IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

E-VOTING:DECENTRALIZED VOTING SYSTEM BASED ON ETHEREUM BLOCKCHAIN TECHNOLOGY

[1]K.Varalakshmi,[2] S.R.HareeshAnand ,[3]GoddumuriRaju, [4]B.Kamalesh
[1]Assist Professor,[2,3,4]students,
Department of Computer Science and Engineering
PERI Institute of Technology, Chennai, India

ABSTRACT*:* Democratic voting is a crucial and serious event in anyplace, the current election scheme in any place, beita school college, or even a country is done through ballot papers or using EVM. This process has many disadvantages such as transparency, low voter turnout, vote tampering, lack of trust in electoral authorities,delayinresults,andaboveallsecurityissues.Sothegrowingdigitaltechnologyhashelpedmany people's lives nowadays. The concept of electronic voting is introduced to combat the disadvantages of the traditional voting system. Electronic voting is essentially an electronic means of casting and counting votes. It is an efficient and cost-effective way of conducting a voting procedure that isdata-rich and real-time and requires high security. Nowadays, concerns about the security of networks and the privacy of communicationsforelectronicvotinghaveincreased.Thus,theprovisionofelectronicvotingisveryurgent and is becoming a popular topic in communication and networking. One way to solve security problems is blockchain.Thepaperproposesanewblockchain-basedelectronicvotingsystemthataddressessomeofthe limitations in existing systems and evaluates some of the popular block chain frameworks to create a blockchain-basedelectronicvotingsystem.Becausetheblockchainstoresitsdatainadecentralizedmanner, the implementation result shows that it is a practical and secure electronic voting system that solves the problemofvoteforgeryinelectronicvoting.Theblockchain-basedelectronicvotingsystemcanbedirectly applied to various network applications

INDEX TERMS: Distributed ledger technology(DLT),elliptic curve discrete logarithm problem(ECDLP), practical Byzantine fault tolerant (PBFT).

BLOCKCHAIN Online Voting system is a web-based voting system that will helps to manage your elections easily and more securely. This voting system can be used for casting votes during the elections held in colleges, etc. It uses face recognition technique to authenticate the user so problems for dummy entries will also be solved. So, thus this system gives the guarantee that no cheating can be done and the voting will be conducted easily where people don't have to go outside in order to cast their votes. Transparent transaction using Block chain technology increases the security of the transaction of crypto that races towards the cyber security. All the data is secure and verified. The encryption is done through cryptography to eliminate vulnerabilities such as unauthorized data tampering and this will increase the crypto payments. The main objective of the electronic voting technology intends to speed of the counting of ballots ,reduce the cost of paying staff to count votes manually and can provide improved accessibility for disabled voters. This can be achieved by designing and developing a software platform for voter registration, election voting, real-time election results collation and monitoring and mostly for remote voters access to elections. In a private block chain context, information is disseminated among participating no des referred to as peers. Each transaction undergoes confirmation through a consensus mechanism, which relies on the collective agreement of the majority of pee rnodes. However, this distributed architecture imposes certain constraints, particularly the necessity for any changes made by a single node to be promptly communicated to all other nodes in the network. Peer nodes bear the responsibility of appending new blocks to the chain and validating them. Only upon successful validation and agreement from the majority of nodes is a new block added to the blockchain, placing the decision- making authority regarding alterations or modifications squarely on the shoulders of peer nodes, rather than relying on a centralized system. Consensus mechanisms are categorized into competitive and non-competitive, with competitive consensus requiring adherence to a single consensus algorithm by all participating nodes. Examples include Proof-of-Work (PoW), Proof-of-Stake (PoS), and Delegated-Proof-of-Stake (DPoS),each plagued by issues such as double voting or double payment and performance uncertainties. Non-competitive consensus, however, allows for more flexibility, adjusting peer agreement and policies overtime, particularly suited for trusted environments where peer nodes can swiftly confirm and respond to agreements. Notably, the performance and uncertainty drawbacks of competitive consensus systems can be mitigated by employing the Practical Byzantine Fault Tolerance (PFBT) consensus algorithm.

Electronic voting, ore-voting ,entails a system where voters can electronically cast their ballots from any location through a secure ballot mechanism. The voting results are tabulated electronically and stored in a ledger or database, facilitating recounting as needed while addressing challenges such as voting queues and potential voter misconduct. This approach ensures the reliability ,transparency, and accuracy of the voting process and results, thereby enhancing the overall integrity of the electoral process.

A. RELATEDWORKS

In this section, various e-voting schemes leveraging block chain technology are examined along side their security strengths and vulnerabilities. Casado-Vara and Corchado (2018)proposed a block chain-based digital voting system to address limitations of traditional paper-based or electronic voting methods, albeit facing challenges like high bandwidth requirements and security concerns. Kotsiuba et al. (2018) introduced a decentralized e-health service platform using a private Exonum blockchain, while Yanovich et al. (2018) proposed a fast consensus algorithm based on Exonum, both susceptible to security breaches due to lack of encryption and anonymity measures.

In 2019, Any shchenko et al. presented a crypto token- based application on Exonum block chain, utilizing Tender mint consensus algorithm but deemed inferior to PBFT. Dhulavvagol et al. (2020) devised a digital e-voting system using block chain, smart contracts, and hashing techniques, aiming to ensure authenticity, privacy, and integrity of voting information. Sadiaetal.(2020)introduced a biometric and blockchain-based e-voting scheme, while Waheed et al. (2020) enhanced it with additional security measures such as encryption and hashing. RohandLee(2020) developed an e-voting system with PBFT algorithm on a private blockchain network, although vulnerable to key management issues and DoS attacks.

In2021,Jainetal.proposed"MATDAAN,"anEthereum- based e-voting system for its speed, reliability, and anonymity features, despite susceptibility to 51% attacks. Waheed et al. introduced an ECC-based sign cryption scheme for e-voting, addressing anonymity and security concerns but facing challenges in key distribution and decentralized implementation. Jumaa and Shakir(2022)proposed an ECC- based e-voting scheme on a public block chain, enhancing security mechanisms but still vulnerable to 51% attacks and high energy consumption.

In 2023, Neloy et al. presented a U.S.-based e-voting system leveraging state-based blockchain, smart contracts, and AI-based authentication to address double voting and enhance voter turnout, though facing complexity and storage overheads. These schemes collectively highlight the need for an efficient, lightweight, and robust e-voting solution ensuring secure and anonymous remote voting, applications where only legitimate voters communicate with secure and anonymous remote voting.

Across various proposals, there's a recurring effort to leverage blockchain technology to address the longstanding challenges associated with traditional voting systems, such as ensuring transparency, integrity, and accessibility while mitigating security risks. Despite the diversity in approaches, each scheme reflects a quest for a balance between security, scalability, and usability.

The early initiatives, like the one by Casado-Vara and Corchado (2018), highlighted the potential of blockchain in revolutionizing the voting landscape by proposing digital alternatives to paper-based or electronic voting methods. However, these early endeavors encountered significant challenges, including bandwidth limitations and security vulnerabilities, indicating the complexity of transitioning from conventional to block chain-based systems. Subsequent proposals, such as those by Kotsiuba et al. (2018)

and Yanovich et al. (2018), delved deeper into blockchain's potential applications beyond voting, exploring its utility in healthcare services and consensus algorithms, respectively. However, despite their innovative approaches, these schemes were susceptible to critical security breaches, underlining the importance of robust encryption and anonymity mechanisms in blockchain-based systems.

The evolution of consensus algorithms, from Tender mint to PBFT, showcased the ongoing quest for more efficient and secure validation mechanisms. However, as demonstrated by Any shchenko et al. (2019), achieving consensus remains a challenge, with each algorithm presenting its trade-offs in terms of performance and security.

Advancements in cryptographic techniques, such as those employed by Dhulavvagoletal.(2020)and Sadiaetal.(2020), introduced novel solutions to address authenticity, privacy and integrity concerns. By integrating biometric authentication and smart contracts, these schemes aimed to enhance the overall security posture of e-voting systems, albeit not without their limitations.

The exploration of alternative blockchain platforms, like Ethereum in the "MATDAAN" scheme proposed by Jain et al. (2021), highlighted the importance of platform selection in achieving specific objectives such as speed, reliability, and anonymity.However,asevidencedbythesusceptibilityto51% attacks, platform choice alone may not suffice in ensuring robust security.

The introduction of ECC-based signcryption schemes by Waheedetal.(2021)and Jumaa and Shakir(2022)represented a shift towards more sophisticated cryptographic solutions aimed at addressing the inherent vulnerabilities of traditional encryption methods. However, challenges in key distribution and decentralized implementation underscored the complexities associated with integrating such advanced cryptographic techniques into e-voting systems.

There cent proposal by Neloyetal.(2023)exemplifies a holistic approach to e-voting system design, integrating state-based blockchain, smart contracts, and AI-based authentication to enhance security and transparency. However, the complexity and storage overheads associated with such comprehensive solutions raise questions about scalability and practicality.

Overall, the journey towards realizing a truly efficient, lightweight, and robust e-voting scheme remains ongoing.

with each proposal contributing valuable insights and lessons learned. As technology continues to evolve, so too will the quest for secure and transparent democratic.

MOTIVATION AND CONTRIBUTION OF THE RESEARCH

From the above discussion in the literature review section,

After analyzing all the previous e-voting schemes, it is seen that all the previous schemes either suffer from security defects or incur huge overheads. Key management, key distribution, anonymity and confidentiality preservation are some other issues that must be achieved to execute secure e-voting from remote places. Then only traditional voting using EVM or other paper ballot voting can be replaced with this smart, digital, and secure e-voting system. The block chain is one of the major one-stop solutions for all the above issues and can provide a huge advantage to society. This research work proposes an e-voting scheme using the private Exo num blockchain and reusable smart contracts

it is concluded that each of the existing e-voting schemes is either suffering from some security attacks or facing several security issues regarding the key management and failing to establish any secure e-voting transactions. On the other hand, some of the existing schemes are not competent considering communication and computation overheads.

The above-stated limitations motivate us to design an oval signature-based e-voting scheme that incorporates exo num blockchain using an ECC cryptosystem. The major contributions of the proposed scheme are summarized below:

i The limitations mentioned above motivate us to design an ECC-based novel e-voting application using a smart contract and Exonum private blockchain scheme.

ii The proposed scheme uses a secure hybrid consensus algorithm, a combination of both RAFT and PBFT algorithms.

iii The scheme ensures the confidentiality and authenticity of the votes using the zero-knowledge protocol, idemix scheme, and anonymity mechanisms.

iv In this application, a lightweight e-voting scheme is proposed using both ECC and one-way hash functions.

v The proposed scheme represents a significant departure from existing e-voting solutions by leveraging ECC- based cryptography within the context of a smart contract and Exonum private blockchain framework. By adopting an ovel approach, the scheme aims to overcome he security vulnerabilities and key management challenges prevalent in current e-voting systems.

vi A key feature of the proposed scheme is its utilization of a secure hybrid consensus algorithm, combining elements of both RAFT and PBFT algorithms. This hybrid approach enhances the robustness and reliability of the consensus mechanism, thereby ensuring the integrity of e-voting transactions while minimizing communication and computation overheads.

vii To safeguard the confidentiality and authenticity of votes, the scheme integrates advanced cryptographic techniques such as the zero-knowledge protocol and ide mix scheme. These mechanisms enable voters to cast their ballots anonymously while providing verifiable proof of their eligibility and the integrity of their votes.

viii Recognizing the importance of efficiency in e-voting systems, the proposed scheme adopts a lightweight architecture by leveraging ECC and one-way hash functions. This ensures that the computational and communication over heads associated with processing e- voting transactions are minimized, thereby enhancing the scalability and usability of the system.

B. ORGANIZATION OF THE PAPER

The remaining part of this paper is organized as: Section II illustrates a detailed discussion regarding preliminaries such as brief functionality of Exonum blockchain technology and id emix technology for a better understanding of the scheme whereas in Section III, different models and related security frameworks are discussed. SectionIV, describes the proposed ECC-EXONUM-eVOTING scheme and its working procedure in detail. In Sections Vand VI, security analysis of the proposed scheme using the Random Oracle Model and simulation results using both AVISPA and Scyther simulation tools are demonstrated, respectively. Section VII shows the comparative discussion of the performance analysis of the scheme concerning other existing e-voting schemes and finally, Section VIII concludes this paper.

II. PRELIMINARIES

In this section, both the architecture as well as the functionality of Exonum blockchain and idexmix technology are illustrated.

A. ARCHITECTURE AND FUNCTIONALITY OF EXONUM BLOCKCHAIN

Exonum blockchain is categorized as a private or consortium permission block chain, characterized by several fundamental features elucidated in Figure 1 and expounded upon below:

a. It operates as an open-source application, fostering a network of full nodes interconnected via a peer-to-peer network alongside lightweight clients. These nodes engage in communication facilitated by middleware, ensuring proper consensus mechanisms are maintained.

b. Full nodes undertake the replication of all blockchain data, constructing replicas allocated within a distributed database for accessibility.

c. A crucial aspect of Exonum's architecture is its authentication and data privacy mechanism, facilitated by communication with Blockchain Storage DLT utilizing Exonum MerkleDB, which relies on public key cryptography for security.

d. Within the network, full nodes are subdivided into validators and auditors. Validators are responsible for creating or appending new blocks to the blockchain utilizing Byzantine Fault Tolerant (BFT) consensus mechanisms, while auditors ensure the overall consistency and integrity of the blockchain.

e. Exonum's functionality is largely contingent upon its Service Oriented Architecture (SOA), comprising three core components: Service, Lightweight client, and Middleware, as delineated in Figure 1.

f. The Service component encapsulates the primary business logic, transaction rules, and service states, while clients, acting as initiators, engage in various key management activities. Middleware applications serve to facilitate interoperability between the service application and lightweight clients, ensuring seamless communication and functionality within the Exonum ecosystem.

B. IDEMIX(IDENTITYMIXTURE) TECHNOLOGY

Idemix is a technology that supports a cryptographic protocol suite developed by IBM Switzerland to provide some eminent features; which are – (i) unlinkability, which is a property that a single identity can launch several transactions without disclosing the identity of the user, (ii) anonymity, it is a privacy-preserving property by which the initiator of the transaction can complete the transaction without trevealing the necessary details. This technology is built on an efficient Zero Knowledge protocol (ZPK) and blind signature scheme

C. COMMUNICATION MODEL

ECC-EXONUM-eVOTING adopts a communication model to perform secure transactions among the lightweight decen- tralized client application (Dapp), validator attached with service interface and auditor. The communication model is depicted in Figure 2. In the diagram, the solid lines indicate that the communication is performed through an insecure path and an invalid transaction mechanism.

a. Participating candidates: They are registered and valid candidates in the e-voting process.
b. Participating voters: They are registered and valid voters as per the voter list used in thee-voting process.
c. Validator with service instance: For the generation of the new block, it validates each transaction and
d. Auditor: It checks the consistency of the whole blockchain used in the e-voting scheme and also maintains an absolute copy of the whole blockchain.

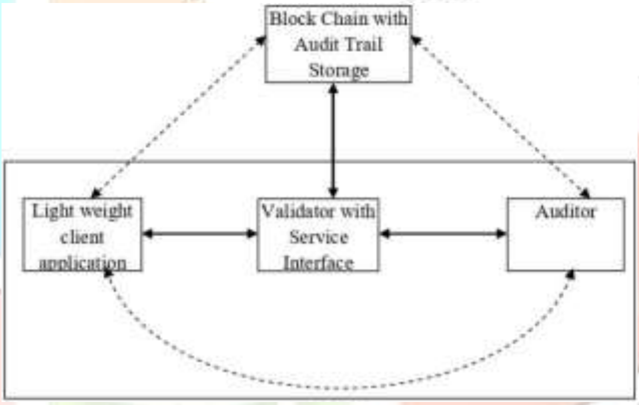

Block Chain with Audit Trail Storage
Light weight client application
Validator with Service Interface
Auditor

FIGURE2.CommunicationmodelusingExonum.

VOTING PROCESS

We now describe a typical user interaction with the proposed scheme based on our current system implementation. So basically the voter logs into the system by scanning their face. After scanning the face, the facial recognition system authenticates the voter. If a match is found, the voter is presented with a list of available candidates with the option to vote against them. Conversely, if the match is unsuccessful, any further access would be denied. This functionality is achieved by using an appropriate implementation of an authentication mechanism(in this case a facial recognition system) and predefined role-based access control. Furthermore, it is also assumed that the voter is assigned to his particular electoral district and this information is used to create a list of candidates for which the voter can vote. Assigning a voter to a constituency is considered an offline process and is therefore beyond the scope of this research.

After successfully casting votes, it is mined by multiple miners for verification, after which valid and verified votes are added to the public ledger. The security aspects of voting are based on blockchain technology using cryptographic hashes to secure end-to-end verification. For this purpose, a successfully cast vote is considered a transaction within the voting application's blockchain. Therefore, the casting vote is added as a new block (after successful mining) in the blockchain and is also recorded in the data tables at the end of the database. The system ensures ownership of voting systems for only one person and one vote This is achieved by using a unique voter face that matches at the start of each voting attempt to prevent double voting. Once miners mine a vote, a transaction is generated that is unique to each vote. If the vote is found to be malicious, the miner is rejected.

After the validation process, a notification is immediately sent to the voter via message or email with the transaction ID defined above, through which the user can track their vote to the ledger. While this works as a voter notification, it does not allow any user to extract information about how a particular voter voted, there by achieving voter privacy. It is important to note here that the cryptographic hash for the voter is the unique hash of the voter by which the voter is known in the blockchain. This feature make sit easier to achieve verifiability of the entire voting.

BLOCKCHAIN

Blockchain technology is shining sort of a star these days when its entry and *wide-spreade*d option of Bitcoin, the terribly initial crypto currency that involves people's minds. Blockchain technology originates from the fundamental subject style of the bit coin crypto currency, wherever it absolutely was initial introduced the net world and previously be came a promising technology thanks to the high degree of transparency within the system, turning into a vigorous space of analysis and study for its varied applications. alternative fields.

Blockchain, simply put, may be a shared, change less ledger that facilitates the method of recording transactions and following assets in a very business network. Associate in Nursing quality are often tangible (house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). during this era nearly we are able to track and trade something on a blockchain network, reducing prices and risk for everybody. Blockchain stores its knowledge in blocks. First, all the info to be keep within the blockchain is reborn into smaller components, that square measure allotted to totally different blocks with in the suburbanized network. The initial block in a very blockchain is understood as a "Genesis Block" or "Block 0". "Block Gene-sis" or "Block 0". The genesis block is sometimes hard-coded into software; is peculiar therein it doesn't contain a link to the previous block. The genesis block is sometime shard-coded into the software; it's special there init doesn't contain a regard to the previous block (the Genesis block).

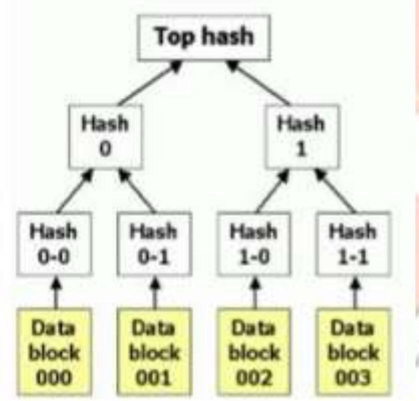


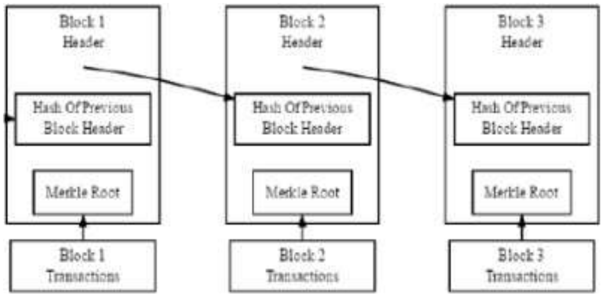
FIGURE5.HashTable

III. CONCLUSION

To conclude in nutshell,by using this project ,the user doesn’t need to worry about any special tool to write in the open space. With optimum use of resources, we can write and convey correct message to other party. In the current situation, online work is unavoidable. Mainly, online education is proving harder as teachers sometimes feel difficult to teach without writing. This is where our project comes into picture. Once the project website is hosted on server, anyone (i.e., teachers) can access it and using the web-camera one can easily do their task using writing. (i.e., Math teacher may use it to show equations to the students in online education) .

To submit up, we can say that using python libraries and OpenCV, Once the genesis block is initialized, "Block 1" is created and when completed is attached to the genesis block. Each block has a transaction data part, a copy of each of the transactions is hashed and then the hashes are matched and hash again, this continues until there is only one hash left; to known as the Merkle root (Figure). The block header is where the Merkle root is stored, which ensures that the transaction cannot be modified by third parties .

Blockchain is designed to be accessed through a peer-to-peer network, each node then communicates with other nodes to exchange blocks and transactions. A blockchain block consists of a block header, a hash value of the previous block header, and a Merkle root. So when we extract data from the blockchain, then all the smaller parts that are in the decentralized network are connected by accessing all the blocks through their hash values. If a person or a third party wants to change the data, they need to know the hash values of all the tables, without them they can't take even a bit of information about our data. Because these data blocks are distributed in thousands and thousands of blocks, it takes a hacker more than millions of years to find the hash values of all the blocks. Thanks to these features, it provides safety, reliability, and robustness.



we have created a tool through which all people who were unable to convey the message properly due to lack writing in real time during online meetings can now do it efficiently**.**

IV. REFERENCES

1. R. Taş and Ö. Ö. Tanrıöver, "A systematic review of challenges and opportunities of blockchain for E- voting", *Symmetry*, vol. 12, no. 8, pp. 1328, Aug. 2020.

2. Onuklu, A. (2019), "Research on Blockchain: A Descriptive Survey of the Literature", Choi, J. and Ozkan,
B. (Ed.) Disruptive Innovation in Business and Finance in theDigitalWorld(InternationalFinanceReview,Vol.20), Emerald Publishing Limited, pp. 131-148. DOI/10.1108/S1569-3767201

3. Zhang K, Zhang Z, Li Z, et al. Joint Face Detection and Alignment Using Multitask Cascaded Convolutional Networks [J]. IEEE Signal Processing Letters, 2016, 23(10):1499-1503.

4. Pranav KB, Manikandan J, " Design and Evaluation of a Real-Time Face Recognition System using Convolutional Neural Networks", April 2020, ScienceDirect

5. Shahzad, B.; Crowcroft, J. Trustworthy Electronic Voting UsingAdjustedBlockchainTechnology. *IEEEAccess* 2019, *7*, 24477–24488.

6. Gao, S.; Zheng, D.; Guo, R.; Jing, C.; Hu, C. An Anti- Quantum E-Voting Protocol in Blockchain with Audit Function. *IEEE Access* 2019, *7*, 115304–115316.

7. Ramya Govindaraj, P Kumaresan, K. Sree harshitha, " Online Voting System using Cloud," 24-25 Feb. 2020, IEEE

8. Fernández-Caramés,T.M.;Fraga-Lamas,P.TowardsPost- Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access* 2020, *8*, 21091–21116.

9. Yi, H. Securing e-voting based on blockchain in P2P network.*EURASIP J. Wirel. Commun. Netw.* 2019,*2019*, 137.

10. Torra, V. Random dictatorship for privacy-preserving social choice. *Int. J. Inf. Secur.* 2019, *19*, 537–543.

11. Alaya, B.; Laouamer, L.; Msilini, N. Homomorphic encryption systems statement: Trends and challenges. *Comput. Sci. Rev.* 2020, *36*, 100235.

12. Khan, K.M.; Arshad, J.; Khan, M.M. Investigating performance constraints for blockchain based secure e- votingsystem.*FutureGener.Comput.Syst.*2020,*105*,13–26