IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

E-VOTING SYSTEM BASED ON PUBLIC BLOCKCHAIN USING PROOF OF STAKED AUTHORITY

Mr.Arokiaraj St. Hubert #1, Dinakar G*2, Giridharran N*3, Sandeep Samuel J*4

- Associate Professor, * - Student.

Sri Manakula Vinayagar Engineering College,

Department of Computer Science and Engineering,Madagadipet, Puducherry – 605107, India.

ABSTRACT:

The contemporary global landscape of democratic voting systems is plagued by a pervasive lack of trust, stemming from violations of fundamental rights and a conspicuous absence of transparency. This crisis extends to both traditional and digital voting methods, leaving voters vulnerable to exploitation and undermining the foundational trust in these systems. The urgency to address these systemic issues is paramount, focusing on eliminating mishaps and injustices that tarnish the integrity of the voting process. The prevalent use of flexible consensus algorithms further complicates matters, amplifying complexity and potential inconsistencies. In response to these challenges, the Binance Smart Chain (BSC) has emerged as a proactive solution provider. BSC adopts the innovative Proof of Staked Authority (PoSA) consensus mechanism, strategically integrating the strengths of both Proof of Stake (PoS) and Proof of Authority (PoA) to enhance security and decentralization. This unique approach is meticulously crafted to elevate the integrity of the voting process, directly addressing the pervasive trust deficit in existing systems. By embracing this groundbreaking consensus mechanism, BSC aims to bring substantial improvements to the overall security, transparency, and trustworthiness of democratic voting systems. The innovative stance of BSC holds promise in mitigating the multifaceted challenges faced by these crucial components of modern governance.

KEYWORDS: PROOF OF STAKE (POS), PROOF OF AUTHORITY (POA), PROOF OF STAKED AUTHORITY (POSA) , BINANCE SMART CHAIN (BSC)

1. INTRODUCTION:

In Democratic countries an election plays a vital role in the selection of the government of the respective country. A voter must cast the vote securely and privately without interference from any political party's agents. There are enormous ways to cast the vote in the different countries. In the traditional voting system, a paper is used to cast the vote. The drawbacks of this system are invalid votes printing of millions of ballot papers transportation storage and distribution of ballot papers stealing or altering a ballot boxes and the counting process is manual which takes too long time.

In India the Postal Ballot system facility is available for the members of the armed forces members of the state police department or any person who is appointed on the election duty. Voter have to punch his / her choice on the ballot paper and then these votes are dispatched to the Returning Officer of the respective assembly using postal services. The drawback of this system is sometimes ballots are not delivered on time papers tore in between the transportation or did not properly punch by voters lead to the cancellation of the vote at the time of the vote counting process. Electronic Voting Machine (EVM) drastically changes this scenario in India. It helps to overcome all the drawbacks of a paper-based voting system. But in this the voter has to visit the polling station on election day. Another way to cast a vote is through an Internet-based or remote voting system. As voter can cast vote from anywhere leads to an increase in voter participation. The system is designed as a web-based application.

Blockchain is a continuously growing distributed database consisting of blocks maintained by a network of consensus nodes (i.e. that run a consensus protocol). Once the consensus nodes agreement on a new block it is added to the blockchain. The blocks are cryptographically linked to ensure the immutability of the entire ledger and they contain records of cryptocurrency transfers executed within the network. Orders to execute transfers are communicated to the network in messages called transactions. The block may also contain application code written in a supported language on blockchain platforms that support smart contracts. This code is invoked by a transaction containing execution orders (i.e. function calls of a smart contract). The blockchain network then acts as a decentralized computation platform the blockchain nodes execute the smart contract code.

Proof of Staked Authority (PoSA) is a consensus mechanism used in blockchain networks. It is a system designed to strike a balance between Proof of Stake (PoS) and Proof of Authority (PoA), combining the best aspects of each consensus mechanism.

Proof of Stake (PoS) is a consensus mechanism where validators are chosen to create a new block based on their economic stake in the network. On the other hand, Proof of Authority (PoA) is a model where validators are pre-selected based on their reputation, so there is no need for validators to stake as their credibility is the key factor.

As Proof of Staked Authority is a combination of the two, participants must hold a certain number of tokens (PoS), and be identified as a trusted node in the network (PoA). However, as with every consensus mechanism, there are advantages and disadvantages associated with it.

One of the benefits associated with PoSA is its enhanced security. Validators have both economic stake and their reputation at risk, discouraging fraudulent activity as this would lead to financial loss and reputational harm. Furthermore, PoSA has equal staking requirements amongst validators, creating a more balanced participation in transaction validation.

Nevertheless PoSA has a potential con associated with it, primarily the risk of centralization. If the validator pool isn't diverse enough, there is the possibility that validators could collude and potentially disrupt the network. However, this is generally unlikely to happen as it would be counterintuitive to the reputation of validators.

In essence, the Proof of Stake Authority consensus mechanism, while robust and secure, has its strengths and challenges. By cleverly combining the best of PoS and PoA, PoSA paves a path to a balanced consensus mechanism for institutional adoption and decentralized economy. However, this advancement also introduces the requirement for prudent oversight and ongoing adaptation to mitigate and overcome potential challenges.

2. LITERATURE SURVEY:

[2.1] Trustworthy electronic voting using adjusted blockchain technology Basit Shahzad and Jon Crowcroft:

The electronic voting has emerged over time as a replacement to the paper-based voting to reduce the redundancies and inconsistencies. The historical perspective presented in the last two decades suggests that it has not been so successful due to the security and privacy flaws observed over time. This paper suggests a framework by using effective hashing techniques to ensure the security of the data. The concept of block creation and block sealing is introduced in this paper. The introduction of a block sealing concept helps in making the blockchain adjustable to meet the need of the polling process. The use of consortium blockchain is suggested, which ensures that the blockchain is owned by a governing body (e.g., election commission), and no unauthorized access can be made from outside. The framework proposed in this paper discusses the effectiveness of the polling process, hashing algorithms utility, block creation and sealing, data accumulation, and result declaration by using the adjustable blockchain method. This paper claims to apprehend the security and data management challenges in blockchain and provides an improved manifestation of the electronic voting process.

[2.2] On the Design and Implementation of a Blockchain Enabled E-Voting Application Within IoT-Oriented Smart Cities Geetanjali Rathee , Razi Iqbal , Omer Waqar and Ali Kashif Bashir:

A smart city refers to an intelligent environment obtained by deploying all available resources and recent technologies in a coordinated and smart manner. Intelligent sensors (Internet of Things (IoT) devices) along with 5G technology working mutually are steadily becoming more pervasive and accomplish users desires more effectively. Among a variety of IoT use cases, e-voting is a considerable application of IoT that relegates it to the next phase in the growth of technologies related to smart cities. In conventional applications, all the devices are often assumed to be cooperative and trusted. However, in practice, devices may be disrupted by the intruders to behave maliciously with the aim of degradation of the network services. Therefore, the privacy and security flaws in the e-voting systems in

particular lead to a huge problem where intruders may perform a number of frauds for rigging the polls. Thus, the potential challenge is to distinguish the legitimate IoT devices from the malicious ones by computing their trust values through social optimizer in order to establish a legitimate communication environment. Further, in order to prevent from future modifications of data captured by smart devices, a Blockchain is maintained where blocks of all legitimate IoT devices are recorded. This article has introduced a secure and transparent e-voting mechanism through IoT devices using Blockchain technology with the aim of detecting and resolving the various threats caused by an intruder at various levels. Further, in order to validate the proposed mechanism, it is analyzed against various security parameters such as message alteration, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attack and authentication delay.

[2.3] An Anti-Quantum E-Voting Protocol in Blockchain With Audit Function. Shiyao Gao , Dong Zheng , Rui Guo , Chunming Jing and Chencheng Hu:

As an important method of making democratic decisions, voting has always been a topic of social concern. Compared with the traditional, e-voting is widely used in various decision scenarios because of the convenience, easy to participate and low cost. However, the proposed e-voting protocols are at the risk of excessive authority and tampered information, which makes it impossible to achieve true fairness and transparency in e-voting. By combining the blockchain technology, it enables to solve these problems with the decentralization and tamper-resistant features. Moreover, the misoperations of the voters will also affect this fairness, such as voting for non-candidates, abstention or repeated voting. Therefore, to ensure the efficiency of the voting process and maintain the fairness of the voting environment, it is important to append the function of audit in e-voting protocol. This paper proposes an e-voting protocol based on blockchain, which provides transparency in the process of voting. At the same time, this scheme has the ability to audit voters operating incorrectly and resist quantum attacks by adopting the certificateless and code-based cryptography. After performance analysis, our scheme is suitable for the small-scale election and has some advantages in security and efficiency when the number of voters is small.

[2.4] Survey on Privacy-Preserving Blockchain Systems (PPBS) and a Novel PPBS-Based Framework for Smart Agriculture. Quang Nhat Tran , Benjamin P. Turnbull , Hao-Tian Wu *:*

Blockchain and smart contracts have seen significant application over the last decade, revolutionising many industries, including cryptocurrency, finance and banking, and supply chain management. In many cases, however, the transparency provided potentially comes at the cost of privacy. Blockchain does have potential uses to increase privacy-preservation. This paper outlines the current state of privacy preservation utilising Blockchain and Smart Contracts, as applied to a number of fields and problem domains. It provides a background of blockchain, outlines the challenges in blockchain as they relate to privacy, and then classifies into areas in which this paradigm can be applied to increase or protect privacy. These areas are cryptocurrency, data management and storage, e-voting, the Internet of Things, and smart agriculture. This work then proposes PPSAF, a new privacy-preserving framework designed explicitly for the issues that are present in smart agriculture.

Finally, this work outlines future directions of research in areas combining future technologies, privacy-preservation and blockchain.

[2.5] Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks. Wei She , Qi Liu , Zhao Tian:

The Internet of Things (IoT) has been widely used because of its high efficiency and real-time collaboration. A wireless sensor network is the core technology to support the operation of the IoT, and the security problem is becoming more and more serious. Aiming at the problem that the existing malicious node detection methods in wireless sensor networks cannot be guaranteed by fairness and traceability of detection process, we present a blockchain trust model (BTM) for malicious node detection in wireless sensor networks. First, it gives the whole framework of the trust model. Then, it constructs the blockchain data structure which is used to detect malicious nodes. Finally, it realizes the detection of malicious nodes in 3D space by using the blockchain smart contract and the WSNs quadrilateral measurement localization method, and the voting consensus results are recorded in the blockchain distributed. The simulation results show that the model can effectively detect malicious nodes in WSNs, and it can also ensure the traceability of the detection process.

[2.6] Proof-of-Event Recording System for Autonomous Vehicles: A Blockchain-Based Solution Hao Guo , Wanxin Li , Mark Nejad and Chien-Chung Shen:

Autonomous vehicles are capable of sensing their environment and navigating without any human inputs. However, when autonomous vehicles are involved in accidents between themselves or with human subjects, liability must be indubitably decided based on accident forensics. This paper proposes a blockchain-inspired event recording system for autonomous vehicles. Specifically, we design the mechanism of Proof-of-Event with a dynamic federation consensus to achieve indisputable accident forensics by providing trustable and verifiable event information. We propose a dynamic federation consensus scheme to verify and confirm the new block of event data in an efficient way without any central authority. We conduct numerical analyses and prototyped experiments based on the proposed fast leader election algorithm and the Hyperledger Fabric blockchain network. The results show that our system is effective and feasible in generating and storing accident records in blockchain-based vehicular networks. The security capability of the proposed scheme is also discussed against multiple threats and attack scenarios.

3. EXISTING SYSTEM:

The traditional and digital voting systems face challenges due to mistrust, lack of transparency, and potential exploitation. Blockchain technology offers a solution by ensuring fairness, transparency, and secure transactions. An existing platform leverages blockchain for digital voting, eliminating physical polling stations and enhancing trust between voters and authorities.

The blockchain-based voting system ensures security, transparency, and reliability. It is tamper-proof, thanks to immutability, and remains operational even if some nodes fail. Key stakeholders include voters, Identification Authorities (IA), and the Administration Authority (AA) of the election commission.

The process of the existing system includes certain parts; the first one is the user interface of the application which also requires front-end security. It is critical because the user enters his credentials on that interface so it should be secure and simple. the system provides full and fair access to every user during voting activity. It also provides traceability after casting of vote. the voter registers in the system by his credentials. VMS uses the ID details of voters and verifies them with online records of IA to register the voter in the system. the user receives a unique OTP to log in to the system. An OTP is generated each time the voter wants to login into VMS. All the detail of the voter is saved in VMS. After successfully registering in the system One Voting Coin (VC) is added to the wallet of each voter. to prevent voters from voting twice each voter is given only one VC.

3.1. DISADVANTAGES OF EXISTING SYSTEM*:*

- The strengths will depend on the implementation.
- Technology is new and there are scalability issues. the performance may degrade on high usage.
- Internal processes and casted votes are less transparent.
- Existing unsuccessful attempts may disrupt the motivations.
- It requires more computational power because it will run hash algorithm multiple times until pattern is matched but it also increase the security since if any malicious party create a hash and try to add that block to the chain, it also has to know the hash pattern.

4. PROPOSED SYSTEM:

The existing democratic voting systems grapple with significant challenges, leading to widespread distrust among the public. Violations of fundamental rights and a lack of transparency have contributed to a decline in public faith in both traditional and digital voting methods. These vulnerabilities expose the democratic process to potential exploitation, intensifying concerns about the integrity of elections. The erosion of trust poses a critical threat to the foundational principles of democracy.

In response to these challenges, the proposed solution introduces a paradigm shift by leveraging the Binance Smart Chain (BSC). BSC's innovative Proof of Staked Authority (PoSA) consensus mechanism combines the strengths of Proof of Stake (PoS) and Proof of Authority (PoA) to enhance security and decentralization. By adopting BSC's approach, the aim is to fortify the voting process's credibility and address the trust deficits prevalent in current systems. The unique features of BSC, such as its robust consensus mechanism, hold the potential to establish a more secure and trustworthy foundation for democratic voting.

The utilization of BSC in democratic voting not only introduces technological advancements but also underscores a commitment to transparency and integrity. This approach seeks to rebuild public confidence in the democratic process by offering a resilient, decentralized, and secure platform for voting. As discussions around the future of

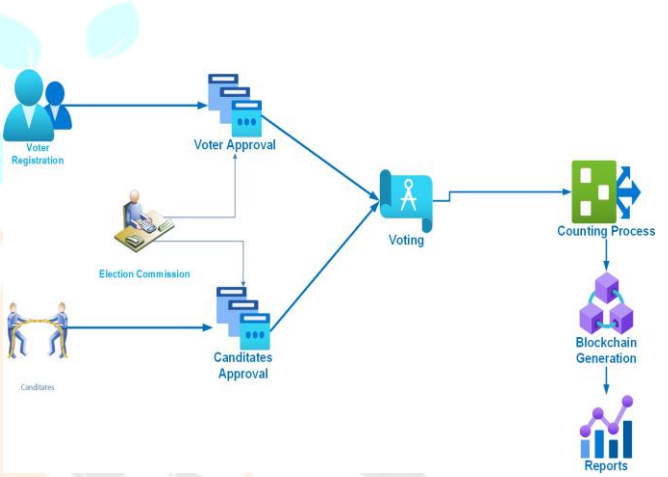
democratic systems unfold, the integration of BSC stands as a promising step towards fostering trust and safeguarding the fundamental tenets of democratic governance.

4.1. ADVANTAGES OF PROPOSED SYSTEM:

- Immutable records. Record deletion is nearly impossible; even if it is successful, the evidence deletion can be prevented.
- Provides transparency with privacy.
- Cheaper in the long term.
- Enables elastic elections: variable durations, conditions, and target groups.
- Provides instant results.

5. METHODOLOGY :

The proposed system addresses the significant challenges faced by existing democratic voting systems, which have led to widespread public distrust. Violations of fundamental rights and a lack of transparency have contributed to a decline in faith in both traditional and digital voting methods, exposing the democratic process to potential exploitation and threatening the foundational principles of democracy. The proposed solution introduces a paradigm shift by leveraging the Binance Smart Chain (BSC). BSC's innovative Proof of Staked Authority (PoSA) consensus mechanism, combining the strengths of Proof of Stake (PoS) and Proof of Authority (PoA), aims to enhance security and decentralization. The adoption of BSC's approach seeks to fortify the credibility of the voting process and address trust deficits prevalent in current systems. Unique features of BSC, such as its robust consensus mechanism, hold the potential to establish a more secure and trustworthy foundation for democratic voting, introducing technological advancements and emphasizing a commitment to transparency and integrity. This approach aims to rebuild public confidence in the democratic process by providing a resilient, decentralized, and secure platform for voting. As discussions about the future of democratic systems progress, the integration of BSC represents a promising step toward fostering trust and safeguarding the fundamental tenets of democratic governance.



5.1. VOTER REGISTRATION MODULE:

The Voter Registration Module plays a pivotal role in the proposed democratic voting system, focusing on the fundamental task of managing the registration of eligible voters. Its overarching purpose is to establish a secure and legitimate foundation for the voting process by ensuring that only authorized individuals have the right to participate. This module incorporates several key features to fulfill its role effectively. Firstly, it employs secure user authentication mechanisms, utilizing robust protocols to verify the identity of individuals seeking registration. This enhances the overall security of the system by preventing unauthorized access. Secondly, the module conducts thorough eligibility verification to confirm that potential voters meet the criteria for participation,

such as age, citizenship, and other relevant qualifications. This step adds an additional layer of assurance to the integrity of the voter pool. Lastly, the module is responsible for maintaining an updated and accurate voter database, reflecting any changes in eligibility status or personal information.

5.2. TRANSPARENT VOTING MODULE:

The Transparent Voting Module is a critical component in the proposed democratic voting system, serving the core function of facilitating the casting of votes by registered users. Its primary purpose is to establish a transparent and tamper-proof voting process, directly addressing concerns related to the integrity of elections. The module incorporates advanced cryptographic techniques to secure votes, ensuring the confidentiality and authenticity of each ballot cast. Additionally, it leverages blockchain technology to enable verifiable and auditable transactions, making the entire voting process immutable and resistant to manipulation. Real-time visibility into the voting process further enhances transparency, allowing stakeholders to monitor and verify the integrity of the election in progress. In essence, the Transparent Voting Module is designed to instill confidence in the democratic process by ensuring a secure, transparent, and tamper-resistant environment for casting and recording votes.

5.3. BLOCKCHAIN INTEGRATION MODULE:

The Blockchain Integration Module is pivotal in the proposed democratic voting system, primarily tasked with integrating the Binance Smart Chain (BSC) and its innovative Proof of Staked Authority (PoSA) consensus mechanism. The purpose is to harness blockchain technology to elevate the security, decentralization, and transparency of the voting system. This module features the seamless integration of BSC's PoSA, enabling robust security measures and decentralized validation of transactions. Smart contract deployment for voting processes ensures automated and tamper-resistant execution, while the immutability of voting records on the blockchain guarantees transparency and trust in the integrity of the electoral data. In essence, the Blockchain Integration Module empowers the voting system with the transformative capabilities of blockchain technology, enhancing its overall reliability and transparency.

5.4. SECURITY AND AUTHENTICATION MODULE:

The Security and Authentication Module serves as a critical component in the proposed democratic voting system, tasked with implementing robust security measures to safeguard against unauthorized access and preserve the integrity of the entire voting process. The primary purpose of this module is to mitigate the inherent risks associated with cybersecurity threats and potential unauthorized manipulation of voter data or election results. To achieve this, the module incorporates a multi-faceted approach, including the implementation of multi-factor authentication to ensure that only authorized individuals can access sensitive systems. Moreover, sensitive data is encrypted, adding an extra layer of protection against unauthorized interception or tampering. Regular security audits are conducted to identify and address vulnerabilities, and continuous monitoring for suspicious activities helps detect and respond to potential threats in real-time. By incorporating these features, the Security and Authentication Module

establishes a robust defense mechanism, fortifying the democratic voting system against cybersecurity risks and unauthorized interference, thereby instilling confidence in the security and integrity of the electoral process.

5.5. RESULTS TABULATION AND VERIFICATION MODULE:

The Results Tabulation and Verification Module in the proposed democratic voting system plays a crucial role in ensuring the reliability and legitimacy of election outcomes. Its primary function involves the automated compilation and verification of voting results for accuracy. The overarching purpose is to provide stakeholders with a transparent mechanism to verify the results, instilling confidence in the integrity of the democratic process. Key features include the automated tabulation of votes, leveraging cryptographic techniques for result verification on the blockchain, and provisions for independent auditing. By incorporating these features, the module contributes to the proposed system's goal of fortifying the credibility and trustworthiness of the democratic voting process, offering a transparent and accountable approach to result tabulation and verification.

6. SUMMARY AND CONCLUSIONS:

In conclusion, the pervasive mistrust and vulnerabilities observed in both traditional and digital voting systems underscore the critical necessity for a more reliable, transparent, and secure solution. The introduction of the Binance Smart Chain (BSC) and its groundbreaking Proof of Staked Authority (PoSA) consensus mechanism, which amalgamates Proof of Stake (PoS) and Proof of Authority (PoA), offers a promising avenue to strengthen the integrity of the voting process. BSC's innovative features and hybrid consensus model have the potential to address systemic issues that contribute to public skepticism and enhance the overall security and decentralization of democratic voting systems.

The implementation of BSC represents a noteworthy departure from conventional approaches, signaling a commitment to leveraging advanced blockchain technology for the betterment of democratic processes. By effectively tackling the root causes of mistrust and vulnerabilities, BSC aims to create a more resilient and transparent framework for democratic voting. The proposed solution, rooted in BSC's unique features, holds the promise of mitigating trust deficits and establishing a solid foundation that fosters confidence in the democratic electoral system. As discussions around electoral reform intensify, the integration of BSC and its PoSA consensus mechanism emerges as a forward-thinking strategy to usher in a new era of secure, transparent, and trustworthy democratic voting systems. This approach reflects a commitment to addressing contemporary challenges and building a foundation for more resilient democratic governance.

7. REFERENCES:

[1] Ayed, A. B. (2017). A conceptual secure blockchain-based electronic voting system. International Journal of Network Security & Its Applications, 9(3), 1-9.

[2] Britannica. (2022). Voting rights act. Retrieved from https://www.britannica.com/event/Voting-Rights-Act.

[3] Clark, W. (2020). What is the paillier cryptosystem? Retrieved from: https://blog.openmined.org/the-paillier-cryptosystem/.

[4] Clear Ballot (2022). Innovation for our nation's elections, Retrieved from: https://clearballot.com/.

[5] Cosmas, K. A., Rikard, H. & Hiroyuki, S. (2018). A proposal of blockchain-based electronic voting system. 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), 22-27.

[6] Daley, S. (2022). 34 blockchain applications and real-world use cases disrupting the status quo. Retrieved from: https://builtin.com/blockchain/blockchain-applications.

[7] EPI Center (2021). Internet or online voting remains insecure. Retrieved from: https://www.aaas.org/epi-center/internet-online-voting. ETH Gas Station (2019). How long does an ethereum transaction really take? Retrieved from: https://legacy.ethgasstation.info/blog/ethereum-transaction-howlong/

[8] Fleming, S. (2020). What is homomorphic encryption and how can it help in elections? Retrieved from: https://news.microsoft.com/on-the-issues/2020/04/13/what-ishomomorphic-encryption-and-how-can-it-help-in-elections/.