Conduction of Online Election using Ethereum: A Survey Paper

[1]Prahlad Nayak,[2]Raj Anand, [3]Dr. Radhika K R

[1]Student, [2]Student, [3]Professor
[1,2,3]BMS College of Engineering, Bangalore, India

Abstract—Voting is one of the most important pillars of any democracy. The current system for voting has a very strong base but at the same time, it has a lot of lacking. The most prominent one is the lack of mobility. As voting is a very crucial process and every citizen of any nation or organization is expected to participate in the activity. E-voting is another trending, yet critical, topic related to online services. The block chain with the smart contracts emerges as a good candidate to use in the development of safer, cheaper, more secure, more transparent, and easier-to-use e-voting systems.Blockchain-enabled e-voting could reduce voter fraud and increase voter access. Eligible voters cast a ballot anonymously using a computer or smartphone. Blockchain-enabled e-voting uses an encrypted key and tamper-proof personal IDs. The voting system built using blockchain is more robust, tamperproof, and cost-effective.

***Keywords*—Ethereum, Blockchain, Solidity, Proof of Work, E-voting, Smart Contract, Security, Consensus, Ballot**

Introduction

Blockchain enables a return to decentralized computing and encryption technology by securely storing information in a way that cannot be revoked from unauthorized access. Its main purpose is to track ownership of tangible and intangible assets. Blockchain is the underlying technology that powers cryptocurrencies and other cryptographic technologies. The technology was first conceived in 1991 and has used blockchain elements in peer-to-peer technologies such as Tor, torrents, cloud computing, and more. Information in a blockchain is stored in cryptographically encrypted pieces called blocks. The next sequential block contains information about the previous block, thus forming a chain. So the name is derived from the blockchain. Blockchain privacy is supported by advanced cryptographic hash functions and public-key cryptography. It also helps to achieve transparency. Blockchain technology provides decentralized nodes for online voting or electronic voting. Recently, widespread ledger technologies such as blockchain have been used to create electronic voting systems, primarily because of their end-to-end verification benefits. Blockchain is an attractive alternative to traditional electronic voting systems with features such as decentralization, non-repudiation, and security protection.

A blockchain is a growing list of records called blocks that are linked together using cryptography. Each block contains a cryptographic hash of the previous block. The Ethereumblockchain is a global open-source platform that supports decentralized applications. It provides programmability and coding is done by smart contracts. A smart contract is where all the business logic of your application resides. Smart contracts are responsible for reading and writing data to and from the blockchain and executing business logic. The overall goal of smart contracts is to fulfill common contractual conditions, such as creating your own token on Ethereum.

Literature Survey

Blockchain based e-voting system can replace the traditional voting system as it provides a secure system where in the voter identity is protected and vote manipulation is also avoided. The below papers provides an in depth analysis into the advantages and security issues with respect to implementing e-voting using blockchain, and ways in which the whole process of e-voting can be conduted.

Hanifatunnisa, Rifa et al. [1] tested a system capable of handling the entire write process of a voting system and computed the average time and memory required for each node at block generation. In the research, simulation was done by using Python programming using PyCharms Community software and tested using small number of nodes for implementation using visualization. The average time required for each node in creating a block is 0.24 seconds and the average capacity required to store Data of 216.04 Bytes for each block.

Qi Wang et al. [2] analyzed the security issues of a voting implementation using blockchain. Voter privacy is mostly protected by the blind signature and hash functions. Blind signatures are used to sign encrypted messages without decrypting them. The protocol plays a crucial role in hiding voters' choices on the ballot when signatures are collected. In proprietary protocols, communication over a blockchain network can lead to the disclosure of the IP address of voters, which can lead to the disclosure of connections between voters and voters through network analysis. The security issues of the system are Voter privacy, Ballot manipulation, forgery, network attack, and ballot collision. The security of the system built by the author mainly relied on the blind signature protocol and the basics of blockchain.

Hsiao, JenHo et al. [3] proposed a complete voting procedure in which voting could actually take place. With the advent of blockchain technology, the basic concept of decentralization is getting more and more attention. In the above context, the main goal of the study is to implement more convenient and secure applications using blockchain technology. Currently, service industries such as finance and banking are transmitting personal information through trusted third parties. However, it faces many challenges and complex procedures. Since the blockchain technology and smart contract have the characteristics of decentralization, the researchers analyzed the architecture of the existing e-voting systems and found the integration of blockchain and smart contract into the application, could enhance data verifiability and lower the cost while maintaining the openness and transparency of the voting. The anonymities of voters, the security of ballot transmission, and the verifiability of votes during the billing phase are the most fundamental requirements for voting. It can be done in 5 phases, i.e., Initial Phase, Registration Phase, Voting Phase, Billing Phase, and Security Analysis.

Pavel Tarasov et al. [4] sited future e-voting scenarios that can be addressed and can be made possible to overcome the present offline elections. The author proposed a standardized electronic voting solution that would be widely adopted has not yet emerged, there are inherent security issues that make these protocols unsuitable for elections, and the advent of blockchain introduced a new way of building secure systems with fewer inherent security issues present in the system. The electronic voting protocol has been implemented in various elections, from college elections to state elections. Many viable protocols have been created since Chaum first proposed Votegrity, one of the first end-to-end verifiable voting methods. Voters will have confidence that their votes have been counted correctly, that is included in the final count, and that the general public can check elections outside without having to participate in the election. These voting protocols also allow verification of the votes and ballots of 4,444 voters prior to candidate selection and ballot submission. It can be concluded that the electronic voting system must be secure and must provide maximum transparency for E2E verification to be possible. Zcash is a decentralized blockchain payment method that aims to ensure the anonymity and confidentiality of transactions. One of the major differences between Zcash and Bitcoin is that Zcash is a proof-of-work system that relies on zero-knowledge proofs. Zcash is an implementation of the Zerocash concept (BenSasson et al, 2014) that describes a similar Zcash concept, but the architecture of Zcash is different. Before delving into the details of the proposed voting protocol.

Harry Halpin et al. [5] investigated hashing techniques that will provide free experiences to blockchain participants using proof-of-work. Proof of work is used to verify and authenticate anyone who wants to be part of the chain, and hashing is used to allow members to join without permission. Proof of Work is the original consensus algorithm in the blockchain network. Algorithms are used to confirm transactions and create new blocks on the chain. Basic cryptographic fundamentals of blockchain and improved privacy and anonymity. A blockchain is simply a cryptographically verifiable list of data. One reason blockchain is so hyped is that it lacks the cryptographic integrity guarantees required for databases running in database-hostile environments. One lesson learned from systems security and privacy techniques after Snowden's revelations is that any database has the potential to operate in a hostile environment. Because it are developed by practitioners, not cryptographers, they generally place their trust in practical resistance to attacks based on the practitioner's general knowledge and experience rather than formal evidence and attributes. The design follows the constant variability of the proposed solution and the lack of common and integrated design options and criteria. So there are many solutions claiming that each one is the best one.

Ahmed Ben Ayed et al. [6] explored different e-voting systems used to date and their basic protocols used in them. Estonia IV Voting System: Estonia was the first country in which citizens could vote using only the Internet and electronic ID cards. The ID card used in the is designed to work on integrated circuits that are Java Chip Platform with a 2048-bit PIN. Cards can generate signatures using SHA1/SHA2. The card is easy to use for authentication, encryption, and signing. Voters must download the voting App and authenticate as an Elector Candidate to be displayed. Then you can vote. Votes are encrypted using the election's public key and signed with the voter's private key. When voting is complete, is sent to a voting storage server managed by the Estonian government. A voter may vote multiple times, and only the last vote is considered valid, and it would prevent the purchase of votes.

Kshetri, Nir et al. [7] pointed out the advantages of using a blockchain-based e-voting system. Blockchain-enabled e-voting can reduce voter fraud and increase voter access. Eligible voters voted anonymously using a computer or smartphone.Blockchain-enabled e-voting uses encrypted keys and personal identifiers that are protected from unauthorized access. Each voter receives one “coin” representing one voting opportunity. When voting, the voter's coins are transferred to the candidate's wallet. Voters can only use their coins once.

Friedrik O. Hjálmarsson et al. [8] analyzed some of the popular blockchain frameworks that offer blockchain as a service. The authors mainly compared three popular frameworks: Exonum, Quorum, and Geth platforms to implement and then deploy election smart contracts. The Exonumblockchain is robust end-to-end as its full implementation is done using the Rust programming language. Exonum is built for private blockchains. Exonum can support up to 5000 transactions per second. Unfortunately, a limitation of the framework is that Rust is the only programming language in the current version. Quorum is an Ethereum-based distributed ledger protocol with transaction/contract privacy and a new consensus mechanism. Quorum has changed the consensus mechanism and is more focused on consensus algorithms based on consortium chains. The above proposed consensus can support hundreds of transactions per second. Geth is one of three original implementations of the

Ethereum protocol; the framework supports development outside the Geth protocol and is the most developer-friendly framework. The transaction speed depends on whether the blockchain is implemented as a public or private network. Because of these features, Geth was the framework on which our work was based, and a similar blockchain framework with the same capabilities as Geth could be considered for such a system. Geth can be considered one of the best ways to implement and deploy because it is inherently flexible as it can be implemented using Go, C, Javascript, as well as smart contracts using Solidity and can process many transactions per second.

Freya Sheer Hardwick et al. [9] proposed a three-phase election process for the conduction of safe and transparent elections. The three phases of the voting process that the author proposed were the Initialization phase, Preparation Phase, and Voting Phase. In the Initialization phase, rules governing the elections are determined and the CA, the blockchain, and all other systems of the protocol are initialized. In the preparation phase, the CA will use the list of eligible voters along with the authentication information, to determine whether the aspiring voter is eligible to vote. In the voting phase, every Voter constructs and then broadcasts to the network their vote and inserts the valid ones in the blockchain.

Ali KaanKoç et al. [10] explored the concept of blockchain and the methodology it uses: an immutable hashing chain that can adapt to voting and elections. Ethereum-provided smart contracts are used to create Ethereum contracts that can validate and calculate votes. Ethereum contracts are smart contracts signed using a language such as solidity, a statically typed programming language. The study prioritizes Ethereum as a development platform and blockchain network, because Bitcoin is only used to validate coin transactions, while the Ethereum network offers a wider range of use cases with the power of smart contracts. Many applications that normally require a web server can run through these smart contracts without using a server. Therefore, it is very difficult, if not impossible, to tamper with or corrupt the source code of suspected software.

Prof.PallaviShejwalet al. [11], aimed to implement voting results using blockchain algorithms from every place of election, so as to build an electronic voting system ready for the conduction of elections using Blockchain technology. The use of Ethereum smart contracts to make it decentralized and impart Privacy and anonymity to Individuals. Smart Contracts were written by a statically typed programming language called solidity also known as the language of making Blockchains Advances in digital technology have revolutionized the way people live. Unlike the electoral system, the conditional use of paper is used for implementation. Security and transparency aspects pose a threat in the election, which is still prevalent in legacy systems (offline). The general election continues to use a centralized system run by people in one organization. Some of the problems that can arise in a traditional election system are organization-related and takes full control of the database and system. The potential for tampering with the database is significant. Blockchain technology is one of the solutions, because it involves a distributed system and the entire database is owned by many users. The blockchain itself was used in the Bitcoin system known as a decentralized banking system. Deploying a database on a new system by introducing the blockchain reduces the number of fraudulent sources of database manipulation.

Curran, Kevin et al. [12] analyzedVotem's vote confirmation. Votem Corp is a three-year blockchain-based mobile voting based in Cleveland, Ohio. The authors created Proof of Vote 6, a digital voting system with end-to-end (E2E) validation of voters that uses blockchain to provide verifiable, secure, and transparent elections. The protocol uses the ElGamal re-encryption mix networks for anonymity, a multi-signature scheme for voter authentication and authorization, and verifiable distributed key generation and verifiable decryption for voting encryption and decryption. Their protocol allows voters to encrypt their votes with a special public key and post them to a public voting repository, and to achieve anonymity using a homomorphic cryptosystem, a series of encrypted ballots are processed using a homogeneous cryptosystem. Proof of Vote differentiates itself from other voting and governance protocols by being designed from the ground up to explicitly optimize for the maximum level of verifiability, accessibility, security, and transparency of an election system deployed in the real world. It offers substantial advantages over more traditional E2E systems via the use of blockchain and a multiparty signature scheme for voter authentication and authorization, aiming to be a mature and tried technological blueprint for how societies, governments, and organizations can build election systems and processes.

Fusco, Francesco et al. [13] proposed a sidechain crypto voting system. Sidechains extend the blockchain and allow the creation of new functions, avoiding both writes to the main blockchain and the need to create new currencies. Sidechains are based on the possibility of creating systems by combining main and sub-blockchains that interact according to certain synchronization criteria. In general, cryptocurrencies can be moved on the sidechain and then returned to the mainchain. Crypto Voting systems seek to use an approved blockchain to ensure access control without compromising anonymity and confidentiality requirements. The assumptions and motivations for choosing the chosen technology are Voters, supervisors, and candidates' need for certified transparency, as well as the need for secure and reliable technology to create a double transparent and public ledger that contains all voting results. The groundbreaking idea of crypto voting is to use two linked blockchains with a one-way peg sidechain. The first sidechain records eligible voters and records voter voting operations. The second sidechain counts the votes given to the various candidates.

Harsha V. Patil et al. [14] studied the decentralized system of blockchain that will be used in e-voting and comparing with the previous offline election model. As per the author, the working of an e-voting system using blockchain is: 1. Requesting to vote: The user logs in to the voting system. 2. Casting a vote: Voters will have to choose to either vote or cast a protest vote. 3.

Encrypting votes: The system will generate an input that contains the voter identification number as well as the hash of the previous vote. 4. Adding the vote to the Blockchain: Each block gets linked to the previously cast vote. Blockchain Transparency enables better control and understanding of elections. These properties are one of the requirements of a voting system. Even the world's largest democracies, such as India, the United States, and Japan, continue to suffer from imperfect electoral systems. Forgery of voting results, Electronic Voting Machine hacking, election manipulation, and takeover of polling places are major problems of the current voting system.

KetulkumarGovindbhaiChaudhari et al. [15] explored some of the popular blockchain networks that use proof of voting to authenticate users or participants. The paper unveiled a unique blockchain-based electronic voting system that uses smart contracts to provide secure and cost-effective elections that ensure voter privacy. The smart contract contains the definition of the roles of election participants such as voters, officers, and nodal officers. In the article, the author has proposed a new consensus method that allows proof of voting. Voter registration is done using a Proof of Vote (POV).

Taş, Ruhi et al. [16] gave an insight into the current e-voting gaps, and how blockchain can improve the gaps in the current system and the major blockchain platforms used today. Reviled specific security problems are identity theft, malware on the voter's computer or device trojan horses, spyware, viruses, worms), server penetration attacks, spoofing, fake web pages, DNS (Domain Name Server) attack, and DDoS (Distributed Denial of Service) attack. System usability, privacy, or authentication issues may occur. Storing data on remote servers is considered safe, but it does not provide protection against hacker attacks and can lead to data loss or corruption if system security is not properly managed. Existing databases are also maintained by one group, which has full control over the database, including the ability to manipulate stored records, because of the bias, online voting is vulnerable to manipulation in terms of counting and fraudulent elections. DDOS attacks are one of the biggest challenges facing major cyber attackers today. If some nodes in the blockchain network go down as a result of a DDoS attack, the system will continue to work without interruption due to its decentralized nature.

Table 1: Table of Comparison

References	Problem addressed	Authors Approach/Method	Results
[1]	Testing an e-voting system to be able to handle the whole process of recording the e-voting system with the average time and memory required for each node in creating block.	In the research simulation is done by using Python programming using PyCharms Community software. Tested using small number of nodes for implementation using visualization.	The average time required for each node in creating block is 0.24 seconds and the average capacity required to store Data of 216.04 Bytes for each block.
[2]	Security analysis of the e-voting system.	Some of the security issues of a blockchain based e-voting system are Voters' Privacy, Ballot Manipulation and Forgery, Network Attack, Ballot Collision.	The security of our e-voting protocol mainly relies on that of blind signature and blockchain.
[3]	A complete guide to the conduction of e-voting	First, to generate their RSA-based public/private key. Second, user code generation, and verification of the voter's identity. Third, provides the voting certificate and asks for a ballot signature, using which the voter can vote.	The system takes advantage of the transparency of smart contract to allow all voters to participate in both the recording and verification of ballots.
[4]	Future e-voting scenarios that can be addressed and can be made possible to overcome the present offline elections.	Zcash is used which is a decentralized blockchain payment scheme, which aims to provide anonymity and privacy of transactions.The final stage of the voting protocol is the vote count and the audit which takes place after the count to review the election process and ensure that the integrity of the election has not been compromised.	A standardized electronic voting solution which would be widely adopted has not yet emerged,there are inherent security issues which make these protocols unsuitable for elections.
[5]	Improving Core Cryptographic Primitives and privacy and anonymity of Blockchain.	Use of Proof Of Work for verifying and for the authenticity of the person trying to be a part of Chain and use of hashing allowing participants to join in permission less manner. Proof of work is the algorithm is used to confirm the transaction and creates a new block to the chain.	Paper explores the hashing methods that will provide fluent experience for the participants of blockchain using Proof Of Work.

[6]	Explored different e-voting system used till date and their basic protocols used in them	Estonian I-Voting System:Voting system was using SHA1/SHA2 for the encryption part.New South Wales iVote System: Voting was done using 6 digit identification pin.Norwegian I-Voting System: the system was developed by e-voting vendor Scytl,and was very similar to estonian.D.C Digital Vote-by-Mail Service: Washington D.C developed a pilot electronic voting system and performed a dummy election to test the security of the system.	All the systems implemented are decentralized. Any registered voter had been giventhe ability to vote using any device connected to the Internet. The Blockchain was be publicly verifiable and distributed in a way that no one will be able to corrupt it.
[7]	Benefits of using blockchain based e-voting system.	Blockchain-enabled e-voting could reduce voter fraud and increase voter access. Eligible voters cast a ballot anonymously using a computer or smartphone.	Each voter gets a single “coin” representing one opportunity to vote. Casting a vote transfers the voter’s coin to a candidate’s wallet. A voter can spend his or her coin only once.
[8]	Exploring some of the popular blockchain frameworks that offer blockchain as a service.	Comparing 3 blockchain frameworks that can be used for implementing and deploying election smart contracts - Exonum, Quorum, Geth.	Geth can be concluded as one of the best ways of implementation and deploying as it is flexible in nature.
[9]	Making an independent e-voting system imparting transparency and privacy to the individuals.	Three phase election process – consisting of the Initialization Phase wherein the election rules are set, Preparation Phase wherein the list of eligible voters is generated and authenticated, and Voting phase wherein the voters will be allowed to vote.	Paper explores the potential of the blockchain technology and its usefulness in the e-voting scheme and maximize the Decentralization of blockchain.
[10]	The concept of blockchain and the methodology it uses.	The study prioritizes Ethereum as a development platform and blockchain network, because Bitcoin is only used to validate coin transactions, while the Ethereum network offers a wider range of use cases with the power of smart contracts.	Ethereum-provided smart contracts are used to create Ethereum contracts that can validate and calculate votes.
[11]	Getting an Electronic Voting system ready for the conduction of elections using Blockchain technology.	Use of Ethereum Smart Contracts to make it Decentralized and imparting Privacy and anonymity to Individuals.Smart Contracts were written by a statically typed programming language called solidity also known as language of making Blockchains.	The paperaimed to implement voting result using blockchain algorithm from every place of election.
[12]	The Votem Proof of Vote	The author created a Proof of Vote protocol, an end-to-end voter verifiable (E2E) digital voting system that uses blockchain to ensure the verifiability, security, and transparency of an election.	It offers substantial advantages over more traditional E2E systems via the use of blockchain and a multi-party signature scheme for voter authentication and authorization.
[13]	Crypto-voting system with a side chain.	Sidechain is based on the possibility of creating a system based on the combined use of a main blockchain and a subordinate blockchain that communicate with each other according to specific synchronization criteria.	The first records voters and voting procedures, the second counts vote and provides voting results.
[14]	Studyof the decentralized system of blockchain that will be used in e-voting and comparing with the previous offline election model	As per the author the working of e-voting system using blockchain consists of 4 steps, i.e., Requesting to vote, Casting a vote, Encrypting votes, Adding the vote to the Blockchain.	The transparency of the block-chain enables more auditing and understanding of elections. These attributes are some of the requirements of a voting system.

[15]	Explored some of the popular blockchain that use Proof of voting to authenticate users or participant.	Smart contracts include identifying the roles that are involved in election like voter, officer, nodal officer.In the paper author proposed new consensus method permissioned Proof of voting. Voter registration made by using proof of voting (POV).	Paper introduced a unique, blockchain based e-voting system that utilizes smart contracts to enable secure and cost-efficient election while guaranteeing voters privacy.
[16]	Cited the Current e-voting gaps, can blockchain improve it, and the appropriate blockchain platforms to be used.	Security problems are identity theft, malware on the voter's computer or device trojan horses, spyware, viruses, worms), server penetration attacks, spoofing, fake web pages, DNS (Domain Name Server) attack and DDoS (Distributed Denial of Service) attack. The most preferred blockchain platform is Ethereum (24%).	The paper represented information on current e-voting systems, the blockchain concept and its applications are introduced. Then a set of gaps of current e-voting systems, potentials of the blockchain concept to improve e-voting.

Conclusion

The system utilizes smart contracts to enable secure and cost-efficient elections while guaranteeing voters' privacy in comparison to offline ones, it also offers new possibilities for democratic countries to advance from the pen and paper election scheme, and it increased the security measures of today's scheme and offer new possibilities of transparency.The system when deployed on the ethereum network addresses almost all of the security concerns, like the privacy of voters, integrity, verification, non-repudiation of votes, and transparency of counting.It aims to speed up ballot counting, lower the expense of paying workers to manually tally votes, and enhance accessibility for impaired voters, so that voter fraud and vote manipulation can be eliminated.

References

[1] Hanifatunnisa, Rifa, and Budi Rahardjo. "Blockchain based e-voting recording system design." 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA). IEEE, 2017.
[2] Liu, Yi, and Qi Wang. "An E-voting Protocol Based on Blockchain." IACR Cryptol. ePrint Arch. 2017 (2017).
[3] Hsiao, Jen-Ho, et al. "Decentralized E-voting systems based on the blockchain technology." Advances in Computer Science and Ubiquitous Computing. Springer, Singapore, 2017. 305-309.
[4]Tarasov, Pavel, and Hitesh Tewari. "THE FUTURE OF E-VOTING." IADIS International Journal on Computer Science & Information Systems 12.2 (2017).
[5] Halpin, Harry, and Marta Piekarska. "Introduction to Security and Privacy on the Blockchain." 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, 2017.
[6]Ayed, Ahmed Ben. "A conceptual secure blockchain-based electronic voting system." International Journal of Network Security & Its Applications 9.3 (2017): 01-09.
[7] Kshetri, Nir and Voas, J. (2018)." Blockchain-Enabled E-voting ", IEEE Software 35(4), 95-99.
[8] Hjálmarsson, Friðrik Þ., et al. "Blockchain-based e-voting system." 2018 IEEE 11th International Conference on Cloud Computing (CLOUD). IEEE, 2018.
[9] Hardwick, Freya Sheer, et al. "E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy." 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2018.
[10] Yavuz, Emre, et al. "Towards secure e-voting using ethereumblockchain." 2018 6th International Symposium on Digital Forensic and Security (ISDFS). IEEE, 2018.
[11] Shejwal, Pallavi, et al. "E-voting using blockchain Technology." IJRAR-International Journal of Research and Analytical Reviews (IJRAR) 5.4 (2018): 895-906.
[12] Curran, Kevin. "E-Voting on the Blockchain." The Journal of the British Blockchain Association 1.2 (2018): 4451.
[13] Fusco, Francesco, et al. "Crypto-voting, a Blockchain based e-Voting System." KMIS. 2018.
[14]Patil, Harsha V., Kanchan G. Rathi, and Malati V. Tribhuwan. "A study on decentralized e-voting system using blockchain technology." International Research Journal of Engineering and Technology (IRJET) 5.11 (2018): 48-53.
[15]Chaudhari, KetulkumarGovindbhai. "E-voting System using Proof of Voting (PoV) Consensus Algorithm using Block Chain Technology." International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering 7.11 (2018): 4051-4055.
[16] Taş, Ruhi, and ÖmerÖzgürTanrıöver. "A systematic review of challenges and opportunities of blockchain for E-voting." Symmetry 12.8 (2020): 1328.