A Decentralized and Immutable E-Voting System using Blockchain

Ashish Balti
Department of Information Technology
Terna Engineering College
Nerul, India
ashishbalti4@gmail.com

Abhishek Prabhu
Department of Information Technology
Terna Engineering College
Nerul, India
prabhuabhi02@gmail.com

Sanskar Shahi
Department of Information Technology
Terna Engineering College
Nerul, India
sanchu26shahi@gmail.com

Shrutika Dahifale
Department of Information Technology
Terna Engineering College
Nerul, India
shrutika.dahifale@gmail.com

Dr. Vrajesh Maheta
Department of Information Technology
Terna Engineering College
Nerul, India
vrajeshmaheta@ternaengg.ac.in

2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS) | 979-8-3503-3360-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICSCSS57650.2023.10169552

***Abstract*—Elections are an important event that is responsible for shaping democracies around the world, but still there are many populations around the world who do not fully trust the electoral system which has become one of the major concerns for democracies around the world. Even the world's greatest democracies, such as India and Japan, have a flawed legal system. Vote rigging, EVM (Electronic Vote Machine) hacking, election tampering, booth capture squares, etc. are the main causes of the problems in the current voting method utilized in these countries. It has proven challenging to develop an electronic voting system that is both secure and safe and that offers a higher level of security, fairness, and privacy than current voting techniques while simultaneously offering the transparency and flexibility. Replacing the existing pen-and-paper (ballot-based voting) approach with a new election system offers the potential to reduce fraud and increase security while also increasing efficiency. Blockchain is a technology that promises to increase the overall robustness and security of various e-voting systems. The paper outlines a great attempt to develop a trustworthy and efficient voting system using blockchain's properties, including its transparency and cryptographic foundations. The system offers end-to-end verifiability and satisfies the fundamental criteria for e-voting methods. The paper covers the electronic voting system and how it would work on the Multichain network.**

Keywords: Blockchain, Electronic voting machine, security, Transparency, Cryptography

I. INTRODUCTION

Elections, which provide the citizens of any country a chance to voice their thoughts by voting, are crucial to the democratic system in today's growing globe. Because voting is such an important aspect of our culture, the voting process should be transparent and trustworthy in order to assure participants of its legitimacy [1]. Nonetheless, voting management has evolved over time. Earlier democracies all around the world used paper ballots to vote. It then developed into electronic voting systems over time. Given the importance of the voting system, ongoing attempts have been worked to enhance its general efficiency and durability [2]-[4].

Significant research has been conducted on the electronic voting systems which will allow people to vote regardless of where or when they choose to vote using any kind of electronic gadgets [5], [6]. However, neither of these technologies have been implemented on a broader scale due to the internal safety risks or problems that such devices may bring correctness of the voting procedure. Satoshi Nakamoto invented Blockchain in 2008 using Distributed Ledger Technology (DLT) [7] – [10], [22]. Blockchain is a new technology having solid ccryptographic foundations that enables apps to use these capabilities to develop durable security solutions.[10]-[12]. It is a distributed, immutable, and unchangeable public ledger [13]-[24]. Since it keeps and distributes every transaction that has been made since it began, a block-chain is analogous to a data structure [15]. Essentially, it is a dispersed decentralized database which manages a comprehensive set of continuously accumulated data records that are protected from unauthorized tampering and amendment as network of computers (or nodes) verifies every transaction that takes place on the blockchain before it is added to a block and cryptographically linked to the previous block [16]. Without the network's consent, a block cannot be changed or removed after it has been added to the chain. Blockchain uses some cryptographic techniques to perform encryption & decryption to ensure security[17]. There are numerous types of cryptographic encryption methods that can be used for encryption and decryption. The private key and public keys are utilised to maintain integrity depending on the type of algorithms [18].

The use of blockchain technology in electronic voting [19] is compelling alternative to the traditional computerized voting system to have benefits such as safety, precautions, confidentiality, and decentralized operations [20],[21]. It is used for both public voting and board meetings voting.. A blockchain was once just a chain of blocks, but it's now a growing list of blocks connected by cryptographic linkages [21]. The transaction data of each block would be a hash, a time stamp, and the transaction details of the prior block. The Blockchain is planned to be resistant to loss of information.[21]-[24]. Researchers are attempting to exploit features as openness, secrecy, and non-repudiation, which are required for various polling applications. Efforts are made such as leveraging blockchain innovation to safeguard and get transparency in election system.

979-8-3503-3360-2/23/$31.00 ©2023 IEEE

II. Literature Survey

A. Votereum: An Ethereum-based E-voting system :

This paper reviews the requirements and propose an Electronic voting system which uses blockchain technology. The Ethereum platform powers the proposed system, which consists of two servers: one in charge of system administration and the other taking care of all demands pertaining to blockchain technology. A Rinkeby testing network deployment is also made as part of the implementation's evaluation of its viability. It is made up of an interface created using the Angular framework, two working NodeJS servers, and a smart contract written in the Solidity language. The purpose is to lessen the trust in the government and improve voting fairness. This system also includes the start and end-time voting feature. Due to this, it helps to provide fairness to the voting system [20].

B. Secure Digital Voting System based on Blockchain Technology:

It presents an attempt to develop a successful system for electronic voting by utilizing the advantages of block-chain, such as their cryptographic underpinnings and transparency. The proposed electronic voting system is described full in the article, along with how it will be implemented on the Multi-chain platform. The suggested solution delivers end-to- end verifiability and transparency and complies with the key criteria for e-voting schemes. The technology demonstrates its capacity to create a digital voting system that guarantees end- to-end verifiability [21].

C. Decentralized Voting Platform Based on Ethereum Blockchain:

In this paper, it discusses implementation based on the blockchain used by Ethereum, a distributed election platform has been created. Software developers can install decentralized apps (DApps) on the Ethereum block-chain, an open- source platform for the distributed system with a full scripting language for Turing, and take advantage of the distribution attribute inherited from block-chain technology. The concept of Block-chain software is used in this system to deal with trust difficulties. Assuring data accuracy, full disclosure, and ensuring one vote per cell phone number for each vote with guaranteed anonymity are some of the system's key characteristics. The block-chain runtime environment for this is the Ethereum Virtual Machine (EVM) [22].

D. Survey on Blockchain-Based E-Voting Recording

It discusses one of the major sources of database tampering can be minimized by implementing block-chain for distributing of datasets on electronic voting machines. It talks about how to combine blockchain technology with current identity management systems, like Aadhaar, to create a trusted identity management system that will prevent fraudulent voting. For encrypting data fingerprint sensor has been used. But sometimes, this sensor could have some fault and thereby it might not be able to detect fingerprints properly. This system will be free from the issue of anonymity and fear of tracking and surveillance [23].

E. Blockchain Based E-Voting Recording System Design:

The paper proposed a blockchain based database recording method for electronic voting. A block-chain permission is employed in this electronic voting system, meaning users with the permission can access the blockchain. This approach seeks to protect data integrity from manipulations that shouldn't take place throughout the voting process. Before starting the voting process, every node creates a public key and a private key. All candidates named in the election process would receive the public key for voting. Every node collects the voting results from each participant once the election has taken place. On the entry of the block on every single node, inspection is done to examine if the block has the validity or not. So, after verification is done then the node is validated to verify his/her identity If a node is given a turn during the formation of a block chain, it will generate a block that has a digital signature filled out to be broadcast to all other nodes in order to prevent collisions and guarantee that every node is included in the chain. The transmitted block includes the node's unique ID, the subsequent node's unique ID that will be used as a token, a date, the outcome of the poll, the preceding node's hash value, and the node's electronic signature [24].

III. PROPOSED SYSTEM

E-voting has evolved through time to be supplementary to paper-based voting in order to decrease errors and expedite the vote-counting process. Nevertheless, like with any technological device, there are flaws in safety and confidentiality. This is a drawback of electronic voting machine that is employed in the election of governments across the world. A system has been developed that allows a voting application in an actual- world scenario while taking particular requirements like confidentiality, eligibility, simplicity and verifiability into mind. A secure online election process is what the suggested technology intends to provide. In this sense, the system is well- built with a web-browser based user interface that encourages simple user participation with features such as terminating voting after a set amount of time to prevent double voting. A easy to use administrator dashboard is created to make it simple to manage participants, audiences, and contenders for constituencies. Additionally, the method guarantees every voter the same rights to participate and promotes a level playing field for all candidates, all the while safeguarding voters' anonymity.

A. Algorithm

Working:

A message of any length can be input into the cryptographic hashing method SHA-256, which outputs a fixed-length 256-bit hash result as shown in Fig1. The algorithm converts the message into the final hash value using a sequence of logical operations and bitwise operations. No matter how big or little the input is, the SHA256 algorithm's output is always 256 bits long. The advantages of SHA-256 include its ability to provide a fixed-length output for every input of any length and its defence against collisions and preimage attacks. This makes it a well-liked option for safe data transfer and storage. The characteristics of a cryptographic hash function are as follow:

Deterministic: This means that the same outcome will occur even if the same input is used over.

Fast Computation: This indicates that the outcome is produced rapidly, which increases system efficiency.

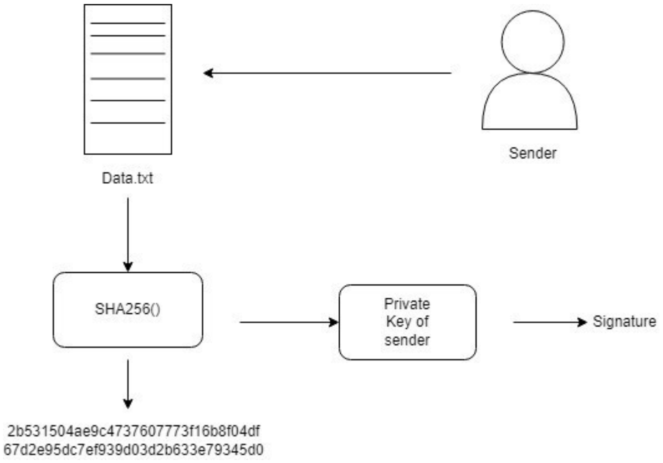

Data.txt
Sender
SHA256()
Private
Key of
sender
Signature
2b531504ae9c4737607773f16b8f04df
67d2e95dc7ef939d03d2b633e79345d0

Fig. 1. Working of SHA-256 algorithm

Pre-Image resistance: Imagine a dot is rolled and instead of a particular number, a hash value is received. The hash value of each integer can be computed and then can be compared to the result. Besides that, with bigger data sets, the brute force approach may be used to break pre-image resistance, but this takes so long that it is ineffective. Slight adjustments in the input affect the entire result: A small alter in the data impacts the entire result.

Slight changes in input affect the entire output: A small alter in the data impacts the entire result.

Collision-Resistant: Each data encrypted value will remain unique.

Puzzle-amiable: Hash value of a new variable is obtained by combining two values.

B. System Architecture

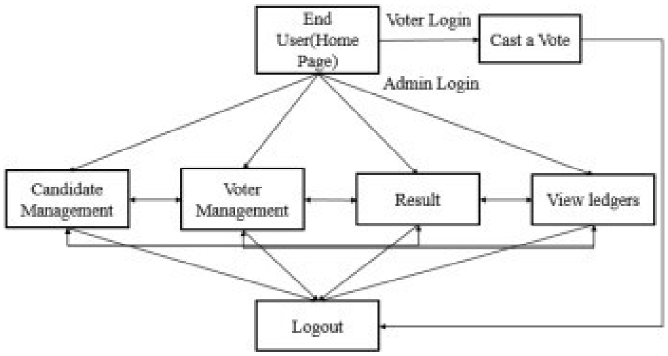


Fig. 2. System Architecture

As shown in the Fig no 2, the registration process is the first step in this system; confirming a voter is critical in establishing a systemsecurity. It is important to make sure that the same person cannot register again, especially when voting is involved because every vote counts. To allow users to register to vote, proposed system verifies whether the user is already in the database and whether he/she is eligible to vote, as the voting age requirement is more than 18 years. Following that, the voter is given a unique hash address with which he/she can vote. The vote can be placed only once. During the voting period, the voter will visit the system's voting section page and then cast a vote, after which they can log out of the system. Voters will come to know the voting results after the voting session is over. There would be an admin section for managing voters, add candidates of different party for voting, and change the phases of voting which includes the voting registration phase, voting phase and end of voting phase.

C. Details of Hardware and Software:

Software Requirements:

- UI development: Visual Studio Code
- Frontend web application: HTML, Bootstrap, Javascript,
- Database: Solidity
- Other tools: Metamask, Ganache

Hardware Requirements:

- Processor: Intel Quad-core 1.7 GHZ Processor or above
- RAM: Minimum 8 GB of RAM.

IV. System Flowchart

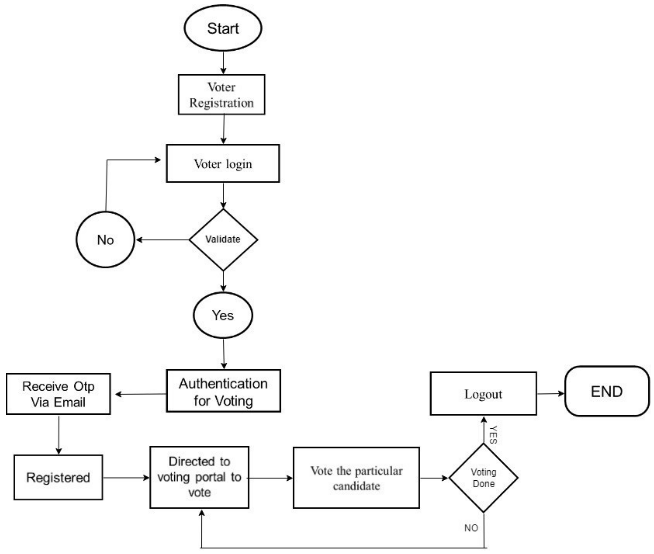


Fig. 3. Flow Chart of E-voting system

This System consists of two parts or the sections: First would be the admin, and the other would-be user. So, the workflow for the user as shown in Fig. 3 begin with the registration process, users will be required to register with the system by providing their personal details such as username, email address, cell phone number, day of birth, etc. All the information provided during registration process will get stored in phpMyAdmin. This data would be useful since it will allow the system to check whether the user is over the age of 18 years or not. If the user is under the age of 18, the system will not permit them to register. After the completion of the registration process, the user can login into the system and can start the voting process for elections. Voter authentication is the initial part of the voting procedure. To begin, the user must enter his or her Aadhar number and the specific address provided by the ganache. Following this, the user will receive an OTP on their email address, after which the authentication process would be completed. Once the authentication process is completed user is entered in the voting section where he/she can see all the candidates who have been nominated for the election and can cast vote to any one particular candidate. Once the user has casted his/her vote he/she will not be allowed to cast the vote again. Even if user will try to vote again, the metamask transaction for voting will not be carried out. Users will be asked to log out of the system after casting their ballots and the final results will be declared by the admin after the voting period is over. This way, the overall voting process will be executed. On the Admins side, the administrator will be able to add candidates for the voting process and will also be able to change different voting phases such as voter registration phase, voting phase, result declaration phase. The administrator would first log in to the system using the credentials. Then the admin can add candidates who are registering their nominations for the electoral process. A specific sum of gas fee will be deducted from the admin side to add the candidate of a particular party. The registered candidate's information along with his/her party name would then be displayed in the subsequent section. All the voters unique address details provided by ganache would be visible to admin.

V. Results and Discussions

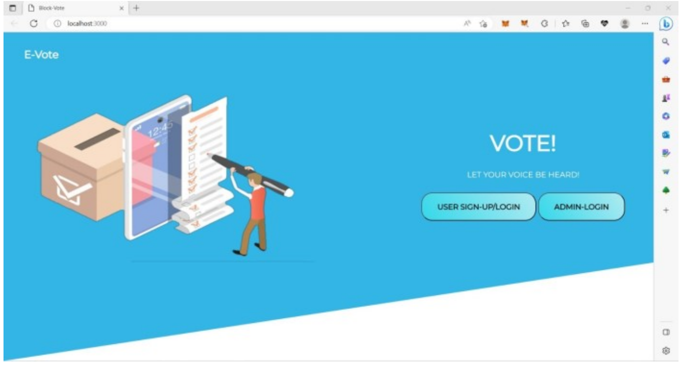
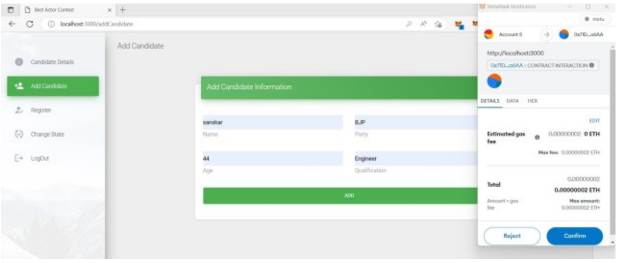


Fig. 4. Dashboard Page

Fig 4 shows the dashboard page of the E-voting system. It consists of the two sections, admin login page from where admin can login to the system and the user signup/login page, which user can use to register or sign in to the system.



Add Candidate Information

sanskar
Name

BJP
Party

44
Age

Engineer
Qualification

ADD

http://localhost:3000
0x71D...a6AA : CONTRACT INTERACTION

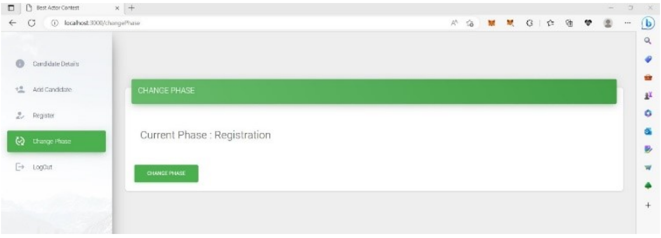
Estimated gas fee 0.00000002 0 ETH
Max fee: 0.00000002 ETH

Total 0.00000002
0.00000002 ETH
Amount + gas fee
Max amount: 0.00000002 ETH

Fig. 5. Admin Page

The admin page as shown in Fig. 5 is further divided into various sub-sections wherein the admin can add the candidates' information such as their name, age, the party that they belong to and their qualification. The candidate data would be added after the final transaction is carried out via the meta-mask after deducting a certain amount of gas fee. Gas fee refers to the transaction fee on the Ethereum block-chain.

It is the fees what users pay to get their transaction validated, or completed.

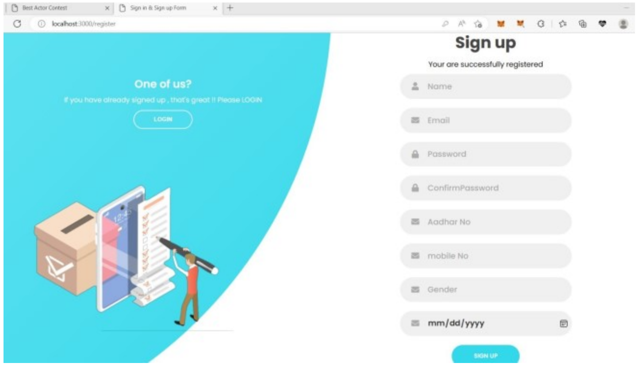


Current Phase : Registration

CHANGE PHASE

Fig. 6. Phase Change

Admin can also change the phases like registration, voting, and result declaration phase as per the voting requirements, as shown in Fig 6.

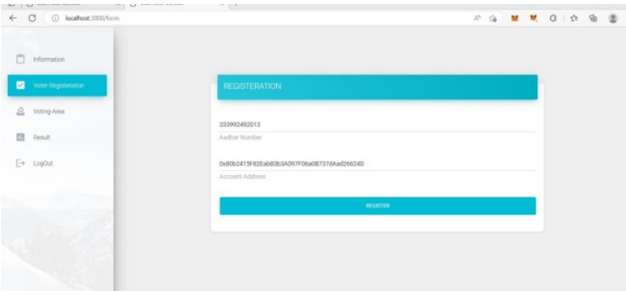


If you have already signed up , that's great !! Please LOGIN

Your are successfully registered

Fig. 7. User Login / Registration page

Fig 7, shows the user section of e-voting system, which is the user login and registration page which can be used by the user to register and login with the e-voting system wherein after the successful login of the user he/she will be directed to the voter authentication page during the voting phase.

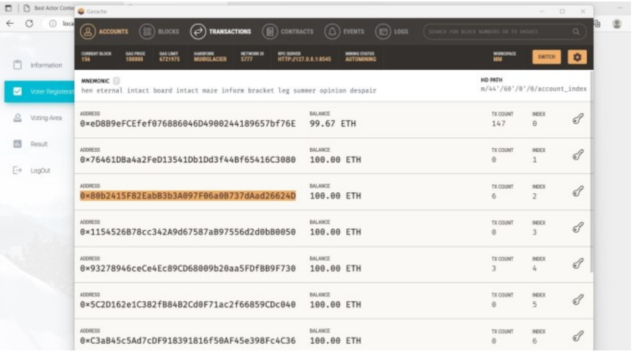


333992492013
Aadhar Number

0x80b2415F82EabB3b3A097F06a0B737dAad26624D
Account Address

Fig. 8. Voter Authentication Page

As shown in Fig 8, the user will be asked to enter their aadhar card number and the unique address generated by ganache for the authentication during the voting phase first.



CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
156	100000	6721975	MUIRGLACIER	5777	HTTP://127.0.0.1:8545	AUTOMINING	MM

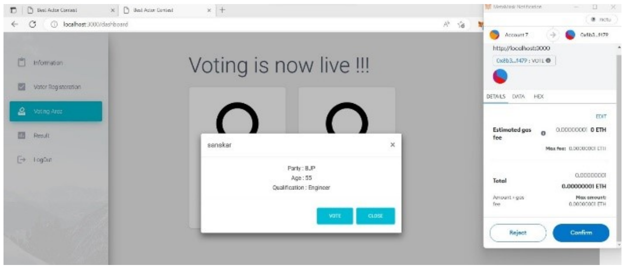
MNEMONIC
hen eternal intact board intact maze inform bracket leg summer opinion despair

HD PATH
m/44'/60'/0'/0/account_index

ADDRESS	BALANCE	TX COUNT	INDEX
0×eD8B9eFCEfef076886046D4900244189657bf76E	99.67 ETH	147	0
0×76461DBa4a2FeD13541Db1Dd3f44Bf65416C3080	100.00 ETH	0	1
0×80b2415F82EabB3b3A097F06a0B737dAad26624D	100.00 ETH	6	2
0×1154526B78cc342A9d67587aB97556d2d0bB0050	100.00 ETH	0	3
0×93278946ceCe4Ec89CD68009b20aa5FDfBB9F730	100.00 ETH	3	4
0×5C2D162e1C382fB84B2Cd0F71ac2f66859CDc040	100.00 ETH	0	5
0×C3aB45c5Ad7cDF918391816f50AF45e398Fc4C36	100.00 ETH	0	6

Fig. 9. Ganache

Fig. 9 shows the list of addresses which is provided on ganache software. From these list of addresses, user can use any one of these addresses as the unique address for their voter authentication process. Once the user clicks on authenticate button in voter authentication page, the individual will get an Otp through email which will be used to complete the whole voter authentication process. After the successful otp validation user will be directed to the voting page.



Voting is now live !!!

sanskar

Party : BJP
Age : 55
Qualification : Engineer

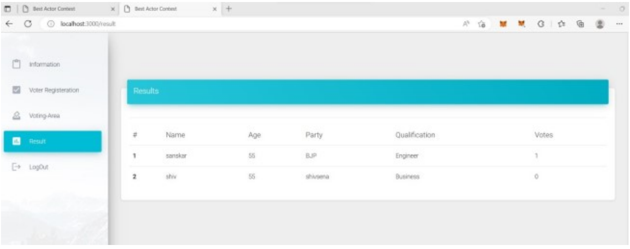
http://localhost:3000
0x8b3...f479 : VOTE

Estimated gas fee 0.00000000 0 ETH
Max fee: 0.00000001 ETH

Total 0.00000001
0.00000001 ETH
Amount + gas fee Max amount: 0.00000001 ETH

Fig. 10. Voting Section

Fig 10 shows the voting section, where user can see all the candidates who have been nominated for the election and user can cast vote to any one particular candidate from those candidates. Once the user has casted the vote he/she will not be allowed to cast the vote again by the system. Even if user will try to vote again, the metamask transaction for voting will not be carried out.



Results

#	Name	Age	Party	Qualification	Votes
1	sanskar	55	BJP	Engineer	1
2	shiv	55	shivsena	Business	0

Fig. 11. Voting Results

Once the election is over the admin can change the phase to the result phase and the voting result page is visible to all as shown in Fig. 11. Once the voting phase is completed, no voter will have the ability to cast their vote.. This system is developed and tested considering all aspects.

VI. CONCLUSION

In this paper, a block-chain-based electronic balloting system that makes use of smart contracts to enable safe and trustworthy and cost-efficient elections while safeguarding confidentiality of participants is discussed. Electoral security and integrity are ensured, and the foundation for transparency is laid, thanks to block-chain technology, which presents a new way to get over the drawbacks and hurdles of electronic voting systems. Implementing each properties of the smart contract to lighten the strain on the block-chain, it is possible to switch numerous transactions per second onto an Ethereum private block-chain. In the future to make the voting process more secure and to correctly identify the person who is voting one can use ML and AI concepts along with image processing. Using these concepts one can verify whether the person voting is the same as the person who has registered during the registration process based on the photograph uploaded by the voter during the registration phase.

VII. ACKNOWLEDGEMENTS

We would like to acknowledge entire staff of the Department of Information Technology, Terna Engineering College for their kind support and valuable guidance in successfully completing this work.

REFERENCES

[1] Elklit, J. and Reynolds, A., 2005. A framework for the systematic study of election quality. Democratization, 12(2), pp.147-162.

[2] Wolf, P., Nackerdien, R. and Tuccinardi, D., 2011. Introducing electronic voting: essential considerations. International Institute for Democracy and Electoral Assistance (International IDEA).

[3] Jafar, U. and Aziz, M.J.A., 2021. A state of the art survey and research directions on blockchain based electronic voting system. In Advances in Cyber Security: Second International Conference, ACeS 2020, Penang, Malaysia, December 8-9, 2020, Revised Selected Papers 2 (pp. 248-266). Springer Singapore.

[4] Adekunle, S.E., 2020. A Review of Electronic Voting Systems: Strategy for a Novel. International Journal of Information Engineering & Electronic Business, 12(1).

[5] Krimmer, R., Triessnig, S. and Volkamer, M., 2007. The development of remote e-voting around the world: A review of roads and directions. In E-Voting and Identity: First International Conference, VOTE-ID 2007, Bochum, Germany, October 4-5, 2007, Revised Selected Papers 1 (pp. 1-15). Springer Berlin Heidelberg.

[6] Gjøsteen, K., 2012. The norwegian internet voting protocol. In E-Voting and Identity: Third International Conference, VoteID 2011, Tallinn, Estonia, September 28-30, 2011, Revised Selected Papers 3 (pp. 1-18). Springer Berlin Heidelberg.

[7] Berentsen, A., 2019. Aleksander berentsen recommends "bitcoin: a peer-to-peer electronic cash system" by Satoshi Nakamoto. 21st Century Economics: Economic Ideas You Should Read and Remember, pp.7-8.

[8] Ferraro, P., King, C. and Shorten, R., 2018. Distributed ledger technology for smart cities, the sharing economy, and social compliance. Ieee Access, 6, pp.62728-62746.

[9] Holotescu, C., 2018. Understanding blockchain technology and how to get involved. The 14th International Scientific Conference eLearning and Software for Education Bucharest, April, 19, p.20.

[10] Liu, Y. and Wang, Q., 2017. An e-voting protocol based on blockchain. Cryptology ePrint Archive.

[11] Al-Maaitah, S., Qatawneh, M. and Quzmar, A., 2021, July. E-voting system based on blockchain technology: A survey. In 2021 International Conference on Information Technology (ICIT) (pp. 200-205). IEEE.

[12] Yi, H., 2019. Securing e-voting based on blockchain in P2P network. EURASIP Journal on Wireless Communications and Networking, 2019(1), pp.1-9

[13] Hj´almarsson, F.., Hreiarsson, G.K., Hamdaqa, M. and Hj´almt´ysson, G., 2018, July. Blockchain-based e-voting system. In 2018 IEEE 11th international conference on cloud computing (CLOUD) (pp. 983-986). IEEE.

[14] Febriyanto, E., Rahayu, N., Pangaribuan, K. and Sunarya, P.A., 2020, October. Using Blockchain Data Security Management for E-Voting Systems. In 2020 8th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-4). IEEE.

[15] Liu, Z., Luong, N.C., Wang, W., Niyato, D., Wang, P., Liang, Y.C. and Kim, D.I., 2019. A survey on blockchain: A game theoretical perspective. IEEE Access, 7, pp.47615-47643.

[16] Pawlak, M. and Poniszewska-Marańda, A., 2021. Trends in blockchain-based electronic voting systems. Information Processing & Management, 58(4), p.102595

[17] Sivaganesan, D. (2019). Block Chain Enabled Internet of Things. Journal of Information Technology, 1(01), 1-8.

[18] Roopak, T.M. and Sumathi, R., 2020, March. Electronic voting based on

virtual id of aadhar using blockchain technology. In 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 71-75). IEEE.

[19] Nagesh, H.R., Prasad, G., Shivaraj, B.G., Jain, D., Puneeth, B.R. and Anadkumar, M., 2022, December. E-Voting System Using Blockchain Technology. In 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N) (pp. 2106-2111). IEEE.

[20] Vo-Cao-Thuy, L., Cao-Minh, K., Dang-Le-Bao, C. and Nguyen, T.A., 2019, March. Votereum: An ethereum-based e-voting system. In 2019 IEEE-RIVF International Conference on Computing and Communication Technologies (RIVF) (pp. 1-6). IEEE.

[21] Khan, K.M., Arshad, J. and Khan, M.M., 2018. Secure digital voting system based on blockchain technology. International Journal of Electronic Government Research (IJEGR), 14(1), pp.53-62.

[22] Khoury, D., Kfoury, E.F., Kassem, A. and Harb, H., 2018, November. Decentralized voting platform based on ethereum blockchain. In 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET) (pp. 1-6). IEEE.

[23] Bhavani, G., 2018. Survey on blockchain-based e-voting recording system design. International Journal of Innovative Research in Science, Engineering and Technology, 7(11).

[24] Hanifatunnisa, R. and Rahardjo, B., 2017, October. Blockchain based e-voting recording system design. In 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA) (pp. 1-6). IEEE.