Secure Electronic Voting using Homomorphic Encryption and Blockchain

Dr. Jyoti neeli[1], Basvaraj P[2], Nandish P[3], Suraj Kumar M[4], Shrinidhi G Atgur[5]

[1]Associate Professor, Department of Information Science and Engineering,

Global Academy of Technology, Bangalore

[2,3,4,5]U G Student, Department of Information Science and Engineering,

Global Academy of Technology, Bangalore

Abstract: The discovery of Blockchain has drawn in tremendous interest as of late as it gives security and protection through unchanging disseminated record. Web based casting a ballot is a pattern that is picking up speed in present day culture. It can possibly diminish hierarchical expenses and increment citizen turnout. It takes out the requirement to printing polling form papers or open surveying stations-citizens can cast a ballot from any place there is a Web association. Because of its cordial agreement instrument and sealed information capacity, it is generally embraced in the fields where trust is given utmost prominence. Encryption using homomorphic calculations can be utilized towards work on the information as it is encoded without the information on private keys. Activities may be achieved on a encoded information without the need of unscrambling the information. An electronic democratic framework ought to be secure, and it shouldn't permit copy casts a ballot and be completely carefully designed, while safeguarding the protection of the electors.

Keywords: Homomorphic Encryption, E-voting, ballot entry, Web based Application

1. INTRODUCTION

Electronic Vote is based on the critical regions that can be fully utilized in blockchain development. The main concept behind electronic majority rule using Blockchain development is to acquire the relationship of modern cash. In the described plan, it furnishes citizens in the wallet which has client credentials for use. As the viable method for pursuing majority rule choices, decisions have for some time which is one of the social concern . As the number of votes cast, in reality, extends, occupants are ending up being more aware of the significance of the optional system. The democratic framework is one of the strategy which judge who is going to address in political and corporate governance. All Engineers from across the globe have made fresh democratic methods that will guarantee some enemy of defilement insurance while as yet guaranteeing that the democratic cycle ought to be right. Innovation presented the new electronic democratic procedures and techniques, which are fundamental and have presented huge difficulties to the majority rule framework. Electronic democratic increments political decision dependability when contrasted with manual surveying. Rather than the customary democratic strategy, it has upgraded both the proficiency and the uprightness of the cycle. As a result of its adaptability, straightforwardness of purpose, and modest expense contrasted with general races, electronic democratic is broadly used in different choices.

Electronic and internet casting a ballot framework can give more protection and uprightness than EVM. It additionally gives protection to the clients; as the qualified electors can project their votes utilizing their PCs or even cell phones, subsequently keeping up with obscurity. It likewise fabricates trust on the framework as it is on the web and totally an open framework. It can likewise expand the quantity of members' association.

2. RELATED WORKS

A Block of squares which contains trades is known as a Blockchain. It is invariable. Whenever trade to a square is added, it can't be changed. It moreover acts like a decentralized record that records trades between various social events. Any part can affirm the legitimacy and decency of the data has been added to the square. The squares incorporate trades. Starting square in the blockchain is called starting square. Whenever a client presents a trade to the association, a one-way hash is delivered including Homomorphic Encryption for the trade and it is taken care of inside the trade. This hashing of trade data is the best approach to keeping the trades secure and constant. A Merkle tree is made with these hashes which keeps the control of the trades that are added to the square. exactly when certain number of trades are added to the square, an arrangement instrument will be begun. Following endorsing the square, it will be added to the

chain and past square's hash is also added to the continuous square. Since the continuous square also contains the previous square's hash, expecting some interloper or software engineer endeavors to change the data inside the trades, they should, change the hash of the trade and the Merkle base of the square. Doing all these of the squares is genuinely burdensome and drawn-out cycle. Thus, when the data is taken care of in the blockchain, it is constant and can't be changed. Blockchains are moreover depicted as structures of verification.

3. PROPOSED METHODOLOGY

Political race Surveying is a perplexing structure and is also more costly system. It also presents a novel Secure, Insurance Protecting, with also useful political choice looking over thought which will use the concept of Web Development with GPRS Accessibility, Cloud Data Limit and also encryption using homomorphic algorithm. The proposed framework has 2 kinds of clients, engaged with directing the races. First one is Chief electoral officer and second one is Booth supervisor. Booth supervisor framework created along the elector's usefulness where the citizens are going to survey.
Chief electoral officer will go probably as the need might arise to do the configuration and its setting for political choice studying. Stall directors are the locale manages the people who are careful to add the resident's nuances into the system and has recuperation structure.
Citizens needs to go the Corner where the Stall supervisor check the citizen and permit him to survey on the Stall's PC where our it is racing to cast a ballot framework.
Benefit of Proposed Framework
1. Decentralized engineering.
2. Straightforward vote projecting interaction.
3. Manipulations of votes are nearly unimaginable.
4. Votes are stored transparently in cloud safely and precise arrangement.
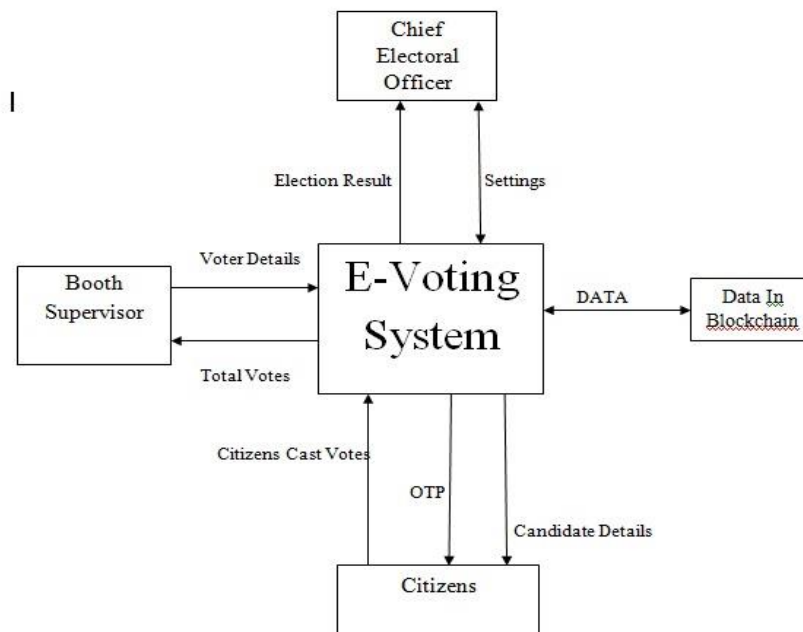

Fig. 1 – Architecture of E-Voting System

In Fig.1, Chief electoral officer will have the situation to perform addition, eradication or adjustment of the political race area list. Candidate nuances which includes name, party, age, and area can be checked, verified, adjusted, added or eradicated. Additionally, without a doubt, even the slow down nuances like the reference number, region and the slow down chief in-control ought to be apparent or modified. Chief electoral officer race official has the power and the mystery key to unscramble the particular votes of each contender from various slow down & proclaim the champion of political race region wise.
In Fig.1, Booth supervisor will have data about his stall with respect to reference number, stall area, number of competitors challenging for political race and all out number of citizens bound to cast a ballot in his corner. He has the position to see the citizen subtleties that have a place with his corner. He can add or erase any elector from the rundown.

In [Fig.1] Citizen is permitted to cast a ballot gave his elector id is legitimate and made his choice. This occurs under the stall administrator helps. In the wake of casting a ballot, Stall supervisor can see the complete votes, in a roundabout way addressing the absolute citizens surveyed yet individual votes per up-and-comer can be seen in the scrambled configuration.

Casting a ballot Interaction:
Citizen subtleties need to show according to the stall. The citizen's character is to be approved, whether he has a place with his doled-out stall and regardless of whether it has surveyed. Given he hasn't currently casted a ballot, he can make his choice. This vote will be scrambled and added to the specific contender to whom he/she has casted a ballot and this information is put away. The pattern of projecting a voting form is sorted out. All of the encoded votes will again be shuffled and mixed with the help of homomorphic encryption.
The votes first enter his qualifications and get an OTP welcome to his enrolled email address then he continues to get checked to cast a ballot
after client has a privilege to cast a ballot, he is permitted to cast a ballot in secrecy under the monitorization of officials and afterward it will continue to counting and show the ideal outcomes

Homomorphic Encryption
Homomorphic approach in Web and frameworks organization applications, security is huge concern in right now of IT. The gigantic proportion of information exchanged across the Web is vulnerable against security risks and attacks. Cryptography gives secure exchange of mixed data by shared key. The huge stress with this strategy is data security as anybody with the key can get to the data. In expansion, client loses control over data once it is moved to the cloud Client should give a key to play out any exercises. It requests to download and unscramble the data and thereafter play out the movement. These procedures lead to security issue and repeated encryption translating. So, in this framework it is ideal to go for Homomorphic encryption. A homomorphic encryption procedure grants client to chip away at ciphertext. Exactly when client deciphers the resultant figure, it is same like undertakings are done on plaintext. As such, using homomorphic encryption ensures clients that their data is secure in all state: storing, transmission and planning

4. LITERATURE REVIEW

The plan of any e-Casting a ballot framework ought to be fulfilling a number of essential and broadened prerequisites. Notwithstanding, it is difficult to fulfill these prerequisites at the same time. In [1], it proposed fostering an e-Casting a ballot framework requires the coordinated effort of numerous members with various foundation. In our framework, there are five taking part entertainers: Administrator, Recorders, Count Specialists, Applicants and Voters. sums up the taking part entertainers and their obligations. The plan of e-Casting a ballot Framework depicted in comprises of four phases: political race arrangement, enrollment, casting a ballot and counting. All of these phases are continuously, that is mean no analysis between one particular stage to another one. It acknowledges such that there is a Declaration Board (BB), which is understandable by everyone. This framework upholds multi-applicant decisions which has nC of candidates. Every elector Vi cast his decision in favor of every competitor. This vote might be Yes or No, this is identical to 1 and -1, separately.
The authors in [2], it has given the plan and execution of a solid and effective nearby e-casting a ballot framework in light of the homomorphic encryption which ensures the positive security prerequisites like protection, qualification, unquestionable status, receipt-freeness and so forth. The definite rundown of fulfilled necessities and utilized cryptosystems for every module of our framework plan. Our framework has been worked with instructive purposes by carrying out cryptographic calculations, thinking about necessities of e-casting a ballot framework and fundamental security capacities. First as presents in, e-casting a ballot execution and plan ought to be assessed by cost of Parlier. Unique homomorphic arrangements can be additionally tried with this secluded plan furthermore, measure their efficiencies.
In [3], it describes Completely Homomorphic Encryption (FHE) □ FHE can play out any activity straightforwardly on encoded information by changing over it into a circuit of a specific profundity □ FHE incorporates four essential calculations: Keygen, Scramble, Decode, and Eval. □ Eval calculation is constructed in light of three unique calculations: Add, Mult, and Recrypt. Recrypt activity: cleans the ciphertext from the commotion. Framework intricacy∘ FHE requires a cross section-based cryptosystem that is altogether more complicated than PHE cryptosystems.□ Monstrous ciphertext sizes∘ While utilizing suggested security boundaries, ciphertexts delivered are on the request for 128MB and a public key of 128PB, which are just not reasonable. Calculation time the key size is still on the request for a few GB, with encryption of solitary piece actually expecting as long as 30 minutes.
The article in [4], it represents Obviousness (both all-inclusive and individual) in electronic democratic is turning out to be more also, more significant. In the wake of having talked about these procedures for a really long time in the research local area, this currently should be carried out in future electronic democratic plans. Because of the way that these

strategies need to guarantee the mystery of the votes, the methodologies are somewhat muddled and experience the ill effects of various limitations. The main one is the hypothesis that an electronic democratic framework can by the same token guarantee unequivocal mystery or unqualified obviousness. Further, the political decision authority needs to conclude which obviousness approach it is agreeable to. This paper makes sense of the various methodologies from a general point of view to likewise empower non-security specialists to choose which strategy to utilize and what its benefits what's more, detriments are. Further, this paper tends to electors to assist them with understanding what the upsides of undeniable democratic plans are and how to utilize them.

The authors in [5], it has given Current blockchain e-voting system, this segment gives some foundation data on electronic democratic strategies. Electronic majority rule is a popularity-based technique where votes are recorded or counted using electronic equipment. Electronic majority rule is by and large described as it is maintained to project a voting form that by some electronic hardware and programming. Such consistencies ought to be skilled in supporting/carrying out different capacities, going from political race arrangement through vote capacity. Booths at political decision workplaces, workstations, and, all the more as of late, cell phones are all instances of framework types. Elector enlistment, confirmation, casting a ballot, and counting should be joined in the electronic democratic frameworks. One of the areas where blockchain may have a huge effect is electronic democratic. The degree of chance is extraordinary to the point that electronic democratic alone is definitely not a feasible choice. In the event that an electronic democratic framework is hacked, the outcomes will far-reach.

The authors in [6], It proposed electronic popularity-based structure close by taking care of the data which is stored in the blockchain, Homomorphic encryption is being used to encode the votes. In this encryption, time which is required to encode & unravel the vote will change along with the size of P, Q values. It has tried various tests on this structure with different P, Q values to learn about these times. Similarly, both of these keys (public private keys) which are used to encode as well as translate the votes will move along with its size of P and Q values. The data is taken care in the cloud, so it would be better accepting the size of keys which have some familiarity.

In [7], it explains unique, blockchain-based electronic democratic framework that uses brilliant agreements to empower secure and cost-effective political decision while ensuring citizens protection. it has illustrated the frameworks engineering, the plan, and a security examination of the framework. By correlation with past work, it has shown that the blockchain innovation offers an additional opportunity for popularity-based nations to progress from the pen and paper political race plot, to a more expense and time-productive political race conspire, while expanding the safety efforts of the present plan and deal additional opportunities of straightforwardness. Using an Ethereum private blockchain, it is possible to send hundreds of transactions per second onto the blockchain, utilizing every aspect of the smart contract tease the load on the blockchain. For nations of more noteworthy size, a few measures should be taken to keep more noteworthy throughput of exchanges each second, for instance the parent and youngster design which diminishes the quantity of exchanges put away on the blockchain at a 1:100 proportion without compromising the organizations security. Our political race conspire permits individual electors to cast a ballot at a democratic locale fitting their personal preference while ensuring that every individual citizen's vote is countervote right region, which might actually increment elector turnout.

The authors in [8], addresses the need of hashing in blockchain: The blockchain is a gathering of squares that contain data, each square has a hash pointer that contains past square's data, Thus, accepting that a developer endeavors to pursue a particular square, the progressions will be reflected to the entire chain of squares. Thusly, the blockchain thought is so moderate. Working: The SHA-256 computation takes a commitment of any unpredictable length and produces an aftereffect of a fixed length(256bits). On account of SHA-256 calculation regardless of how large or little is the info, the result is of fixed length (256 bits).

In [9], it presents a blockchain based e-projecting a voting form system that abrupt spikes popular for Ethereum. It demonstrates the way that blockchain advancement can overcome limitations of united majority rule structures. This execution uses Ethereum blockchain as an organization as well as data base for taking care of resident's records, rival nuances and votes. This execution utilizes smart arrangements. This execution is taken a stab at virtual client. In future it might be taken a stab at Ethereum test net with huge number of records. In future work, the reachability of blockchain based e-projecting a voting form system for gigantic extension political race should be analyzed.

The authors in [10], The proposition targets fostering an e-Vote-as-a-Administration in view of Blockchain conquering the limits of the current ventures utilizing a cloud-based approach. Regardless of whether a number of cloud suppliers, for example, IBM and Prophet are offering prepared to-utilize blockchain establishment on cloud with a charge in light of the quantity of exchanges, the test of adynamic and on-request framework design and optimization in view of end client's business necessities remains. The present methodology permits the end clients to indicate useful furthermore, non-practical prerequisites of administrations and the Cloud foundation where administrations are conveyed on request to advance expenses and administration execution.

The article in [11], it portrays The Hyperledger Sawtooth structure is a versatile construction it might be planned to go probably as a public blockchain network, or a permissioned one. This design comprises of a component called the trade processor, which gives a phase to the computational and business reasoning of blockchain, the wise agreement, to

execute. The validator in this blockchain network is responsible for endorsing the characteristic of the got block, directing it to the trade processor, and adding the square to the blockchain whenever it is sent back by the trade processor.
In [12], it presents Assurance OF THE Reasonable Innovation Stage TO Guarantee Obscurity, Protection, Furthermore, SECURITY The e-casting a ballot interaction requires the elements like security, obscurity, and unquestionable status as the center capacity of this arrangement, it is critical that the decision of the fundamental innovation is predictable to address these difficulties. It has been recognized that the Blockchain innovation adequately bargains with every single such test.
In [13], The proposed projecting a voting form show utilizes the blockchain to store the cast surveying structures, thusly in this setting the blockchain goes about as a clear surveying stall. The key avocation behind using the blockchain in an e-projecting a polling form show is to take advantage of reality that it engages a social affair to keep a public data base, that is guaranteed, revived, and stayed aware of by every client, nonetheless, obliged by no one. Since the show relies upon the blockchain, it will be recognized as an association of partners. Every voter will be a companion for instance a center point in an association of reciprocals. Every voter will be obligated for guaranteeing that bogus votes are excused, from now on that understanding is stayed aware of agreeing to the political choice standards. The blockchain similarly has the additional advantage of being dynamically outstanding and particularly trusted to function true to form, as affirmed by the sheer size of the cryptographic currency market.

The paper proposes an e-projecting a polling form plot, which is then completed. The execution and related execution assessments are given in the paper close by the hardships acquainted by the blockchain stage with make marvelous application like e-projecting a voting form. The paper includes a couple of deficiencies and presents two likely ways ahead to chip away at the key stage (blockchain advancement) to help e-projecting a polling form and other near applications. Blockchain advancement has a lot of assurance; regardless, in its current status it presumably will not show up at its most extreme limit. There ought to be deliberate effort in the middle blockchain advancement assessment to improve is components and sponsorship for complex applications that can execute inside the blockchain network.

Sl No	Author Name	Problem Statements	Techniques	Contributions	Limitations
1	UzmaJafar ,MohdJuzaiddin Ab and Zarina Shukur	The paper provi overview Blockchain-based electronic systems.	Public key Encrypti Digital Signatures	This paper provi introduction Blockchain Technology.	
2	Prof. Anita A. Lahane, Junaid Talif Pathan and Pra Potdar ,Juhu Versova	E-voting model could address such as vote tamp	SHA-256 algorithm Elliptic Curve Signature Algorithm	Elliptic Cryptography is encrypt block Blockchain.	In the front end application, there lack of la compatibility.
3	Vivek S K, Yashank R S	An Expl Literature Revie Blockchain-Base Voting Systems	Public Key Encr Digital Signatures	This paper prov brief overviev current researc Blockchain-base voting.	Because most tech is still primitive paper did not pro clear conclusion the technologies t be used.
4	Basit Shahzad And Jon Crowcro	This paper prop framework for er data privacy employing an ef hashing technique	SHA 512 and Bloc technology	This paper provi overview of voting system ba Blockchain, blocks hashed SHA 512.	The system doe employ homon encryption.
5	Kriti Patidar, Dr. Swapnil Jain	This study of blockchain-based voting system solves some o constraints of e voting systems.	Smart Contract (Ethereum)	This paper descr Ethereum-based voting system.	The use of contracts and the homomorphic encr will raise the c implementation.

6	Emanuele Bellini Ceravolo,Ernesto Damiani	This article will p a new flexibl multifunctional electronic solution based blockchain archit	Blockchain Tech and SHA	The article provi outline of hov electronic system may be u as a service.	The most encryption tech are not used.
7	C. Sravani, G Murali	This article prop Blockchain bas voting System	Homomorphic Encryption,Paillier cryptosystem	This research provided an ov of the use of the l Cryptosystem in voting Process.	Paillier Cryptosys not as secure as most ad encryption system
8	Freya Sheer Hardwick, Ap Gioulis, Raja Naeem Akran Konstantinos Markantonakis	This article prop potential new e system that mak of the blockchai transparent ballot	Blockchain Tech and SHA-3	This article provi overview of the mechanism tha distributed technology.	Homomorphic Encryption is not as a Block Encr option.
9	Friðrik Þ. Hjálmarsson, Gunnlau	This article evalu blockchain-as-a-s application implementing distributed ele voting systems.	Distributed Technology and El Curve Cryptography	The article provi overview of application decentralised architecture.	The system pre here is ineffici terms of cost.
10	L. Tekin , H. G. Ozgur , B. Sa Karatas, P. Senkula, E. Irtem , Sahin1	This paper of Blockchain appli	Paillier cryptos elliptic curve crypto	This doc describes applications of cryptosystems.	Not scalable for democracy
11	Ihsan Jabbar and Saad Najim Als	The usage homomorphic encryption distributed technology is pr in this research.	El-Gamal Cryptos Blockchain Technol	This article expla use of the El- cryptosystem blockchain-base electronic system.	There is no use OTP method verification.
12	Mohamed Tarek Ibn Ziad Mc Hassan Supervised By Dr. Mohamed Shehata Bedour Dr. Mohsen Ali Alkabani	The use of Bloc technology for E- is proposed ir study.	SHA-256 Algorithm	This article provi overview of the of SHA-256 Blockchain-base voting.	The OTP method utilised for authentication verification.
13	RojanGharadaghy, Melanie Voll	This study provi overview and a of methods implementing verifiability.	Elliptical Cryptography	This paper prov quick overview verification Elliptical Cryptography.	

5. CONCLUSION

The goal of this investigation is to examine and evaluate energy research on blockchain based electronic majority rule systems. The article analyzes late electronic popularity-based assessment using blockchain advancement. The blockchain thought and its motivations are presented first, followed by existing electronic majority rule structures. Then, an absence of bundle of in existing electronic popularity-based systems are recognized and tended to. The blockchain's actual limit is key to redesign electronic majority rule, current responses for blockchain-based electronic vote based, and possible
research ways on blockchain-based electronic majority rule systems as sorted out in the project, if utilization of blockchain advancement along with mix of Homomorphic encryption, it would rather make more stronger electronic majority rule instrument which would change how choices are coordinated in future. It do not simply get the data, yet also further creates straightforwardness in popularity-based cycle. This would also moreover diminish the cost of races as it shouldn't worry about any upkeep by a central power.

REFERENCES

1. Jafar, U.; Aziz, M.J.A.; Shukur, Z. Blockchain for Electronic Voting System—Review and Open Research Challenges. Sensors **2021**, 21, 5874. https://doi.org/10.3390/s21175874

2. H. S. Govinda, Y. Chandrakant, D. S. Girish, S. Lokesh, Ravikiran and B. S. Jayasri, "Implementation of Election System Using Blockchain Technology," 2021 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), 2021, pp. 1-9, doi: 10.1109/ICSES52305.2021.9633828.

3. Lahane, Anita & Patel, Junaid & Pathan, Talif & Potdar, Prathmesh. "Blockchain technology based e-voting system". ITM Web of Conferences, 2020 Doi: 32. 03001. 10.1051/itmconf/20203203001.

4. S. K. Vivek, R. S. Yashank, Y. Prashanth, N. Yashas and M. Namratha, "E-Voting Systems using Blockchain: An Exploratory Literature Survey," 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), 2020, pp. 890-895, doi: 10.1109/ICIRCA48905.2020.9183185.

5. A. Kaudare, M. Hazra, A. Shelar and M. Sabnis, "Implementing Electronic Voting System With Blockchain Technology," 2020 International Conference for Emerging Technology (INCET), 2020, pp. 1-9, doi: 10.1109/INCET49848.2020.9154116.

6. C. Sravani, G Murali, "Secure Electronic Voting using BlockChain and Homomorphic Encryption" International Journal of Recent Technology and Engineering (IJRTE), September 2019, ISSN: 2277-3878,Volume-8, Issue-2S11

7. A. Pandey, M. Bhasi and K. Chandrasekaran, "VoteChain: A Blockchain Based E-Voting System," 2019 Global Conference for Advancement in Technology (GCAT), 2019, pp. 1-4, doi: 10.1109/GCAT47503.2019.8978295.

8. B. Shahzad and J. Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology," in IEEE Access, vol. 7, pp. 24477-24488, 2019, doi: 10.1109/ACCESS.2019.2895670.

9. K. Teja, M. Shravani, C. Y. Simha and M. R. Kounte, "Secured voting through Blockchain technology," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 1416-1419, doi: 10.1109/ICOEI.2019.8862743.

10. K. Patidar and S. Jain, "Decentralized E-Voting Portal Using Blockchain," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019, pp. 1-4, doi: 10.1109/ICCCNT45670.2019.8944820.

11. E. Bellini, P. Ceravolo and E. Damiani, "Blockchain-Based E-Vote-as-a-Service," 2019 IEEE 12th International Conference on Cloud Computing (CLOUD), 2019, pp. 484-486, doi: 10.1109/CLOUD.2019.00085.

12. F. Sheer Hardwick, A. Gioulis, R. Naeem Akram and K. Markantonakis, "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), 2018, pp. 1561-1567, doi: 10.1109/Cybermatics_2018.2018.00262.

13. F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, "Blockchain-Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2018, pp. 983-986, doi: 10.1109/CLOUD.2018.00151.

14. A. Singh and K. Chatterjee, "SecEVS : Secure Electronic Voting System Using Blockchain Technology," 2018 International Conference on Computing, Power and Communication Technologies (GUCON), 2018, pp. 863-867, doi: 10.1109/GUCON.2018.8675008.

15. Tekin, Leyla, Hüseyin Güven Özgür, Burcu Sayin, Arzum Karataş, Pelin Şenkula, Emre İrtem, and Serap Şahin. "EDU-VOTING: An educational homomorphic e-voting system.", International Conference on Advanced Technologies, Computer Engineering and Science (ICATCES'18), 2018, pp: 114-119

16. Jabbar, Ihsan & Alsaad, Saad."Design and Implementation of Secure Remote e-Voting System Using Homomorphic Encryption". International Journal of Network Security, 2017, 694-703. Doi: 10.6633/IJNS.201709.19(5).06.

17. Gharadaghy, Rojan & Volkamer, Melanie , "Verifiability in Electronic Voting - Explanations for Non Security Experts", CASED—Center for Advanced Security Research Darmstadt ,Technische Universität Darmstadt, 2010, pp: 151-162