Decentralized E-Voting System Using Blockchain

Prajwal Shiwal
Student , Computer EngineeringTrinity Academy of Engineering
Pune , India

Harshad Shivankar
Student , Computer Engineering Trinity Academy of Engineering
Pune, India

DhruvMorey
Student ,Computer Engineering Trinity Academy of Engineering **Pune, India**

Suraj Jagtap
Student , Computer EngineeringTrinity Academy of Engineering **Pune, India**

Prof Sushadevi Shamrao Adagale
Professor , Computer EngineeringTrinity Academy of Engineering **Pune, India**

***Abstract*—Election procedures must be legitimate, precise, secure, and easily accessible. Because of blockchain technology, our suggested approach delivers security, sequestration, and integrity. In blockchain, every stoner or knot is confidential, and all activity is a sale that is encrypted and kept on the network. We tested our solution on the Ethereum blockchain platform, which generates smart contracts. The foundation of the blockchain system is smart contracts. The implementation of smart contracts guarantees a safe way for name authentication, certifying the correctness of voting results, allowing people to view the counting process, and avoiding malicious voting.**

Keywords: Blockchain Technology, Smart Contracts, Ethereum, Encryption, etc.

I. INTRODUCTION

Voting is a procedure that is characterized as a person's ability to select their leaders. Voting is a crucial activity that gives citizens a say in who leads their nation. The electoral process need to be widely accepted, impartial, and independent. As a result, it must be a clear and secure process that enables everyone to express their opinions without restriction. Many people around the world have lost faith in the electoral process. Traditional voting is regulated and replete with intercessors. Similarly, Individuals are coping with wide range of problems, such as cell prisoners, ersatz voting and the issue of adequate supervision, a long queue of voters in the midst of voting kiosks, illegitimate casting their votes, pre-voting, casting spare votes, an inadequate level of understanding, polling places being far from the homes, etc. The following issues can be resolved utilizing blockchain technology, which will result in a reliable system that one can trust to be honest. Blockchain is a decentralized network in which participants trade data but each stoner keeps a copy of the same data. Blockchain technology offers features like data segregation, delicate handling, and other comparable ones. Because of the consolidated voting area, it is impossible for voters to keep track of their votes while using an EVM (Electronic Voting Machine). As a result, voters have absolutely no means of acknowledging if their vote went to the intended candidate or was misdirected into the account of another voter. To ensure that their vote has been securely counted, choosers can utilise the blockchain to track their votes because it keeps everything as a sale and assigns a vote damage to each name in the form of a sale ID.

II. LITERATURE SURVEY

A. Related Works

Blockchain-based Decentralised E-Voting Portal. Dr. Swapnil Jain and Kriti Patidar. The research presented here provides an e-voting system based on blockchain that overcomes some of the shortcomings associated with conventional voting systems. The investigation additionally addresses the current condition of several blockchain fabrics fore-voting. The offered perpetration is suitable for small size alternatives such as within business homes, board homes, and so on.[1]

Decentralised voting by electronic means based on Smart Contracts and Blockchain Technology. Ali Mansour Al-Madani, Dr.AshokT. Gaikwad, Vivek Mahale, and ZeyadA.T.Ahmed are among those who made significant contributions to this work. Using blockchain, this article recommends to provide an E-voting system with high levels of safety. Blockchain delivers a decentralised conduct that makes the network reliable, safe, adaptable, as well as capable of supporting real-time services.[2]

DVT Chain is a blockchain-based decentralised medium that assures the security of digital systems for voting. Syada Tasmia Alvi, Mohammed Nasir Uddin, Linta Islam, and Sajib Ahamed are among the contributors. The approach outlined in this paper allows namer obscurity by maintaining the namer information in the blockchain as a hash.[3]

Design of an E-Voting Recording System Based on Blockchain. Huaimin Wang, Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Zibin Zheng. This article conveys an overview of blockchain infrastructure and compares multiple standardised algorithms implemented in various blockchains.[4]

Blockchain Technology underpins a safe digital voting system. Budi Rahardjo, Rifa Hanifatunnisa. The study gazes at the recording of outcomes of voting using the blockchain technology from every voting site.[5]

Headliners are developing a decentralised electronic voting

system based on blockchain technology. Alexandr Kuznetsov, Kateryna Isirova, Anastasiia Kiian, Mariia Rodinko, and Kateryna Isirova. The publication puts forward an innovative methodology for putting together a decentralised electronic voting system that uses blockchain technology.[6]

A system of decentralised voting. Aron Sandstedt, Jack Ahlkvist, Anton Gustafsson, Carl Lundborg, Joakim Mattsson Thorell Slavnic, Sanjin. This thesis explores the possible viability of a decentralised voting system and considers the probable concerns regarding sequestration, accuracy, and integrity.[7]

A powerful and efficient Decentralised Anonymous Voting System. Ja- Ling Wu and Wei- Jr Lai. In this paper, a featherlightE-voting practise is presented for voters to reduce their reliance on authority or government. We offers election full disclosure by putting all communication on the Ethereum blockchain; in the meantime, individual namer sequestration is protected by a secure and effective ring hand medium.[8]

Blockchain-based e-voting system. Albin Benny, Aparna Ashok Kumar, Abdul Basit, Betina Cherian, and Amol Kharat are among the cast members. We implemented and tested ane-voting as a smart contract for the Ethereum network utilising Ethereum and the dependability language in this design.[9]

A Discussion on Distributed Blockchain Technology for E-voting Systems. EmanS. Al- Shamery and Rihab H Sahib. This article provided a variety of various concepts for enforcing e-voting systems based on Blockchain, as well as how the druggies (choosers and campaigners) interact with the system, demonstrating the voting process from the initial step of registration through authentication to displaying the final results.Users are verified using their mobile phone numbers, eliminating the requirement for a third-party garçon. The results demonstrated that the system is feasible and may provide a step towards perfect environments for comparable experiences.[10]

Review and Open Research Challenges for Blockchain in Electronic Voting Systems. Zarina Shukur, Mohd Juzaiddin Ab Aziz, and Uzma JafarThe following composition provides an overview of blockchain-based electronic voting methods. The primary goal of this research was to evaluation the present state of blockchain-based voting exploration and online voting systems, as well as any associated obstacles, in order to forecast future advances.[11]

Platform for Decentralised Voting Based on the Ethereum Blockchain. ElieF. Kfoury, Ali Kassem, and Hamza Harb. In this work, they suggest a novel solution for a decentralised uncertain voting platform.[12]

Blockchain-Enabled E-Voting. Nir Kshetri and Jeffrey Voas. In this paper Blockchain-enabled e-voting (BEV) could reduce voter fraud and increase voter access. Eligible voters cast a ballot anonymously using a computer or smartphone. BEV uses an encrypted key and tamper-proof personal IDs. This article highlights some BEV implementations and the approach's potential benefits and challenges.[13]

Blockchain-Based E-Voting System. Friorik P. Hjalmarsson, Gunnlaugur K. Hreioarsson, Mohammad Hamdaqa and Gisli Hjalmtysson. The paper proposes a novel electronic voting system based on blockchain that addresses some of the limitations in existing systems and evaluates some of the popular blockchain frameworks for the purpose of constructing a blockchain-based e-voting system.[14]

A Critical Review of Blockchain and Its Current Applications. Bayu Adhi Tama, Bruno Joachim Kweka, Youngho Park and Kyung-Hyune Rhee. This paper discusses about The decentralized transaction ledger of blockchain could be employed to register, confirm, and send all kinds of contracts to other parties in the network. In this paper, we thoroughly review state-of-the-art blockchain-related applications emerged in the literature. A number of published works were carefully included based on their contributions to the blockchain's body of knowledge.[15]

Election Voting Using Block Chain Technology. Hiren M Patel, Milin M Patel and Tejas Bhatt. This paper discusses about the how blockchain technology can be used to implement Election Voting while solving issues like security, integrity and ambiguity.[16]

E-voting with blockchain: an E-voting protocol with decentralisation and voter privacy. F. S. Hardwick, A. Gioulis, R. N. Akram, and K. Markantonakis, This paper discusses about the The protocol that has been designed to adhere to fundamental e-voting properties as well as offer a degree of decentralisation and allow for the voter to change/update their vote (within the permissible voting period). This paper highlights the pros and cons of using blockchain for such a proposal from a practical point view in both development/deployment and usage contexts.[17]

III. METHODOLOGIES

• HASH FUNCTIONS

A hash function is a deterministic function that converts arbitrary (large) input into a fixed-size integer. A hash function's objective is to characterise an input by utilising the output fixed-size integer. According to the description above, a hash function is a function that computes an output as a manner of characterising an input. SHA256 is a well-known hash algorithm that converts any message (a text) into a binary number of 256 bits (which is often expressed as a 64-digit hexadecimal number)

• MERKLE TREE

A Merkle Tree is a method of storing potentially massive amounts of data while offering a simple means for the user to ensure that the data has not been updated. Consider a hash function H and the following data set to construct a Merkle tree: D = {d1, d2, ... , dn} The hash values of the items within D are used to generate the tree's leaves: H(d1), H(d2), and so on. The tree may then be built recursively.

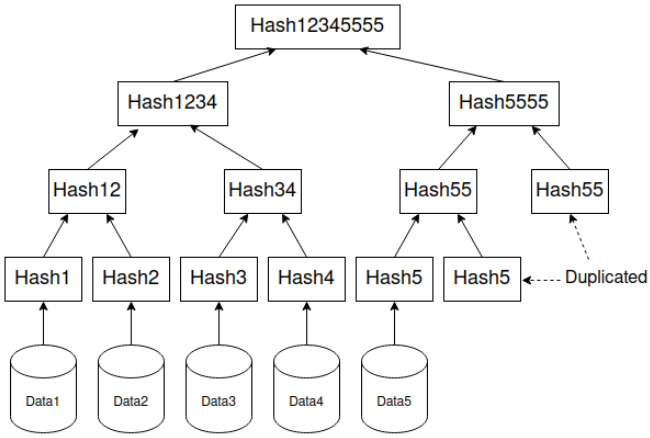

Fig. 1. **Merkle Tree**

• RSA Alogorithm

Ron Rivest, Adi Shamir, and Leonard Adleman created the RSA algorithm, which is an asymmetric cryptographic algorithm. Their study was initially published in 1977, and asymmetric meaning that it operates with two separate keys, namely public and private keys. The Public Key is distributed to everyone, whereas the secret Key is kept secret, as the name implies.

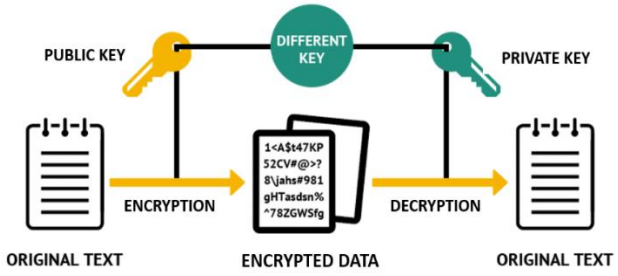

Fig. 2. **RSA Algorithm**

IV.RESULTS

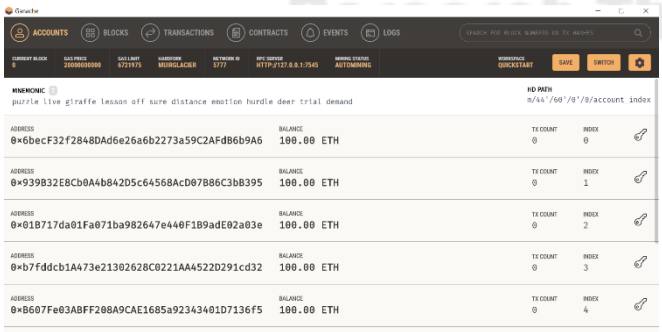

Fig. 3. **Ganache UI**

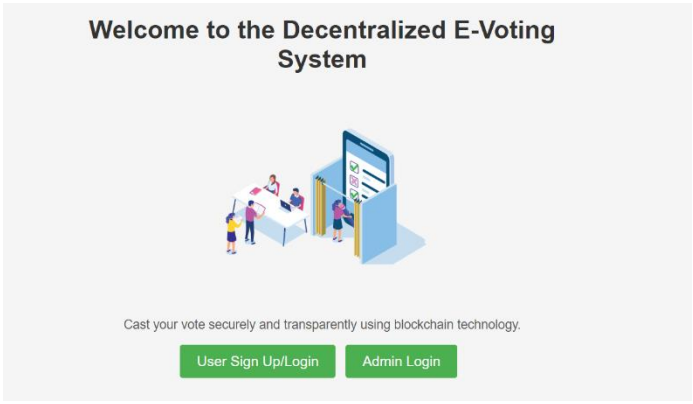

Fig. 4. **Home Page UI**

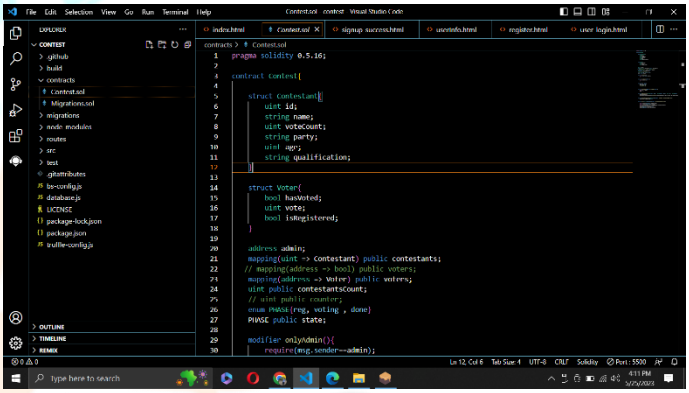

Fig. 5. **Smart Contract**

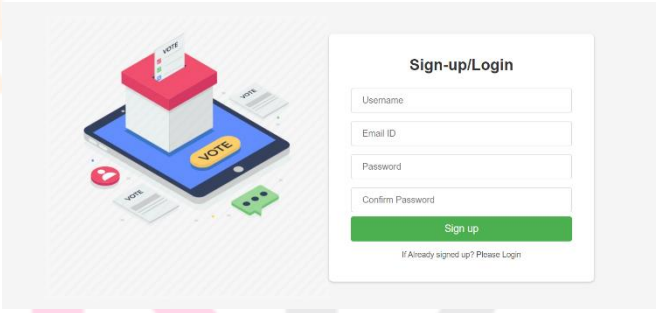

Fig. 6. **User Signup**

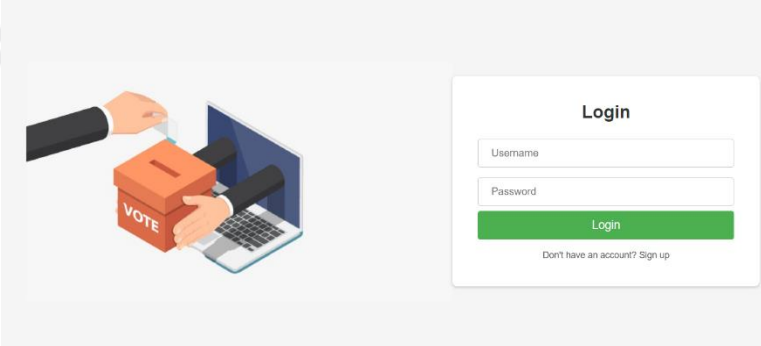

Fig. 7. **User Login**

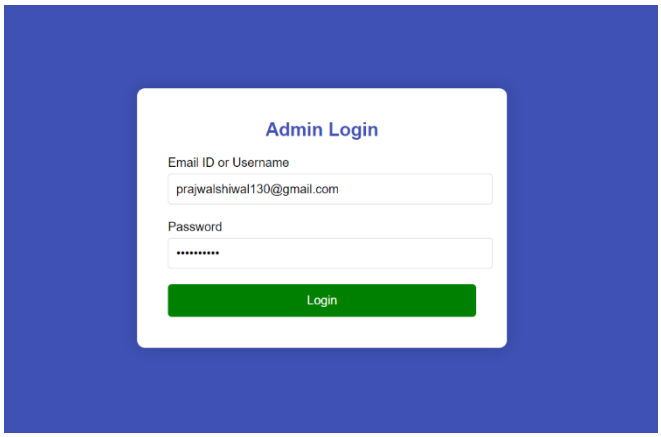

Fig. 8. **Admin Login**

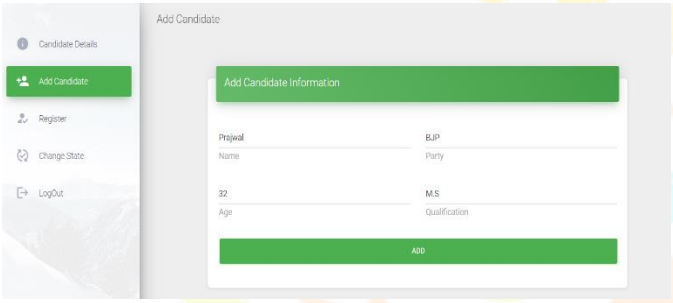

Fig. 9. **Add Candidate Details**

V.CONCLUSION

Several countries confront critical concerns about voting system stability. Considering the electorate's participation and credibility,The legitimacy of polling data, along with non-manipulative vote counting, we created a digital voting mechanism built on blockchain utilising smart contracts. In this medium, three smart contracts accomplish multiple responsibilities of the complete voting procedure. As a result, involvement from outside parties tends to be less than in other being systems. The translated votes remain preserved till the election is concluded. As a result, no bone can figure out the association between vote and namer. We encrypted the namer's information so that nobody in the network can identify the namer. The data is then saved as a hash rather than complete information, which reduces the cost. After the election has ended, voters can also use the vote id they received at the time of voting to confirm their vote. This approach allows choosers to bounce for their seeker from all around the world using smart bias. This would lead to growing the number of votes requisite for successful republicanism in every region. In summary, our system may be deployed smoothly in the election process since it serves as maximum safeguards such as obscurity, integrity, security, sequestration, fairness, verifiability, and mobility.

This system works on Ethereum. It demonstrates how blockchain technology may solve the shortcomings of centralised voting methods. This performance makes use of the The Ethereum blockchain performs the roles of a network of nodes as well as a database for recording namer accounts, candidature information and and votes. This performance employs smart contracts. Blockchain has a bright future ahead of it, with the opportunity to confront multiple states real-world obstacles that arise from having to rely on third-party centralised authority in everyday affairs. People ambition a less misty system that ensures everything is crystal unmistakable while at the same time safeguarding the confidentiality and reliability of their (stoners') data. Blockchain-based voting systems would definitely unquestionably minimise all of the hurdles that people or inhabitants of a particular nation have and give them with an atmosphere in which they will no longer have to rely on and commit to these old practises. When we saw a smash in the Web 2 period, which is the fleck com period, everything was digitalized but also consolidated, nevertheless this revolution of Web 3 period brings a lot of alarming and one incrementally beyond cutting edge technology by removing the barricade of reliance, which will be espoused by the tech sedulity truly soon and also increasing the number of participants.

VI.REFERENCES

[1]Kriti Patidar and Dr. Swapnil Jain "Decentralized E-Voting Portal Using Blockchain".10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019.

[2]Ali Mansour Al-madani, Dr.Ashok T. Gaikwad, Vivek Mahale, Zeyad A.T.Ahmed, "] Decentralized E-voting system based on Smart Contract by using Blockchain Technology." June 05, 2021.

[3]Syada Tasmia Alvi, Mohammed Nasir Uddin, Linta Islam, Sajib Ahamed "DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system". Journal of King Saud University – Computer and Information Sciences 34, 6855–6871,2022.

[4]Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang "Blockchain Based E-Voting Recording System Design". Institut Teknologi Bandung, 2017.

[5] Rifa Hanifatunnisa, Budi Rahardjo" Secure Digital Voting System based on Blockchain Technology." 'IGI Global' 1 May 2018.

[6]Kateryna Isirova, Anastasiia Kiian, Mariia Rodinko and Alexandr Kuznetsov "Decentralized Electronic Voting System Based on Blockchain Technology Developing Principals." CEUR-WS.org/vol-2608/

[7]Jack Ahlkvist, Anton Gustafsson, Carl Lundborg, Joakim Mattsson Thorell, Aron Sandstedt Sanjin Slavnic, "A Decentralized Voting System." Department of Computer Science and Engineering Chalmers University of Technology Gothenburg, Sweden 2019.

[8]Wei-Jr Lai, Ja-Ling Wu, "An efficient and effective Decentralized Anonymous Voting System." International Conference on Financial Cryptography and Data Security. Springer, Cham2019.

[9]Albin Benny, Aparna Ashok Kumar, Abdul Basit, Betina Cherian and Amol Kharat "Blockchain based E-voting System." Benny, Albin, Blockchain based E-voting System ,July 11, 2020.

[10]Rihab H Sahib and Eman S. Al-Shamery, "A Review on Distributed Blockchain Technology for E-voting Systems".

ICMAICT Journal of Physics: Conference Series IOP Publishing, 2020.

[11]Uzma Jafar, Mohd Juzaiddin Ab Aziz and Zarina Shukur, “Blockchain for Electronic Voting System—Review and Open Research Challenges.” Review and Open Research Challenges. Sensors 21, 5874. https://doi.org/10.3390/ s21175874, 2021.

[12]David Khoury, Elie F. Kfoury, Ali Kassem, Hamza Harb, “Decentralized Voting Platform Based on Ethereum Blockchain.” Chance, vol. 23, no. 1, pp. 6–15, 2010.

[13]Nir Kshetri and Jeffrey Voas, "Blockchain-Enabled E-Voting."IEEE Software, pp. 95-99, 2018.

[14]Friorik P. Hjalmarsson, Gunnlaugur K. Hreioarsson, Mohammad Hamdaqa and Gisli Hjalmtysson, "Blockchain-Based E-Voting System."IEEE 11th International Conference on Cloud Computing, pp. 983-986, 2018.

[15]Bayu Adhi Tama, Bruno Joachim Kweka, Youngho Park and Kyung-Hyune Rhee, "A Critical Review of Blockchain and Its Current Applications."IEEE International Conference on Electrical Engineering and Computer Science (ICECOS) 2017, pp. 109-113, 2017.

[16]Hiren M Patel, Milin M Patel and Tejas Bhatt, "Election Voting Using Block Chain Technology."IEEE International Journal of Scientific Research and Review, vol. 07, no. 05, pp. 1-4, May 2019.

[17]F. S. Hardwick, A. Gioulis, R. N. Akram, and K. Markantonakis, "E-voting with blockchain: an E-voting protocol with decentralisation and voter privacy."IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, pp. 1561–1567, Halifax, Canda, August 2018.

Truffle : https://truffleframework.com.

Ethereum project : https://ethereum.org.

Ganache : https://truffleframework.com/ganache.