HACETTEPE
University

Computer Science And Engineering Department

Final Report

Name Surname-No	:	Coşkun Yusuf ÇETİN	21791709
		Pelin FİLDİŞ	21827412
		İhsan Çağatay ERASLAN	21827335
Course	:	BBM-443	
Subject	:	**Voting System**	
Date Due	:	31.12.2021	
Advisors	:	Dr.Öğr.Üyesi ADNAN ÖZSOY	
E-mail	:	b21791709@cs.hacettepe.edu.tr b21827412@cs.hacettepe.edu.tr b21827335@cs.hacettepe.edu.tr	

ABSTRACT

“Elections are a critical component of democratic administration. The general election still uses a centralized system, and there is an organization to manage it. Some problems that may arise in standard election systems are that an organization that has complete control over the database and the system has a great chance of manipulating with the database and in some types of voting systems, ballots are still used as paper. This is actually wastage. Considering this situation, A system that includes certain conditions of voting and that will benefit everyone has been sought. With the development of technology, new ways have emerged. Blockchain technology is one of them and improves a solution to voting systems and promises to increase the overall durability of voting systems. In fact, the possibilities offered by the blockchain are: transparency, decentralization, irreversibility, nonrepudiation, etc. This paper proposes a type of blockchain-based electronic voting system, which solves some of the limitations of the existing system and evaluates some popular blockchain frameworks to build a blockchain-based electronic voting system.”

1-INTRODUCTION

From past to present, election systems have been made with very physical and primitive methods, which have been customary for many years. However, some countries have gone beyond this primitiveness and switched to electronic voting methods. The first electronic voting was applied in Estonia (2005) [1]. After they switched to this system, they set an example for the European Union. Thus, the transition to a new voting system began. Traditional voting is done under a centralized organization, and countries that continue this voting system use this system because the system is reliable, anonymous and secure and they think that e-voting (online elections) is unsafe. For example, electronic voting in Germany was abolished in 2009, after the German Federal Constitutional Court ruled that it was unlawful due to the lack of meaningful public oversight [2]. Electronic voting is cheaper and easier to handle than traditional voting in many ways, but there are also many security and trust problems that come with e-voting. Detecting and identifying the source of mistakes and technological malfunctions is more challenging than using a traditional voting system. At this stage, Blockchain technology showed up in our lives. In a network, blockchain offers a permanent record of transactions. It's similar to a system database, but instead of using an end-to-end traditional ledger, it employs a decentralized ledger, enabling each network participant to have their own copy of the ledger and observe all transactions. The system is difficult to attack or hack because each block is safeguarded by an encrypted reference to the preceding block [3]. Imagine a future in which every contract, transaction, task, and payment is digitally recorded and signed in a form that can be identified, confirmed, preserved, and shared. Because every modification in this system requires consensus, every step of the blockchain is transparent and safe. This assures the system's high degree of dependability while also removing hazards and the need for third parties [3]. Considering these situations, a development for the voting system is inevitable. Blockchain technology can bring a new way of reliable and transparent voting. Also, people who are unable to vote in person on election day will be able to vote remotely using the blockchain-based e-voting system. In this paper, we explain our decentralized e-voting proposed model and discuss its strengths and weaknesses. To briefly branch our proposed model, It is composed in 4 parts: Setup, Voting, Counting of Votes and Announcement of Votes and in following pages, we explain details of parts.

2-Literature Review

Our primary goal while preparing this paper is that voting processing is in security. As we mentioned in the previous sections, there are problems with traditional voting and some e-voting systems. These problems can happen unexpectedly during the voting process. We have to minimize redundant problems. On the other hand, the systems we have mentioned also have advantages.

Traditional Voting System:

This system, which is still in use today, is done through an official institution. In this method, ballot papers are usually paper. Voters go to the polls to vote and cast their votes in closed rooms, in a way that no one can see. In this way, anonymity is ensured. In other words, we can say that there is a safe environment during voting. After the voting process is over, the results will take a long time to be announced since the counting will be done manually. Today, some people still think that this system is the safest way. However, it is much easier to manipulate the votes they cast compared to other systems. Persons who take part in the voting can take action against the voters. In general, since these processes are always passed by human hands, it is inevitable that there will be an error in the voting. That's why a trusted institution should do the job [4].

E-Voting System:

As we know, e-voting already existed before blockchain existed. In fact, e-voting is not a new technology today. In 2005, Estonia used the first e-voting system. There have been many developments in e-voting since then. System based on ID cards of citizens. The validation process of ID cards is done with digital certification, so people can log in to the system to vote via the internet. In addition, in this system, voters can change the vote until the voting period ends. To talk about the advantages. Remote voting provided convenience for those who could not go to the polls. People can use the game by simply connecting to the internet [1]. In addition, there is no extra cost for ballot papers. Since most of the transactions are in a digital environment, they are handled cheaper and these advantages can be written even more with certain improvements. In addition, this system also has disadvantages. Since the voting process is over the internet, malicious people can attack the system. They may want to crash the database where the votes are collected. Another disadvantage is that the voter can change the game later, because there is a transfer over the internet for the change of the previous game and this can be attacked. Assuming that the vote is safely in the database, the changed vote may not be recorded correctly due to a problem with the database [5]. Also, Switzerland has a similar system but it has similar disadvantages as Estonia [6]. With DDOS attacks, the system can be rendered inaccessible to voters.

A Besides, there is no official blockchain-based voting system yet. But there are many improvements related to them. In other articles, a commonly important thing is verification of the voter. In [8] the solution brought to verify the voter is to make the user via email. This is not a very correct solution. It is possible that the user's email account is stolen during voting. In another, the user can register himself on behalf of someone else so that there is no anonymity. In another article[7], it does the verification through the voice recognition system. This system is not very healthy either. The manipulation of the user's voice is obvious. As we mentioned in the previous example, such approaches for straightening are not very accurate. Biometric verification is more appropriate for the solution, because each person has their own unique characteristics. Methods such as finger recognition, ID card, face recognition can be applied for biometric recognition.

3-PROPOSED MODEL & IMPLEMENTATION DETAILS

We can examine the election management of the regulator in four stages.

1.Setup

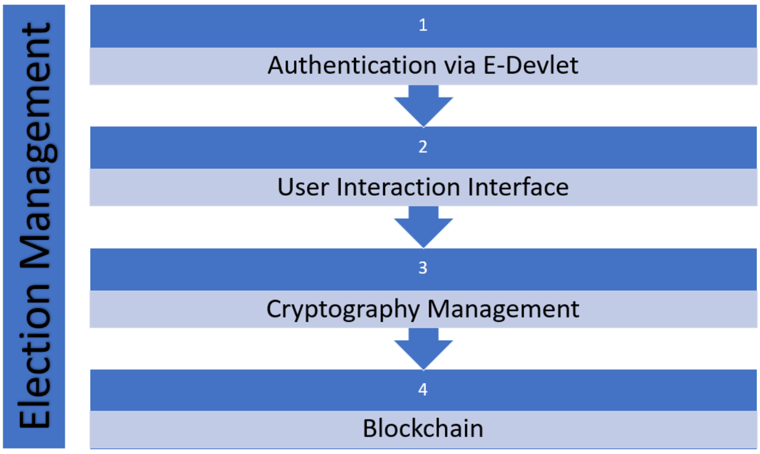
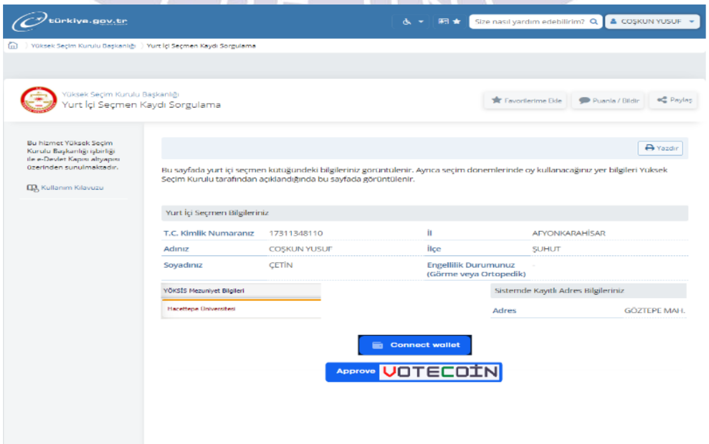


Figure 1: Election Management Of The Regulator

Authentication via E-Devlet

The regulator should use the official websites of the states known as e-government in our country in order to perform identity control and voting control of the voters. For this reason, the regulatory agency should make the necessary arrangements regarding the section reserved for it on the official website of the government. On the current E-government voter inquiry screen, only identity information is available. In the model we propose, the education level and residence (abroad) status of the voters affect the voting power of the voters. For this reason, education information and residence information of the voter is also needed on this inquiry screen.



Yüksek Seçim Kurulu Başkanlığı
Yurt İçi Seçmen Kaydı Sorgulama

Bu hizmet Yüksek Seçim Kurulu Başkanlığı işbirliği ile e-Devlet Kapısı altyapısı üzerinden sunulmaktadır.

Bu sayfada yurt içi seçmen kütüğündeki bilgileriniz görüntülenir. Ayrıca seçim dönemlerinde oy kullanacağınız yer bilgileri Yüksek Seçim Kurulu tarafından açıklandığında bu sayfada görüntülenir.

Yurt İçi Seçmen Bilgileriniz

T.C. Kimlik Numaranız	17311348110	İl	AFYONKARAHİSAR
Adınız	COŞKUN YUSUF	İlçe	ŞUHUT
Soyadınız	ÇETİN	Engellilik Durumunuz (Görme veya Ortopedik)	-

YÖKSİS Mezuniyet Bilgileri

Hacettepe Üniversitesi

Sistemde Kayıtlı Adres Bilgileriniz

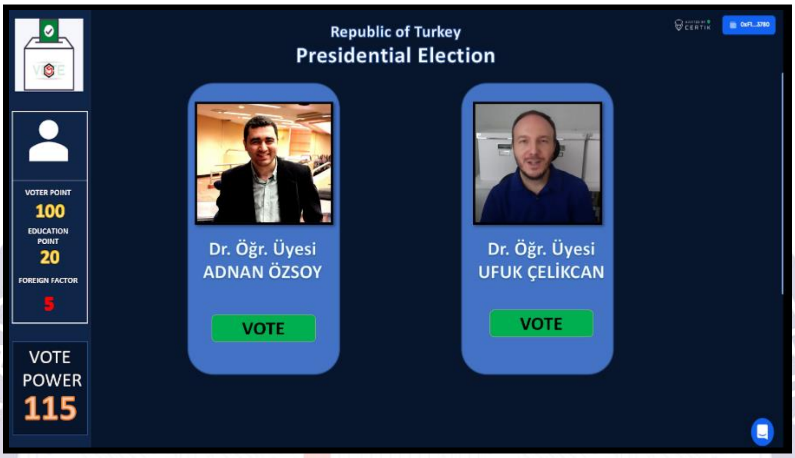
Adres GÖZTEPE MAH.

Figure 2: Suggested E-Government Voter Inquiry Screen

Wallet integration and necessary arrangements must be made by the regulator so that the voter can easily connect his/her wallet on the official site of the government, such as decentralized exchanges, and receive the VoteCoins that will be provided by the system to vote.

User Interaction Interface

One of our main goals in our proposed model is to enable all voters to vote easily online with devices such as computers, tablets and mobile phones. For this reason, the regulator should develop a web client. This developed client can also be used to announce the results. To this web client, the voter should be able to connect her/his wallet as easily as decentralized exchanges.


Republic of Turkey
Presidential Election

VOTER POINT 100
EDUCATION POINT 20
FOREIGN FACTOR 5
VOTE POWER 115

Dr. Öğr. Üyesi ADNAN ÖZSOY
Dr. Öğr. Üyesi UFUK ÇELİKCAN

Figure 3: Suggested Web Client Interface

This web client has to be reliable and transparent. To ensure reliability and transparency, the regulator should develop the web client using an up-to-date and generally accepted programming language, such as JavaScript, and share their code as open source. The source codes of the web client should always be able to be checked instantly by the people or authorized persons.

For people who are not related to technology or who do not have the opportunity to use electronic devices due to their age or special situation, the regulatory agency may prefer to place voting machines integrated into the system in some centers in the cities. A machine such as the new voting machine from Polys, which is a Kaspersky Innovation Hub project and develops an online voting platform, can be used for this purpose. [9]

Cryptography Management

The regulator should set up VoteCoins, which are considered the voting seals of our blockchain-based electronic election model, so that they cannot be sent to another voter's wallet and automatically sent to the burning address some time after the election ends. With this method, it will be possible to prevent people from selling their votes and voting for others, and when the election is over, the details of the unused votes will be accessed transparently from the burn address.

In the model we propose, the education and residence status of the voter will be taken into account in determining the number of VoteCoins to be provided to the voter.

The proposed model uses the following calculation method to better understand the calculation and the characteristics of the votes.

-Every voter who has completed or not completed compulsory education is entitled to 100 VoteCoins corresponding to 100 basic vote points.

-University graduates have the right to Votecoin, which corresponds to 10 basic vote points for associate degree graduates and students, and 20 basic vote points for undergraduate graduates and students, and above.

-In addition, voters residing abroad have a disadvantage as long as they reside abroad. This disadvantage is up to a maximum of 9 years.

-In this calculation, the tens digit for the education level and the ones digit for the residence status are used to simplify the calculation.

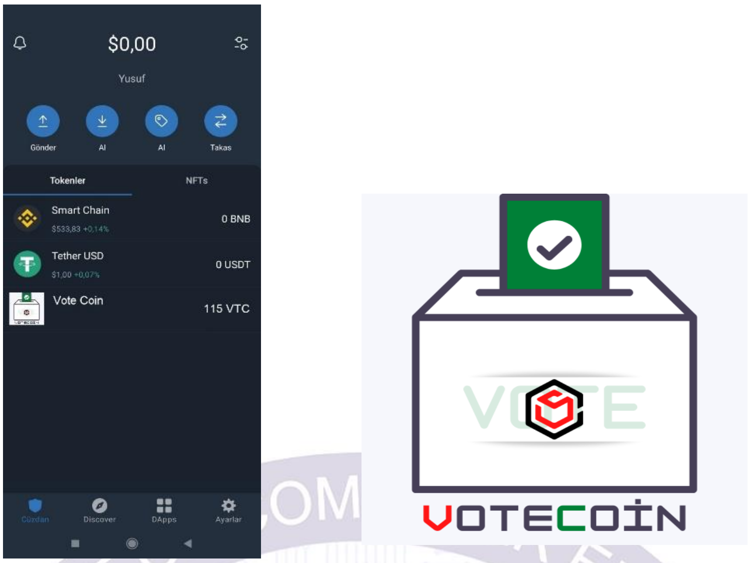
-Vote Power, which represents the vote power of the elector, is calculated as the:

Basic Vote score + Education score - Abroad factor.

In cases where more than one election is made at the same time, the amount of VoteCoins that the voters will receive is increased in proportion to the number of elections. The voter has voting power equal to the amount of VoteCoin divided by the number of elections in each separate election.

Blockchain

In the setup phase, first of all, it setup the necessary systems according to the selection of the regulatory institution. At this stage, the regulator must select the blockchain network to be used and make the necessary adjustments. These networks can be binance smart chain, Ethereum and the like. If the regulator wants to, it can create its own blockchain network. The regulatory agency must provide the voters with the coins necessary to run smart contracts according to the network they choose.



$0,00

Yusuf

Smart Chain $533,83 +0,14%	0 BNB
Tether USD $1,00 +0,07%	0 USDT
Vote Coin	115 VTC

Figure 4-5: Sample Wallet View and Representative VoteCoin Token

At this stage, voters are expected to be provided with a smart wallet like metamask or trustwallet.The regulatory agency may provide an educational introduction or guide to voters on the acquisition and use of smart wallets and the necessary network settings.

2.Voting

Our proposed blockchain-based voting model is expected to happen step by step as follows.

-The voter provides himself/herself with a smart wallet and makes the necessary network settings.

- Checks the voter information by entering the official website of the government.

-Connects his/her wallet to the official site and transfers the VoteCoins provided to him/her to his/her wallet.

-The voter checks whether the VoteCoins supplied to him/her are transferred to his/her wallet.

-The voter enters the web client and connects his/her wallet.

-The voter can calculate the attributes of the VoteCoins provided to him/her and the Vote Power himself/herself through the steps or view them through the web client.

- Voters cast their votes through the web client and can check their votes through transactions.

-Votes are encrypted with the RSA algorithm.

RSA

RSA encryption is used to secure the symmetric key to the node safely. RSA is an asymmetric encryption algorithm. In RSA encryption, the user has 2 keys which are hidden and open. The party who wants to send a message will send the message that the other user wants to send with the public key by encrypting. The user who receives the encrypted message can access the open message value by decrypting the encrypted text with the private key.[10]

-The votes cast by the voters are approved and recorded on the chain as encrypted.

- Since each candidate's separate address will affect the security of the election, all the votes sent by the voters must go to a single address.

-If the regulator wants to create their own nodes or contribute to mining, they can use a semi-closed blockchain method.

Authorization of transactions to be carried out on a semi-closed blockchain is very difficult.is important. In addition, it is even more difficult to do this while protecting the privacy of the people performing the transaction.it is difficult. Various methods have been proposed to solve this problem. most widely used One of the methods is the use of blind signature. [11]

Blind Signature

Blind signature is used for signing encrypted messages with no need for decrypting them. In our protocol, it plays a crucial role in hiding voters' choices on the ballots while getting signatures.[12]

- Since the vote of the voter is encrypted, the choice of the voter cannot be seen or controlled by others.

-At this stage, a Rule is added to the contract so that the voter's choice cannot be accessed until the end of the voting, thus providing extra security.

Two of the most popular cryptocurrencies, Bitcoin and Ethereum, support the feature to encode rules or scripts for processing transactions. This feature has evolved to give practical shape to the ideas of smart contracts, or full-fledged programs that are run on blockchains. [13]

- Just in case, whether the voter voted more than once can be checked on the blockchain.

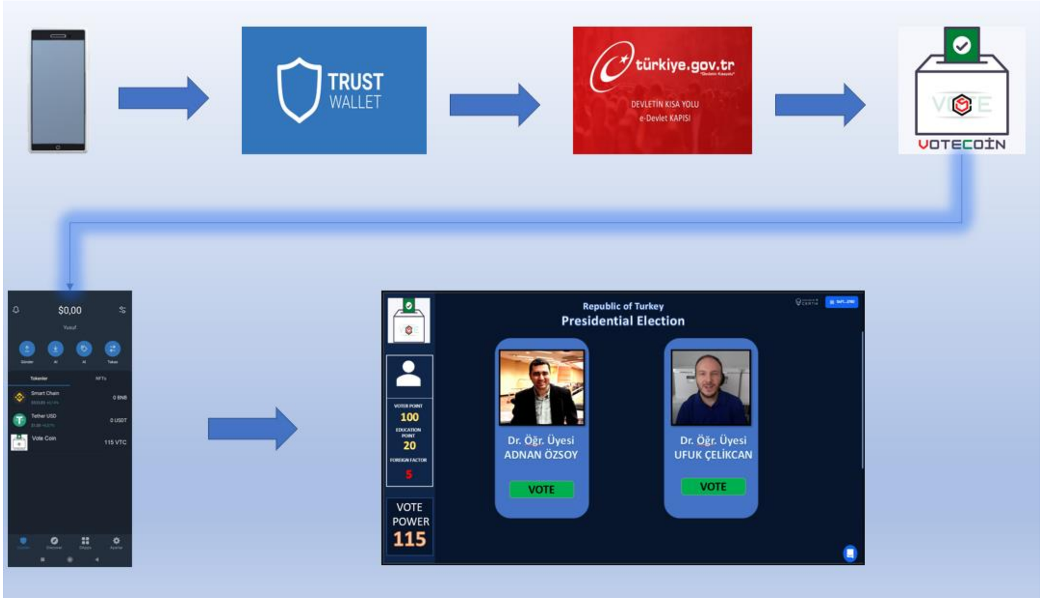


Figure 6: Proposed Model Flow Diagram

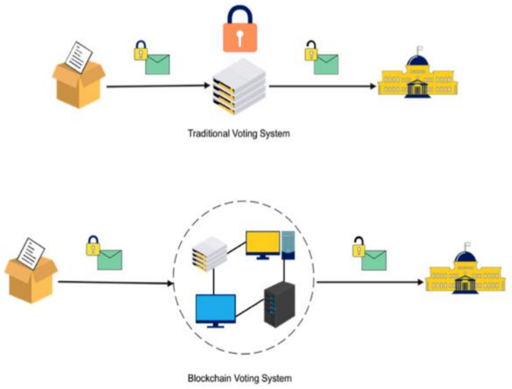
3.Counting Of Votes And Announcement Of Results

Due to the Rule added to the contract, the results cannot be accessed until the voting period ends. When the voting period is over, the blocks are decrypted and the block vote counting is done transparently. When the vote count is over, the results are announced on the client or through different channels.

Thanks to the features of VoteCoin, the votes collected by the candidates can be categorized according to their education level and residence, and a relationship can be established between them.

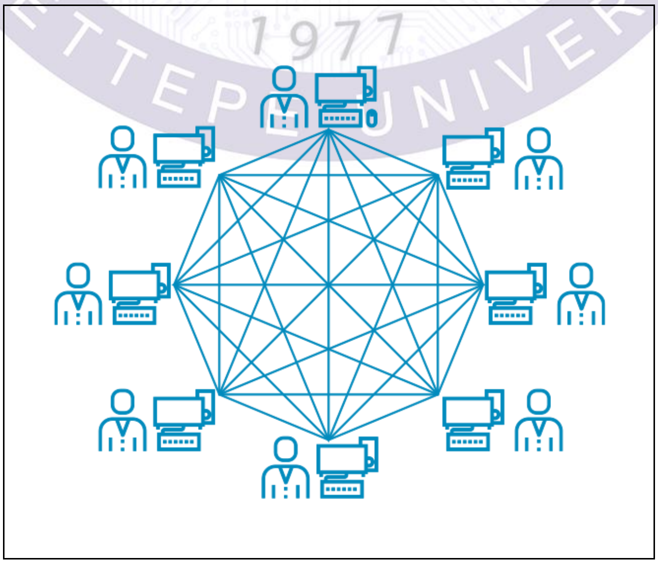
4.ANALYSİS

1.Security analysis and potential attacks

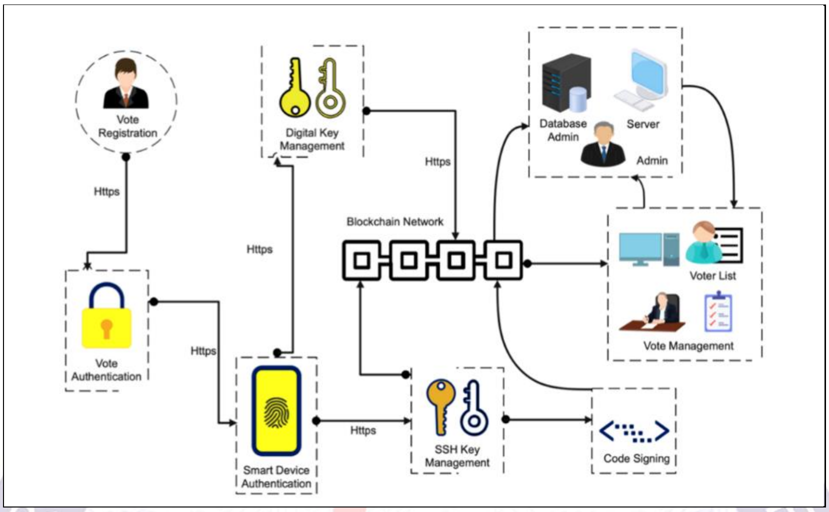


The blockchain technology guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party. Because of the decentralization principle of blockchain-based technologies there'd be no need to have some centralized power to conduct the voting, which makes voting more reliable and secure.

Thanks to blockchain, counting of votes is open and transparent. In the blockchain model, voting information is stored on the network and anyone with access to the network can read the information on the blockchain. So, everyone can verify the accuracy of the vote count. Exchange on ballots is not possible in blockchain technology.



Every node that has access to the blockchain network contains a copy of the blockchain itself, and it updates with every insertion. So that no one can interfere with the results and even if they try since the data entry in the ledger is distributed among all the nodes it will not be effective on the outcome. Thus, the votes cannot be changed, a recount can be performed if necessary.



As described in the compliance with the voting requirements, double voting is not possible. When servers inevitably disagree on the order of the two blocks, they each keep both blocks temporarily. As new blocks arrive, they must commit to one history or the other, and eventually a single chain will continue on, while the other(s) will not. Since the longest (more technically "heaviest") chain is considered to be the valid data set, miners are incentivized to only build blocks on the longest chain they know about in order for it to become part of that dataset (and for their reward to be valid).

The voter can see the VoteCoins obtained from the e-government system in her wallet, VoteCoins obtained from the system cannot be transferred to another voter wallet. Unused VoteCoins are sent to the burning address automatically after a certain period of time when the election is over. In addition, the voters are provided with the necessary coins to run the contracts. The limited coins and their non-transferability prevent double voting.

Attacks like Sybil Attack (Done by creating many fake identities),Denial-of-Service (DoS) Attacks will have no effect on the outcome of the election because the distribution of the service on ifferent nodes and POW algorithm will not allow a false change on the blockchain by any third parties.

2.Compliance of voting requirements by the blockchain e-voting system

Privacy

In each voting method, the voter's vote must be kept secret and in order to achieve this confidentiality, the votes are encrypted. And since the blockchain systems, in addition to being transparent, also provide anonymity, it ensures the privacy of the individual. Everyone has a public address but they are not associated with individuals and they are not traceable.

Eligibility

In this voting model, no one cannot vote in place of another voter. Each voter can only create a single wallet with his own T.C. identity number through the E-Government system. In this way, it was prevented that someone else would vote instead of the voter. This system can be made more secure by using facial recognition, fingerprint, and biometric data. The information of the voters who voted is recorded in the blockchain network. In Blockchain technology, it is not possible to change or delete the information recorded on the network. Therefore, each voter can only cast one vote.

All of these adjustments ensure that only registered/authorized voters can vote with each one of them voting only once.

Receipt Freeness

Every vote is encrypted with a key according to Blind Signature encryption method and they are all sent to a pool. When the voting period expires, the votes in the pool are counted by opening the key. Since the votes are encrypted, it is not possible to extract information to prove a third party the vote of the voter.

Verifiability The ability to trust the vote tallying process

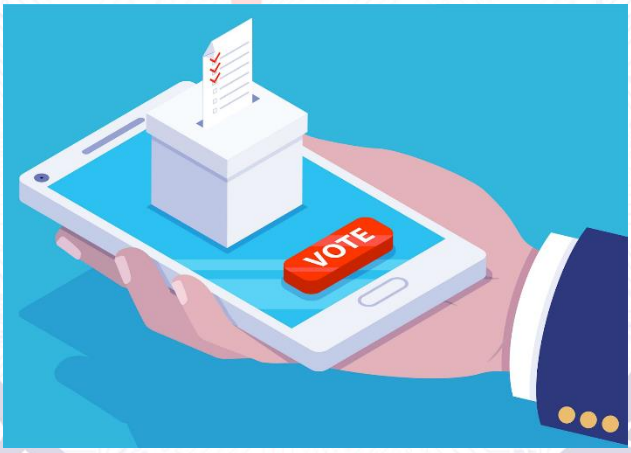
The decentralization principle of blockchain technology increases the integrity of elections and their controllability by different entities. Thanks to blockchain, counting of votes is open and transparent. In the blockchain model, voting information is stored on the network with this distributed structure; anyone with access to the network can read the information on the blockchain. So everyone can verify the accuracy of the vote count.

Convenience

The ease of transportation provided by every e-voting system also makes this voting system more convenient compared to other voting systems. With an easy-to-use interface, the system only requires minimal effort from the user.

3.Financial and social aspects and environmental effects of our system

On the plus side, it will ensure that the trees are not cut down for the papers needed for the ballots, and that water and energy are not wasted in the process. This system will also minimize the damage caused to the environment by all the vehicles used for transportation on the voting day. It will also minimize all the chaos that we encounter on the day which will have a positive impact on social segment of this day. But in order to make this system work and function correctly, it will need a high amount of energy.



4.The difference of VoteCoin from the other blockchain systems

Thanks to VoteCoin, the voter's contribution to the election can be determined by evaluating their education, country of residence, etc. socio-economic status. This model assures that foreign nationals who are far from the affairs of their country will not be able to have the same impact on the voting compared to their local voters. Taking the well-being of the country into account the amount of coins varies depending on the educational status, with a minimal change in voting competence, this ensures a more accurate choice is made on behalf of the country and the majority.

5.CONCLUSION

Blockchain technology can bring a new way of reliable and transparent voting. Thanks to the blockchain, e-voting system can enter our lives. With e-voting system, people who cannot reach the polls on election day will also have the chance to vote from wherever they are. With blockchain model, all voters are guaranteed to one vote with. The information of the voters who voted is recorded in the blockchain network. In Blockchain technology, it is not possible to change or delete the information recorded on the network. Therefore, each voter can only cast one vote.

In this voting model, no one cannot vote in place of another voter. Each voter can only create a single wallet with his own T.C. identity number through the E-Government system. In this way, it was prevented that someone else would vote instead of the voter. This system can be made more secure by using facial recognition, fingerprint, biometric data.

Thanks to blockchain, counting of votes is open and transparent. In the blockchain model, voting information is stored on the network and anyone with access to the network can read the information on the blockchain. So everyone can verify the accuracy of the vote count.
Exchange on ballots is not possible in blockchain technology. So that no one can interfere with the results.

No one can follow the election results until the election time is over. The fact that anyone with access to the blockchain network can read the data on the chain may have some undesirable consequences during the election. For example, estimating the election results before the end of the election may mislead the voters. To avoid this, votes can be encrypted with a key.
In this system, since a copy of the votes, namely the block, is on each node, recounting can be done easily.

Thanks to VoteCoin, the voter's contribution to the election can be determined by evaluating their education, country of residence, etc. socio-economic status.

References

[1] Madise, Ülle, and Tarvi Martens. "E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world." Electronic Voting 2006–2nd International Workshop, Co-organized by Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting. CC. Gesellschaft für Informatik eV, 2006.

[2] Volkamer, Melanie. "Electronic voting in Germany." Data protection in a Profiled World. Springer, Dordrecht, 2010. 177-189

[3] Nofer, Michael, et al. "Blockchain." Business & Information Systems Engineering 59.3 (2017): 183-187.

[4] Cranor, Lorrie Faith. "In search of the perfect voting technology: No easy answers." Secure Electronic Voting. Springer, Boston, MA, 2003. 17-30.

[5] Krimmer, Robert, et al. "How much does an e-Vote cost? Cost comparison per vote in multichannel elections in Estonia." International Joint Conference on electronic voting. Springer, Cham, 2018.

[6] Braun, Nadja. "E-Voting: Switzerland's projects and their legal framework–In a European context." Electronic voting in Europe-Technology, law, politics and society, workshop of the ESF TED programme together with GI and OCG. Gesellschaft für Informatik eV, 2004.

[7] Mikail, Olaniyi Olayemi, Folorunso Taliha Abiodun, and Abdullahi Ibrahim. "Design and Development of Secure Electronic Voting System Using Radio Frequency Identification and Enhanced Least Significant Bit Audio Steganographic Technique." published in Dec (2014).

[8] Pawlak, Michał, Aneta Poniszewska-Marańda, and Natalia Kryvinska. "Towards the intelligent agents for blockchain e-voting system." Procedia Computer Science 141 (2018): 239-246.

[9] https://www.aa.com.tr/tr/sirkethaberleri/bilisim/blokzincir-tabanli-oylama-makinesi-tanitildi/656015

[10] Orak, Ilhami. (2020). A Suggestion for Electronic Election System based on Bocckchain Burak Esen.

[11] Aydın, Muhammed Emin. Blokzincir Tabanlı Oy Verme Sistemi Önerisi. MS thesis. Necmettin Erbakan Üniversitesi Fen Bilimleri Enstitüsü, 2018.

[12] Chaum, D.: Blind signatures for untraceable payments. In Chaum, D., Rivest, R.L., Sherman, A.T., eds.: Advances in Cryptology: Proceedings of CRYPTO '82, Santa Barbara, California, USA, August 23-25, 1982., Plenum Press, New York (1982) 199–203

[13] Luu, Loi, et al. "Making mart contracts smarter." Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016.