WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Challenges and Opportunities of Blockchain for E-Voting

Vedant Dere[1], Dr. Harshali Patil [2]

[1] Department of Information Technology S K Somaiya College, Vidyavihar, Mumbai, India vedant.dere@somaiya.edu
[2] Department of Information Technology S K Somaiya College Vidyavihar, Mumbai, India harshali.yp@somaiya.edu

ABSTRACT:

Technology evolution depicts the new opportunities about electoral processes, especially electronic voting systems, as well as the challenges related to them. Based on blockchain's decentralized and immutable characteristics, it can manage the serious issues of voter fraud and data integrity causing distrust by the people. However, the adoption of blockchain with electoral systems poses severe problems related to technical complexity, regulatory barriers, and the need for mass acceptance of voters and electoral officials. Our analysis reveals that while blockchain's innovation is promising for e-voting, its successful integration requires overcoming significant barriers, including technical complexity and regulatory challenges. This paper explores these barriers and proposes an integrated adoption framework, which indicates that while blockchain is very high on innovation, use of it in e-voting can only thrive if considerable barriers are created toward the view of making electoral processes much more secure and accessible.

Keywords—Blockchain; Voting; Consensus; bitcoin; Ethereum; ballot

1.Introduction :

Digital technologies are transforming most aspects of our lives. And the electoral process stands at a very decisive crossroads. E-voting has taken its place as one of the promising alternatives to traditional voting methods-in terms of increased convenience, accessibility, and efficiency. At the same time, it is marked by serious barriers related to security, transparency, and trust in electoral outcomes. It is here where blockchain technology can pose challenges and opportunities for deepening the e-voting landscape.

The decentralized and tamper-resistant nature of blockchain presents a framework through which most of the weakness could be mitigated in an electronic voting system. According to proponents, making e-voting more secure and trustworthy is possible with intrinsic qualities of blockchain, such as cryptographic security giving it a tamper-proof nature and its record-keeping nature. However, challenges abound in the application of blockchain into electoral processes. The efficacy of such a procedure is determined mainly by the level of faith that people have in the election process. The creation of legislative institutions to represent the desire of the people is a well-known tendency. Such political bodies differ from student unions to constituencies [1].

Bitcoin's technology allows for immediate and transparent tracking of all transactions and coin totals, thanks to its distributed ledger system. There is no need for a central authority to approve or complete the operations on this P2P-based system. Because of that, not only the money transfers but also all kinds of structural information can be kept in this distributed chain, and with the help of some cryptological methods, the system can be maintained securely [2].

This paper elucidates the dualistic nature of blockchain in the context of e-voting, unveiling its potential for transformation of the election process against the backdrop of challenges, thus raising necessary questions to be answered

Figure 1. Characteristics of blockchain architecture [1].

- Immutability: The original text of any blockchain paper cannot be edited or removed.
- Cryptography: The calculation and the proof that cryptography offers between the parties doing the transaction assures error-free and safe blockchain transactions.
- Provenance: This term means that each transaction can be traced in a blockchain ledger.
- Decentralization: The whole distributed database can be open for any of the entities in the blockchain network. Thus, a consensus algorithm does help keep the control of the system as seen above in an effortless process.
- Anonymity: In the blockchain network, one participant has created an address in place of giving the identity of the user. As a result, their identity is not shown while using the system, especially within the public blockchain network.
- Transparency: It simply means no one controls the blockchain network. This is impossible because the destruction of the blockchain needs an enormously large computational power.

2. Literature Review :

Blockchain is the emerging peer-to peer distributed computing platform used for recording and verifying transaction activity. First it occurred with the emergence of Bitcoin from Satoshi Nakamoto in 2008. Blockchain is decentralized, immutable, and transparent-and these properties make it very suitable for the applications that go beyond developing cryptocurrencies, namely, supply chain management, healthcare, voting, etc. These systems are developed with efficiency and easier access to voting in mind.

Those, however, are major disadvantages-major security wise, transparency, and even fraud concerns. From them, interest among the scientific community to explore the possibilities of applying blockchain technology for augmenting the credibility and integrity of electronic voting systems was huge. Academic literature has analyzed blockchain technology in applications on electronic voting, and many projects and trials found potential utility for the e-voting system. The pilot blockchain voting program developed in West Virginia might be the first-ever example of really experiencing electoral processes with blockchain technology. From the findings researched above, it can be said that blockchain has the potential to fight most of the constraints attributed to a conventional electronic voting system in terms of security, anonymity, and more specifically, verifiability.

A blockchain consists of a chain of blocks that are connected in such a way that each block has a unique hash value for its identification. The blocks are connected by icing so that each block contains the hash value of its antedating block, thereby creating a nonstop chain in the form of a distributed digital tally [3,4]. The blocks in a blockchain are distinct and independent computing bumps that interact grounded on a cryptographic protocol. All deals in a blockchain are validated by other bumps before it's recorded in the blockchain. A new block can only be created grounded on a predefined agreement protocol, which defines the rules of commerce amongst the bumps of blockchain [5]. The creation of a new block and the confirmation of deals are done by the agreement algorithm. The most common agreement algorithms include evidence of work, evidence of stake, and delegated evidence of stake [6], which are used to authenticate all deals in the blockchain to help illegal manipulation by external agents [5].

Limitation:

1. Scalability Issues: Scaling issues in public blockchain networks is primarily due to the restriction imposed by their own consensus mechanisms. Because of the complexity of the transactions, mainly in voting processes, managing the same can be quite strenuous.
2. Cyber Security Threats: Despite its inherent nature of being much safer than the traditional versions, blockchain technology never makes it any cyberattack-proof.
3. Regulation and the Law: As blockchain-based e-voting appears, they will follow established legal implications associated with every election that takes place in a region. The law is not exactly well defined across authorities.
4. Technological Complexity: Since blockchain technology is to be integrated within the current architecture of an e-voting system, there are vast technical details involved. These complexities arise in interoperability, usability, security, and privacy considerations, making it difficult to overcome such challenges.

Opportunities:

1. Transparency: This stands for the clarity of the voting process with regards to all participants within a blockchain-based voting system that may confirm no manipulation or fraudulent activities have occurred.
2. Voter Anonymity: Blockchain ensures that the voter will vote anonymously, but at the same time, authenticates the vote, hence addressing two issues of voter coercion and violation of privacy.
3. Decentralization: Decentralizing the voting system reduces risk to a single point of failure, so it stands for a crucial factor in promoting and increasing the robustness of the electoral process.
4. Trust and Confidence: It will contribute to adding confidence of the public to the electoral process as it can lead to increased voting since security features are inherent attributes of blockchain technology and transparency.

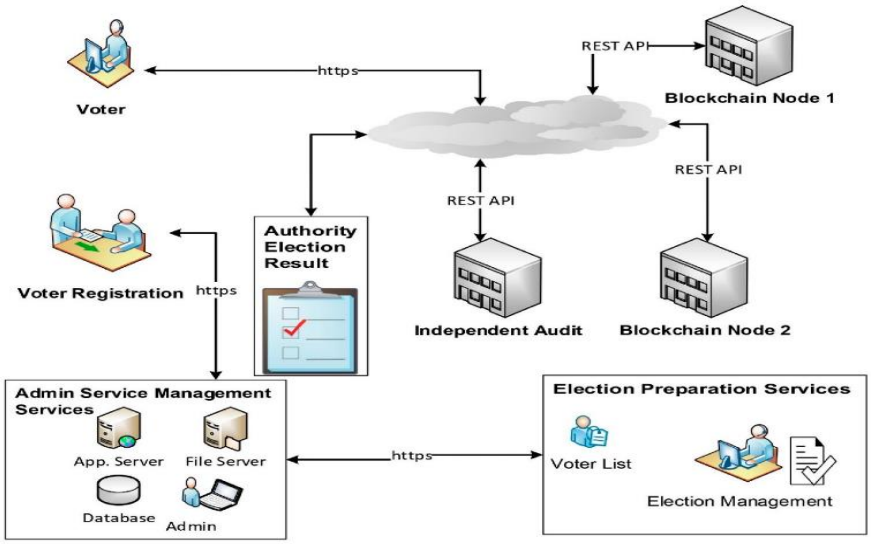

Figure 2. A Blockchain voting systems architectural overview [7].

5. Research Objectives :

Objectives:

1. Recommend the most significant threats that could be associated with blockchain technology on the use of electronic voting systems.
2. Describe potential advantages that could be attributed to a blockchain for use with e-voting.
3. Conduct an in-depth analysis of blockchain technology based electronic voting systems.
4. Outline strategies to address identified problems and mechanisms for exploiting opportunities.
5. To send propositions of future studies with a view to finding emerging lacunae in literature.

Research Problem:

E-voting systems with blockchain technology, in the same way as other innovations, have disadvantages and advantages. The most significant advantages of such a technology include better security attributes, increased transparency, and the ability to vote anonymously. Apart from technical glitches, some issues relate to scalability and cybersecurity, regulatory, and legal aspects. All these must be grasped to provide the best e-voting systems based on blockchain technology.

6. Expected Findings:

There have been multiple criticisms of blockchain-based e-voting over the past few years. Some researchers said that the blockchain system cannot solve e-voting problems and may create new vulnerabilities, such as keeping malware out of voters' phones and computers. As examples, MIT (Massachusetts Institute of Technology) experts have identified the vulnerability that has occurred in a mobile voting application used during the 2018 mid-term elections in West Virginia [18].

Challenges:

1. The consensus mechanisms of blockchain causing scalability issues.
2. Security hole (potential cyber-attacks).
3. Inconsistent and conflicting regulatory or legal challenges across different jurisdictions
4. Integration of blockchain into existing e-voting infrastructure poses technical challenges.

Opportunities:

1. Increased transparency and accountability of the election voting mechanism.
2. Protection of voter anonymity and confidentiality
3. Proximity and decentralization mitigate risks of single points of failure.
4. Public trust and confidence in administration of the electoral process was significantly enhanced.

These results will give a global perspective on the current state of research related to blockchain-based e-voting systems and direction for future research in this area.

Electronic voting systems with blockchain technology Implementing electronic voting systems using blockchain technology: A review electronic voting systems using blockchain technology Contemporary blockchain based electronic voting systems.

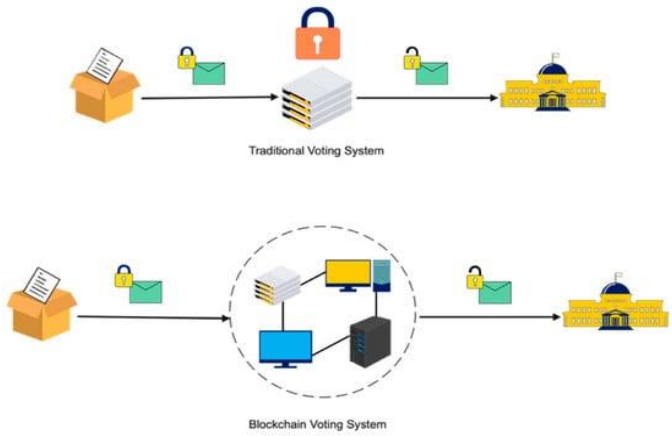

Figure 3. Comparison of Traditional and Blockchain Voting System [1].

Some of the newly formed institutions and establishments, a good majority of which are less than five years old, have dedicated themselves to electoral sector development: Each has a sharp vision relating to the very practical implementation of transparency through the blockchain network.

1.Follow My Vote

The organization provides safe online voting using blockchain technology while offering real-time follow-up of what goes on in the democratic process. This makes the system enable voters to put their votes while being in a secure environment and thus make their choices of preferred candidates for elections. This would further be applied to literally enter the ballot box physically, find where to locate their ballots, and as a verification of what has been enclosed inside the ballot is right, and thus the electoral results are mathematically valid [8].

2.Polyas

Although it is a start-up firm from Finland, it managed to set up an electronic voting system that utilizes blockchain in 1996 for both the public and private sectors [9].

3. Agora

It is a group that has just recently launched the blockchain digital voting platform. Introduced 2015 and partially tested during the Presidential vote of Sierra Leone that occurred in March 2018. Agora's technological architecture depends on several innovative technologies: a decentralized ledger, identity of individual contribution and distributed consensus by laws. Vote is the native token of the Agora's ecosystem. It obliges citizens and elected bodies, authors of elections worldwide, to adopt a clean electoral process [10].

4. Voatz

The firm has thus developed a smartphone-based voting system that makes use of blockchain in respect to voting, encryption verification, and correct processing of votes. People embrace the candidates whom they wish to be alongside themselves in the application. This is done for which an image is provided, and acceptable identification through biometric validating methods or distinctive marks like a fingerprint or retinal scan is given [11].

7. Conclusion and Future Work :

Even today, e-voting is an object of heated discussions among political scientists as well as technologists. As mentioned in the earlier sections, while few gave almost perfect examples to implement and are still functioning; many more were unable to offer the security and privacy features of a traditional election or else were critically or substantially impaired in their usability and scalability factors [12]. Conversely, the blockchain-based e-voting solutions such as this we have developed employing smart contracts and Ethereum network, may effectively respond to (or with adjustments made) virtually all these vulnerabilities for example, the voter anonymity, vote genuineness, vote verification, and certified record of the voting and tallying processes. However, there are also some properties that are still inaccessible by using only the blockchain, for example, a specific aspect of authentication of voters (not account-based but on the per-person basis), can only be supplemented with other authentication factors including biometrics.

REFERENCES:

1. U. Jafar, M. J. A. Aziz, and Z. Shukur, “Blockchain for Electronic Voting System—Review and open Research Challenges,” *Sensors*, vol. 21, no. 17, p. 5874, Aug. 2021, doi: 10.3390/s21175874
2. Yadav, “E-Voting using Blockchain Technology,” *International Journal of Engineering Research and*, vol. V9, no. 07, Jul. 2020, doi: 10.17577/ijertv9is070183.
3. E. Yavuz, A. K. Koc, U. C. Cabuk, and G. Dalkilic, “Towards secure e-voting using ethereum blockchain,” *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, Mar. 2018, doi: https://doi.org/10.1109/isdfs.2018.8355340.
4. P. McCorry, S. F. Shahandashti, and F. Hao, “A Smart Contract for Boardroom Voting with Maximum Voter Privacy,” *Financial Cryptography and Data Security*, pp. 357–375, 2017, doi: https://doi.org/10.1007/978-3-319-70972-7_20.
5. O. Daramola and D. Thebus, “Architecture-Centric Evaluation of Blockchain-Based Smart Contract E-Voting for National Elections,” *Informatics*, vol. 7, no. 2, p. 16, May 2020, doi: https://doi.org/10.3390/informatics7020016.
6. S. Zhang and J.-H. Lee, “Analysis of the main consensus protocols of blockchain,” *ICT Express*, vol. 6, no. 2, Aug. 2019, doi: https://doi.org/10.1016/j.icte.2019.08.001.

7. R. Taş and Ö. Ö. Tanrıöver, "A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting," *Symmetry*, vol. 12, no. 8, p. 1328, Aug. 2020, doi: https://doi.org/10.3390/sym12081328.
8. "Secure Decentralized Application Development," *Follow My Vote*. https://followmyvote.com
9. "Online elections, nominations & voting with POLYAS," *polyas.com*, Mar. 12, 2021. https://www.polyas.com
10. "Agora," *Agora*. https://www.agora.vote
11. "Home - Voatz secure and convenient voting anywhere," *Voatz*. https://voatz.com
12. F. Hao and P. Ryan, *Real-world electronic voting : design, analysis and deployment*. Boca Raton, FL: Taylor & Francis Group, LLC CRC Press is an imprint of Taylor & Francis Group, an Informa Business, 2017.
13. K. Cao, G. Xu, J. Zhou, M. Chen, T. Wei, and K. Li, "Lifetime-aware real-time task scheduling on fault-tolerant mixed-criticality embedded systems," *Future Generation Computer Systems*, vol. 100, pp. 165–175, Nov. 2019, doi: https://doi.org/10.1016/j.future.2019.05.022.
14. M. Specter, J. Koppel, D. Weitzner, M. Daniel, and W. Mit, "The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections the Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections *," 2020. Available: https://www.usenix.org/system/files/sec20-specter.pdf
15. Y. S. Astle, X. Tang, and C. Freeman, "Application of dynamic logistic regression with unscented Kalman filter in predictive coding," *2017 IEEE International Conference on Big Data (Big Data)*, vol. 52, pp. 1381–1389, Dec. 2017, doi: https://doi.org/10.1109/bigdata.2017.8258071.