International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/CSEIT2390615

VoteCoin : A Blockchain Perspective on E-Voting Infrastructure

Ardon Kotey[1], Keya Gupta[1], Jahanvi Agarwal[1], Prof. Harshal Dalvi[2], Prof. Neha Khatre[2]

[1]Students, Department of Information Technology, Dwarkadas J. Sanghvi College of Engineering, Mumbai, Maharashtra, India

[2]Proffesor, Department of Information Technology, Dwarkadas J. Sanghvi College of Engineering, Mumbai, Maharashtra, India

ARTICLEINFO

Article History:

Accepted: 01 Nov 2023

Published: 22 Nov 2023

Publication Issue

Volume 9, Issue 6

November-December-2023

Page Number

87-97

ABSTRACT

The implementation of a dependable and equitable decision-making process is of paramount importance and carries substantial influence within any organizational context. At present, decision-making procedures frequently depend on either traditional manual approaches or sophisticated technological resolutions. There are several challenges associated with these approaches, which encompass a dearth of transparency, low rates of participation, the possibility of manipulation, skepticism towards the decision-making body, counterfeiting of unique identification, prolonged delays in the dissemination of results, and significant security concerns. When contemplating the integration of a digital decision-making system, security throughout the entire process is invariably the foremost consideration. In light of the seriousness of the matters under consideration, it is indisputable that the system must ensure data security and prevent potential breaches. One plausible solution for mitigating these security challenges entails the utilization of blockchain technology. Blockchain, an implementation of decentralized ledger technology, enables the decentralized exchange of digital assets in a secure and transparent manner. In this regard, distributed ledger technology signifies a substantial progression; every block comprises an exhaustive ledger of every transaction. The defining features of blockchain technology are anonymity, decentralization, security, and transparency. The convergence of smart contracts and blockchain technology presents a profoundly auspicious prospect in the realm of constructing decision-making systems that place utmost importance on transparency, safety, and security. A prototype decision-making application was effectively developed and evaluated in this research endeavor by leveraging smart contracts on the Ethereum network. By integrating digital wallets, blockchain technology, and the Solidity programming language, this accomplishment was realized. A finite quantity of tokens, analogous to gas, is assigned to each user within their wallet. By depleting these tokens upon user participation in the decision-making process, duplicate actions are ensured to be prevented. In addition to examining

the advantages and disadvantages of blockchain technology, the study presents a working prototype of a web application that is specifically engineered to optimize the process of making decisions. This highlights the intrinsic constraints of the system.

Keywords: Blockchain, Voting, Ethereum

I. INTRODUCTION

The emergence and widespread adoption of Bitcoin [1], the pioneering cryptocurrency, has propelled blockchain technology into the spotlight, making it a prominent subject in contemporary software discourse [2]. The genesis of blockchain technology can be traced back to its foundational architectural framework within the realm of the cryptocurrency bitcoin. Initially introduced to the digital landscape, it swiftly garnered attention and emerged as a technology with immense potential. Its notable attribute of possessing a high level of transparency within the system propelled it into a realm of active research and study, exploring its applicability across diverse domains. Within the domain of Bitcoin, the decentralized characteristics of wallets facilitate the real-time and transparent surveillance of the global coin supply and the volume of transactions occurring at any given moment. The elimination of a central authority is a prerequisite for authorizing or finalizing operations within this peer-to-peer (P2P) system. This allows not only monetary transactions but also various types of structural data to be stored in the distributed chain. Furthermore, the system can be secured through the implementation of cryptographic techniques.

Analogous to personal assets, marriage certificates, bank account records, and medical information, this methodology can accommodate a wide range of data with suitable modifications [3]. Following in the footsteps of Bitcoin, Ethereum, also referred to as Ether, has emerged as a flexible development environment. As previously mentioned, it differentiates itself from conventional blockchain technology through its capacity to produce software that is effective at storing structured data. The software programs that are executed by smart contracts are encoded into the blockchain and have an immutable nature (as will be elaborated upon later). These documents are resistant to unauthorized removal or manipulation once they have been recorded. As a result, it can be inferred that they have the capacity to function efficiently, independently, and completely openly indefinitely, without being impacted by external factors [5].

Transactions are recorded in blocks on the blockchain, and as more take place, a block will eventually be completed. After reaching completion, the transaction is appended to the blockchain in a sequential and chronological fashion. Common designations for the first block of a blockchain are "Genesis block" and "Block 0." The genesis block, which is commonly hardcoded into the software, is characterized by the absence of any reference to the block that came before it. The aforementioned details are recorded in the source referenced as "Genesis Block" in 2015. After the genesis block is initiated, the subsequent block, represented as 'Block 1,' is produced and subsequently connected to the genesis block. Every individual block in the blockchain is allocated a specific section to store transaction data. Prior to execution, each transaction within the block undergoes a transformation into a hash value. The hashes of these transactions are subsequently paired and hashed iteratively until the Merkle root, which is a single hash value, remains.

The merkle root is kept within the block header. To guarantee the immutability of a transaction, each block

additionally maintains a record of the header of the preceding blocks. Consequently, any attempt to modify the contents would necessitate the alteration of many blocks. The blockchain technology is specifically engineered to facilitate access through a decentralised peer-to-peer network. In this network, individual nodes or peers engage in communication with one another to facilitate the exchange of blocks and transactions. Upon establishing a connection to the network, peers initiate the transmission of messages pertaining to other peers inside the network, hence facilitating a decentralised approach to peer discovery. The primary function of the nodes in the network is to authenticate unverified transactions and newly generated blocks. Prior to commencing this task, a new node must undergo an initial block download process. The process of initial block download entails the downloading and validation of all blocks from the genesis block to the latest block on the blockchain. Once this procedure is completed, the node is deemed to be synchronised.

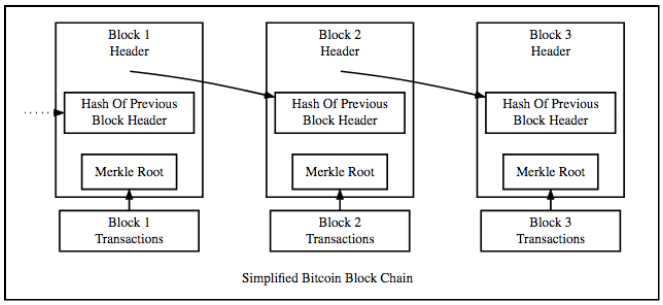

Fig 1 – Simplified Block Chain

The utilisation of blockchain technology has the potential to serve as a viable option for electronic voting initiatives. Extensive research is being conducted about electronic voting (e-voting), with numerous implementations being rigorously evaluated and then employed for a period. Nevertheless, there is a scarcity of dependable implementations that remain in active utilisation. Undoubtedly, numerous instances of efficacious online polls and questionnaires exist; nevertheless, the same level of effectiveness cannot be attributed to online elections conducted by governments and corporations. This is mostly since official elections are integral components of democracy and democratic governance, which are widely favoured as the predominant administrative approach in contemporary society. In democratic cultures, a highly esteemed aspect is the presence of a strong electoral process that ensures both transparency and privacy. Currently, there is a significant prevalence of decision-making being conducted by individuals.

The present voting scheme elicits numerous inquiries regarding the reliability and transparency of the system, the potential alteration of votes prior to their tabulation, and how we might ascertain the transparency of the system. In this study, we aim to address the inquiries by examining and proposing a web-based application that leverages blockchain technology on the Ethereum server through the deployment of smart contracts.

II. METHODS AND MATERIAL

A. Literature Review

The digital voting method proposed by G. Rathee et al. [14] utilizes blockchain technology and is designed for implementation in a technologically sophisticated setting. The assumption made by the system is that all external entities that are connected are reliable and trustworthy. Nevertheless, the presence of security vulnerabilities within the system poses a significant potential threat, as unauthorized individuals may use these weaknesses to manipulate the voting process. In our suggested voting system, the implementation of encryption and secure networks serves to mitigate the potential threat of unauthorized access to the votes.

B. Shahzad and J. Crowcroft present a framework for secure and transparent blockchain-based electronic voting in their paper "Trustworthy Electronic Voting Using Adjusted Blockchain Technology". A blockchain can be customised for an election. Their architecture can address security, privacy, and verifiability issues in conventional electronic voting systems, according to the authors. The paper begins with a history of electronic voting and its challenges. The authors then

explain their consortium blockchain structure for governing bodies. The system uses hashing techniques to protect data and block sealing to make the blockchain adaptable. The authors believe blockchain technology can solve the security, privacy, and verifiability issues by creating an immutable ballot ledger. The conclusion discusses blockchain technology's potential benefits for electronic voting. The authors believe their architecture can improve electronic voting security, transparency, and efficacy. Their framework also addresses issues like the need for a trustworthy governing body and the need to educate voters on how to use it. The article is a complete overview of blockchain technology in electronic voting. The authors' well-designed system addresses security, privacy, and verifiability issues. The article advances electronic voting scholarship.

P. Mccorry et al. discussed voting without polling stations [17]. If implemented properly, blockchain-based online voting can yield good results. Technical issues with digital voting systems were highlighted. System robustness was uncontrollable. End-to-end verification reduces user duplication. Voter privacy was compromised by these low latency voting technologies. The suggested blockchain voting system controls latency with a customizable consensus mechanism and smart contracts.

A system was proposed by M. Pawlak et al. [15] that eliminates the need for any operating entities. It was unable to verify the identity of voters, and it also demanded intricate computing. Although the system successfully gathered user ballots, it encountered latency issues as the complexity of computation increased with the number of concurrent users. Voter identities were rendered vulnerable. Due to its inability to process substantial volumes of data, the system has been unable to be deployed on a significant scale. In contrast, our proposed voting system minimises latency through the adaptable implementation of consensus algorithms. By utilising cryptographic hashes in blockchain, the vulnerability of a voter's identity is eliminated.

The system that D. Chaum et al. [16] proposed enhanced the integrity and impartiality of vote tallying. The implementation of end-to-end verification enabled electors to have confidence that their vote counts were consolidated. Every voter had the opportunity to verify that his vote had been accurately counted and recorded. Voters were provided with a distinct code for electronic verification of their ballots. In contrast, our proposed voting system has implemented additional simplifications in the verification of ballots. Voters may use registered email addresses and phone numbers to verify their ballots. Election verification subsequent to the voting process engenders confidence among the electorate.

Estonia serves as a noteworthy example, given that its government was a trailblazer in the digital implementation of a comprehensive electronic voting system. Estonia is particularly noteworthy as an example. The notion of electronic voting was initially proposed for deliberation within the nation in 2001; however, its implementation was not sanctioned by the national authorities until the summer of 2003 [18]. Despite undergoing several revisions and advancements since its inception, their methodology is presently regarded as dependable and resilient. To ensure individual authentication, the organization utilizes smart digital ID cards and government-issued personal card readers [19]. The utilization of a specialized web portal and corresponding desktop software enables members of the public to participate in electoral processes through the acquisition of candidate information and the casting of ballots. Voting remotely is possible for anyone with a computer, an internet connection, and an identification card using this system.

Scantegrity is described in the work [20], which has minimal effects on election procedures. It is the first

independent E2E verification mechanism that keeps optical scan as the underlying voting system and doesn't interfere with manual recounts. Additionally, it is the first mechanism of its kind

B. Limitations of Existing System

Contemporary significant technical obstacles associated with electronic voting systems include, but are not limited to, secure digital identity management. It is imperative that all prospective citizens enrol in the electoral system prior to the events of elections.

Anonymous vote-casting: Following submission through the system, each vote, which may or may not contain a candidate-specific option, should remain anonymous to all parties, including the system administrators. The way individualised ballot processes represent votes in online applications or databases remains a subject of ongoing debate. While a transparent text message represents an unfavourable strategy, a hashed token is willing to provide both confidentiality and integrity. In the interim, the vote itself should be deemed unreliable, as it cannot be endorsed by the token resolution.

Verifiability of ballots by the voter (and only by the voter): At the time of submitting the ballot, the elector should have the ability to observe and validate his or her own vote. This is frequently crucial to understand to prevent, or at the very least, to become aware of, any possible malevolent activity. This counterargument, except for offering evidence of non-repudiation, has the potential to significantly enhance the electors' sense of trust. A portion of these concerns have been addressed in recent applications. Notwithstanding, electronic voting is currently operational in numerous nations, including Brazil, the United Kingdom, Japan, and the Republic of Estonia. In contrast to the other countries, the Republic of Estonia should be assessed uniquely due to its comprehensive electronic voting system, which is purportedly equivalent to traditional paper-based elections.

Increasing security issues: Cyberattacks pose a significant risk to public opinion surveys. A degree of responsibility would not be accepted if an associate degree hacking attempt were to prevail during an election. While DDoS attacks are well-documented, they are not prevalent during elections.

III.RESULTS AND DISCUSSION

A. Our Approach

This part will elucidate the design and functional portion of our application. The user interacts with the web application, which is the hosting platform, and proceeds to register and cast their vote in a secure and transparent manner. Figure 2 provides an overview of the application

1. Registration Procedure: To engage in the voting system, the prospective voter is required to complete the registration process, which entails the provision of a unique identification number and personal particulars including name, roll number, and mobile number. The entirety of this data is stored in a secure database.

2. User Login: Opponents log in to cast ballots following the registration process. Authentication is accomplished via a password-based system, and to ensure the legitimacy of the voter in real-time, an OTP verification process is implemented after the login.

3. Security via Blockchain: This stage employs blockchain technology predominantly for its security functionalities. The voter's message (i.e., the cast vote) is encrypted utilizing an asymmetric encrypting algorithm. To ensure transparency and security, blockchain technology implements a public key that is utilized for verification by the ledger.

4. User Database Management: A database is utilized to store all user information, encompassing their name, gender, and unique ID. MySQL is the database of

choice for storing and retrieving user information in an efficient manner.

5. Integration with the Ethereum Network The Ethereum network provides the infrastructure for the generation and storage of blockchain blocks. The specifics of every block are encrypted and securely stored in a ledger. Due to the distributed nature of these blocks across nodes, the fault tolerance of the system is enhanced.

6. Results Announcement: During the results phase, votes are tallied and processed by the system. The outcomes are produced and presented on the online platform, enabling participants to validate the integrity and precision of their ballots.

B. Voting System Architecture

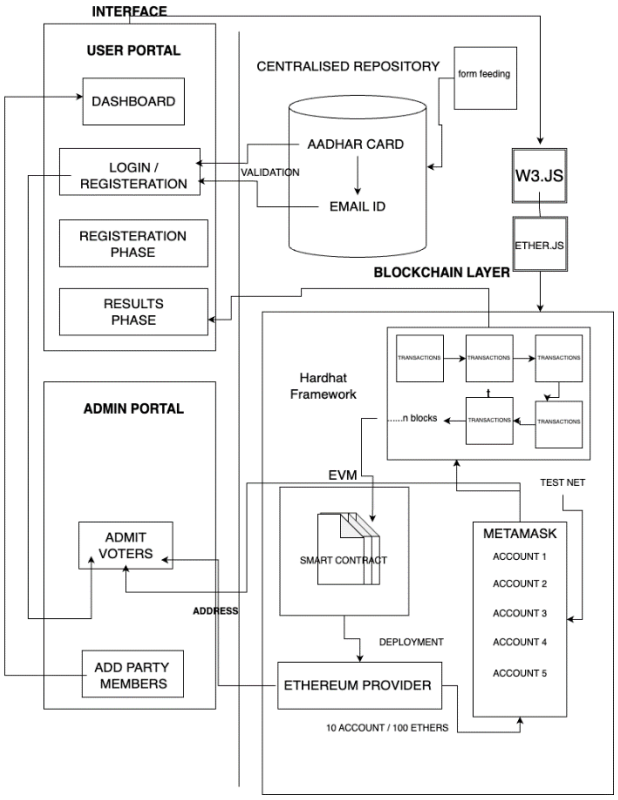

Fig 2 – Voting System Architecture

The application has been constructed utilising the architectural framework known as Model-View-Controller. Furthermore, this architectural style is extensively employed. The application is partitioned into three primary logical components, namely the model, the view, and the controller.

1. View: The uppermost stratum of the system facilitates user interaction with the application by means of various actions such as button clicks, data input, camera access, radio button selection, song uploads, and so on. The primary function of this layer is to provide data to the user, either in its entirety or in a selected subset, in accordance with the specific needs of the application. The layer serves as an intermediary connecting the user and the application.
2. Controller: The controller serves as an intermediary layer within the programme, housing the business logic and primary functions of the system. Upon the user's interaction with the programme, the response is subsequently handled within this layer. This layer encompasses all the functions that operate in the background, starting from the log-in process and extending to the casting of votes. The primary components of this system primarily encompass the various functions and the transmission of output to the view layer.
3. Model: The model layer is tasked with the responsibility of managing and preserving the user's data. A relational database is a structured collection of data organised in tables, where each table consists of rows and columns. This type of database MySQL is utilised for the purpose of storing user data.

For users to engage in the voting process of our application, they must provide a wallet address and Ether, which serves as the network's currency. Users cast their votes and incur a nominal transaction fee, denoted as "gas," in order to have their votes recorded on the blockchain, upon connecting to the network. This system-denominated transaction fee (referred to as "gas") may be linked to coins. The network's miner-nodes are remunerated with "gas" in exchange for

transaction processing. In Ether, there is a fee associated with writing to the blockchain; however, retrieving information from it is complimentary. This implies that while voting on the blockchain incurs a fee, viewing the candidates does not.

During application development, the Ethereum blockchain enables us to execute code via smart contracts on the Ethereum Virtual Machine (EVM). Smart contracts are integral components of our application as they facilitate the reading and writing of data to the blockchain, as well as the execution of requisite logic. The programming language where these intelligent contracts are constructed is Solidity. In the context of blockchain technology, smart contracts serve as the repository for all business logic that interacts with the public ledger, which functions as the database layer. Within our application, smart contracts represent an accord that guarantees the counting of every user's vote, the counting of each vote exclusively once, and the declaration of victory to the candidates who have received the most votes.

C. RESULTS:

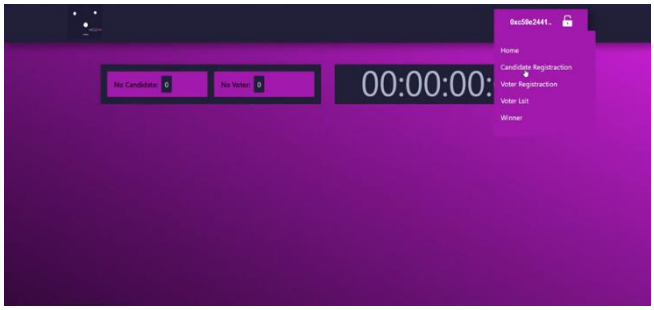

Fig 3 – Home Page (before voting starts)

On the homepage, there is a total candidate and voter counter that is always being brought up to date to display the total number of people who have registered to vote or run for office. Users will receive an overview of their present participation in the voting process because of this information being made available. The amount of time that is left before the conclusion of the voting period may be seen on the countdown timer that is located on the homepage. Before casting their votes, voters are aware of the deadline that has been set.

It can redirect to one of four different sites, including winner, voter list, candidate registration, and voter registration. The home page of our blockchain-based voting system serves as a user-friendly center for all components of the system, delivering transparency, efficiency, and accessibility throughout the whole electoral process.

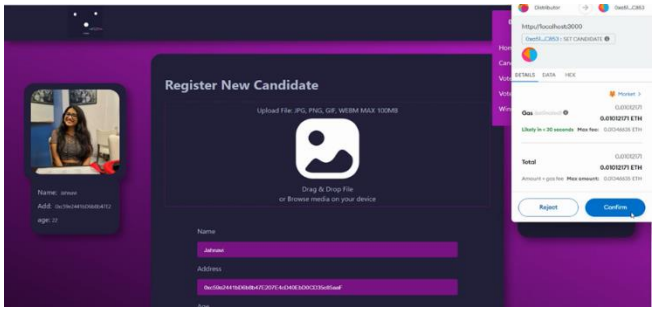

Fig 4 – Candidate registration page

New candidates must register themselves using their MetaMask ID (They will use their MetaMask ID to register, ensuring a secure and decentralized identification process), and the admin confirms whether the candidate is eligible. There is a verification mechanism that cross-checks the provided MetaMask ID to prevent fraudulent entries. The registration request is then sent to the admin for confirmation. The admin then decides if the candidate is eligible. Then the candidate is usefully registered.

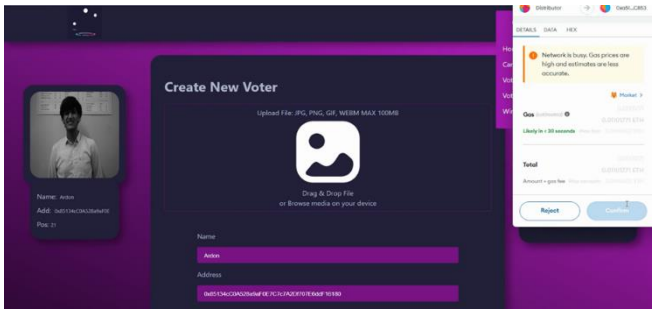

Fig 5 – Voter Registration Page

This page facilitates the registration of voters, requiring everyone to register and verify their identity with a unique MetaMask ID, providing a secure and

immutable link between their digital identity and the blockchain. This integration not only streamlines the registration process but also adds an extra layer of security and authenticity to the voter database. The admin then holds the authority to review the voter's information and determine eligibility. Then the voter is successfully registered.

Fig 6 - MetaMask

It generates and manages unique MetaMask IDs for each user. Every candidate, voter, and admin is assigned a distinct MetaMask ID, which acts as a cryptographic identifier. MetaMask IDs are securely stored on the blockchain, fostering transparency and immutability in the registration and authentication processes. To perform any action within the voting system, participants need a certain number of ethers. Ethers, though simulated or "fake" in this context, serve as the transactional currency on the Ethereum blockchain. This includes tasks such as candidate registration, voter registration, and other administrative actions. The usage of fake ethers allows users to engage with the system without any real-world financial implications, creating a risk-free environment for testing and participating in the voting process.

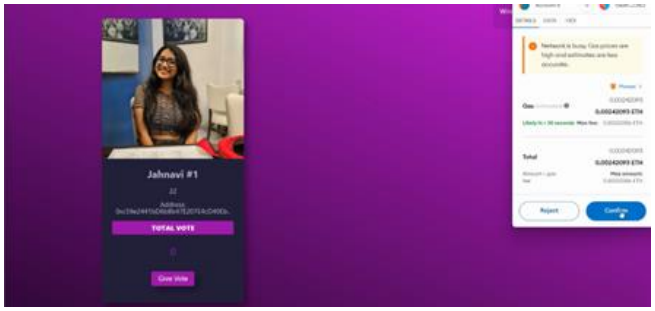

Fig 7 – Home Page (after candidate has registered)

Display a comprehensive list of all candidates who are participating in the election. Each candidate's entry should include essential details such as their name, age, total votes. Allows voters to carefully review the information about each candidate. This helps voters to make informed decisions about whom to vote for. Voters cannot cast more than one vote. system recognizes and prohibits any additional votes from the same MetaMask ID.

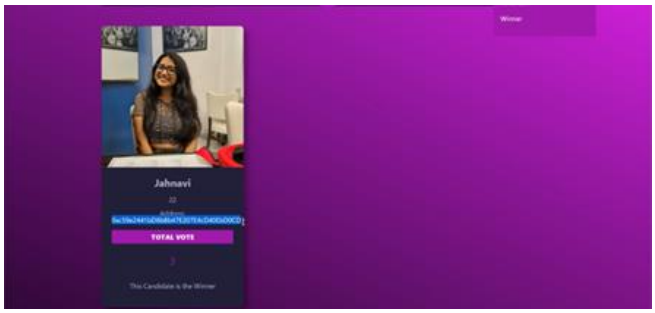

Fig 8 – Winners Page

Mechanism that automatically calculates and identifies the candidate with the maximum votes once the voting timer expires. This process should be transparent, secure, and based on blockchain technology to ensure the integrity of the results. Clearly display the name, photo, age and total number of votes of the winning candidate on the winner's page.

IV.CONCLUSION

In conclusion, our voting system-VoteCoin offers a secure, transparent, and efficient solution for modernizing the electoral process. By leveraging blockchain technology, the system ensures the integrity of votes, eliminates the risk of tampering or fraud, and provides a verifiable and auditable record of the entire voting process.

The system incorporates key features such as voter registration, candidate registration, and authorization of candidates by the admin through MetaMask IDs. The integration of MetaMask wallets adds an additional layer of security and user authentication.

Through the user-friendly interface, voters can easily cast their votes, and candidates can monitor their campaign progress.

Furthermore, the proposed system addresses several challenges faced by traditional voting methods, such as geographical limitations, logistical complexities, and manual errors. By embracing blockchain's decentralized nature, the system offers increased accessibility, cost efficiency, and streamlined processes. The integration of additional technologies like chatbots for user guidance and machine learning algorithms for detecting potential attacks further enhances the system's capabilities.

While the system shows great promise, it is important to acknowledge that further research, development, and collaboration are required to address scalability, privacy concerns, user adoption, and regulatory frameworks. Continued efforts in these areas will be crucial for realizing the full potential of blockchain-based voting systems.

Overall, our online blockchain-based voting system has the potential to revolutionize the way elections are conducted, ensuring transparency, security, and trust in the democratic process. By embracing technological advancements and leveraging blockchain's unique features, we can pave the way for more inclusive, efficient, and democratic voting systems in the future.

V. FUTURE SCOPE

Integration of Chatbot for User Guidance: Adding a chatbot to the blockchain-based voting system can enhance user experience and provide guidance to users regarding their MetaMask accounts. The chatbot can assist users in setting up their MetaMask wallets, connecting to the voting system, and addressing any technical or usability queries they may have. By offering real-time support and guidance, the chatbot can improve user engagement and ensure a smoother voting experience.

Machine Learning Algorithms for Detecting Potential Attacks: Implementing machine learning algorithms to detect potential attacks on the smart contracts used in the voting system can enhance security. By analyzing patterns and anomalies in transaction data, ML algorithms can identify suspicious activities, attempted breaches, or tampering attempts. These algorithms can provide early warnings, allowing system administrators to take appropriate preventive measures, such as implementing additional security measures or initiating audits, to protect the integrity of the voting system.

These future enhancements leverage emerging technologies like chatbots, and machine learning to further improve the user experience and strengthen the security of blockchain-based voting systems. By incorporating these advancements, the voting system can become more user-friendly, secure, and resilient against potential threats and attacks.

VI. REFERENCES

[1]. S. S. Hossain, S. A. Arani, M. T. Rahman, T. Bhuiyan, D. Alam, and M. Zaman, "E-voting system using blockchain technology," in Proc. 2nd Int. Conf. Blockchain Technol. Appl., Dec. 2019, pp. 113–117, doi: 10.1145/3376044.3376062.

[2]. B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," IEEE Access, vol. 7, pp. 24477–24488, 2019, doi: 10.1109/ACCESS.2019.2895670.

[3]. F. P. Hjálmarsson, G. K. Hreiòarsson, M. Hamdaqa, and G. Hjálmtýsson, "Blockchain-based E-Voting system," in Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD), Jul. 2018, pp. 983–986.

[4]. M. S. Farooq, M. Khan, and A. Abid, "A framework to make charity collection transparent and auditable using blockchain technol- ogy," Comput. Electr. Eng., vol. 83, May 2020, Art. no. 106588, doi: 10.1016/j.compeleceng.2020.106588.

[5]. N. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology—Beyond bitcoin," Sutardja Center Entrepreneurship Tech- nol., Univ. California, Berkeley, CA, USA, Tech. Rep., Oct. 2015. Accessed: Jan. 24, 2018. [Online]. Available: http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf

[6]. T. Dimitriou, "Efficient, coercion-free and universally verifiable blockchain-based voting," Comput. Netw., vol. 174, Jun. 2020, Art. no. 107234, doi: 10.1016/j.comnet.2020.107234.

[7]. S. Shah, Q. Kanchwala, and H. Mi. (2016). Block Chain Voting System. Economist. [Online]. Available: https://www.economist.com/sites/default/files/northeastern.pdf

[8]. S.Park,M.Specter,N.Narula,andR.L.Rivest,"Goingfrombadtoworse: From internet voting to blockchain voting," J. Cybersecurity, vol. 7, no. 1, pp. 1–15, Feb. 2021, doi: 10.1093/cybsec/tyaa025.

[9]. K. M. Khan, J. Arshad, and M. M. Khan, "Secure digital voting sys- tem based on blockchain technology," Int. J. Electron. Government Res., vol. 14, no. 1, pp. 53–62, Jan. 2018, doi: 10.4018/IJEGR.2018010103.

[10]. C. K. Adiputra, R. Hjort, and H. Sato, "A proposal of blockchain- based electronic voting system," in Proc. 2nd World Conf. Smart Trends Syst., Secur. Sustainability (WorldS), Oct. 2018, pp. 22–27, doi: 10.1109/WorldS4.2018.8611593.

[11]. A. Barnes, C. Brake, and T. Perry. Digital Voting with the use of Blockchain Technology Team Plymouth Pioneers-Plymouth University. Accessed: Feb. 14, 2022. [Online]. Available: https://www.economist.com/sites/default/files/plymouth.pdf

[12]. J. Huang, D. He, M. S. Obaidat, P. Vijayakumar, M. Luo, and K.-K.-R. Choo, "The application of the blockchain technology in vot- ing systems: A review," ACM Comput. Surv., vol. 54, no. 3, pp. 1–28, Apr. 2022, doi: 10.1145/3439725.

[13]. F. Fusco, M. I. Lunesu, F. E. Pani, and A. Pinna, "Crypto-voting, a blockchain based e-voting system," in Proc. 10th Int. Joint Conf. Knowl. Discovery, Knowl. Eng. Knowl. Manage., 2018, pp. 223–227, doi: 10.5220/0006962102230227.

[14]. G. Rathee, R. Iqbal, O. Waqar, and A. K. Bashir, "On the design and implementation of a blockchain enabled E-Voting application within IoT- oriented smart cities," IEEE Access, vol. 9, pp. 34165–34176, 2021, doi: 10.1109/ACCESS.2021.3061411.

[15]. M. Pawlak, A. Poniszewska-Marańda, and N. Kryvinska, "Towards the intelligent agents for blockchain e-voting system," Proc. Com- put. Sci., vol. 141, pp. 239–246, Jan. 2018, doi: 10.1016/j.procs.2018. 10.177.

[16]. D. Chaum, A. Essex, R. Carback, J. Clark, S. Popoveniuc, A. Sherman, and P. Vora, "E-voting 40 scantegrity: End-to-end voter- verifiable optical-scan voting," IEEE Secur. Privacy, vol. 6, no. 3, pp. 40–46, May 2008. Accessed: Feb. 14, 2021. [Online]. Available: https://www.computer.org/security/

[17]. P. McCorry, S. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in Financial Cryptography and Data Security. Sliema, Malta: Springer, 2017, pp. 357–375, doi: 10.1007/978-3-319-70972-7_20.

[18]. N. Braun, S. F. Chancellery, and B. West. "E-Voting: Switzerland's projects and their legal framework–In a European context", Electronic Voting in Europe: Technology, Law, Politics and Society. Gesellschaft für Informatik, Bonn, pp.43-52, 2004.

[19]. NirKshetri,JeffreyVoas,"Blockchain-EnabledE-Voting".

[20]. Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A. and Vora, P. (2008)."Scantegrity: End-to-end voter-veriable

optical- scan voting.", IEEE Security Privacy, vol. 6, no. 3, pp. 40-46, May 2008.

Cite this article as :

Ardon Kotey, Keya Gupta, Jahanvi Agarwal, Prof. Harshal Dalvi, Prof. Neha Khatre, "VoteCoin : A Blockchain Perspective on E-Voting Infrastructure", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 6, pp.87-97, November-December-2023.
Available at doi :
https://doi.org/10.32628/CSEIT2390615
Journal URL : https://ijsrcseit.com/CSEIT2390615