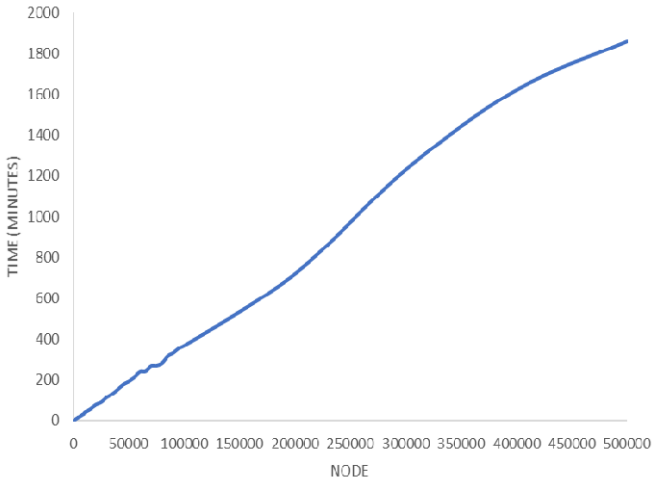

Figure 4. Time required in the number of different nodes

In the implementation, it can be done two things if it has finished recording all nodes for nodes that have not been defaced because of that disorder. First, the node that is experiencing the disturbance manually updating by simply pressing the Broadcast command because it is difficult to detect when the node is finished interrupt or the system can be repeated to do the recording and only detects nodes whose databases are still empty but in Blockchain done with the last Block parameter stored on System because it can't insert nodes in an existing blockchain. In verification, there are two variables that are used previous hash and digital signature checked.

V. Conclusion

This recording system occurs when the vote is over. Blockchain technology can be one solution to solve the problems that often occur in the electoral system. The use of hash values in recording the voting results of each polling

station linked to each other makes this recording system more secure and the use of digital signatures makes the system more reliable. The use of the sequence proposed in the blockchain creation process in this system considers that in an electoral system not required for mining as in the Bitcoin system because the voter data and numbers are clear and are not allowed to select more than once, the proposed sequence ensures that all nodes Which is legally connected and can avoid collision in transportation. Also make sure all nodes that have registered the results are included in the calculation process. In terms of cost can also be more efficient because it does not require equipment that is always remade in each election carried out.

Based on the design and the results of research conducted, it can be concluded that the system is successful functionality of recording the e-voting system based on Blockchain technology. The blockchain permission protocol used is a distributed record-keeping system operated by known entities, in other words having the means to identify nodes that can control and update data together in achieving the participants trust goals. The known entity in this system is any node that has been registered before the process runs, with the public key on each node owned by all the nodes in the system. Any data that is broadcast by the node that gets a turn is always verified and updated its data by the recipient. The verification system performed by all receiving nodes can identify if there are previous hashes and / or public keys that are not registered in the database. The counter-time system becomes a parameter when there are nodes that have interference functioning in accordance with the design. Nodes that experience interference can perform manual data or system broadcast can be repeated to update data when the process has reached the last turn node. Each previous hash that is used by the block in the system has proven the same as the hash value on the calculation results using the data in the previous block. Each hash value in the previous block has been included in the calculation of hash values by the block that gets a turn on the system, making anyone who wants to change the data in the database will have difficulty because if one data is changed it must make changes to data on other blocks.

In non-functional tested it was found that the system implemented with Python programming language able to handle the whole process of recording the e-voting system with the average time required for each node in creating block is 0.24 seconds and the average capacity required to store Data of 216.04 Bytes for each block.

References

[1] S. Shah, Q. Kanchwala, and H. Mi, “Block Chain Voting System,” 2016.

[2] Christian, “Desain Dan Implementasi Visual Cryptography Pada Sistem E-Voting Untuk Meningkatkan Anonymity,” Institut Teknologi Bandung, 2017.

[3] C. Dougherty, “[Vote Chain : Secure Democratic Voting],” 2016.

[4] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *Www.Bitcoin.Org*, p. 9, 2008.

[5] D. A. Wijaya, *Bitcoin Tingkat Lanjut*. 2016.

[6] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. J. Kishigami, “Blockchain contract: A complete consensus using blockchain,” *2015 IEEE 4th Glob. Conf. Consum. Electron. GCCE 2015*, pp. 577–578, 2016.

[7] C. Cachin and M. Vukolić, “Blockchain Consensus Protocols in the Wild,” 2017.

[8] C. Meter, “Design of Distributed Voting Systems,” no. September, 2017.

[9] A. Barnes, C. Brake, and T. Perry, “Digital Voting with the use of Blockchain Technology Team Plymouth Pioneers – Plymouth University,” 2016.

[10] T. Martens, “Verifiable Internet Voting in Estonia,” *October*, pp. 1–7, 2009.

[11] Follow My Vote, “Why Online Voting.” [Online]. Available: https://followmyvote.com/. [Accessed: 01-Jan-2017].

[12] L. J. Wu, K. Meng, S. Xu, S. Q. Li, M. Ding, and Y. F. Suo, “Democratic Centralism : a hybrid Blockchain architecture and its applications in Energy Internet,” pp. 176–181, 2017.

[13] Gemalto, “Benefits of Elliptic Curve Cryptography,” no. March, 2012.

[14] D. Hankerson, S. Vanstone, and A. J. Menezes, *Guide to elliptic curve cryptography*. 2004.

[15] A. G. Malvik and B. Witzoee, “Elliptic Curve Digital Signature Algorithm and its Applications in Bitcoin,” pp. 1–5, 2016.

[16] D. I. Wang, “Secure Implementation of ECDSA Signatures in Bitcoin,” 2014.

[17] E. Barker and Q. Dang, “Recommendation for Key Management – Part 3: Application-Specific Key Management Guidance,” *NIST Spec. Publ. 800-57*, pp. 1–142, 2007.

[18] F. P. NIST, “Digital Signature Standard (DSS),” vol. 1, 2000.

[19] K. A. M. F. M. Kirby, “Votebook : A proposal for a blockchain-based electronic voting system,” 2016.

[20] F. P. NIST, “FIPS 180-2 Secure Has Standard,” vol. 1, 2002.

[21] Saylor.org, “SHA,” pp. 1–10, 2010.

[22] Y. Sasaki, L. Wang, and K. Aoki, “Preimage Attacks on 41-Step SHA-256 and 46-Step SHA-512,” pp. 1–15, 2009.