# A Blockchain-based Framework for Voting System on Ethereum Blockchain

Anshika Jain
*KIET Group of Institutions*
Delhi-NCR, Ghaziabad
ajain20032@gmail.com

Sejal Joshi
*KIET Group of Institutions*
Delhi-NCR, Ghaziabad
sejaljoshi2002@gmail.com

Sukrit Kaur Oberoi
*KIET Group of Institutions*
Delhi-NCR, Ghaziabad
Sukritoberoi2004@gmail.com

Yash Chawla
*KIET Group of Institutions*
Delhi-NCR, Ghaziabad
yashchawla1205@gmail.com

Vipin Deval
*KIET Group of Institutions*
Delhi-NCR, Ghaziabad
vipin.deval@kiet.edu

***Abstract*—With respect to centralized control, transparency, fraud risk, and voter privacy compromise, different electronic voting systems have certain limitations. Through various studies conducted on such topics, consideration is made on the need for such systems to become distributed to overcome the security and trust issues. Voting using a blockchain has been studied, but most implementations do not scale and include inefficient modes of access and mechanisms for duplication of votes. The work describes a blockchain-based electonic voting system utilizing Ethereum smart contracts for its functioning. Built using Solidity and Truffle and integrated with MetaMask for authentication, this system guarantees that each elector casts only one vote. It is secure and exhaustive in counting votes on an immutable blockchain ledger which prevents unauthorized access and data tampering as the risk has been eliminated through the use of centralized servers that pose threats. With these features, research is made easy and highly secured using the encrypted wallet facilities provided by MetaMask. The results indicate that this system assures transparency, anonymity, and fraud resistance thus making it a good alternative to traditional methods among others. Future work will focus on improving scalability, large scale usability, and adopting advanced cryptographic techniques to enhance security within this electronic voting system. The study, therefore, indicates that blockchain has an impact on developing very secure, transparent, and decentralized systems of voting.**

***Index Terms*—ethereum, blockchain, transparent, vote, ballot**

## I. Introduction

Opportunities to express political opinion or exercise basic rights of individuals are provided by voting systems. These offer legitimacy regarding the democratic process. The old-fashioned voting modes of doing paper ballots or centralized electronic systems have loopholes of manipulation, security, and transparency [1], [10]. With rapid technological innovation, aspects of election voter fraud, vote manipulation, and opacity in counting negatively affect public trust in the democratic process.

The developing technology regarding accountability, integrity, and trust through distributed ledger to secure each vote with immutable, decentralized storage could probably house an impenetrable voting environment in which threat nor relative view would not affect outcome of the voting [1].

Ethereum is the most favored platform among other blockchain platforms for developing decentralized applications such as voting systems [2], [6]. As already established, smart contracts are speedy, which allows the creation of self-executing agreements; with their advantages, all votes can be recorded and tallied very quickly without any mediators. The decentralized system would hence be expected to remedy this shortcoming of traditional voting methods, hence paving a way to a more trusted and safer electoral system in the digital age.

To summarize, the EtherVote system promises a safe and decentralized alternative to the disadvantages of both conventional and modern electronic voting systems. Phase one could be maybe realized with a UI being created on React.js and then linking the Gmail account utilized in the registration to receive a one-time password (OTP). This type of verification provides the assurance that one vote shall be cast by one single voter thereby increasing the integrity of the system. According to smart contracts deployed on the Ethereum blockchain, all operations related to the process of voting, beginning from identification of voter onwards to recording of vote, are maintained.Blockchain technology thus acts as a setting against fraud and manipulation since all transactions in favor of one: voting and identity become transparent and immutable [3], [4]. EtherVote then decentralizes the control of the vote so that no such overriding centralized authority may alter or meddle with the data.

This breakthrough combines security, privacy, and scalability, giving a sturdy infrastructure that makes digital elections more transparent and credible. The EtherVote system implements blockchain technology to enhance the voting process, efficiency, security, and transparency. Voter authentication using an OTP sent to the registered Gmail address assures the legitimacy of persons allowed to cast a vote. Every vote is stored via smart contracts on the Ethereum blockchain in a manner that is immutable and publicly verifiable in terms of its integrity. Thus providing accurate and fair results, manipulation and unauthorized alterations are made impossible [7]. Since no personal information is streamed into one repository, voter anonymity is sustained, and possibilities of data breaches are diminished. Such a distributed architecture renders attacks even harder.

EtherVote stands as a scalable, user-friendly system dealing with privacy issues and providing a secure, transparent, and trustworthy alternative to conventional means of voting. The proposed solution works along the lines of these securing and irrevocable transactions on the Ethereum blockchain to practically eliminate central control with its consequent manipulation. The system was then built as a prototype, simulating scenarios beyond the boundaries of the conventional methods to demonstrate its robustness and efficiency. The findings suggest that the blockchain-enabled electronic voting systems can stand as a safe and scalable alternative to the existing means. Potential further advancements may include large voter base scalability, improved encryption methods, and biometric authentication methods [3]. The technology is set to play an important part in transforming the electoral process and giving a more accessible, transparent, and secure electoral solution globally.

### A. MOTIVATION

In every democratic establishment, free, fair, and transparent elections characterize its polity; but electoral processes encounter different challenges, including voter fraud, ballot tampering, and loss of faith in the electoral outcome. Their operational methods are cumbersome, thus making them prone to human errors and being opaque. Automated voting systems, which might have gained some credibility for their advantages, have in practice become the battleground for cyber-attacks and centralised control, remaining the eroding evils of public and voter trust.

Problems in developing countries are thus lessened by the use of outdated methods, heavy costs of implementation, and limited access to modern accessible infrastructure. These inefficiencies often lead to disputes and voter apathy, thus assaulting the credibility of the elections in the first place. Hence, since there is no trustworthy and efficient voting system, public resources, time, and energy are wasted as well.

Thus, blockchain technology provides an answer to these problems by inserting decentralization, transparency, and immutability features. The project aims at improving election integrity through the design of a decentralised voting system based on the Ethereum Blockchain. This method guarantees secure and tamper-proof recording of votes using smart contracts, thereby enhancing public trust while at the same time reducing dependence on centralised authorities.

It is the intention of this project to have a robust yet cheap, easily scalable and user-friendly platform by which the democracies of developing countries will easily modernize elections and secure citizens' voices.

### B. STRUCTURE OF PAPER

The remainder of the paper is structured as follows. Section II contains the State of the Art. Section III enlightens us about the System Architecture. The detailed description of the Proposed Methodology is provided in Section IV. Section V tells us about the Algorithms used in the project. Section VI provides a detailed discussion of the method's Result, and lastly Section VII draws the final Conclusions and informs about the Future Scope.

## II. State of the Art

Multiple investigations have shown that centralized voting systems harbor multifold deficiencies such as vulnerability to fraud, privacy problems, and absence of transparency. These considerations hardly add merit to the need for a decentralized alternative based on blockchain technology. While blockchain can guarantee transparency and immutability, on the other hand, issues with scalability and accessibility remain ever-present.

Although initial attempts at electronic voting were usually cryptographic in design, by the turn of the century the field has witnessed the rise of blockchain-based systems that promise transparency and trustless-ness [10]. The combination of secret sharing and homomorphic encryption in the first blockchain e-voting scheme eliminated trusted intermediaries-from-voting without compromising vote anonymity and public verification [1]. Still, there was no way for participants to tally the results themselves. This loophole was later filled by an Ethereum-based design that employed ring signatures and stealth addresses, which allowed anyone on the network to self-tally on the vote without compromising privacy [2].

Yet self-tallying schemes still left the ballots vulnerable to being revealed before the time of tallying, so combine linkable ring signatures with threshold encryption to ensure that votes remain confidential until decryption prevent double-voting [6]. The earliest decentralized models were still dependent on external identity services, so a follow-up advanced one with a phone-identity verification through the Ethereum Virtual Machine (EVM) to enforce "one-person-one-vote" without involving any central server [3]. Meanwhile, analyses of web-based e-voting systems have highlighted the evils of centralized databases-data alteration and lack of real-time results-thus making a strong case for fully on-chain solutions [7].

The design is peer-to-peer, unlike any other design it provides flexibility to voters and strong cryptography through Elliptic Curve Cryptography. This allows voters to alter their ballot by the designated cut-off date, overcoming the static ring signature model [8]. Secure voting environments demonstrate a series of prototype DApps built using Truffle, Ganache, and MetaMask, yet lack the real-world diversity, legality, and difficulty of the interface [5]. A very explicit case study presents such DApps as crucial for enabling the donation workflow and lowering user friction so as to encourage adoption [9].

To some of these limitations on usability and scalability, such implementations have introduced low-gas ring-signature optimizations with stealth-address variations over Ethereum, which have actually lowered transaction costs, yet it remained to be tested in large-scale scenarios [12].Therefore, secret sharing in conjunction with aggregation on-chain homomorphically improved the efficiency of processing votes while large-scale deployment had not been tried until then [11]. The extensive survey of blockchain e-voting prototypes revealed the long-lasting threats of 51 percent attacks, leaking privacy, and uncertainties of governance while calling for formal audits and regulatory frameworks [16].

Biometric fingerprint authentication was directly embedded into smart-contract workflows, thus strengthening identity assurance without reintroducing any heavy infrastructure. Biometric fingerprint authentication turned out to be successful in greatly reducing identity fraud while creating hardware dependencies [15]. Finally, it is a full stack implementation that integrates optimized consensus tweaks wallet-based authentication and real electoral pilots, which shows that with appropriate tuning, latency, cost, and accessibility can be overcome at large-scale [18].

Blockchain indeed forms a likely solution to electronic voting systems given its apparent capacities to ensure data integrity and transparency [9]. There are, however, issues on scalability, voter authentication, and legal and regulatory challenges that require further studies. Current studies often lack the required characteristic of large testing, and no proven solution exists so far for real-world elections [10]. More research must be done to get around these practical barriers and provide real answers on a grand scale as the blockchain prevails as a likely remedy for received answers for age-old problems in voting systems [7].

## III. System Architecture

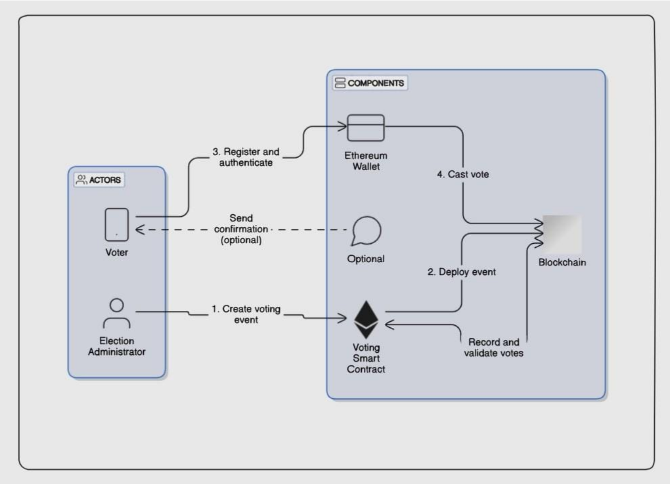


Fig. 1. System Architechture

The architecture of blockchain acts like a decentralized voting system that relies on interactions of transparency and robustness [1]. These are the main components and more general description of the work process:

- **ACTORS**

1) **VOTER**:People enroll, validate themselves, and cast their votes using Ethereum wallets, and they further use the system to vote carefully [5].
2) **ELECTION ADMINISTRATOR**: Planning, execution, and conduct of election procedures fall under this procedure. The overall integrity of the entire system, including the execution of smart contracts, is ensured by the administrators [3]. Must-have features. An election may differ in some aspects, such as the submission dates for papers, but it is bound to some basic method.

- **COMPONENTS**

1) **ETHEREUM WALLET**: Each vote is uniquely identified through cryptographic mechanisms. This works effectively in keeping all unauthorized people from accessing personal information [5].
2) **VOTING SMART CONTRACT**: It uses a smart contract based on the blockchain for voting. It is fully automated with regard to the procedures such as the generation, registration, and confirmation of votes, which means that there are middlemen [6].
3) **BLOCKCHAIN**:It is an unalterable, impermeable ledger recording and documenting all events around voting and actual votes cast. It causes total transparency for the whole process of voting while still verifying it [1].

- **WORKFLOW**

1) **CREATE VOTING EVENT**: This will lead to the commencement of the election, and the election official will make arrangements for conducting an event that will make provision for casting votes. By means of the Voting Smart Contract, the vote casting event is defined, which would later be recorded onto the blockchain [2].
2) **DEPLOY EVENT**: In order to commence elections, the election administrator organizes an event for casting votes. The event is defined by a Voting Smart Contract and, afterward, is recorded onto the blockchain [2].
3) **REGISTER AND AUTHENTICATE**:In order to verify the identity of each voter and keep those who are eligible to cast their votes, voters register for elections by connecting the unique cryptographic identifiers from their Ethereum wallets with their accounts in the election [7].
4) **CAST VOTE**:Voters cast their ballots through their Ethereum wallets by interacting with the Voting Smart Contract. The blockchain provides security and validation in recording each vote [4].

## IV. Proposed Method

**USER AUTHENTICATION**: EtherVote seeks to authenticate its users at the entry level by registering them through

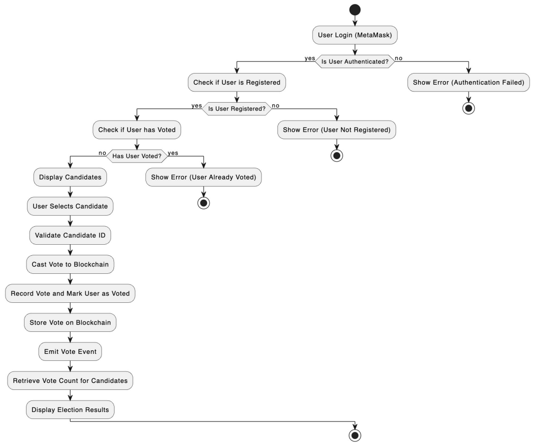


Fig. 2. Workflow of Project

secure email. [1] The user would be entering a valid email address at the time of registration. An OTP is generated and sent to the user-specified email ID, which the user must use to access the system. Thus, allowing only authenticated users into the voting system. Email authentication is a simple yet significant security mechanism, thus suggesting that identity confirmation is to be undertaken before being granted access to the voting platform. In contrast to other systems with OTP login, this way is rather considered to have far less chances of passing any unauthorized entry and thus safeguards the voters' pins but certainly provides a secure option.

**USER VALIDATION**: Upon completion of authentication, the eligibility of a user to vote is confirmed. [5] Generally, they will have to be 18 years or older to enter the voting process. The user's date of birth will be fed and compared with the age criteria for eligibility. After it is being confirmed that the user is eligible, he is allowed to enter. This system is created to uphold the integrity of the entire process in such a way that only lawful qualified voters are permitted to cast their votes.

**DISPLAY CANDIDATES**:Once verified and authorized, the candidates or options to vote are being shown to the users. [9] The goal of the user interface is to present logically and understandably various options or candidates for consideration. Information pertinent to each candidate or option is displayed, including names, positions, and any other information that might be helpful in making decision choices. The interface dynamically generates the display and updates it in realtime in cases where there have been updates or new candidates added. By affording a mechanism for transparency to voters, they are thereby able to contemplate their options prior to making a final choice, thus buttressing a fair and informed electoral process.

**VOTING PROCESS**:Voting in the EtherVote System is a rather easy process which beside that is made secure by the technology of blockchain [2]. Once he see the candidates, the user would select a person to vote for - this marks the beginning of his voting process. The process records the vote through smart contract on the Ethereum blockchain, once a voter confirms the choice. Each and every voter has an individual MetaMask address preloaded with sufficient Ether for voting. The smart contract ensures that no two votes are cast per address, thereby eliminating the possibility of multiple votes by one user. It is an automated, anonymous, and airtight voting mechanism, making simple and safe elections possible.

**BLOCKCHAIN STORAGE**: Once a vote is cast, these are securely stored on the Ethereum blockchain [6]. This ensures votes remain immutable and irretrievable after their insertion in the database. The decentralized nature of blockchain technology prevents any unauthorized command from being enacted. Each transaction is validated through smart contracts so that only real votes enter into the records. All transactions in the blockchain are made public, confirming their verifiability and traceability to the voting process. Voting data will further be fortressed by the cryptographic signature of the blockchain against fraud and unauthorized changes, creating a scenario whereby tampering or alteration becomes almost impossible.

## V. Algorithms Used

1) **ADD CANDIDATE**
**Description**: The addCandidate-function is responsible for adding a candidate precisely into the voting system [5]. This function increments the candidatesCount variable (the total count of candidates), assigns a candidateID to this particular candidate, and initializes the vote count of this candidate to zero. Candidate details are then stored in a mapping or a list.

2) **VOTING PROCESS**
**Description**: This function allows a voter to cast a vote for a candidate. First, it checks whether the voter has already voted, and if not, it further checks whether the candidate ID given was valid. If everything checks out, the voter is updated to indicate that he has voted and the votes count for this candidate is incremented. Thus, making it possible for a person to vote for only one specific candidate [3].

3) **CALCULATE TOTAL VOTES FOR ALL CANDIDATES**
**Description**: In this function, the total number of votes cast for the election is counted. It adds up from the candidate's votes count [7]. This will also help quantify the voter turnout and ensure that the election is conducted smoothly.

4) **CHECK ELECTION WINNER**
**Description**: The most recent addition examines which candidate had the maximum number of votes, thereby declaring the winner of the election [2]. The function iterates through the list of candidates, comparing their votes to determine the maximum. This function would then return the winner with the most votes. Additional

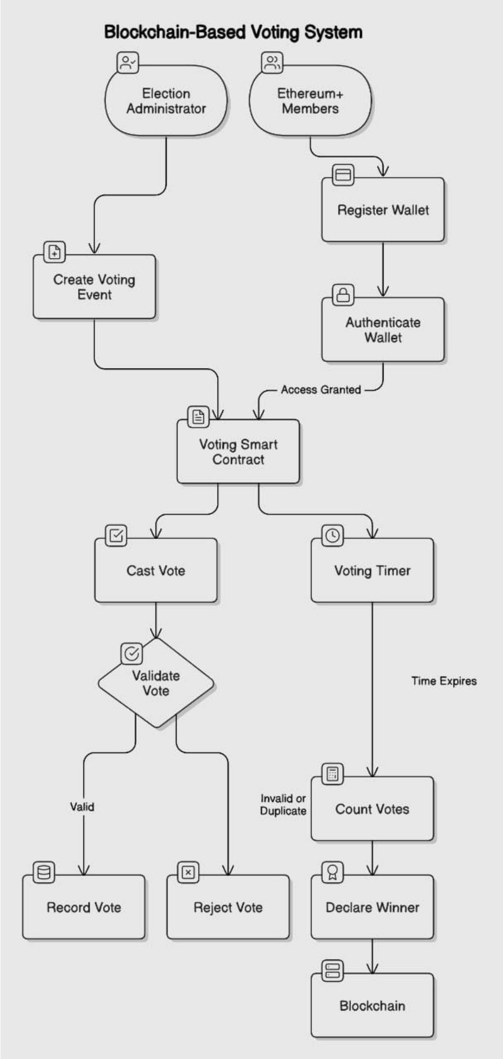
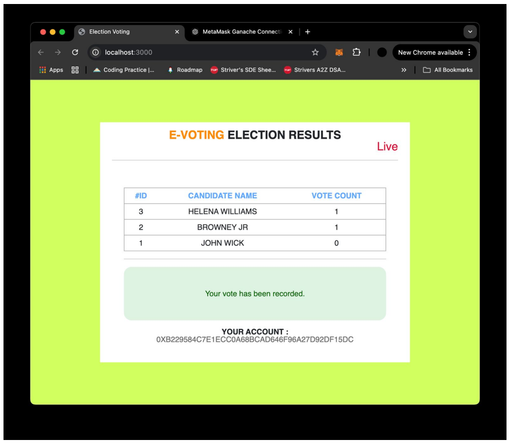


Fig. 3. Voting Mechanism

tie-breaking logic can be incorporated when needed if more than one candidate obtains the same largest vote.

5) **VALIDATE CANDIDATE ID**
**Description**: This function validates the candidate's ID as specified by the voter. It checks to see whether the ID lies between the range of registered candidates [6]. In case the ID is invalid, it will throw an error, and it will otherwise return true, allowing the voting process to proceed. Thus, it is guaranteed that votes are not cast on nonexistent candidates.

6) **REMOVE CANDIDATE**
**Description**: This method allows a candidate to be removed from the election processes. First, it validates a candidate's ID, and if valid, deletes that candidate from the candidates mapping [4]. It also decrements the count of candidates to maintain the integrity of the voting process. Be careful using this function as improper use may result in anomaly behavior where candidates are removed during the voting process. This is particularly useful for non-candidate registration issues that should be corrected before the start of an election.



E-VOTING ELECTION RESULTS

Live

| #ID | CANDIDATE NAME | VOTE COUNT |
|---|---|---|
| 3 | HELENA WILLIAMS | 1 |
| 2 | BROWNEY JR | 1 |
| 1 | JOHN WICK | 0 |

Your vote has been recorded.

YOUR ACCOUNT :
0XB229584C7E1ECC0A68BCAD646F96A27D92DF15DC

Fig. 4. Screenshot of the Voting Process

## VI. Results and Discussion

The voting system called EtherVote is perhaps an ideal example of a decentralised voting system with such operational features commendable for their efficiency, accuracy, scalability, utility, security, transparency, and positive user experiences.

- **PERFORMANCE**:EtherVote has made much progress compared to previous blockchain-based e-voting systems. VoteChain simplified blockchain system for secure voting [23]. It , however, showed a long delay during times of heavy voting because it was very dependent on unoptimized execution of smart contracts and limited throughput transactions. Such latency could make citizens lack confidence in the voting process as well as reduce electoral efficiency. EtherVote caters to this problem by utilizing smart contracts of Ethereum with MetaMask and simulating voting in Ganache under condition of stress testing . In this way , EtherVote provides low-latency vote casting and processing even under heavy concurrency of voters and thus guarantees smooth voting experience without lagging .

- **ACCURACY**:The foundation of any e-voting system is count accuracy and assurance that the voter votes once. The system/model by Pramulia and Anggorojati [17] utilized Ethereum for recording votes on the blockchain, thereby providing it with immutability but did not impose a well-defined one-person-one-vote constraint. In this way, the system is vulnerable to duplicate submissions by users managing multiple wallet addresses.EtherVote resolves this issue by binding each vote message to a unique MetaMask wallet address verified via an OTP-based authentication layer. By enforcing this one-vote-per-wallet rule and leveraging Ethereum's inherent tamper-proof features, EtherVote ensures vote uniqueness and prevents fraudulent or duplicate voting, thus improving system reliability and electoral fairness.

- **SCALABILITY**: Scalability is indeed a bottleneck in any blockchain voting system for large-scale implementations like nation-wide elections. Alam et al. [21] proposed an Ethereum-based system with primitive smart contract functions; it does not allow provisions to cater to thousands of transactions performed simultaneously, thus causing network congestion, or may also incur higher transaction costs approaches. EtherVote offers scalability using dynamic gas management, asynchronous confirmatory transaction mechanisms, and decentralized contract deployment across Ethereum test networks. This scalability feature allows EtherVote to process millions of voters with minimal performance degradation, allowing its timely use in real-life, high-turnout election environments without sacrificing responsiveness or affordability.

- **FEASIBILITY**: While proving sound from a technical point of view, real-life realizability is compromised because of poor user accessibility. For instance, Yavuz et al. [22] proposed a secure voting solution based on the use of Ethereum smart contracts; yet, it entailed the manual configuration of wallets and complex signing operations for users. Such kind of technical overhead limits the wider spread adoption, especially among non-technical users. EtherVote improves the feasibility by an OTP-based login system, covering users from technical complexity and allowing them to authenticate them before casting their vote via MetaMask. The user flow resembles that of traditional web apps reducing the blockchain learning curve while making EtherVote cryptographically secure thereby improving its viability for mass civic participation.

- **SECURITY**:Block-chain-based e-voting systems are prone to attacks, including the steal of private keys, phishing, and other unauthorized access to wallets. Hjálmarsson et al. [13] discussed a smart-contract-based voting system that assured immutability of transaction records but could not provide extra measures that would guarantee secure interaction with the user's wallet. EtherVote provides an additional level of security at the level of the wallet by enforcing MetaMask wallet signature validation for every vote. EtherVote does not store sensitive credentials, and the frontend and the blockchain layer communicate in encrypted form. Therefore, these measures reduce the chances of tampering with votes, unauthorized submissions, and man-in-the-middle attacks, making EtherVote a more secure environment for digital elections.

- **TRANSPARENCY**: The very hallmark of blockchain technology is that it provides a kind of transparency; it must also be expanded to include both system-level and user-level verification. Whereas Pandey et al. [23] mention that blockchain is used for storing tamper-proof records, it unfortunately lacks real-time visibility to be able to confirm vote receipt or traceability from the voter's perspective. Of course, EtherVote further enhances transparency through a public ledger interface with which users can verify their transaction hashes against their votes. Besides, election observers can audit the entire election process through systems like Etherscan. Such verifiability engenders user trust and removes the requirements for centralized election authorities, thereby enhancing democratic accountability.

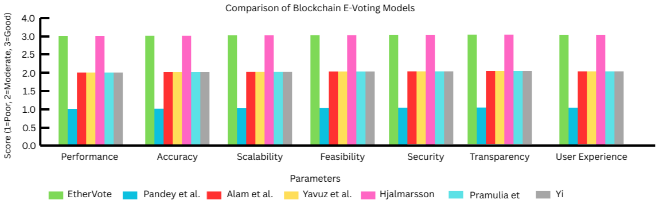


Fig. 5. Comparison of EtherVote with Other Systems That Are Based on Blockchain Technology for Voting.

The bar chart evaluates EtherVote against other major e-voting systems based on blockchain on various attributes. Each score represents the relatively strong performance associated with the model on the scale from 1 (Poor) to 3 (Good), denoting how well EtherVote compares with its peers.

- **USER EXPERIENCE**:Generally, the acceptance of systems based on blockchain will rely heavily on the intuitive and accessible design of its user interface. Yi [20] proposed a decentralized voting model based on the principles of P2P networking yet found the operation overly limited through its rather complex wallet setup, which is seen as a detractor for less tech-savvy users. EtherVote settles directly on the other side and instead focuses on usability with a clean, guided interface that requires minimal interaction steps: users receive OTPs for logging in and are automatically directed to MetaMask for authentication before clicking once to vote. This frictionless flow enables first-time blockchain users to participate confidently, thus extending accessibility across various demographic lines.

## VII. Conclusion and Future Scope

The Ethereum-based decentralised voting system expands the possibilities for elections, increasing them into a completely new realm of transparency, security, and affordability for ballots. The way it does that is by using immutable blockchain smart contracts to record votes so that they are anonymous, proving without third parties that votes cannot be manipulated [1]. Its successful validation via simulations signifies good potential application in the real world [3]. However, high reception scenarios present scalability and deployment problems in the long term. Such previous schemes as one which focused on smart contract-based electronic voting systems mentioned Ethereum advantages, with limitations on broader usability and deployment positioning [13]. This shows the importance of further evolutions before implementation at the practical nationwide level will be possible.

Improvements must be made in the future to consider the scalability of the system to cope with a high number of voters without experiencing latency or bottlenecks in the data-processing [5]. Biometric authentication methods, like fingerprints or facial recognition, can enhance approachability and increase security [15]. Additionally, hybrid models that combine smart contracts with biometric encryption could create secure avenues for validating identities within voting systems [14]. Usability to non-technical users continues to be a priority; real-world implementations with Ethereum and MetaMask suggest that simplified interfaces are needed to ensure accessibility [17]. Moreover, ecosystem threats and risks need to be analyzed for securing the ecosystem against cyber vulnerabilities, as emphasized from studies assessing blockchain-based voting risks [19].

## References

[1] Hsiao, JH., Tso, R., Chen, CM., Wu, ME. (2018). Decentralized E-Voting Systems Based on the Blockchain Technology. In: Park, J., Loia, V., Yi, G., Sung, Y. (eds) Advances in Computer Science and Ubiquitous Computing. CUTE CSA 2017 2017. Lecture Notes in Electrical Engineering, vol 474. Springer, Singapore.

[2] W. -J. Lai, Y. -c. Hsieh, C. -W. Hsueh and J. -L. Wu, "DATE: A Decentralized, Anonymous, and Transparent E-voting System," 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, 2018, pp. 24-29, doi: 10.1109/HOTICN.2018.8605994.

[3] D. Khoury, E. F. Kfoury, A. Kassem and H. Harb, "Decentralized Voting Platform Based on Ethereum Blockchain," 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), Beirut, Lebanon, 2018, pp. 1-6, doi: 10.1109/IMCET.2018.8603050.

[4] K. Garg, P. Saraswat, S. Bisht, S. K. Aggarwal, S. K. Kothuri and S. Gupta, "A Comparitive Analysis on E-Voting System Using Blockchain," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-4, doi: 10.1109/IoT-SIU.2019.8777471.

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

[6] J. Lyu, Z. L. Jiang, X. Wang, Z. Nong, M. H. Au and J. Fang, "A Secure Decentralized Trustless E-Voting System Based on Smart Contract," 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 2019, pp. 570-577, doi: 10.1109/TrustCom/BigDataSE.2019.00082.

[7] A. M. Al-madani, A. T. Gaikwad, V. Mahale and Z. A. T. Ahmed, "Decentralized E-voting system based on Smart Contract by using Blockchain Technology," 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC), Aurangabad, India, 2020, pp. 176-180, doi: 10.1109/ICSIDEMPC49020.2020.9299581.

[8] R. Widayanti, Q. Aini, H. Haryani, N. Lutfiani and D. Apriliasari, "Decentralized Electronic Vote Based on Blockchain P2P," 2021 9th International Conference on Cyber and IT Service Management (CITSM), Bengkulu, Indonesia, 2021, pp. 1-7, doi: 10.1109/CITSM52892.2021.9588851.

[9] H. Garg, M. Singh, V. Sharma and M. Agarwal, "Decentralized Application (DAPP) to enable E-voting system using Blockchain Technology," 2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA), Gunupur, India, 2022, pp. 1-6, doi: 10.1109/ICCSEA54677.2022.9936413.

[10] R. L. Almeida, F. Baiardi, D. Di Francesco Maesa and L. Ricci, "Impact of Decentralization on Electronic Voting Systems: A Systematic Literature Survey," in IEEE Access, vol. 11, pp. 132389-132423, 2023, doi: 10.1109/ACCESS.2023.3336593.

[11] C. K. Adiputra, R. Hjort and H. Sato, "A Proposal of Blockchain-Based Electronic Voting System," 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 2018, pp. 22-27, doi: 10.1109/WorldS4.2018.8611593.

[12] R. Hanifatunnisa and B. Rahardjo, "Blockchain based e-voting recording system design," 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), Lombok, Indonesia, 2017, pp. 1-6, doi: 10.1109/TSSA.2017.8272896.

[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), San Francisco, CA, USA, 2018, pp. 983-986, doi: 10.1109/CLOUD.2018.00151.

[14] S. T. Alvi, M. N. Uddin and L. Islam, "Digital Voting: A Blockchain-based E-Voting System using Biohash and Smart Contract," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2020, pp. 228-233, doi: 10.1109/ICSSIT48917.2020.9214250.

[15] M. Ibrahim, K. Ravindran, H. Lee, O. Farooqui and Q. H. Mahmoud, "ElectionBlock: An Electronic Voting System using Blockchain and Fingerprint Authentication," 2021 IEEE 18th International Conference on Software Architecture Companion (ICSA-C), Stuttgart, Germany, 2021, pp. 123-129, doi: 10.1109/ICSA-C52384.2021.00033.

[16] M. -V. Vladucu, Z. Dong, J. Medina and R. Rojas-Cessa, "E-Voting Meets Blockchain: A Survey," in IEEE Access, vol. 11, pp. 23293-23308, 2023, doi: 10.1109/ACCESS.2023.3253682.

[17] D. Pramulia and B. Anggorojati, "Implementation and evaluation of blockchain based e-voting system with Ethereum and Metamask," 2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), Jakarta, Indonesia, 2020, pp. 18-23, doi: 10.1109/ICIMCIS51567.2020.9354310.

[18] Tanwar, S., Gupta, N., Kumar, P. et al. Implementation of blockchain-based e-voting system. Multimed Tools Appl 83, 1449–1480 (2024). https://doi.org/10.1007/s11042-023-15401-1

[19] Y. Abuidris, A. Hassan, A. Hadabi and I. Elfadul, "Risks and Opportunities of Blockchain Based on E-Voting Systems," 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, Chengdu, China, 2019, pp. 365-368, doi: 10.1109/ICCWAMTIP47768.2019.9067529.

[20] Yi, H. Securing e-voting based on blockchain in P2P network. J Wireless Com Network 2019, 137 (2019). https://doi.org/10.1186/s13638-019-1473-6

[21] A. Alam, S. M. Zia Ur Rashid, M. Abdus Salam and A. Islam, "Towards Blockchain-Based E-voting System," 2018 International Conference on Innovations in Science, Engineering and Technology (ICISET), Chittagong, Bangladesh, 2018, pp. 351-354, doi: 10.1109/ICISET.2018.8745613.

[22] E. Yavuz, A. K. Koç, U. C. Çabuk and G. Dalkılıç, "Towards secure e-voting using ethereum blockchain," 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 2018, pp. 1-7, doi: 10.1109/ISDFS.2018.8355340.

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