Vol. 3, Issue III, 2024 (October – December)
International Journal of Politics & Social Sciences Review (IJPSSR)
Website: https://ijpssr.org.pk/ OJS: https://ojs.ijpssr.org.pk/ Email: ijpssrjournal@gmail.com
ISSN 2959-6467 (Online) :: ISSN 2959-6459 (Print)
ISSN 2959-6459 (ISSN-L)
Recognized by Higher Education Commission (HEC), Government of Pakistan

Implementing Blockchain Technology for Enhanced Security in Voting Systems

Jamshaid Iqbal Janjua[1], Usama Aslam[2], Tahir Abbas[3] & Anaum Ihsan[4]

[1] Al-Khawarizmi Institute of Computer Science (KICS), University of Engineering & Technology (UET), Lahore, Pakistan Email: jamshaid.janjua@kics.edu.pk
[2] Department of Computer Science, TIMES Institute, Multan, Pakistan
[3] Department of Computer Science, TIMES Institute, Multan, Pakistan Email: drtahirabbas@t.edu.pk
[4] Al-Khawarizmi Institute of Computer Science (KICS), University of Engineering & Technology (UET), Lahore, Pakistan

Abstract

In response to the growing demand for more secure, transparent, and trustworthy voting systems, this study explores the application of blockchain technology as a transformative solution. The research delves into an extensive analysis of existing literature, case studies, and real-world implementations to highlight the significant advantages that blockchain offers for voting systems, including immutability, decentralization, and enhanced security. Moreover, a comprehensive approach is presented in responding to additional aspects of such systems as the ability to scale, the rule of anonymity and other regulation-related issues. Another novel aspect of this legislation includes a technique that aims to solve major challenges related to the issues of voters' anonymity, data theft, and multiple voting. Our results demonstrate, however, that the true revolutionizing ability of blockchain in the electoral process is not in question but calls for various resources- technological, legal, and human-to enhance its implementation. This paper advances the debate on ways of updating the voting processes and sets a direction on what more needs to be done in terms of the research and technological development.

Keywords Blockchain, E-voting System, Secure Voting, Digital Voting System.

Introduction

In democratic norms, it is regarded as an important aspect, that the will of the citizens is accurately and fairly reflected in every electoral process through the technicalities of free and fair electoral processes. However, Conventional voting techniques have been affected by a number of factors, including third-party influences such as corruption, vote rationing, or vote e-rigging. These problems are not just of a hypothetical nature - they have been observed in some elections around the world and have caused many problems such as disputed results, lawsuits, and sometimes even riots. Of particular concern is the growing attitude of the general population towards the conduct of the elections, as this is practically the tilt of the very essence of democracy. In circumstances where ordinary voters feel elections will be rigged in a way that will alter the results or votes cast by individuals will not be taken into account, such people tend to distance themselves from any elections hence low turnout in the elections which eventually compromises the democracy achieved.

Traditional or conventional systems of voting have their various limitations. There are limitations related to the sensitivity of these systems, which are due to dirty tricks in general, which include any system constraints if any such as hacking or burials of extra ballots and contesting of vote counts. Malpractices like those mentioned above are complemented by non-technical problems e.g. one of the most difficult tasks is to find and count every vote in a vote.

Furthermore, the concentration of power in a few hands in most of the voting systems makes the systems prone to corruption by any of those who possess the voting infrastructure either the state, election managers, and contractors.

However, over the last few years, many people have turned to the use of the blockchain in an attempt to put problems associated with the traditional voting system to rest. The blockchain was initially used for Bitcoin and other crypto currencies among its users, it is regarded as a ledger technology that is distributed and not centralized where preferences are recorded In a more secured And Open Way. Each such transaction or record is protected by cryptography and linked to previously existing records so that it is virtually impossible to modify or forge any information included in this record chain. The blockchain also does not allow any particular central governing body to reside, which contributed to the resilience on the tampering of the results by the bad parties in the political context.

This analysis investigates how these powerful features could be utilized towards the betterment of our voting systems in addressing issues of security, transparency, and voter confidence among numerous other challenges. Using the advanced features of blockchain technology a novel voting system design is developed which is highly secure yet completely transparent and verifiable.

Such a system would allow the voters to establish the correctness of the votes cast without compromising their identities and in this way maintaining the anonymity of the ballot more effectively. Also, the inclusion of technology of blockchain could provide a comprehensive enhancement of the book of numbers in regard to documenting the votes since it cannot be altered.

However, even though that could solve issues in voting system, there are drawbacks in introducing bloc chain into voting systems. In order for the voting systems using Blockchain to be mainstream, a number of obstacles need to be addressed including technical, regulatory and societal ones. For example, the first point is quite self-evident; very few people have any experience with it in a setting as risky as a national vote, and so there are apprehensions over whether it is optimally versatile and intricately costly to operate such like systems. Furthermore, regarding the use of the problem of law, it is also quite evident that all countries are not on the same level concerning the progress in the adoption and implementation of the technology which is a constraint.

Furthermore, the ability of the public or society to accept this kind of system is one of the factors that: should never be ignored. Even though there is increased interest in blockchain technology, people's understanding of the technology is still low, and there is a possibility that people may not be willing to use a different system, especially one that is used for something so vital as voting.

It will be crucial to undertake efforts aimed at engaging the public and building trust about voting with the use of blockchain technology.

Literature Review

Blockchain technology was initially introduced as the foundation for Bitcoin, establishing a peer-to-peer electronic cash system [1]. Recent advancements have applied blockchain to voting, with one proposal suggesting a privacy-preserving e-voting system supporting score voting using blockchain [2]. A decentralized computation platform that guarantees privacy, Enigma, was developed to secure e-voting processes [3]. Blockchain has also been shown to enhance security in voting systems, particularly in its implementation for secure voting [4]. The broader potential of blockchain, including secure digital voting, has been explored as part of a blueprint for the future economy [5]. Practical Byzantine Fault Tolerance, which is critical for blockchain's resilience in voting systems, has also been introduced [6]. Additionally, the Ethereum blockchain has been demonstrated as a suitable platform for creating secure e-voting mechanisms [7]. The core principles and applications of blockchain technology, including its role in secure voting, have been thoroughly explored [8]. Blind signatures, a key concept for ensuring voter privacy in blockchain-based voting, remain relevant in contemporary e-voting systems [9]. Finally, blockchain's transformative potential in various sectors, including financial services, has been highlighted, drawing parallels to its application in secure and transparent elections [10].

Conventional or traditional voting systems especially in voting with paper ballots or implementing electronic methods have served as a primary mode of conducting democratic processes. Nonetheless, there are some inherent flaws with these systems that are critical in any election. The use of paper ballots is the oldest conventional type of voting yet very prone to problems such as ballot

snatching, personating fraud, and accidental vote miscounting. Such weaknesses were brought vividly to light during the highly provocative presidential election in the US of the year 2000 where cases of scattered votes and in solution of the ballots puzzle illustrated dead ends of the paper. This prompted the emergence of electronic voting systems, seeking to remove the flaws associated with the paper-based voting systems. More recent trends have inherent issues as well. Electronic systems may help mitigate some of the issues created by paper ballots; however, they bring their own problems, especially in the area of cyber security. These comprise software glitches, system malfunctions, and hacking of applications. Also, most traditional voting infrastructure is localized meaning that election security differs from one area to another; therefore, some electoral areas from abusive attacks than others. Another area is that too much confidentiality concerning the electronic voting system may breed distrust of the public toward the system, as people may feel that there is no assurance that every vote cast is accounted for.

This combination of technical flaws and public skepticism indicates that the current formula of voting must improve in terms of security, transparency, and trustworthiness. Block chain technology has sparked great interest as a possible means of addressing the many issues that characterize the voting systems in existence. In simple terms, a blockchain can be defined as a distributed database that is employed for various purposes. In this case, it ensures that all transactions or activities that are carried out within the network are recorded in a permanent and accessible cloud platform. A transaction will be entered into a block and that block will be compared to an already existing block known as the previous block thus culminating into an endlessly chained sequence of records which would be especially difficult to tamper with without getting caught. This arrangement provides some degree of safety and soundness that may not be realized in the normal systems, as people have to rely on institutions and their security measures to guarantee such safety. The fact that power is distributed to different users makes it hard for any one person to play with the entire ledger. Towards that end, data is protected from such angles through the use of cryptographic techniques. Such features make the adoption of the use of blockchain technology for secure voting systems attractive. In such a voting procedure, every participant would cast a vote in the form of a transaction that would further be registered in the conciliated system of the blockchain and would be accessible to each stakeholder for verification.

This may help reduce some of the intrinsic risks which are inherent in any traditional voting system such as tampering, miscounts and concealment of processes. Additionally, the functionality of self-executing contracts enables confidence in procurement and execution of a vote by replacing the processes of registration, counting of votes and broadcasting of results.

Enhancing Blockchain Voting Systems with AI and Optimization

There is a primary and also a detailed objective of addressing the problems of the emergence of technology developed to be used for voting security. Examples of such strategies include secure data storage techniques discussed in [11], which tackles the problem of how to cope with pressures on the logistics of a lot of data, in order to use it to risk privacy loss and high efficiency in storage systems. In the same spirit, the transfer learning architecture adopted in [18] is applicable in improving the verification and validation of transactions in blockchain voting systems to ensure that there are no vote tampering activities. The AI techniques used in combating breast cancer as shown in [12] also apply in enhancing blockchain system security by applying machine learning algorithms to identify voting fraud or anomalies from the patterns. As with the employment of Explainable AI methods in smart grid predictions of [14], this aspect will guarantee that elections processed on the Blockchain will facilitate accountability by ensuring that all voters and election officials understand what actions were undertaken to process and verify the votes. Similarly, the predictive analytics to ensure electricity consumption resilience in [15] resonate with the need to perform pre-emptive approaches in anticipation of possible counter activities or sabotage on, or within, the blockchain voting systems.

The chest X-ray anomaly detection techniques seen in [13] are also transferable to blockchain where something out of order can be spotted in the voting ledger thus preventing tampering of the election. Load balancing strategies in datacenter networks as discussed in [17] helps to apportion the facets of the calculation that is carried out at the various parts of the blockchain network in a more resourceful manner so that in instances of high demand voting security is maintained while ensuring scalability. Lastly, power loads in [16] with the use of dynamic modeling techniques can be applied in

estimating voter turnout or system loads ensuring that the blockchain network does not experience any hitches at critical peak times that coincide with elections.

Previous Studies on Blockchain Voting Systems

Several studies have addressed the issue of how the technology of blockchain can be utilized to implement voting systems. The notion of applying any technology that has just been introduced (at that time), as a currency system, which was Bitcoin only, is presented in this study. Since then many authors have researched how the systems of voting can be made better with the use of block embedded in the web and computer systems. It was such a system of block-chains which Zyskind Nathan and Pentland proposed for a voting system based on blockchain. Scientists have come up with yet another sustainable development, which consists of continuous usage of the shift and modulates the dentures. In other research, attention has been paid to the difficulties associated with this technology, namely, to the volume and speed with which processing is able to take place. Despite the security benefits enjoyed from the decentralised nature of blockchain, it has its share of complications regarding the speed and size of processing.

Further, there are studies which have analyzed the potential impact of the implementation of blockchain voting systems on the legal order and the law. It is also worth noting that since blockchain technology is still in its bottom up process, a careful consideration of how the technology will be used within a comprehensive legal regime has been difficult. This poses a barrier in terms of mass usage, as legal certainty is an important prerequisite for the launch of any new development, especially if it is aimed at providing new ideas for voting systems with an additional layer of security jurisdiction. In spite of such hurdles, the research so far indicates that blockchain technology, when applied to the voting process, can prove to be extremely beneficial in terms of the security and accountability of the voting systems in place. However, more research has to be carried out to tackle the other technical, legal and sociological obstacles before technology can be used for such purposes at a regmass scale.

Methodology Framework

Research design

The purpose of this study is to evaluate the integration and functioning of blockchain within the voting systems. In accordance with this feature, it tends to be efficient and accurate in capturing the story from a few interviews instead of more complicated and time-consuming quantitative approaches since it offers a descriptive but deeper view of the technology. Sorting, organizing and analyzing qualitative material rely on preceding research, case studies and the literature regarding more broadly based and particular types of systems, including those related to online and blockchain based voting. It therefore becomes quite productive to use the qualitative strategy in order to describe and discern the richness and diversity of the area of study by allowing for and detecting order within randomness which cannot easily be achieved in a more structured approach such as a quantitative one. The undertaking understands its scope in terms of the articles, conference papers and business publications in the field of security, privacy and technical details of the voting systems based on blockchain technology. So as to achieve the objective of the research design, the use of case studies from different countries was incorporated in the research in order to provide a better understanding of the practical application of blockchain in voting and what can be taken from those applications.

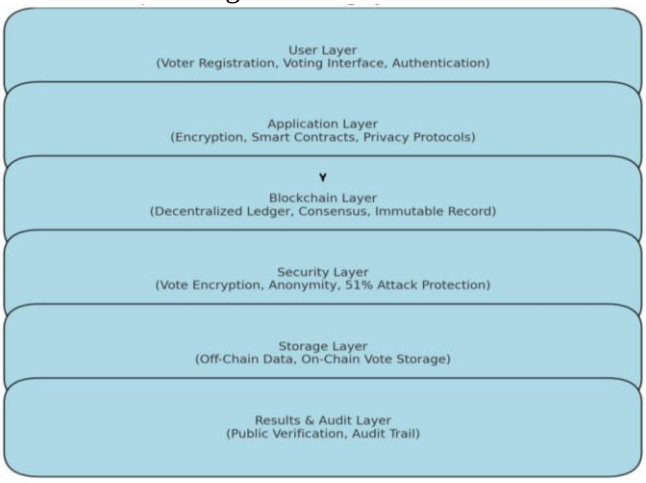

Fig.1 Proposed Enhanced Multi-Layer Blockchain Model

The multi-layer architecture of the current mix-method extends includes voting system based on the proposed Enhanced Multi-Layer Blockchain Model shown in Fig.1. The User Layer (Frontend) contains authorized voter registration page where users are registered directly using verified credentials like a government issued ID. This ensures that only eligible voters participate in the election. The voting interface provides users with a simple way to cast their votes supported by means of authentication like two factor authentication (2FA) and digital signatures which limit illegal access to the system.

In the Application Layer, the contents of vote are encrypted and only those who have been authorized after encrypting with a particular key submit it. Submission, authentication and recording of the votes is done by smart contracts without human involvement. Vote anonymity is achieved using advanced cryptographic protocols like Zero-Knowledge Proofs and Blind Signatures which does not affect the ability to verify the vote.

On the Blockchain Layer, a global electronic voting system consists of a distributed database where votes are held in blocks. Each block is contained in different peers such that one central authority is unable to change the records stored in the database. Concurred mechanisms such as Proof of Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT) are employed to ascertain votes within nodes however, blockchain's uniqueness makes it impossible to modify previous votes regardless of how many more advanced votes will be cast.

In the Security Layer, voting data is encoded in a way that even outsiders cannot access, while methods of counting votes and assuring voters' secrecy such as Homomorphic Encryption and Ring Signature techniques, are applied to assist at that stage. Protection against 51% attacks is achieved through the use of advanced cryptographic solutions as well as the decentralisation of the verification process.

The Storage Layer progress includes leaving no trace of sensitive data like voters' identities but such information is kept within encrypted databases, votes content hashes being put on the chain so as to maintain the sanctity and irrefutability of the electoral process.

Eventually, the Results and Audit Layer equips the system with an assurance that the votes and any related actions that must be performed after, have all been done satisfactorily exposed verification system for below all stakeholders. A robust audit trail that is impervious to tampering is established, making the conduct of post-election audits less burdensome.

The complete architecture flow begins with a safe portal for voter registration and to terns of how voting is done, votes are cast using the encrypted interface. The cast votes are then processed by a smart contract and stored in the blockchain with votes as well as the decentralized network and the counting is done finally. The public verification of the results makes it rather transparent as the timely auditing by the blockchain will increase trust. Fig.2 shows the blockchain voting process flow for the proposed system.

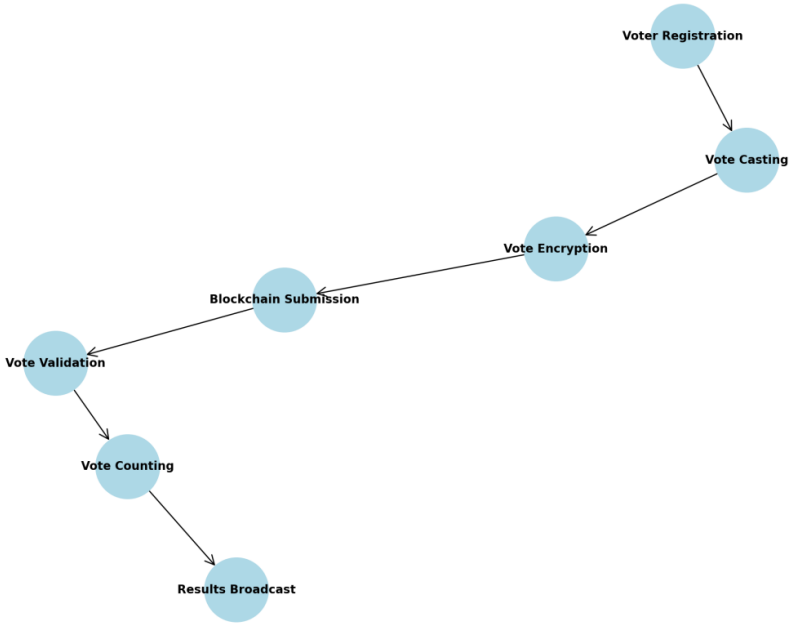

Fig.2 Blockchain based Voting Process Flow

It is impossible to achieve these objectives in one architecture. Thus the proposed architecture combines such important features as security, privacy and transparency constructing an effective voting system based on the blockchain technology. Table.1 provides an overview of the purpose of each component of the proposed model.

Table.1 Proposed Blockchain based Voting System Layers

Layer	Components	Purpose
User Layer	Voter Registration Portal, Voting Interface, Voter Authentication	Allows eligible voters to register, authenticate, and cast votes securely.
Application Layer	Encryption Mechanism, Smart Contracts, Voter Privacy Protocols	Ensures the confidentiality of votes and automates vote handling through smart contracts.
Blockchain Layer	Decentralized Voting Ledger, Consensus Mechanism, Immutable Record	Maintains a decentralized, immutable record of votes across a peer-to-peer network.
Security Layer	Vote Encryption, Anonymity Protection, 51% Attack Protection	Provides security features to protect votes from tampering and ensure anonymity.
Storage Layer	Off-Chain Data Storage, On-Chain Vote Storage	Stores sensitive voter data securely and maintains vote integrity on the blockchain.
Results and Audit Layer	Public Verification Portal, Audit Trail	Offers transparency through public verification and provides a tamper-proof audit trail.

Data Collection Methods

Data collection for this study used multi-resources in an effort to capture multi-views on the blockchain voting systems. First, there are secondary data sources where the primary source is white papers, articles, and journal papers which include theoretical considerations useful in understanding blockchain technology. They have been selected in relation to the subject matter of the research work and the existing gap in literature. Also, this research includes examples of countries that have tried or are currently using a full-scale implementation of democratic elections through the use of block chain technology voting systems. These allow one to understand the application of blockchain technology in elections including its merits and demerits. In addition to these data sources, an interview with domain experts in blockchain, cyber security and electoral processes was conducted in order to augment the data further. These interviews provided first-hand accounts and expert opinions on the feasibility, security, and scalability of blockchain voting systems. The use of these data sources enables researchers to present an integrated analysis that incorporates both theoretical and practical issues.

Analysis Techniques

The study aimed to collect data from a variety of sources in order to achieve a wide understanding of the context of blockchain voting systems. Data collection was done through the use of white papers and empirical research that is considered democracy encloses although pivoted to the concept of digital reconstruction of participation in the electoral process in order to better understand the blockchain technology. The selection of these documents was based on their scope and the available knowledge gap in the field. Furthermore, it reviews the work carried out in countries that have attempted to test or implement a full module of voting using blockchain technology. These case studies further expand the scope of the study by providing real life experience in application of the blockchain technology for the electoral purposes, its advantages, and the problems faced. Also, the study was complemented by interviews of experts on this issue, including blockchain technology specialists, and cyber security and electoral processes professionals. These interviews were directed towards understanding the issues associated with blockchain voting systems with respect to feasibility, security and robustness. It should be noted that these sources of data complemented each other in that each one brought both theoretical and practical angles into the study.

Understanding blockchain technology in voting systems

The blockchain technology is a distributed and secure ledger which can effect profound changes in many sectors. Ancient voting systems included such components as sanctioning for monitoring voter behaviour and sanctioned information control. Each of these transactions, or votes, is stored within a block that is always appended onto a prior block forming a chain of blocks, which is known as a blockchain. This way of structuring information guarantees that it is both accessible and cannot be changed at will, whether a requirement has been fulfilled or not since changing recurring information

would affect all those that are created later. Such characteristics of the information design are one of the reason as to why the blockchain is able to stand up against any malicious tampering and other fraudulent activities. Data consistency within the blockchain is achieved with the use of consensus techniques such as PoW and PoS. These computational techniques manage networks of nodes that are devices deep within the blockchain ecosystem which are in charge of transaction validation by either solving some intricate equations (PoW) or showing the control of some crypto (PoS). Such a system makes it impossible for a single authority to change any information recorded in the blockchain which in turn protects all the data structures. Fig.3 shows these security features for the proposed blockchain voting system.

The introduction of the blockchain technology in voting systems presents several benefits in terms of enhanced security, reliability and building trust between voters. Enhanced security is one of the key advantages that is derived from the distributed and unalterable aspect of blockchain. In traditional electoral processes, almost all power lies with central authorities overseeing the voting process and many doors are left open for such authorities to be corrupt or abused. In such a case, the role of central authorities is eliminated since once a vote is recorded into the blockchain there is no erasing or editing which aggravates security risks of subsequent systems. This feature greatly lowers the chances of fraud and vote tampering; in the case of disagreement on the votes, it is only possible to change the votes by changing every single subsequent block and this requires substantial computer resources. At the same time, the use of a blockchain enhances the level of transparency in elections. In addition, voters are able to ensure that their votes were received and accepted and accounted for without revealing personal information, as all actions are entirely visible in a completely anonymous manner in a system where all transactions are recorded onto a transparent blockchain. Such openness creates an assurance to those who were not involved that the outcome was true and independent verification could be performed.

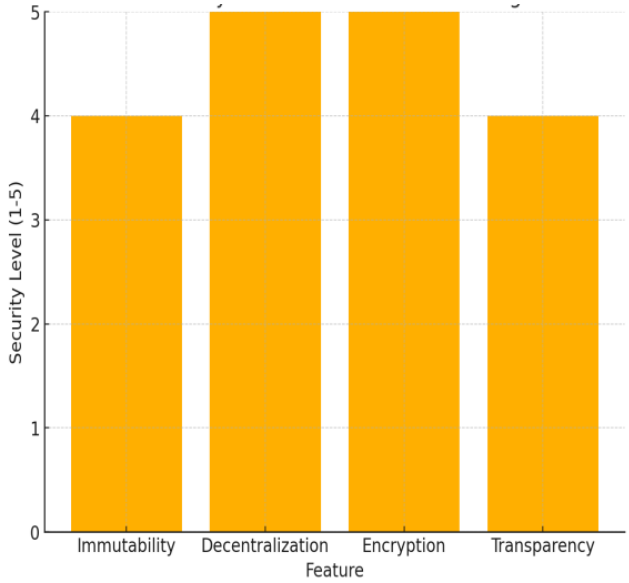

Fig.3 Security Features of Blockchain Voting

Moreover, the application of blockchain technology may allow for speedy and efficient counting of votes. This will further assist in the timely declaration of election results heightening the confidence of the electorate in the voting systems.

Case studies and Examples

A few countries have taken the first steps toward introducing a blockchain-based electoral system and have made significant advancements in this process. This would revolutionize the manner in which people conduct their elections. Estonian countries with experience in the field of distance voting systems using the Internet have applied the principles of blockchain technology to e-Residency which allows them to cast their vote through the internet securely. This innovative use of blockchain has ensured that the elections held in Estonia are above board and fair thereby assisting other countries wishing to protect their elections. Likewise, Swiss authorities undertook several such pilot projects with the aim of realizing the possibility of ballot using a blockchain. The experiments showed that blockchain can improves security of such systems and electronic voting as a whole. In particular,

these studies show that administrative units of Switzerland used the blockchain for the conduct of municipal elections and that this enabled greater turn out of voters by making the election processes faster and safer. These case studies indicate that blockchain voting systems are not only possible but also can overcome a great deal of problems that have hindered other voting systems since time immemorial. Such significant progress punctuates sensitivity, impact and the rule of law on territorial integrity: and as such, equal opportunity for fair democratic practices, especially where constitutional proxy allows.

Challenges and Solutions

Technical Challenges

Nonetheless, blockchain-based voting systems present several practical difficulties despite the notable advantages they lay against the traditional voting systems. A primary concern is the fact that there are relatively high costs each time a high volume of votes is processed through the blockchain. Each vote is regarded as a transaction and therefore has to be verified and recorded which can pose a problem especially with large elections. Apart from high transaction costs, there is also a network delay which is another problem. With many people transacting, the time taken to process and to have the network confirm each of the transactions increases. These delays might result in delays in counting of the votes cast and reporting of results which in turn might affect the trust the public has in the voting process. Scalability is probably the most serious challenge of all since a blockchain voting system will in all likelihood needs to cope with millions of votes cast in a very limited time frame. Existing systems like the blockchain for the currency are too low in their structure that they cannot take demand of this magnitude without stalling. To overcome these difficulties, researchers and developers have started to consider new approaches like off-chain transactions.

Sharding is a process by means of which the blockchain is divided into several small and easy to use units, allowing for transactions to be validated separately in each unit. This method, in principle, provides a good measure of scalability as it increases the amount of interaction that can be carried out in a system at any given point. Off-chain transactions, on the album's cover, include particularly the transactions that are performed without being recorded in the primary blockchain which helps to reduce the load and speed as well as the costs for transactions. The introduction of these and others, technical devices will increase the specifics and usability of the systems of voting by means of blockchain technology.

Security Concerns

Being a voting system, security is a central element strategically with no exception for blockchain based voting systems. Most notable is the concept of 51% attack, where a singular or coordinated group is able to amass power that constitutes greater than half of the network. An attacker, in this case, would be able to reconfigure vote records on the blockchain or execute a double spend to jurisdictions which compromises the election process. Although the distributed ledgers make this category of attacks hard to perform, it is still a challenge that needs to be considered. The protection of the identity of the voter is also a critical area that requires attention. It is tough to achieve the right equilibrium where disruptors will be in a position to ensure that the votes are non-identifiable whereas the credibility as well as openness of the elections is upheld. Recently proposed cryptographic protocols such as zero-knowledge proofs may aid in resolving such concerns. Zero-knowledge proofs by some extension permit verification of votes without identifying the voter. This ensures both privacy and transparency during the voting process reducing the interference of vote anonymity and vote data integrity issues.

Also, refining modern cryptographic techniques and secure multi-party computation methods can also increase the security of blockchain-based voting systems and protect them from different kinds of attacks.

Implementation Issues

By all means, when a voting system utilizing blockchain technology is to be put into practice, it is necessary to resolve a number of political, regulatory and sociological issues. In order to use any innovative voting technology, including blockchain, one of the most important elements is the positive attitude of the people towards it. It is necessary to prepare people to trust tokenized voting by explaining its advantages and security features. However, that is not enough. There are also political and legal ‘walls’ that need to be overcome. There is in fact a sequence of measures that ought to be undertaken by the State and regulatory agencies and electoral authorities who adopt certain legal

measures to render framework that endorses the use of blockchain technology but that is ensured that there is adequate accountability and adherence to the electoral laws that achieve the desired results. However, constructing these types of frameworks is not simply an ordinary exercise and personnel needs to bear in mind some specific features of the blockchain and its possible influence on the political sphere. The trials and pilot projects regarding the block voting systems serve there, expressing new possible developments and possible workarounds to current voting systems. Trust among the population can be increase through these initiatives and practical measures can be taken to assimilate the technology with existing electoral processes.

In addition, the inclusion of other actors such as political leaders, election officials and the voters themselves is necessary in order to resolve the issues at hand and to create a conducive environment for the implementation of the blockchain based voting systems.

Proposed Solutions

Given the political, technical, security, and implementation concerns encountered with voting based on blockchain technology, it would seem that the best way forward is to consider hybrid systems that integrate blockchain and traditional voting practices. Under such systems, the merits of blockchain as well as the old techniques are utilized in voting systems that are efficient and secure. For example, votes can be maintained via a blockchain system which would limit manipulation of the votes while voter registration and verification could be done by the offline approach to make the system more efficient. Moreover, incorporating highly sophisticated encryption methods and more practical consensus mechanisms like Proof of Stake (PoS) will also boost the security and efficacy of the blockchain voting systems. The PoS method for instance makes sure that those who validate a block are the ones who own a number of coins. This greatly mitigates the chances of a fortieth – fifty percent attack as well as the energy costs required in the validation procedures. Therefore, a solid legal framework and constant dialogues with stakeholders is necessary to ensure the effective utilization of blockchain votes for elections. Such regulations will cover issues with electoral primacy such as ensuring the privacy of voters, the safety of data, and the openness of elections that will enable the application of blockchain technology to election processes.

On account of technological sophistication, extensive exploration and involvement from the stakeholders, there is the likelihood of coming up with a ballot system through the utilization of blockchain technology which all modern democracies would appreciate.

Discussion

Analysis of Findings

The outcomes of this research show that voting systems that employ blockchain technology can be adopted with ease. In the use of blockchain technology, votes cast can be recorded in a ledger that cannot be changed fraudulently. This is where the positive note comes because for quite some time the traditional forms of voting have faced a lot of risks, whether it’s a bombing of the ballot box physically balloting or hacking electronically voting systems. However, in spite of the aforementioned benefits, the study also exhibits some major issues that need to be resolved in order to implant blockchain in supranational elections. The first one of such issues is that of how large scale there is going to achieve. Fine, attention seeking and close security of blockchain can be activity on managing resources in the lower confines. A problem comes in estimation of how many votes a national election would entail using the technology. Most, if not all, currently existing structures that pertain to the basic architecture of most blockchain networks were not meant for such large quantities of data whereby anxiety about the expenses of transaction and latency of the network arises. And also, the presence of voting public and the assurance of the security and confidentiality of their votes are still regarded as delicate and highly evaluative aspects.

Blockchains may protect the tampering of the votes cast, yet information on voters’ ballots cannot be made available for viewing and at the same time independent verification of election results should be made possible. Therefore advanced cryptography is required in this case. There are such methods in the arms of cryptography, like zero knowledge proofs and homomorphic encryption, that can work but still too abstract for voting as they are.

Implications for Future Voting Systems

The advent of blockchain technology can bring extensive changes to the electoral systems of the future. It would be possible to conduct elections in a different manner if the problems mentioned in the present research are solved. This would help put voters' minds at ease by providing an election

process that can be secured, opened and confirmed, and thus reduces the likelihood of any disagreements on election results and increases the number of people who will vote. Nevertheless, the introduction of blockchain voting systems will be possible only after all technical, legal and social barriers have been addressed. Addressing these challenges will require the use of research resources that are resilient, adaptable and possess the technology capabilities necessary for running national elections utilizing blockchain without any sacrifice on safety or efficiency. Furthermore, people have to be taught the advantages and downsides of a blockchain since almost every new system that states that it incorporates such technology will need a degree of public trust in order to work. Governments, the tech industry and academic institutions may play a large part in enhancing voting technology based on blockchains. Pilot projects and public-private schemes might be effective as such new settings for such promising solutions so that the technologies and the current problems are optimised and solved in an experimental way.

A proactive stance on the creation of blockchain voting systems can encourage the way and make it paves the way for a new generation of secure and open elections.

Policy Recommendations

Policymakers ought to be prepared for the future by integrating provided blockchain voting technologies because these will seek to improve the transparency and performance of elections. As given the misuse of those in the current situation, those stakeholders are warranted to be trying out new technology if there are any pros of these: this study suggests those pilot projects along with other analysis to develop this technology and deal with the issues addressed in this study. They can help in experimenting, assessing and refining the technology for easier and safer deployment in the future. They should also direct efforts towards educating people and creating acceptance towards the use of blockchain voting systems. Such campaigns can help the public increase comprehension regarding the utility and safety of the trust holders and help in trust enabling even in the discriminative environment that exists currently regarding the electorate against the systems being used. Similarly, adequate jurisdictions also need to be established for the blockchain voting systems to work effectively. Such policies must include clear legal requirements that will govern elections conducted and managed on blockchain to demonstrate efficiency and solvable accountability. International relations and agreements could also play an important role as well since it would be easier for all the states applying their westernized methods of conducting elections to build on one and trueness of their systems.

The collaboration of governments and international organizations will guarantee that voting will be secure and trustworthy in the future, making way for a more transparent and democratic electoral process.

Conclusion

The process of the complete migration to blockchain voting systems has its own peculiar problems. This research suspected and identified several challenges that have to be removed in order to introduce electors voting through a blockchain system. For instance, the main factor that hinders the true use of blockchain around the world is the scalability or in simple terms – how many transactions will be able to be processed at once given that multiple transactions must be done within a single day being an election day. Additionally it requires development and utilization of sophisticated and not well developed Algorithms and Architecture that can be used to improve the Verification and Integrity of election results while taking care of the privacy of the voter.

References

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Alshehri, A., Baza, M., Srivastava, G., Rajeh, W., Alrowaily, M., & Almusali, M. (2023). Privacy-Preserving E-Voting System Supporting Score Voting Using Blockchain. Applied Sciences, 13(2), 1096. doi:10.3390/app13021096.

Zyskind, G., Nathan, O., & Pentland, A. S. (2015). Enigma: Decentralized Computation Platform with Guaranteed Privacy. arXiv preprint arXiv:1506.03471.

Cohen, J., Goonetillake, S. S., & Bhuta, R. (2020). Implementing Blockchain Technology for Secure Voting Systems. Journal of Information Security and Applications, 54, 102563. doi:10.1016/j.jisa.2020.102563.

Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media.

Castro, M., & Liskov, B. (1999). Practical Byzantine Fault Tolerance. Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI).

Yavuz, E. A., Koc, C. K., & Cataltepe, Z. (2018). Towards Secure E-Voting Using Ethereum Blockchain. Proceedings of the 2018 International Conference on Computational Science and Computational Intelligence (CSCI), 547-552. doi:10.1109/CSCI46756.2018.00112.

Pilkington, M. (2016). Blockchain Technology: Principles and Applications. In F. Xavier Olleros & M. Zhegu (Eds.), Research Handbook on Digital Transformations (pp. 225-253). Edward Elgar Publishing.

Chaum, D., Rivest, R. L., & Sherman, A. T. (1988). The Blind Signature System. Advances in Cryptology – CRYPTO '88, Lecture Notes in Computer Science, vol 403. Springer, Berlin, Heidelberg.

Garratt, R. J., & Lee, M. (2018). Blockchain and the Future of Financial Services. In R. Rau, R. Wardrop, & L. Zingales (Eds.), The Handbook of Blockchain, Digital Finance, and Inclusion (pp. 101-136). Academic Press.

J. I. Janjua, T. A. Khan, S. Zulfiqar, and M. Q. Usman, "An architecture of MySQL storage engines to increase the resource utilization," in Proc. BalkanCom, 2022, pp. 68–75.

A. Fatima, A. Shabbir, J. I. Janjua, S. A. Ramay, R. A. Bhatty, and M. Irfan, "Analyzing breast cancer detection using machine learning & deep learning techniques," J. Comput. Biomed. Informatics, vol. 7, no. 2, pp. 230–248, 2024.

J. I. Janjua, T. A. Khan, and M. Nadeem, "Chest X-ray anomalous object detection and classification framework for medical diagnosis," in Proc. ICOIN, 2022, pp. 711–718.

J. I. Janjua et al., "Enhancing smart grid electricity prediction with the fusion of intelligent modeling and XAI integration," Int. J. Adv. Appl. Sci., vol. 11, no. 5, pp. 230–248, 2024.

J. I. Janjua et al., "Predictive analytics and machine learning for electricity consumption resilience in wholesale power markets," in Proc. ICCR, 2024, pp. 102–110.

W. Alomoush, T. A. Khan, M. Nadeem, and J. I. Janjua, "Residential power load prediction in smart cities using machine learning approaches," in Proc. ICBATS, 2022, pp. 123–132.

T. A. Khan, S. Abbas, J. I. Janjua, and M. Asif, "Topology-aware load balancing in datacenter networks," in Proc. APWiMob, 2021, pp. 156–165.

R. Javed, T. Abbas, J. I. Janjua, M. A. Muhammad, S. A. Ramay, and M. K. Basit, "Wrist fracture prediction using transfer learning: A case study," J. Popul. Ther. Clin. Pharmacol., vol. 30, no. 18, pp. 1050–1062, 2023.