➔ ***Regular Research Paper – NS***

Future of Democracy: Blockchain Voting

A comparative analysis between conventional paper-based voting, electronic voting and blockchain voting

Varol Tepecik
Informatics Institute, Dept. of Management Information Systems, Gazi University, Ankara, Turkey
varol.tepecik@gazi.edu.tr

Abstract

Today, elections are one of the most important means of sustaining democracies. Due to the opportunities brought by technology, the necessity of making the elections in the physical environment is decreasing with each day. Instead, the issue of making elections in electronic environment is becoming more and more popular. With the emergence of Blockchain technology, the security of the elections in the electronic environment has also been ensured to a great extent. On the other hand, moving the election system to the electronic environment will eliminate the physical costs, ensure the election security in the authoritarian regimes by eliminating the central authority through blockchain, and increase the participation rates in the elections due to the fact that people can vote from any place with internet access. One of the most important elements in the block chain-based voting system is the connection between the voter and the vote, in other words the user privacy. Various cryptological methods are used to break the connection between the user and the vote which anonymizes the user completely. ElGamal cryptology, mix-nets and zero knowledge proof method are some of these. In this article, voting systems from the past to the present will be examined and as an alternative block chain-based voting system will be examined and a sample block chain-based voting system concept will be introduced.

Keywords: *blockchain, election, democracy, voting, cryptology*

1. INTRODUCTION

Since the emergence of democracy, people used a tool to carry out it. Elections are currently the best tools to carry out democracies. Rise of the Athenian democracy for example had been accomplished by the widespread use of elections (Katz, 1997). Throughout the history many forms of elections are used from vote by voice, by stone, by paper to electronic means. Today one of the most widespread type of voting is paper based voting. It has many strong and weak sides when security and economic aspects are considered. High costs to conduct election is one of the most important drawbacks of paper-based voting. Having a central authority that everyone has to trust can be regarded another weak side.

Electronic voting is a more recent and more developed term compared to paper-based voting. As the technology advanced, it made possible to conduct elections in electronic environment. This new concept has many advantages over paper-based voting system mainly it decreases economic costs considerably as all the transactions occur electronically and there is not needed for any physical setup. This new concept also has some drawbacks like the problem of trust. As long as the election is carried out by a central authority, the problem of trust continues. Problem of trust can arise from both the central authority and the external sources such as hackers.

Blockchain voting is a new term in political area but has a huge potential to shape our understanding of democracy. First of all, prior to blockchain voting all the voting systems are centralized whether they are applied online or paper based. One of the biggest advantages of blockchain voting is that it eliminates central authority namely board of election as every user of the system can hold an entire copy of the transactions. There are some electronic systems that use Tor infrastructure to conceal the identity of voters but this technique does not provide total anonymity or integrity. (Meter, Schneider, Hagemeister, & Mauve, 2017) With the help of various cryptology techniques such as ElGamal encryption, Mix Networks and Homomorphic encryption anonymity of voters is fully provided. Ensuring a total anonymity allows voters to vote freely and without feeling pressure which is not possible in paper-based voting systems. (Aitzhan & Svetinovic, 2018) The only centralized part of blockchain voting is user authentication. It has to be in order to decide who has right to vote and give permission to those legal voters. In order to verify legal users, systems need the voters' information such as citizenship id, address, social security number and so on. There might be used various verification methods like fingerprint scan, facial recognition or creating user with personal information which has to match with the info that government has.

2. TRADITIONAL VOTING

Voting is electing someone or something among many other options. In political area people use voting in many aspects of their life, from choosing mayor to choosing head of state. In conventional physical voting, ballot place and time are defined prior and people need to go that exact place on that exact day to make their preference. Voting sometimes carried out by marking a checkbox on paper, impressing a seal on their favorite candidate or writing down a name on a paper. Election is the name of voting that is carried out to choose a political leader (Murphy, 2001).

Voting system has been changed in many aspects for a few hundred years. At the time there was no registry book for voters, people used to swear an oath by keeping a hand on sacred book that

he has not voted before. Even if someone tried to cheat and vote for the second time, people around would recognize and prevent him voting again. That worked in the past when the population was small enough that everyone knows each other. "In ancient Athens, votes were taken by issuing clay or metal tokens to each voter, and the voter would vote by depositing the appropriate token in the appropriate ballot box, or perhaps in a clay pot that served as a ballot box" (Jones D. W., 2007). In some systems, there were no secret voting. People were just saying their preference in front of a jury and their vote was recorded with their names along.

Then paper ballot was invented in the time of Roman Empire, 1500 years before the first paper ballot used in the USA. There was serious problem with paper votes. It was easy to put more than one paper into the ballot box. To prevent this problem, people were required to give their papers to officials to check possible multiple voted. At this stage official would unfold the papers and check if there is any other paper inside the folded paper. This application would damage voter confidentiality. At the same time during checking, official would add a paper inside voter's ballot. (Jones D. W., 2007)

As the technology advanced, central authorities started 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. Envelope is glued and put into the ballot box. Voter signs side of his name on the voter list that is printed before. To date, this is the most widespread used way of making an election and carrying out the democracy on physical means.

2.1. Problems with conventional voting system

Although paper based, traditional voting system is used widely among all over the world, it has many problematical aspects and downsides. These are downsides of conventional voting systems;

2.1.1. Election security:

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

2.1.2. Economic costs:

(1) there needs to be hundreds of thousands of ballot boxes for each electoral zone, (2) there needs to be ballot box officials for each unit to carry out electoral procedures during the election, (3) transportation of ballot boxes to electoral zones and back to local board of election place, (4) there needs to be more than one security staff for each unit, (5) depending on the size of population, possibly millions of voting papers and hundred thousands of stamps.

2.1.3. Low participation:

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

3. ELECTRONIC VOTING

Internet was started to be swiftly using among all over the world since 1990s. This wide range of Internet use made people think that if elections could carry out in 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 Internet." (Kersting & Baldersheim, 2004)

Internet would be used as a tool to make elections more gauze thus it would help pave the way for a better democracy (Slaton, 1992). Electronic voting has many advantages over conventional voting which is carried out on physical setting. There is no need to physical ballot boxes and officials who spend all their day near them. Consequently, voters do not need to move to a specific place to vote. After the voting has been completed, counting and transferring results to computer as happened in conventional systems does not take hours, instead it takes only seconds to get the results from the database. In some underdeveloped regions, people do not have enough medium of transport to ballot boxes therefore this obstacle cause low participation of voters. (Coleman & Blumler, 2001). In addition to these benefits, electronic voting is much cheaper than physical voting. Cost of hundreds of thousands of ballot boxes, officials, stamps, ballot papers, envelopes are eliminated through the electronic voting. However, there are many problems and concerns regarding the digitalization of the democracy.

3.1. Problems with electronic voting

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

3.1.1. Hacking Threat

One of the biggest problems of electronic voting is that it is open to vulnerabilities like hacking attempts. Unless an electronic system is hundred percent immune to hacking it can lead to 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 close polling station. System might be designed with weak cryptography algorithms. System configuration can be accessed and modified thus a voting terminal thus the voting terminal can be able to impersonate any other voting terminal. It would cause duplications on the systems because there will be two identical terminals with different results and it will be impossible to

know which one is the genuine and which is the fake. Another possible result of hacking is modification of ballot definitions. On the user side of the system, candidate definitions may be edited or even replaced therefore one user intending to for candidate A will in fact be voting for candidate B. Another threat is modifying election results when they are collected on the central database. This might be done by altering ballot definitions due to poor cryptography used. Except from modifying the results, another threat with hacking is, matching voters with their votes. This could be a threat for voters in countries where democracy is not strong enough. (Kohno, Stubblefield, Rubin, & Wallach, 2004)

3.1.2. Insider threats

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

4. BLOCKCHAIN VOTING

The term has emerged as blockchain gained popularity and thought to be used in other areas of life than economic usage. In 1923, in the Central Committee of the Communist Party of the Soviet Union Joseph Stalin said “I consider it completely unimportant who in the party will vote, or how; but what is extraordinarily important is this — who will count the votes, and how.” (Bazhanov, 2002). Blockchain voting solves the problem of who will count the votes and how they will count due to its decentralized structure. In blockchain voting system a central authority which counts the votes is eliminated, each vote casted by the users is automatically added to the public ledger. Thus, everyone can observe the results live during the voting process. Before introducing blockchain voting system we need to know what blockchain is and how it works.

4.1. What is blockchain?

Blockchain is basically a database that combines asymmetric cryptography, peer to peer networking where there is not any central authority managing the database. Blockchain network is decentralized public ledger. The first application which uses blockchain technology was first developed by person known as Satoshi Nakamoto. In his article written 2008, Satoshi says he

proposed that system for electronic transactions without relying on trust (Nakamoto, 2008). When there is a transaction on the network, it is broadcasted to all other stations on the network. All the stations have a copy of the entire transaction history thus if one of the stations tries to cheat or hack the network it is seen by all the other stations and thus rejected. Blockchain is based on cryptographic proof and probability instead of trust between stations on the network. (Berg, 2017) That is the reason it can be adapted and used in elections as a voting mechanism.

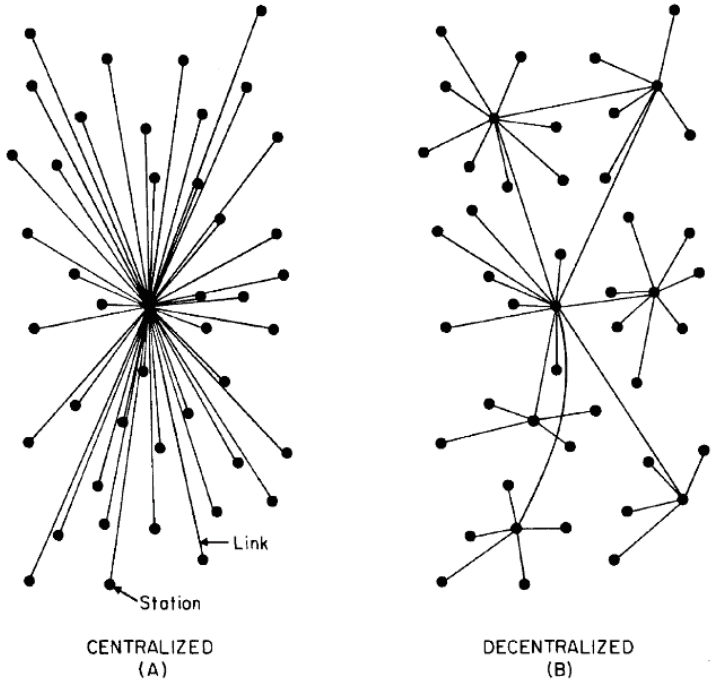

Figure 1: Ceantralised and Decentralized network.[1]

4.1.1. Blockchain Transaction Structure

Blockchain is composed of a chain of digital signatures. Each user on the network adds the new information to the chain and transfers it to the next user by digitally signing a hash of the previous transaction. Even when a small change occurs on a specific block, it changes its hash value thus it affects all the blocks coming after it. Unless all the blocks are verified and changed after that specific block, that modification cannot come into effect and ignored. This feature makes the chain unbreakable and irreversible. Once an information is added into the chain, it stays there forever and it is impossible to modify it.

1 https://cdn-images-1.medium.com/max/1600/1*QkoWWTUFpMdYJTmMAW4zIQ.png, 22.11.2018

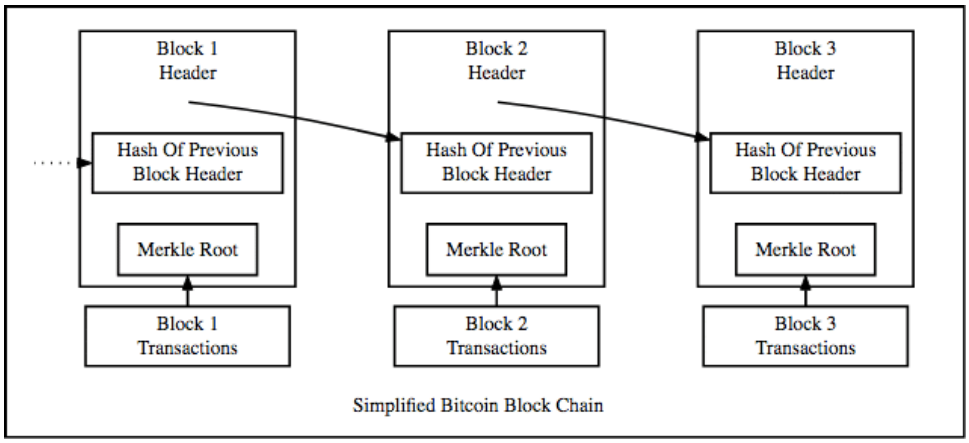

Figure 2: Blockchain transaction structure.[2]

Inside each block, there are mainly four different parts. One of them is the hash of previous block header which connect two consecutive blocks.

Other information is timestamp which shows the exact time when a block was created. Timestamp can be created with this simple piece of code timestamp = new Date().getTime();.

Another information in each block is the hashes of each transaction. We first get hashes of two transactions separately and then again get 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, and that nodes again merge and create higher level nodes. This structure is called merkle tree (Gandhi, Gawde, & Shahid, 2018).

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

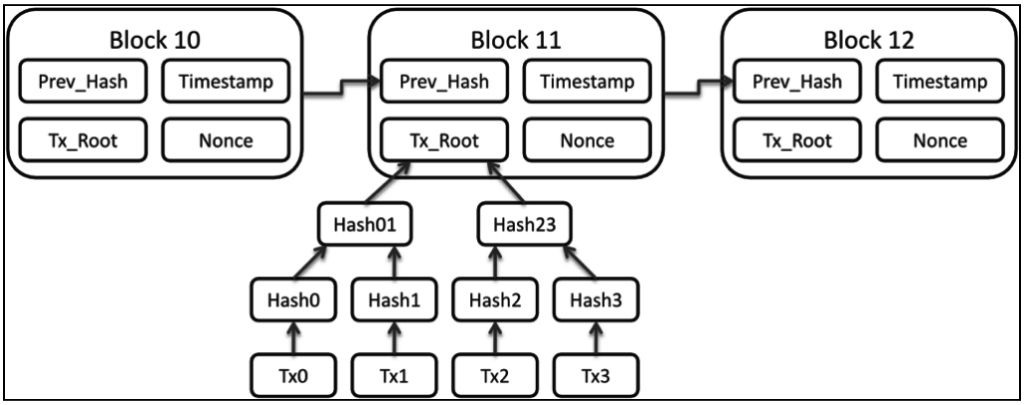

Figure 3: Information stored in each block.

[2] https://blockgeeks.com/wp-content/uploads/2017/08/image5.png, 22.11.2018

4.2. Concept for blockchain voting

Proposed blockchain voting is the system that is composed of many stages and properties. At the first stage of the system, all the users are need to be authenticated to check they are eligible for the election. In this stage, election authorities, government and voters work together. Election authorities get valid voter information from government and then users apply to election authorities with their personal data to get verified. This stage is prior to election and does not need to be on public ledger. On the second phase verified users are with a right to vote, each user one voting right. From this stage on, all the transactions are carried on the blockchain. Users cast their vote, votes are encrypted and then re-encrypted and shuffled through mix-net and then written on the blockchain. At this stage vote and voter information is unlinked which ensures the anonymity for voters. There is also a feature of the system that each person can audit and prove his or her vote. It is accomplished through a QR code and a private pin number. Because the voters are recorded on the blockchain, counting of votes is done live.

4.2.1. Authentication of Voters

As blockchain eliminates central authority which counts votes, there emerges a first problem of who will validate who has right to vote. At this stage prior to voting, we need a central authority again to validate and give permission to eligible voters. I will call them Central Authentication Committee from now on. This Central Authentication Committee will act as a trusted source to prove the identity of a voter. To ensure security at this stage, there has to be more than one Authority to confirm voter identity. Voter may send different parts of information of his or her identity to different Authorities to get validated, or he or she may send all to Authorities to same identity information. Such as, one authority can get user social security number info, other gets unique citizen identity number, other gets registered address information. All the authorities confirm the identity of the voter and they give right to vote.

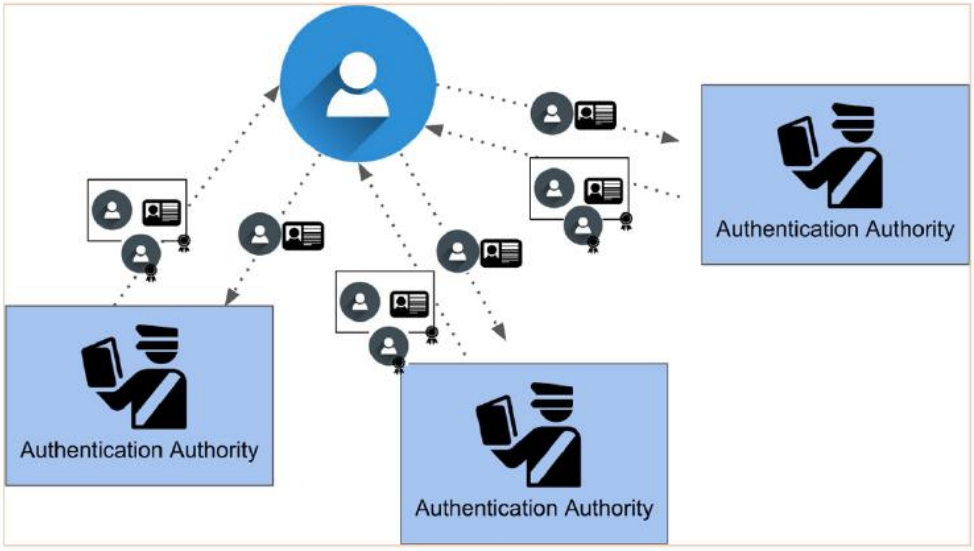

Figure 4: Voter sends Proof-Of-Identity to authenticators. Authenticators check the information and approve the voter and give permission to vote. *(Becker, ve diğerleri, 2018)*

4.2.2. Delivering the ballots

After voter authentication part of the election is completed, election specific ballots are delivered to the verified voters. Depending on the type of the 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 voter can be sure that ballot is unique to himself only.

4.2.3. Encryption of Votes

Voter privacy is one of the most important terms when the voting is conducted online. In collecting data online such as for electronic votes we need to encrypt these data such a way that they are collected anonymously. Votes are privacy sensitive data when they are matched with the voter. In order to overcome this problem, vote information and voter information should be encrypted and then they should be unlinked to ensure anonymity of voter. The name of this approach in general is called anonymity-preserving data collection (Yang, Zhong, & Wright, 2005). ElGamal encryption technique is a triumphant method to unlink voter and the vote information, in other words it ensures not to know which vote is coming from which voter. That technique also should be combined with mix networks in order to guarantee the randomization and unlinking of votes from voters (Magkos, Kotzanikolau, & Douligeris, 2007). Mix network basically gets both and voter and vote information and then shuffles the set of these two datasets.

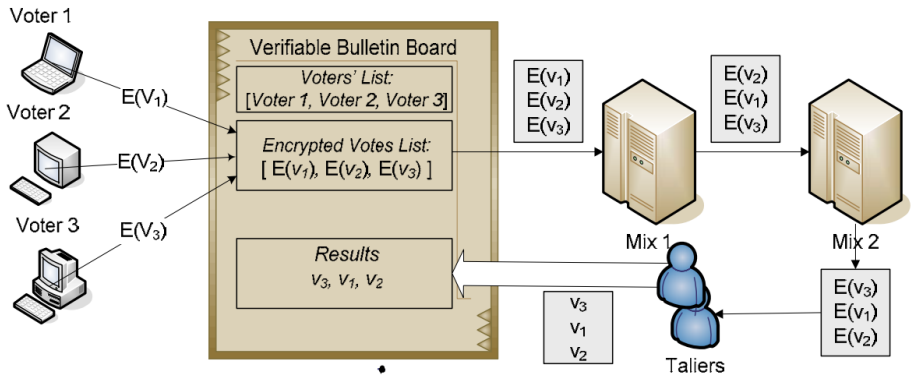

Figure 5: A typical re-encryption mix-net *(Magkos, Kotzanikolau, & Douligeris, 2007)*

Zero Knowledge Proof (ZKP) method is another very useful method to ensure the anonymity of voter by unlinking from the vote. ZKP method was first introduced by MIT and University of Toronto professors Shafi Goldwasser, Silvio Micali and Charles Rackoff. In ZKP method, voter sends his or her vote without revealing anything other than the vote information. This method does unlinking by blocking eavesdroppers from discovering secret information which is voter personal information. In addition, it enforces hones behavior at the same time maintaining privacy, therefore no one can cheat in the election (Quisquarter, Louis, Annick, & Berson, 1990).

4.2.4. Auditing Votes

Audition of votes is one of the essential parts of the election. In case of a situation where a voter needs to prove for whom he or she voted for, auditing becomes a part of the activity. Let us assume that in an election there are two candidates respectively candidate A and candidate B. Assume that everyone has voted for candidate A and only one person voted for candidate B. At the end of the day, results are announced and we see candidate A got all the votes and candidate B got zero vote. In this situation it is obvious that there has been a mistake because candidate B had one vote. To prove this, person who voted for candidate B needs to be able to show that his or her vote is casted for candidate B. In the system I propose, a QR code is and a pin number created after one person cast a vote. That QR code and pin number combination shows his or her vote on the blockchain. In case someone else reads the QR code, there is a pin number that voter should save and keep private.

5. ADVANTAGES OF BLOCKCHAIN VOTING

As can be understood from the various election systems above, blockchain based voting system has some superiorities and advantages over traditional paper based voting and centralized

electronic voting. Obviously, one of the advantages of blockchain based voting system over traditional paper-based systems is its economic aspect. Compared to paper-based voting, it does not require physical ballots and ballot boxes which constitutes a considerable amount of paper, plastic or other material used to make boxes and countless envelopes. In addition, there needs to be thousands of authorities, security guards, transportation vehicles are required in paper-based system.

Blockchain voting system eliminates almost all of these costs because each individual can cast their vote from their personal computer or smartphone without not going to any specific election place. Possibly the biggest and most epochal advantage of blockchain based voting system is its decentralized nature. In other words, it does not require any local and central authority to govern the election and count the results. In centralized voting system, both online and paper based, all the data is collected by a central authority and counted by them, which makes the system vulnerable to various kinds of attacks and makes it untrustworthy. On the contrary, in blockchain based voting system all the votes are recorded on a public ledger anonymously that cannot be deleted or altered by anyone. At the same time, it allows the counting of votes by live as they are live. Participation rates to the elections can also be increased with blockchain voting because people will be able to cast their votes wherever they are and thus they don't feel the pressure in certain voting places. Also disabled people or people on vacation does not have to go their registered place to cast their votes.

6. CONCLUSION

Elections are the most important tools to carry out democracies. With opportunities brought by latest technology, the requisite of conducting elections in physical environment is decreasing with day by day. Instead of this, issue of carrying out elections in electronic environment is becoming more and more popular. With the emergence of Blockchain technology, the security of the elections in the electronic environment has also been ensured considerably. Moving the election system to the electronic environment will eliminate the physical costs, ensure the election security in the authoritarian regimes by eliminating the central authority through blockchain, and increase the participation rates in the elections due to the fact that people can vote from any place with internet access.

Having all these innovative and epochal features, blockchain voting has considerable potential to affect and shape the concept of democracy or at least the tools to carry out democracies.

REFERENCES

Aitzhan, N. Z., & Svetinovic, D. (2018). Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. *IEEE Transactions on Dependable and Secure Computing*, 840-852.

Bazhanov, B. (2002). *The Memoirs of Stalin's Former Scretary.* Moscow: III Tysiacheletie.

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.

Berg, C. (2017). Populism and Democracy: A Transaction Cost Diagnosis and a Cryptodemocracy Treatment. *SSRN eLibrary*, 6.

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

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

Jones, D. W. (2007). Voting and elections. *Computer, 16*, 18.

Jones, D. W. (2007). Voting and elections. *Computer, 16*, 18.

Katz, R. S. (1997). Democracy and Elections. Oxford University Press.

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

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.

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.

Meter, C., Schneider, A., Hagemeister, P., & Mauve, M. (2017). Tor is not enough: Coercion in Remote Electronic Voting Systems. *arXiv preprint*, 2-12.

Murphy, P. J. (2001). *Voting and elections.* Capstone.

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

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

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

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.