Teknika 14 (01): 41 – 50

JURNAL TEKNIKA
ISSN: 0854-3143
e-ISSN: 2622-3481
Journal homepage: http://jurnal.polsri.ac.id/index.php/teknika
Journal Email: teknika@polsri.ac.id

KawalPilkada: A Conceptual Secure ElectronicVote System Based Blockchain Technology

Riko Herwanto*[1]Firmansyah YA[2]
[1,2]Institut Informatika dan Bisnis Darmajaya;
Jalan Z.A. Pagar Alam, No.93. Labuhan Ratu, Bandar Lampung
Lampung, Indonesia 35141
Telp : 0721-787214, Faks : 0721-700261
e-mail: ***[1]rikoherwanto@darmajaya.ac.id**, [2]firmansyahyunialfi@darmajaya.ac.id

Abstrak

Saat ini, pemilihan umum adalah salah satu cara terpenting untuk mempertahankan demokrasi. Berkat peluang yang dibawa oleh teknologi, kebutuhan untuk menciptakan pemilu dalam lingkungan fisik semakin berkurang setiap hari. Sebaliknya, kesulitan menciptakan pemilu dalam lingkungan elektronik menjadi semakin populer. Dengan kemunculan teknologi Blockchain, keamanan pemilu dalam lingkungan elektronik juga telah dipastikan dengan sangat baik. Sebaliknya, memindahkan sistem pemilu ke lingkungan elektronik akan menghilangkan biaya fisik, memastikan keamanan pemilu dalam rezim otoriter dengan menghilangkan otoritas pusat melalui blockchain, dan meningkatkan tingkat partisipasi dalam pemilu karena orang dapat memilih dari mana saja. dengan akses internet. Salah satu elemen terpenting dalam sistem pemilu berbasis blockchain adalah hubungan antara pemilih dan pemungutan suara, dengan kata lain, privasi pengguna. Pada artikel ini, kami mungkin ingin memperkenalkan ide tentang sistem pemungutan suara berbasis blockchain.

Kata kunci*—3-5 kata kunci, Algoritma A, algoritma B, kompleksitas*

Abstract

Today, elections are one of the foremost important means of sustaining democracies. thanks to the opportunities brought by technology, the need of creating the elections within the physical environment is decreasing every day. Instead, the difficulty of creating elections within the electronic environment is becoming more and more popular. With the emergence of Blockchain technology, the safety of the elections within the electronic environment has also been ensured to an excellent extent. On the opposite hand, moving the election system to the electronic environment will eliminate the physical costs, make sure the election security within the authoritarian regimes by eliminating the central authority through blockchain, and increase the participation rates within the elections because people can vote from anywhere with internet access. one of the foremost important elements within the blockchain-based electoral system is that the connection between the voter and therefore the vote, in other words, user privacy. during this article, we might wish to introduce an idea of blockchain- based voting systems.

Keywords— *blockchain, e-voting, electronic voting, internet voting.*

1. INTRODUCTION

General Election (ELECTION) which is free and periodically becomes a prerequisite for a democratic form of government, because Election as a way of exercising sovereignty the people that are administered directly, public, free, confidential, honest, and fair (LUBERJURDIL) within Negara Kesatuan Republik Indonesia (NKRI) for leading to state governance democratic supported Pancasila and therefore the Constitution 1945. The impact of Pilkada is what proportion it costs the state for its implementation administered ranging from voter data collection to recapitulation of the ultimate vote count. aside from that, there are obstacles in terms of voters double or voters who don't meet the wants but still allowed to vote [1], late distribution of ballots and there are damaged ballots causing a scarcity of ballots sometimes of day election [2]. A security box is additionally a drag due to that an unsealed box or damaged to result from a dispute between Candidate Pairs (PASLON) because it's suspected that there was the manipulation of ballots.

One way to beat the matter with conventional elections is by implementing the Electronic electoral system (E-Voting). Even so, the e-voting system still requires a security system strong because many digital systems security holes might be wont to break a system. By using blockchain then every transaction that happens are going to be encrypted using Secure Hash Algorithm 256 (SHA-256) and by continued to make sort of a chain or block then send it everywhere the network connected there to by peer - to - peer so that all can validate the transaction and not required by the server single to store the info [3].

2. METHODOLOGY

This research is development research to implement blockchain in an e-vote system. In conducting the research, several stages will be carried out, namely literature study, needs analysis, structural design, and communication in a licensed blockchain organization, designing smart contracts, designing user nodes.

2.1. TRADITIONAL VOTING

Voting is electing someone or something among many other options. within the political area, people use voting in many aspects of their life, from choosing the mayor to picking the top of the state. In conventional physical voting, ballot place and time are defined prior and other people got to go that exact place thereon exact day to form their preference. Voting is sometimes administered by marking a checkbox on paper, impressing a seal on their favorite candidate, or writing down a reputation on a paper. An election is that the name of voting that's administered to settle on a politician [4].

The electoral system has been changed in many aspects for a couple of hundred years. At the time there was no registry book for voters, people wont to swear an oath by keeping a hand on a sacred book that he has not voted before. albeit someone tried to cheat and vote for the second time, people around would recognize and stop him from voting again. That worked within the past when the population was sufficiently small that everybody knows one another. "In ancient Athens, votes were taken by issuing clay or metal tokens to every voter, and therefore the voter would vote by depositing the acceptable token within the appropriate box, or perhaps during a clay pot that served as a ballot box" [5]. In some systems, there was no secret voting. People were just saying their preference ahead of a jury and their vote was recorded with their names along.

Then paper ballot was invented within the time of the Roman Empire, 1500 years before the primary paper ballot was utilized in the USA. There was a significant problem with paper votes. it had been easy to place quite one paper into the box . to stop this problem, people were required to

offer their papers to officials to see possible multiple voted. At this stage, the official would unfold the papers and check if there's the other paper inside the folded paper. This application would damage voter confidentiality. At an equivalent time during checking, a politician would add a paper inside the voter's ballot. [5]

As the technology advanced, central authorities began to print formatted ballot papers that the candidates' names were on them. At the time of voting each voter was given one formatted paper and one envelope. They were required to stamp the seal on their candidate and put the ballot on the envelope. The envelope is glued and put into the box. Voter signs side of his name on the voter list that's printed before. To date, this is often the foremost widely used way of creating an election and completing democracy on physical means.

2.1.1. Problems with the conventional electoral system

Although a paper-based, the normal electoral system is employed widely among everywhere the planet, it's many problematical aspects and drawbacks. These are downsides of conventional voting systems;

2.1.1.1. Election security:

(1) ballots are often altered during transportation to a local board of election place, (2) ballots are often stolen during transportation, (3) people can vote with fake id within the name of real id owner, (4) results are often manipulated during transfer to computer, (5) getting to polling units in some terror zones.

2.1.1.2. Economic costs:

(1) there got to be many thousands of ballot boxes for every electoral zone, (2) got to be box officials for every unit to hold out electoral procedures during the election, (3) transportation of ballot boxes to electoral zones and back to the local board of election place, (4) there must be quite one staff for every unit, (5) counting on the dimensions of the population, possibly many voting papers and hundred thousand of stamps.

2.1.1.3. Low participation:

(1) People living underdeveloped areas cannot afford to succeed in the closest voting location, (2) disabled and elderly electorates might not be ready to reach the voting location by themselves, (3) people living in high tension or terror zones may abstain from getting to vote, (4) people on vacation may feel too lazy to travel their electoral zone, (5) people working in several locations than their registered address might not have opportunity to their electoral zones.

2.2. ELECTRONIC VOTING

The Internet was beginning to be swiftly using everywhere the planet since the 1990s. This wide selection of Internet users made people think that if elections could perform in an electronic environment. "Electronic voting is voting supported by electronic devices. The range of devices may include electronic registration of votes, electronic counting of votes, and lately, channels for remote voting, especially the web ." [6]

Internet would be used as a tool to form elections more gauze thus it might help pave the way for a far better democracy [7]. Electronic voting has many advantages over conventional voting which is administered within the physical setting. there's no need for physical ballot boxes and officials who spend all their day near them. Consequently, voters don't get to move to a selected place to vote. After the voting has been completed, counting and transferring results to the pc as happened in conventional systems doesn't take hours, instead, it takes only seconds to urge the results from the database. In some underdeveloped regions, people don't have enough medium of transport to ballot boxes therefore this obstacle cause low participation of voters. [8]. additionally, to those benefits, electronic voting is far cheaper than physical voting. The cost of many thousands of ballot boxes, officials, stamps, ballot papers, envelopes is eliminated through the electronic voting. However, there are many problems and concerns regarding the digitalization of democracy.

2.2.1. Problems with electronic voting

Electronic voting has been a most developed sort of conducting the elections and it brought many advantages in its wake like being economically advantageous, fast and being non-spatial. Nevertheless, it's some deficiencies or vulnerabilities like these;

2.2.1.1. Hacking Threat

One of the most important problems of electronic voting is that its hospitable vulnerabilities like hacking attempts. Unless an electronic system may be a hundred percent resistant to hacking it can cause indecisive or erroneous election results. Through hacking, many problems can occur with the system. A user of the system can vote multiple times or can access administrative functions and shut polling stations. The system could be designed with weak cryptography algorithms. System configuration is often accessed and modified thus a voting terminal thus the voting terminal is often ready to impersonate the other voting terminal. it might cause duplications on the systems because there'll be two identical terminals with different results and it'll be impossible to understand which one is genuine and which is that the fake. Another possible result of hacking is that the modification of ballot definitions. On the user side of the system, candidate definitions could also be edited or maybe replaced therefore one user's meaning for candidate A is going to be voting for candidate B. Another threat is modifying election results once they are collected on the central database. This could be done by altering ballot definitions thanks to poor cryptography used. apart from modifying the results, another threat with hacking is, matching voters with their votes. this might be a threat for voters in countries where democracy isn't strong enough. (Kohno, Stubblefield, Rubin, & Wallach, 2004).

2.2.1.2. Insider threats

Independently from the strong cryptography of the electronic electoral system, insider threats are serious risks as long as there's a central authority. The system will use the foremost advanced cryptography and has the simplest security measures for hacks and leaks but there's not much to try to to with insiders. Thus, being centralized is one of the most important handicaps of the electronic electoral system. Even in most democratic countries, central electoral officials can't be trusted because they could be bought either by candidates or foreign countries or they could be biased. Insiders also can collaborate with electronic electoral system developers and link voters with t heir votes which may be a serious threat to voters in less developed democracies.

2. BLOCKCHAIN VOTING

The term has emerged as blockchain gained popularity and thought to be utilized in other areas of life than economic usage. Blockchain voting solves the matter of who will count the votes and the way they're going to count thanks to its decentralized structure. within the blockchain electoral system, a central authority that counts the votes is eliminated, each vote cast by the users is automatically added to the general public ledger. Thus, everyone can observe the results live during the voting process. Before introducing the blockchain electoral system we'd like to understand what blockchain is and the way it works.

3.1. What's blockchain?

Blockchain may be a database that mixes asymmetric cryptography, peers to see networking where there's not any central authority managing the database. A Blockchain network may be a decentralized public ledger. the primary application which uses blockchain technology was first developed by an individual referred to as Satoshi Nakamoto. In his article written 2008, Satoshi says he proposed that system for electronic transactions without counting on trust [9]. When there's a transaction on the network, it's broadcasted to all or any other stations on the network. All the stations have a replica of the whole transaction history thus if one among the stations tries to cheat or hack the network it's seen by all the opposite stations and thus rejected. Blockchain is predicated on

cryptographic proof and probability rather than trust between stations on the network. ([10] that's the rationale it are often adapted and utilized in elections as a voting mechanism.

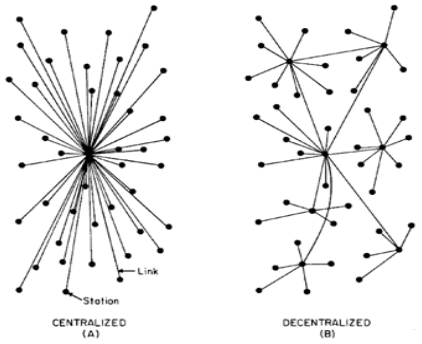

Figure 1: Centralized and Decentralized network.1

3.2.. Blockchain Transaction Structure

Blockchain consists of a sequence of digital signatures. Each user on the network adds the new information to the chain and transfers it to a subsequent user by digitally signing a hash of the previous transaction. Even when a little change occurs on a selected block, it changes its hash value thus it affects all the blocks coming after it. Unless all the blocks are verified and altered then specific block, that modification cannot inherit effect and ignore. This feature makes the chain unbreakable and irreversible. Once information is added into the chain, it stays there forever and it's impossible to switch it

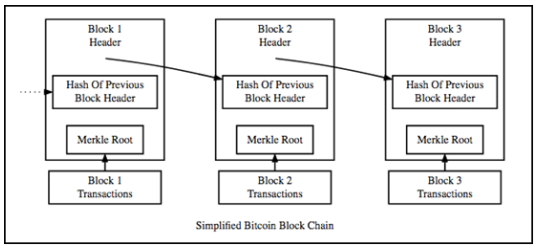

Figure 2: Blockchain transaction structure.2

Inside each block, there are mainly four different parts. one among them is that the hash of the previous block header which connects two consecutive blocks.

Other information is timestamp which shows the precise time when a block was created. Timestamp are often created with this easy piece of code timestamp = new Date().getTime();.

Another information in each block is that the hashes of every transaction. We first get hashes of two transactions separately then again get the hash of that hashes. In each block, there are hashed data blocks containing transaction information. These data blocks are like leaves of a tree, they merge and generate parent nodes, which nodes again merge and make higher-level nodes. This structure is named a Merkle tree [11].

The other a part of the block is named nonce which may be a 32-bit arbitrary random number. Users
of the blockchain network, which are called miners, brute force all possible nonce values to seek out a hash value that's smaller than the target hash. Whoever finds this value first, he solves the cryptographic puzzle and adds the subsequent block to the chain.

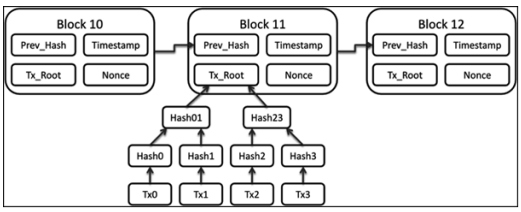

Figure 3: Information stored in each block.

3.3. The concept for blockchain voting

Proposed blockchain voting is that the system that's composed of the many stages and properties. At the primary stage of the system, all the users got to be authenticated to see they're eligible for the election. during this stage, election authorities, government, and voters work together. Election authorities get valid voter information from the govt then users apply to election authorities with their data to urge verified. This stage is before an election and doesn't get to get on the general public ledger. On the second phase verified users are with a right to vote, each user one right. From this stage on, all the transactions are carried on the blockchain.

Users cast their votes, votes are encrypted, then re-encrypted and shuffled through mix-net then written on the blockchain. At this stage vote and voter information is unlinked which ensures the anonymity for voters. there's also a feature of the system that every person can audit and prove his or her vote. it's accomplished through a QR code and a personal PIN. Because the voters are recorded on the blockchain, counting of votes is completed live.

3.3.1. Authentication of Voters

As blockchain eliminates the central authority which counts votes, there emerges a primary problem of who will validate who has the proper to vote. At this stage before voting, we'd like a central authority again to validate and provides permission to eligible voters. i will be able to call them the Central Authentication Committee from now on. This Central Authentication Committee will act as a trusted source to prove the identity of a voter. to make sure security at this stage, there has got to be quite one Authority to verify voter identity. The voter may send different parts of data of his or her identity to different Authorities to urge validated, or he or she may send all to Authorities to equivalent identity information. Such as, one authority can get user Social Security number info, others get a singular citizen identity number, others get registered address information. All the authorities confirm the identity of the voter and that they give the proper to vote.

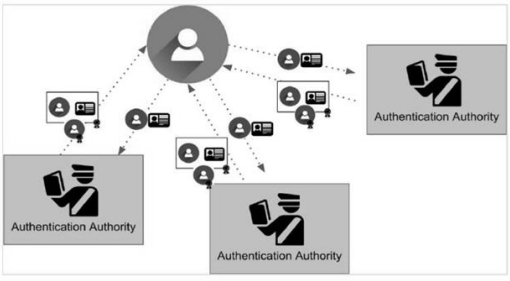

Figure 4: Voter sends Proof-Of-Identity to authenticators. Authenticators check the information and approve the voter and give permission to vote

3.3.2. Delivering the ballots

After the voter authentication, a part of the election is completed, election specific ballots are delivered to the verified voters. counting on the sort of election these ballots may include the list of local and country-wide candidates and election rules. Each ballot has the ballot ID produced from voter's information so that voters are often sure that the ballot is exclusive to himself only.

3.3.3. Encryption of Votes

Voter privacy is one of the foremost important terms when voting is conducted online. In collecting data online like for electronic votes we'd like to encrypt these data such as how that they've collected anonymously. Votes are privacy-sensitive data once they are matched with the voter. to beat this problem, vote information and voter information should be encrypted then they ought to be unlinked to make sure the anonymity of voters. The name of this approach generally is named anonymity- preserving data collection [13]. ElGamal encryption technique may be a triumphant method to unlink voters and therefore the vote information, in other words, it ensures to not know which vote is coming from which voter. That technique also should be combined with mixed networks to ensure the randomization and unlinking of votes from voters [14]. Mix network gets both and voter and vote information then shuffles the set of those two datasets.

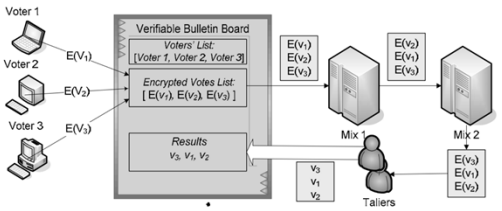

Figure 5: A typical re-encryption mix-net

Zero-Knowledge Proof (ZKP) method is another very useful method to make sure the anonymity of voters by unlinking from the vote. ZKP method was first introduced by MIT and therefore the University of Toronto professors Shafi Goldwasser,

Silvio Micali, and Charles Rackoff. within the ZKP method, the voter sends his or her vote without revealing anything aside from the vote information. This method does unlink by blocking eavesdroppers from discovering secret information which is voter personal information. Besides, it enforces hones behavior at an equivalent time maintaining privacy, therefore nobody can cheat within the election [15].

3.3.4. Auditing Votes

The audition of votes is one of the essential parts of the election. just in case of a situation where a voter must prove for whom he or she voted for, auditing becomes a neighborhood of the activity. allow us to assume that in an election there are two candidates respectively candidate A and candidate B. Assume that everybody has voted for candidate A and just one person voted for candidate B. At the top of the day, results are announced and that we see candidate A got all the votes and candidate B got zero votes. during this situation, it's obvious that there has been an error because candidate B had one vote. To prove this, one that voted for candidate B must be ready to show that his or her vote is cast for candidate B. within the system I propose, a QR code is and a PIN created after one person cast a vote. That QR code and PIN combination show his or her vote on the blockchain. just in case somebody else reads the QR code, there's a PIN that voters should save and keep private.

4. SOLUTION DESIGN

This chapter will discuss in detail the design of an online voting application that uses Blockchain technology.

4.1. E-voting flow

will explain the e-voting stream. Figure 6 illustrates the designed e-voting stream. The first thing it does is generate a public and private key pair. After that, the private key is partitioned and distributed to all stakeholders. This is done so that no one can do the decryption on their own. After that, we announce the public key that will be used for encryption during voting. When voting participants vote, homomorphic encryption is carried out using a pailier algorithm using the public key that has been generated earlier. After voting enters the Blockchain. The blockchain is divided into several regions. Blockchain is in charge of collecting votes from each region. After voting is complete, all Blockchain results are collected into one.

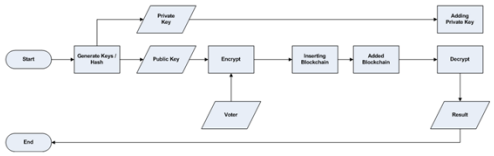

Figure 6. E-Voting Flow

The results from Blockchain cannot be replaced because they are still in ciphertext form. Results from the Blockchain can be combined or added because it uses partial homomorphic encryption using a pailier algorithm.

After all the results from the Blockchain are collected, a decryption is carried out to find out the voting results. Decryption is done by combining all private keys that have been distributed to stakeholders.

4.2 .. Blockchain architecture in E-voting

The e-voting architecture system designed consists of several blockchains. Each voter will be registered into one Blockchain. So voters will only be able to vote on the Blockchain where they are registered. This blockchain can be accessed via the internet so people don't have to go to a polling station to vote. To conduct voting voters only need to enter the private key given. This architectural system consists of three main parts, namely Blockchain, backend and frontend. The backend here acts as a bridge between the Blockchain and the frontend.

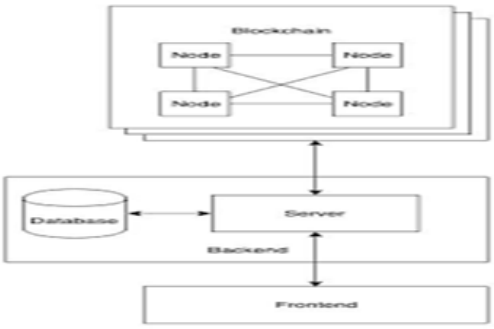

Figure 7. Blockchain E-Voting Architechture.

4.3. Designing the Organization

In a permitted blockchain, a channel consists of one or more peer organizations. Peer organizations can be likened to members or members who are licensed members of a blockchain network. Apart from peer organizations, there are also ordering organizations. Ordering organizations are organizations that provide services for collecting transactions and forming blocks. An overview of the shape of each organization can be seen in Figure 8 below:

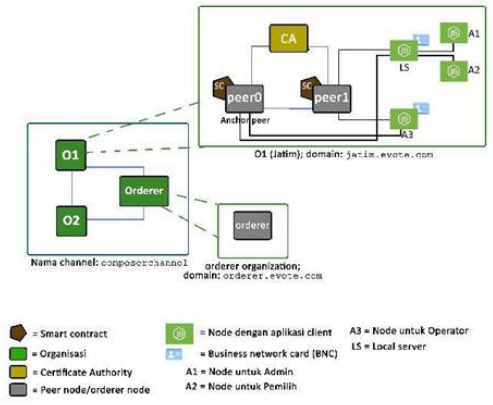

Figure 8. Organizational design in the scope of blockchain

From Figure 8 above, it can be seen how the relationship between peers, CAs, and orderers in organizations. In an orderer organization, there is an orderer node that will provide services for compiling transactions. To form an orderer node, a machine will be used which contains a container for the orderer image provided by Hyperledger Fabric. Likewise, to form a peer organization, a machine with several containers is needed that acts as a peer and a CA.

A smart contract consists of three parts, namely resource structure, access control, and transaction logic. A resource structure can be called a template for each object that is involved in the transaction. The structure of one of the required resources is for options. The structure consists of several fields such as id, selected candidate object, voter owner, and vote marker that has been used or not. Next, access control will control what activities can be performed by a voter on these options. The definition of voters' access control to their voting rights is that they must be able to read and update these votes. Meanwhile, transaction logic is a function that shows what a transaction will do. Transaction logic to use voting rights can be seen in the following pseudocode.

```
Procedure GunakanSuara begin
(NomorUrutKandidat = 1) Def
suaraReg <-
getAssetRegistry("Suara")
Def suara <- suaraReg.getFirst()
suara.kandidatDipilih <-
NomorUrutKandidat suara.pemilih <-
null
suara.sudahDigunakan <- true
suaraReg.update(suara)
end.
```

Furthermore, to access the permissioned blockchain, a node is required for users to submit transaction proposals. The types of nodes can be seen in Figure 1, namely LS and A3. LS is a local server that acts as a bridge between the permissioned blockchain and A1 or A2, because both nodes require an authentication process that occurs on the local server in order to be used.

4.3. Working of E-Vote Using Blockchain

- The first transaction added to the block will be a special transaction that represents the candidate [1].
- When this transaction is created it will include the candidate's name and will serve as the foundation block, with

every vote for that specific candidate placed on top of it. Unlike the other transactions, the foundation will not count as a vote, and it will only contain the name of the candidate.

- Our e-Voting system will allow a protest vote, where the voter may return a blank vote to demonstrate dissatisfaction with all candidates or a refusal of the current political system and/or election.
- Every time a person votes the transaction gets will be recorded and the blockchain will be updated.

To ensure that the system is secure, the block will contain the previous voter's information. If any of the blocks were compromised, then it would be easy to find out since all blocks are connected to each other [16-17].The blockchain is decentralized and cannot be corrupted, no single point of failure exists. The blockchain is where the actual voting takes place. The user's vote gets sent to one of the nodes on the system, and the node then adds the vote to the blockchain. The voting system will have a node in each district to ensure the system is decentralized

5. ADVANTAGES OF BLOCKCHAIN VOTING

As are often understood from the varied election systems above, the blockchain-based electoral system has some superiorities and advantages over traditional paper-based voting and centralized electronic voting. one of the benefits of the blockchain-based electoral system over traditional paper- based systems is its economic aspect. Compared to paper-based voting, it doesn't require physical ballots and ballot boxes which constitutes a substantial amount of paper, plastic, or other material wont to make boxes and countless envelopes. Besides, there got to be thousands of authorities, security guards, vehicles that are required during a paper-based system.

The blockchain electoral system eliminates most of those costs because each individual can cast their vote from their pc or smartphone without not getting to any specific election place. Possibly the most important and most epochal advantage of the blockchain-based electoral system is its decentralized nature. In other words, it doesn't require any local and central authority to control the election and count the results. during a centralized electoral system, both online and paper-based, all the info is collected by a central authority and counted by them, which makes the system susceptible to various sorts of attacks and makes it untrustworthy. On the contrary, during a blockchain-based electoral system, all the votes are recorded on a public ledger anonymously that can't be deleted or altered by anyone. At an equivalent time, it allows the counting of votes by life as they're life. Participation rates to the elections also can be increased with blockchain voting because people are going to be ready to cast their votes wherever they're and thus they do not feel the pressure in certain voting places. Also, disabled people or people on vacation don't need to go their registered place to cast their votes.

6. CONCLUSION

Elections are the foremost important tools to hold out democracies. With opportunities brought by the newest technology, the requisite of conducting elections within the physical environment is decreasing with day by day. rather than this, the difficulty of completing elections within the electronic environment is becoming more and more popular. With the emergence of Blockchain technology, the safety of the elections within the electronic environment has also been ensured considerably. Moving the election system to the electronic environment will eliminate the physical costs, make sure the election security within the authoritarian regimes by eliminating the central authority through blockchain, and increase the participation rates within the elections since people can vote from anywhere with internet access.

Having these innovative and epochal features, blockchain voting has considerable potential to affect and shape the concept of democracy or a minimum of the tools to hold out democracies.

REFERENCES

[1] Ramdhani, J. (2017). Bawaslu Temukan Pelanggaran Pemilih Gunakan Formulir C6 dan A5 Palsu. Disitas pada tanggal 29 Juni 2018. dari: https://news.detik.com/berita/d-3425720/bawaslu-emukanpelanggaran-pemilih-gunakanformulir-c6-dan-a5-palsu

[2] Andayani, D. (2018). KPU: 9 Daerah Lakukan Pemungutan Suara Ulang. Disitasi pada tanggal 29 Juni 2018. dari: https://m.detik.com/news/berita/40 8 8159/_kpu-9-daerah-lakukanpemungutan-suara-ulang.

[3] Schneier, Bruce. 1996. Applied Cryptography, Second Edition: Protocols, Algorithms, and

[4] Source Code . C. John Wiley & Sons, Inc.

[5] Murphy, P. J. (2001). Voting and elections. Capstone.

[6] Jones, D. W. (2007). Voting and elections. Computer, 16, 18.

[7] Kersting, N., & Baldersheim, H. (2004). Electronic Voting and Democracy. Palgrave Macmillan UK.

[8] Slaton, C. D. (1992). Televote : expanding citizen participation in the quantum age / Christa Daryl Slaton. New York: Praeger.

[9] Coleman, S., & Blumler, J. G. (2001, March). Realizing Democracy Online: A Civic Commons in Cyberspace. Citizens Online Research Publication No.2. Institute for Public Policy Research.

[10] Kohno, T., Stubblefield, A., Rubin, A. D., & Wallach, D. S. (2004). Analysis of an electronic voting system. IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004, 27-40.

[11] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf adresinden alındı

[12] Gandhi, S. A., Gawde, M. N., & Shahid, H. M. (2018). 'Blockchaining' Democracy. Asian Journal of Convergence in Technology, Volume 4, Issue 1, 1-2.

[13] Yang, Z., Zhong, S., & Wright, R. N. (2005). Anonymity-Preserving Data Collection. Proceddings of the 11th ACM SIGKDD International Conference on Knowledge Discovery and Data mining, (s. 1-10). Piscataw, NJ.

[13] Magkos, E., Kotzanikolau, P., & Douligeris, C. (2007). Towards secure online elections: Models, primitives and open issues. Electronic Government an International Journal 4(3), 249-268.

[14] Quisquarter, J. J., Louis, G., Annick, M., & Berson, T. (1990). How to Explain Zero-Knowledge Protocols to Your Children. Advances in Cryptology.

[15] Becker, M., Chandler, L., Hayes, P., Hedrick, W., Jensen, K., Kandikattu, S., . . . Zweben, N. (2018). Proof of Vote®: An end-to-end digital voting protocol using distributed ledger technology (blockchain). Cleveland, OH, USA: Votem Corp.

[16] Ahmed Ben Ayed(2017);A Conceptual Secure Blockchain –Based Electronic Voting System; International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, [10] Borglet, C, 2003,Finding Asscociation Rules with Apriori Algorithm,http://www.fuzzy.cs.uni agdeburgde/~borglet/apriori.pdf, diakses tgl 23 Februari 2007.