Blockchain-Based Architecture And Smart Contract For E-Voting

Diwan Chand[1], Jawahar Thakur[2]
[1, 2] Dept of computer science
[1, 2] Himachal Pradesh University Shimla -171005

Abstract- *A smart contract serves as a digital ledger or agreement between two entities or nodes, that helps to outline specific rules and regulations for successful transactions. In tandem, blockchain technology creates a decentralized and distributed environment, fostering trust and security without any need for central managing and controlling authority, Unlikethe traditional system, blockchain operates without a central controller, offering autonomy and transparency. BTC (bitcoin) is an example of Blockchain based smart-contract.*

This research aims to implement smart (chain code) ad devise a robust architecture for blockchain-based e-voting, revolutionizing the voting process. The utilization of smart contracts in the Blockchain voting system is facilitated through three platforms, namely Ganache, Metamask, and Remix IDE. While these platforms are open-source, they offer limited access to task demonstrations.

Blockchain technology has demonstrated significant data security, reliability, and decentralization achievements. Embracing these advantages, the proposed contracts' blockchain-based architecture and smart contracts for e-voting reduce voters' transaction processing time while providing a secure environment for storing voting records, thus enhancing overall security.In summary, the primary focus of this paper is to harness the power of smart contracts and blockchain technology to create an efficient, transparent, and secure e-voting system. By embracing the decentralized nature of blockchain, we establish a trustworthy and reliable environment for voters, paving the way for the future of democratic processes.

Keywords- Blockchain, Ethereum, Solidity, Smart-contract, Chain code

I. INTRODUCTION

Now a days, various types of elections are held in every country.It may befrom a superficial level to a challenging level like universities students' unions, presidents' elections, etc. for celebrating this festival voters cast ballots for the election of their choice. The election is an inherently democratic process that acts as a medium for public sovereignty. An election's outcome substantially impacts the credibility of any work or organization[1]. Therefore, elections must be legitimate and credible. The foundation of every established country depends on its electoral system, which allows residents to choose the most deserving candidates. Every voter who goes to the pools and shows their voter card to the committee ad election supervisors to access whether their choice is valid as a viable alternative following the disaster[2].

However, currently, the management of the voting systems is centralized or controlled by a single organization (election commission). Which usually creates errors in the electoral process .Many developing nations have a history of difficulty, mistakes, and abuse of power, which has led to a lack of confidence and legitimacy in elections with excessive news coverage of vote tampering, hooliganism, and machine hacking, leading to a loss of trust and legitimacy in elections[3].To reduce these things, everyone has to take immediate action, everyone has to change a system that establishes a reliable, open, and decentralized election environment[4].

By using an alternative method, it is possible to mitigate the shortcomings of the current electronic voting system and paper voting system. A new technology called Blockchain, which started in 2008, is known for some of its unique features Blockchain provides a variety of features such as voter privacy, and verifiability[5]. It allows the use of smart contractswith special algorithms and esoteric features such as SHA256 encryption, and MD5 in the blockchain[6]. After the creation of Bitcoin by Santoshi Nakamoto, this technology has presented a great example of distributed technology[7].Creating a wave or impact can be achieved through the utilization of blockchain, a decentralized and immutable technology that enhances data security and reduces the risk of fraud. Blockchain finds applications across diverse sectors like finance, healthcare, education, industry, and voting. Several countries, including India, have initiated efforts to explore blockchain initiatives[8]. The development of smart contracts involves open-source technologies such as Ethereum and Hyperledger, offering decentralized environments and utilizing programming languages like

Solidity (for Ethereum) and Chaincode (for Hyperledger)[9]. To facilitate smart contract creation and kill advancement, developers often employ tools like Ganache, MetaMask, Kaleido, and Remix IDE in conjunction with the Ethereum platform.

Methods/Experimental:

This paper sets out to examine the transformative effects of blockchain on real-time voting systems. The Blockchain voting system, being decentralized and transparent, holds the promise of ensuring voter protection. With the implementation of blockchain-based electronic voting, the process of vote counting becomes tamper-proof, yet individual voter identities remain anonymous. The research employs diverse methodologies to explore and validate the effectiveness of blockchain technology in revolutionizing voting systems. Below, we outline some of the key methodologies utilized in this comprehensive investigation.

Adopted Research:

By Integrating Blockchain technology into voting and election processes, a sophisticated blend of technological advancement is achieved, enabling the analysis of voting procedures and the creation of robust predictive models. To gain comprehensive insights into this domain, both descriptive and qualitative research methods are expertly employed, effectively addressing potential security concerns[10]. As a result, the implementation of blockchain ensures a secure and trustworthy voting and election procedure, instilling confidence in every user and safeguarding the integrity of the democratic process.

Tools and Techniques:

The research encompasses three pivotal phases, each systematically advancing the study. Phase 1 delves into exploration, comprehensively understanding the current voting system and its inherent challenges. In Phase 2, and initial design I formulated, drawing from diver subject matter expertise and cutting-edge technology, with a strong focus on blockchain. Finally, Phase 3 culminates in the practical execution of the study, manifesting through the architecture and implementation of smart contracts tailored for blockchain-based voting.

Ethereum: At the heart of this research lies Ethereum, a globally accessible open-source platform. It can underpin the innovative blockchain network, enabling decentralized financial transactions and fostering an inclusive, open financial ecosystem for all participants[11].

Solidity: Solidity, is a high-level contract-oriented language inspired by well-known programming languages. including C, C++, Python, and JavaScript, plays a pivotal role in scripting within the Ethereum Virtual Machine (EVM).Itremains an indispensable tool for creating robust smart contracts[12].

Hyperledger: In the realm of open-source communities, Hyperledger stands out as an invaluable platform, offering bundles opportunities for developing blockchain-based solutions tailored to various business domains worldwide[13]. Its unique emphasis on industry-specific application standing clauses sets it apart as a powerful resource.

Critical tools and technologies utilized in this research include:

1. Smart contract programming: The indispensable programming language solidity, Viper and Rust are utilized for crafting smart contract code[14], renowned for their EVM compatibility and pivotal role in powering voting platforms.
2. Libraries and Oracles: Remix IDE emerges as a notable tool for creating smart contracts, empowering researchers to incorporate unique functionalities seamlessly. The utilization of Remix IDE oracles serves as a fundamental component in the infrastructure of nearly all smart contracts[15], bridging the gap between blockchain and real-world data through off-chain support.

This fusion of methodologies and cutting-edge tools ensures a comprehensive and successful exploration of the blockchain's transformative potential a secure and trustworthy democratic process that inspires confidence among all stockholders involved democratic process.

Classification of Blockchain:Blockchain can be categorized based on its architectural features and authentication models, divided into permissionless (public) and permissioned (private) types.

In a public blockchain, any user can join the network ad actively participate in the consensus process to both submit and validate transactions. However, these blockchains often suffer from high computational needs due to the involvement of a large number of participants ad complex consensus methods like proof of work (POW)[16]. Bitcoin serves as a prime example of a permissionless blockchain, open to unrestricted usage by anyone who complies with its regulations. Public blockchains are transparent ad accessible

for review by anyone, earning them the name of public blockchains[17].

On the other hand, private blockchains operate oppositely. AS permission network, central organizations are responsible for authenticating each peer before granting access to the P2P network. Private blockchains, such as Ripple, leverage their industry expertise to guide optimal blockchain consensus procedures[18]. In permissioned blockchains, only trusted nodes can execute transactions, ensuring a restricted communication network among legitimate participants[19].

A consortium blockchain offers a middle ground, combining elements of both permissioned and permissionless blockchains[19]. It permits a limited number of nodes to partake in distributed consensus, making it ideal for various industries like banking. While consortium blockchains are partially accessible to the general public, they remain centralized in diverse sectors, including insurance firms, banks, and governmental organizations, which can open up to public access while still maintaining centralized trust[20]

In summary, blockchain's classification into portionless, permissioned, and consortium types offers a versatile range of applications across different sectors, providing varying degrees of decentralization and accessibility while ensuring secure and efficient transaction processing.

Table:1 Comparison of blockchain networks

Blockchain Type	Public	Private	Hybrid	Consortium
Algorithms	PoW, PoS, CloudPoS	PoET, Raft, PoA, PoM	PoV, PoT	BFT Raft, pBFT
Smart Contract	Yes	Yes	–	Yes
Permission Required	Yes	Yes	No	Yes
Advantages	Open Environment, anonymity	High Security, Triple-entry Accounting	Transactions are cheap and fast	It offers access control

Characteristics of Blockchain Technology:

Blockchain exhibits several key characteristics that make it a robust technology for variousapplications

Decentralizations: -Blockchains operate in a decentralized manner, allowing all participants on the network to participate in validating transactions[21]. This distributed nature ensures that the blockchain does not rely on a single centralized authority.

Traceability: - With all participants having access to copies of transactions recorded in the ledger, blockchain enables easy auditability. Data transfer (transactions) for specific blockchain addresses can be verified by network participants[22].

Tamper-Proof: -The immutability of the blockchain ensure that once a record is added, it cannot be altered without consensus from the majority of network users[23]. This tamper-proof feature enhances the integrity and reliability of the blockchain.

Transparency: -In public blockchain frameworks like Bitcoin and Ethereum, the recorded data in the ledgers is transparent to all participants since they possess access rights. This transparency fosters trust and accountability in the system[23]. The subsequent section of this essay provides an overview of blockchain-based voting, analyzing a recent paper on blockchain technology, proposing an architecture for electronic voting, and depicting the implementation of a smart contract for electronic voting. Smart contracts, benefiting from the permanence of blockchain ledgers, can effectively record changes and data operations. The study then delves into the results and analysis, culminating with a conclusion and a glimpse into the future potential of e-voting and smart contracts for blockchain-based voting.

By leveraging the powerful characteristic of blockchain technology, electronic voting can be revolutionized to become more secure, transparent, and efficient, paving the way for a more democratic and inclusive voting process.

II. RELATED REVIEW

Dagher, G. et al.present Broncovote, a novel blockchain-based voting system designed to uphold voter privacy, accessibility, transparency, security, and cost efficiency. By leveraging the Ethereum blockchain and mat contract technology, Broncovote establishes a university-scaled voting platform that guarantees auditable voting records and efficient voter administration. The system incorporates various cryptographic techniques, including homomorphic encryption, to safeguard voter privacy during the voting process. To assess its usability, scalability, and efficiency, Broncovote underwent rigorous testing on the Ethereum Testnet[24].

Garg, K. et, al. This paper introduces a decentralized voting system aimed at simplifying, securing, and anonymizing the voting process for the public. Through an empirical review of the existing voting system, this study sheds light on the challenges faced by traditional approaches. By delving into various methodologies in voting, this research provides valuable insights into the development of the proposed system[25].

Knirsch, F et.al.This paper explores the practical application of blockchain technology in the energy industry, specifically focusing on the trading of photovoltaic power pants using a custom private blockchain. The researchers present a comprehensive architectural overview and delve into specific aspects of their implemented system, designed to address security liabilities in idle chains through the innovative approach of mining empty blocks, etc[26].

Patidar, K et.al.This paper explores the application of blockchain technology to address the limitations of existing e-voting systems. The study presents an overview of various blockchain frameworks for e-voting and highlights the implementation of a blockchain-based e-voting system using Ethereum's smart contracts. The truffle framework is employed for the development, testing, and deployment of Smart contracts, while Ganache servers as the Ethereum client for testing purposes. Additionally, the paper utilizes MetaMask as a browser wallet to enhance the security and user experience of the e-voting system[27].

Pramulia, D et, al.This paper presents the design and implementation of a blockchain-based e-voting system using Ethereum and Metamask, aiming to address security and trust issues prevalent in traditional e-voting systems. The proposed system offers enhanced transparency, but the study also identifies potential vulnerabilities where input data in vote transactions could be correlated through reverse engineering techniques[28].

Kaudare et al. in this research study, the authors conduct a comparative analysis between Ethereum and Hyperledger for the development of a blockchain-based electronic voting system. The system, implemented using Hyperledger, ensures secure elections while preserving user privacy. The study's findings indicate that Hyperledger Outer performs Ethereum in various performance metrics, making it a more efficient choice. Furthermore, the use of permissioned chains in the system allows voters to maintain their anonymity, enhancing voter privacy during the voting process [29].

Yi, H. In this paper, the author addresses the pressing need for secure e-voting and explores the use of blockchain technology in a peer-to-peer (P2P) network to enhance e-voting security. The proposed solution includes three key components:

1. A synchronized model of voting records-baseddistributed ledger technology (DLT) to prevent vote forgery.
2. A user credential model using elliptic curve cryptography (ECC) to ensure authentication and non-reputation[30].
3. A withdrawal mechanism that enables voters to modify their votes before the pacified deadline. The research contributes to the growing interest in sure e-voting within the communication and networking domain, showcasing how blockchain technology can be leveraged to meet the essential requirements of the e-voting process.meets the essential requirement of the e-voting process. Secure e-voting is very urgent and has become a popular topic in the area of communication and networking[31]. They present technology to exploit blockchain in a P2P network to improve the security of e-voting. First, he designed a synchronized model of voting records based on distributed ledger technology (DLT)it avoid forgery of votes, he designs a user credential model based on elliptic curve cryptography (ECC) to provide authentication and non-repudiation, third they design a withdrawal model that allows the voter to change their vote before the present deadline [31]-[32].

Friorik P. Hajalmarsson, et al.This paper presents a proposal for a Blockchain-Based E-voting System, developed to overcome the limitation of the existing voting systems concerning transparency, flexibility, fairness, and privacy. The study explores distributed ledger technologies and demonstrates the implementation of blockchain-based application security for nationwide elections[33].

III. PROPOSED BLOCKCHAIN ARCHITECTURE FOR E-VOTING

Blockchain technology plays a pivotal role in the e-voting system, and a proposed blockchain architecture is presented in Figure 1, organized into three levels of phases:

User Phase/ Client Phase:

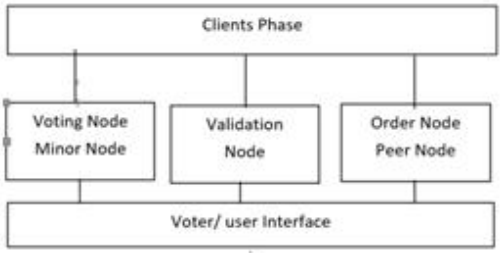

Figure 1. Client/User Phase

In this phase, multiple electronic systems and devices interact with the blockchain-based electronic voting process as

peer nodes. These devices participate in the e-voting blockchain through smart contracts, commonly known as “Chain Code” in Hyperledger Fabric. The user phase encompasses several nodes, each assigned distinct duties and functions crucial to the success of this phase.

A) Electronic Voting Nodes:The primary objective of blockchain technology in this type of node is to enable voters to verify their identities, cast their ballots securely, and record all voting transactionson the blockchain.
B) Administrator/Minor Nodes:These nodes hold the specific authority or power to mine new blocks. They regulate the degree of access control for certain nodes, granting authorization for transactions and other essential operations [34].
C) Validator or Vote Validation Nodes:These nodes are responsible for validating votes. They authenticate new information and verify its details to ensure the legitimacy of transactions [34].
D) Committing Nodes:The committing nodes are tasked with performing validation and confirmation of new blocks in the blockchain, ensuring the integrity and consistency of the voting data [34].

In summary, the proposed blockchain architecture Figure 2. demonstrates a robust framework for an e-voting system, where various nodes collaborate to provide transparency, security, and efficiency in the voting process.

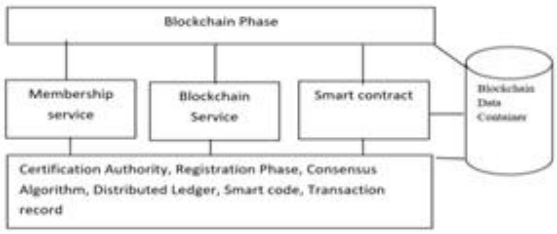

Figure 2. Proposed Architecture Blockchain e-voting**.**

Blockchain-BasedPhase: The most crucial phase in this structure is the Blockchain phaseFigure 3, also known as the interfacing phase, which provides essential functionalities for the e-voting system. This phase offers various services, including Membership Service, which involves Certification Authorities, Voter Registration, Protocols Configuration, and Identity Management, ensuring that only authorized users can participate in the voting process[35].

The heart of the Blockchain phase is the blockchain Service, encompassing Decentralization P2P Protocol, Consensus Algorithm Manager, and Distributed Ledger. These components ensure the decentralized and secure nature of the e-voting system, maintaining a consensus among nodes and an immutable and transparent ledger of votes.

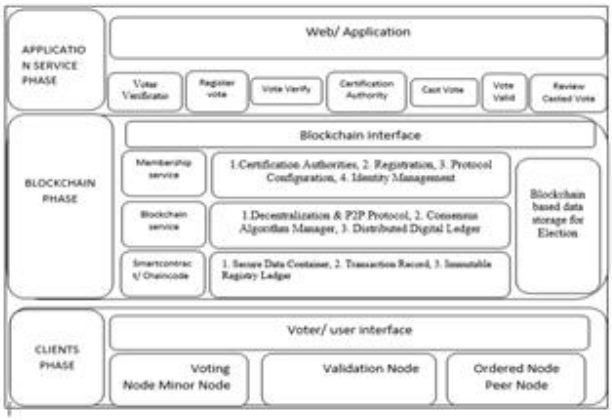

Figure 3. Blockchain Phase

The Smart Contract/Chaincode step involves writing actual data or code using suitable programming languages and storing real-time data. It utilizes smart contracts or Chaincode to facilitate secure data containers, transaction records, and an immutable registry ledger, enduring the integrity of the voting process[36].

Furthermore, Blockchain-Based Data Storage for Elections provides tamper-proof, secure, and transparent cloud-based storage for blockchain transactions. Only authorized users or valid individuals can access voter details, ensuring the validity of the voting process.

Application Phase: In the Application Phase, acting as the front end of the e-voting process, voters interact with the system to cast their votes. This phase comprises steps such as Register Vote, Voter Verification, Certification, and Reviewing the Casted Vote. It presents a user-friendly interface, allowing users to see an actual representation and overview of the e-voting framework[37].

Figure 2 illustrates the cycle of the Blockchain Application Phase, showing the seamless flow of action and interactions between the user and the blockchain-based e-voting system.

Figure 4. The cycle of the Application phase

IV. SMART CONTRACT IMPLEMENTATION FOR BLOCKCHAIN-BASED E-VOTING

It seems like the paragraph describes the implementation and evaluation of a web-based platform for e-voting using blockchain technology and smart contracts. The platform utilizes the Remix IDE for smart contracts development, and the transactions are deployed and executed on the Ganache blockchain network with MetaMask serving as a gateway for user transactions[38]. The main goal of the evaluation is to assess the system's performance based on the requirements for e-voting.

The evaluation process includes several steps:

Carrying out several transactions: This involves simulating the voting process by executing multiple transaction representationsrepresenting a vote cast by a voter.

Verifying each transaction: After a transaction is executed, it needs to be verified to ensure its accuracy and validity. This verification step is crucial to maintaining the integrity of the voting process.

Mining transactions into the blockchain: Once transactions are verified, they are grouped into blocks and added to the blockchain through a process called mining. Mining helps in achieving consensus and securing the network.

Reflecting changes to all nodes: in a decentralized blockchain network, changes made to the public ledger (e.g., adding new blocks) are propagated to all nodes in the network. This ensures that every participant has access to the same information[39]

Testing system usability: The evaluation also involves assessing the usability of the e-voting system, focusing on its effectiveness and fluency in terms of user experience. This could include aspects like ease of use, responsiveness, and user satisfaction.

Overall, the evaluation aims to validate whether the e-voting system meets the requirements of security.

Figure5. Code for Smart contract

In the test run mode, the e-voting system utilizes Multichain as the underlying blockchain framework, starting with the creation of nodes[40]. These nodes can be considered a voter in the context of the e-voting system. Multichain, by default, is primarily designed for cryptocurrency operations, but in this case, it is adapted to handle smart contracts for voting purposes as shown in Figure4.

To perform transactions (votes) in Multichain, the system identifies the address and balance associated with each node's Multichain wallet[41]. Each node's address represented a unique identifier, similar to an account number, and the balance reflects the amount of currency or tokens held in that address.

When a voter casts a vote, a transaction I initiated in Multichain. The vote (transaction) is sent from the voter's address to the designated recipient, which could be the candidate or a specific contract address representing the vote[41]. This transaction Is recorded on the blockchain, ensuring transparency, security, and immutability of the voting process.

The e-voting system utilizes a smart contract, the details of which are presented in Figure5 the smart contract is programmed to handle the voting process, including voter verification, ballot casting, and recording the votes on the blockchain. This ensures that the voting process is decentralized, transparent, and tamper-proof[42].

```
pragma solidity >=0.7.0 <0.9.0;
contract Ballot {
                    struct Voter {
                   uint weight;
                    bool voted;
                   address delegate;
                   uint vote;
                    }
```

```
   struct Proposal {

                    bytes32 name;
                   uintvoteCount;
            }

                   address public chairperson;

          mapping(address => Voter) public voters;

          Proposal[] public proposals;
   constructor(bytes32[] memory proposalNames) {
                 chairperson = msg. sender;
                   voters[chairperson].weight = 1;

          for (uinti = 0; i<proposalNames.length; i++) {

          proposals.push(Proposal({
            name: proposalNames[i],
voteCount: 0
          }));
              }
            }
function giveRightToVote(address voter) public {
require(
msg.sender == chairperson,
          "Only the chairperson can give the right to vote."
       );
require(
!voters[voter].voted,
          "The voter already voted."
       );
       require(voters[voter].weight == 0);
       voters[voter].weight = 1;
   }



   function delegate(address to) public {
       Voter storage sender = voters[msg.sender];
require(!sender.voted, "You already voted.");
require(to != msg.sender, "Self-delegation is disallowed.");

       while (voters[to].delegate != address(0)) {
          to = voters[to].delegate;


require(to != msg.sender, "Found loop in delegation.");
       }
sender.voted = true;
sender.delegate = to;
       Voter storage delegate_ = voters[to];
       if (delegate_.voted) {
   proposals[delegate_.vote].voteCount += sender.weight;
       } else {

delegate_.weight += sender.weight;
       }
   }

   function vote(uint proposal) public {
       Voter storage sender = voters[msg.sender];
require(sender.weight != 0, "Has no right to vote");
require(!sender.voted, "Already voted.");

sender.voted = true;
sender.vote = proposal;



       proposals[proposal].voteCount += sender.weight;
   }
   function winningProposal() public view
          returns (uintwinningProposal_)
   {
uintwinningVoteCount = 0;
       for (uint p = 0; p <proposals.length; p++) {
          if (proposals[p].voteCount>winningVoteCount) {
winningVoteCount = proposals[p].voteCount;
winningProposal_ = p;
       }
   }
   function winnerName() public view
          returns (bytes32 winnerName_)
   {
winnerName_ = proposals[winningProposal()].name;
}
```

In summary, the test run mode of the e-voting system using Multichain involve creating node (representing voters), using smart contracts to facilitate voting, and performing transaction (votes) on the blockchain by sending them from the voter's address to the designated recipient.

V. RESULTS AND DISCUSSIONS

In the proposed architecture for blockchain-based electronic voting, the voting process is efficiently managed using smart contracts and a bespoke smart contract API. When a voter casts a vote, a unique transaction hash is generated, representing the vote transfer to the candidate's address. This transaction is then added to the public ledger and mined, ensuring its legitimacy and immutability.

They maintain the integrity of the voting process; the smart contract API restricts the safeguarding them from the

third-party interface. Voters can conveniently log in with their blockchain-based voting IDs from any location with an internet connection, providing flexibility and accessibility.

Furthermore, the application or web service stage offers an interactive interface for voters to examine their already cast votes This feature allows voters to verify that votes were accurate adding transparency and confidence to the voting process.

Overall, this blockchain-based electronic voting architecture streamlines vote to process ensures security and transparency, and provides a user-friendly experience for voters. Number votes per address. This prevents the casting of repeated votes from the same address, except in the case of candidates. This mechanism helps ensure fairness and accuracy in the voting system.The use of various encryption mechanisms in the Blockchain phases enhances the security of the voter's identification and information.

Figure 6. displays a straightforward transaction inside the proposed system. For transaction records, the ganache and online platform provide ten dummy accounts which are very useful for testing whether the transaction properly works or not in the figure we transact many truncations during the voting process this table shows how many blocks (voters) are there and how voted or not, etc.

Figure6. Transaction Smart-contract for e-voting

The table 2. shows the result of the smart contract, and Figure 7. Show the result isbased on gas prize gas cost voting time and processing time in Ethereum Network.

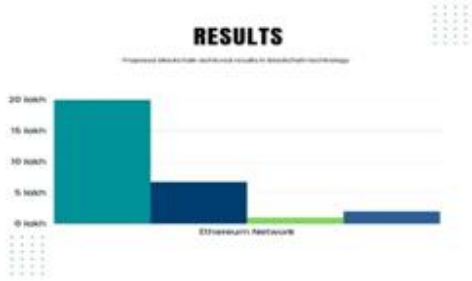

Figure 7. Gas and Processing time

VII. CONCLUSIONS

A Blockchain-based voting system presents a promising solution to address several critical issues in voting, such as vote tampering, non-reusability, correctness, and immutability, ensuring precise and reliable voting operations. The system leverages blockchain technology's distributed data storage, which ishighly regarded for its decentralized nature and the paramount importance of transparency in voting processes. This article proposes a straightforward, easy-to-understandsmart contract architecture based on blockchain principles.

Table: 2 Proposed Archived Results

Method	Platform	Gas prize	Used Gas Cost per Block	Voting Time	Processing Time
Smart Contract	Ethereum Network	20000000000	672195	1 sec	2 sec

The transaction processes within this design are designed to be transparent and easily comprehensible, contributing to user trust and confidence in the voting system's integrity. Moreover, the suggested design prioritizesefficiency, aiming to accelerate activities while minimizing memory and time consumption.

Post-voting, voters are provided with the capability to observe and verify the entire voting process, fostering transparency and accountability. This feature that their ballots are accurately recorded and counted.

Looking to the future, blockchain voting systems are anticipated to evolve using diverse platforms such as Hyperledger Fabric, Visual Studio Code, and Remix IDE sophistication and versatility of blockchain-based voting systems.

In conclusion, the proposed Blockchain-based voting system offers a compelling solution to critical voting challenges, emphasizing transparency, reliability, and user-friendliness.

This technology contributes to developingan even more robust and innovative blockchain voting system.

REFERENCES

[1] S. S. Bush and L. Prather, “The promise and limits of election observers in building election credibility,” *J. Polit.*, vol. 79, no. 3, pp. 921–935, 2017, doi: 10.1086/691055.

[2] R. Bauböck, “Stakeholder citizenship and transnational political participation: A normative evaluation of external voting,” *Fordham Law Rev.*, vol. 75, no. 5, pp. 2393–2447, 2007.

[3] A. Wicaksana and T. Rachman, “済無No Title No Title No Title,” *Angew. Chemie Int. Ed. 6(11), 951–952.*, vol. 3, no. 1, pp. 10–27, 2018, [Online]. Available: https://medium.com/@arifwicaksanaa/pengertian-use-case-a7e576e1b6bf

[4] U. Jafar, M. J. A. Aziz, and Z. Shukur, “Blockchain for electronic voting system—review and open research challenges,” *Sensors*, vol. 21, no. 17. MDPI, Sep. 01, 2021. doi: 10.3390/s21175874.

[5] H. Al-Breiki, M. H. U. Rehman, K. Salah, and D. Svetinovic, “Trustworthy Blockchain Oracles: Review, Comparison, and Open Research Challenges,” *IEEE Access*, vol. 8, pp. 85675–85685, 2020, doi: 10.1109/ACCESS.2020.2992698.

[6] “immplement unique certification authntication.pdf.”

[7] R. Tonelli, M. I. Lunesu, A. Pinna, D. Taibi, and M. Marchesi, “Implementing a Microservices System with Blockchain Smart Contracts.”

[8] P. Dutta, T. M. Choi, S. Somani, and R. Butala, “Blockchain technology in supply chain operations: Applications, challenges and research opportunities,” *Transp. Res. Part E Logist. Transp. Rev.*, vol. 142, no. July, p. 102067, 2020, doi: 10.1016/j.tre.2020.102067.

[9] V. Brown, “Introduction of solidity,” *CryptoStars*, 2022. https://blog.cryptostars.is/introduction-to-solidity-remix-i-d-e-16ca6609db66

[10] D. Skarbek, “Qualitative research methods for institutional analysis,” *J. Institutional Econ.*, vol. 16, no. 4, pp. 409–422, 2020, doi: 10.1017/S174413741900078X.

[11] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H. N. Lee, “Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract,” *IEEE Access*, vol. 10, pp. 6605–6621, 2022, doi: 10.1109/ACCESS.2021.3140091.

[12] P. Hegedűs, “Towards Analyzing the Complexity Landscape of Solidity Based Ethereum Smart Contracts,” *Technologies*, vol. 7, no. 1, 2019, doi: 10.3390/technologies7010006.

[13] A. A. Amponsah, A. F. Adekoya, and B. A.Weyori, “Blockchain in Insurance: Exploratory Analysis of Prospects and Threats,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 1, pp. 445–466, 2021, doi: 10.14569/IJACSA.2021.0120153.

[14] K. J. Fandl, “Can smart contracts enhance firm efficiency in emerging markets?,” *Northwest. J. Int. Law Bus.*, vol. 40, no. 3, pp. 332–362, 2020.

[15] H. Al Breiki, L. Al Qassem, K. Salah, M. Habib Ur Rehman, and D. Sevtinovic, “Decentralized access control for IoT data using blockchain and trusted oracles,” *Proc. - IEEE Int. Conf. Ind. Internet Cloud, ICII 2019*, no. November, pp. 248–257, 2019, doi: 10.1109/ICII.2019.00051.

[16] H. Wang, Z. Zheng, S. Xie, H. N. Dai, and X. Chen, “Blockchain challenges and opportunities: a survey,” *Int. J. Web Grid Serv.*, vol. 14, no. 4, p. 352, 2018, doi: 10.1504/ijwgs.2018.10016848.

[17] J. Dattani and H. Sheth, “Overview of Blockchain Technology,” *Asian J. Converg. Technol.*, vol. V Issue I, [Online]. Available: https://dev.to/damcosset/blockchain-what-is-in-a-block-48jo

[18] B. Koteska, E. Karafiloski, A. Mishev, and U. S. Cyril, “Blockchain Implementation Quality Challenges: A Literature Review.”

[19] M. Liu, K. Wu, and J. J. Xu, “How Will Blockchain Technology Impact Auditing and Accounting: Permissionless versus Permissioned Blockchain,” *Curr. Issues Audit.*, vol. 13, no. 2, pp. A19–A29, 2019, doi: 10.2308/ciia-52540.

[20] M. Hölbl, M. Kompara, A. Kamišalić, and L. N. Zlatolas, “A systematic review of the use of blockchain in healthcare,” *Symmetry (Basel).*, vol. 10, no. 10, 2018, doi: 10.3390/sym10100470.

[21] J. Zarrin, H. Wen Phang, L. Babu Saheer, and B. Zarrin, “Blockchain for decentralization of internet: prospects, trends, and challenges,” *Cluster Comput.*, vol. 24, no. 4, pp. 2841–2866, 2021, doi: 10.1007/s10586-021-03301-8.

[22] T. Mitani and A. Otsuka, “Traceability in Permissioned Blockchain,” *IEEE Access*, vol. 8, pp. 21573–21588, 2020, doi: 10.1109/ACCESS.2020.2969454.

[23] A. Iftekhar, X. Cui, M. Hassan, and W. Afzal, “Application of Blockchain and Internet of Things to Ensure Tamper-Proof Data Availability for Food Safety,” *J. Food Qual.*, vol. 2020, 2020, doi: 10.1155/2020/5385207.

[24] T. M. Hewa, Y. Hu, M. Liyanage, S. S. Kanhare, and M. Ylianttila, “Survey on Blockchain-Based Smart Contracts: Technical Aspects and Future Research,” *IEEE Access*, vol. 9. Institute of Electrical and Electronics Engineers Inc., pp. 87643–87662, 2021. doi: 10.1109/ACCESS.2021.3068178.

[25] Institute of Electrical and Electronics Engineers, *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*.

[26] F. Knirsch, A. Unterweger, and D. Engel, "Implementing a blockchain from scratch: why, how, and what we learned," *Eurasip J. Inf. Secur.*, vol. 2019, no. 1, Dec. 2019, doi: 10.1186/s13635-019-0085-3.

[27] K. Patidar and S. Jain, "Decentralized E-Voting Portal Using Blockchain."

[28] D. Pramulia and B. Anggorojati, "Implementation and evaluation of blockchain based e-voting system with Ethereum and Metamask," in *Proceedings - 2nd International Conference on Informatics, Multimedia, Cyber, and Information System, ICIMCIS 2020*, Institute of Electrical and Electronics Engineers Inc., Nov. 2020, pp. 18–23. doi: 10.1109/ICIMCIS51567.2020.9354310.

[29] [T. Adekeye, "Securing the Electoral E-Voting System Using Blockchain Technology," *Researchgate.Net*, no. January, 2022, [Online]. Available: https://www.researchgate.net/profile/Taiwo-Adekeye-4/publication/357811593_Securing_the_Electoral_E-Voting_System_Using_Blockchain_Technology/links/61e095f28d338833e368d03d/Securing-the-Electoral-E-Voting-System-Using-Blockchain-Technology.pdf

[30] M. Y. Alshahrani, "Implementation of a blockchain system using improved elliptic curve cryptography algorithm for the performance assessment of the students in the e-learning platform," *Appl. Sci.*, vol. 12, no. 1, 2022, doi: 10.3390/app12010074.

[31] Y. Abuidris, R. Kumar, and W. Wenyong, "A survey of blockchain based on e-voting systems," *ACM Int. Conf. Proceeding Ser.*, no. December, pp. 99–104, 2019, doi: 10.1145/3376044.3376060.

[32] S. Sharma and A. Ganpati, "Detection of VN Attack in Iot Using Trust-Based Technique," vol. 8, no. 12, 2022.

[33] F. P. Hjalmarsson, G. K. Hreioarsson, M. Hamdaqa, and G. Hjalmtysson, "Blockchain-Based E-Voting System," in *IEEE International Conference on Cloud Computing, CLOUD*, IEEE Computer Society, Sep. 2018, pp. 983–986. doi: 10.1109/CLOUD.2018.00151.

[34] O. Daramola and D. Thebus, "Architecture-centric evaluation of blockchain-based smart contract E-voting for national elections," *Informatics*, vol. 7, no. 2, Jun. 2020, doi: 10.3390/informatics7020016.

[35] U. C. Çabuk, E. Adıgüzel, and E. Karaarslan, "A Survey on Feasibility and Suitability of Blockchain Techniques for the E-Voting Systems," *IJARCCE*, vol. 7, no. 3, pp. 124–134, Mar. 2018, doi: 10.17148/ijarcce.2018.7324.

[36] K. B. Nawari O Nawari and S. Ravindran, "Blockchain technology and BIM process: review and potential applications," 2019. [Online]. Available: http://www.itcon.org/2019/12

[37] R. H. Sahib and E. S. Al-Shamery, "A Review on Distributed Blockchain Technology for E-voting Systems," in *Journal of Physics: Conference Series*, IOP Publishing Ltd, Mar. 2021. doi: 10.1088/1742-6596/1804/1/012050.

[38] A. K. Yadav and R. K. Bajpa, "KYC Optimization using Blockchain Smart Contract Technology," *Int. J. Innov. Res. Appl. Sci. Eng.*, vol. 4, no. 3, pp. 669–674, 2020, doi: 10.29027/ijirase.v4.i3.2020.669-674.

[39] H. Yi, "Securing e-voting based on blockchain in P2P network," *Eurasip J. Wirel. Commun. Netw.*, vol. 2019, no. 1, Dec. 2019, doi: 10.1186/s13638-019-1473-6.

[40] H. Hassan, R. Hassan, and E. Gbashi, "E-voting System Based on Ethereum Blockchain Technology Using Ganache and Remix Environments," *Eng. Technol. J.*, vol. 41, no. 4, pp. 1–16, 2023, doi: 10.30684/etj.2023.135464.1273.

[41] G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework," *White Pap.*, vol. 21, no. 2327, p. 4662, 2016, [Online]. Available: https://assets.polkadot.network/Polkadot-whitepaper.pdf

[42] Y. Soni, L. Maglaras, and M. A. Ferrag, "Blockchain based voting systems," *Eur. Conf. Inf. Warf. Secur. ECCWS*, vol. 2020-June, pp. 241–248, 2020, doi: 10.34190/EWS.20.122.