Survey of Techniques for Security of E-Voting System using Blockchain

Anjali J. Rajput[1], Pratik K. Patel[2], Jaimeel Shah[3]

Department of Computer Science and Engineering

Parul Institute of Engineering and Technology, Parul University

Email: *190303201004@paruluniversity.ac.in[1], pratik.patel2988@paruluniversity.ac.in[2], jaimeel.shah@paruluniversity.ac.in[3]*

DOI:- https://doi.org/10.47531/SC.2022.17

Abstract

In a democratic country like India (which is the largest democracy in the world), voting plays a significant role in selecting government officials and showing our opinion on how the governing body to be formed. Blockchain platforms are already available, and many companies have already begun applying blockchains to their business. It is used in industry, but it can also be applied as a service and make voting more accessible. Online voting is an alternative to the old paper ballot system and the currently popular electronic voting machines (EVM). An electronic voting portal should offer security and integrity and the transparency of votes and voters' privacy. Therefore, NRIs and adult internet users can cast their ballots in a matter of seconds despite their location on the day of the election. This will be easy and more secure. In the current system, there's a high risk of false votes and damage to property. People don't want to stand in enormous queues and wait for a long time. Also, people who conduct the election have to follow a completely different procedure for voting, which takes more time, and there's no transparency. The paper also presents the state of the art of some blockchain frameworks for e-voting. This paper presents a literature review of the techniques used to tackle voting challenges.

Keywords: - *Blockchain, E-voting system, P2P network, Smart Contract, Ethereum, Decentralised, High security, Solidity, Truffle*

INTRODUCTION

Elections can easily be manipulated and corrupted, particularly in small cities and extended to polluted big cities housed in corrupted nations [1]. In traditional voting, the voters have to be physically present in their native place. Despite the government declaring a holiday on the said date, it is challenging for people to stay afar from their native. This issue can be solved using e-voting.

Issues in e-voting security are (i) failures in security, (ii) stealing secrets (username and password), (iii) modifying already casted votes, and (iv) modifying future votes by hacking the voting software [1]. In addition, the following

assets should satisfy any e-voting system. (A) Completeness (B) Robustness (C) Privacy (D) Unrepeatable (E) Eligibility (F) Individual verifiability.[7] elections are institutions that are meant to bring democracy to countries. They largely play a crucial role in the life of the country and the citizen. Therefore, it has a lot of significance for every single person involved in these elections. Whatever the organisation, elections should be credible. They have to ensure people's privacy and vote's security. Additionally, the authority responsible for counting votes should not spend too much time counting votes since waiting long. Duration before result increases concerns about manipulation of results. However, due to the different reasons depending on the areas that elections have been made, trust has been a controversial issue for each election. Especially as a centralised authority manages paper elections, there is always a risk of manipulating ballots and election results [4]. Voting is a method to make a collective decision or express an opinion among a group or a meeting or electorates [1]. Voting is usually following debates, discussions, and election campaigns. During voting, the person to be elected is the candidate of an election, and the person who casts a ballot for their chosen candidate is the voter [2]. Usually, the voter can vote following the list of candidates or vote for any other person they prefer.

So the question is," how to be sure about the election results that it's correct and how to find out if it's wrong?". There is always a trusted party responsible for counting the votes in paper voting, and the voters must rely on that. In this type of election, the process of verifiability and tallying is performed only by the trusted party, so the voters cannot find a way to check and verify the correctness of the final results. In end to end voting verifiable systems, this dependency on a trusted party is reduced to give the right to the voter to check and verify the results if it's correct or not.

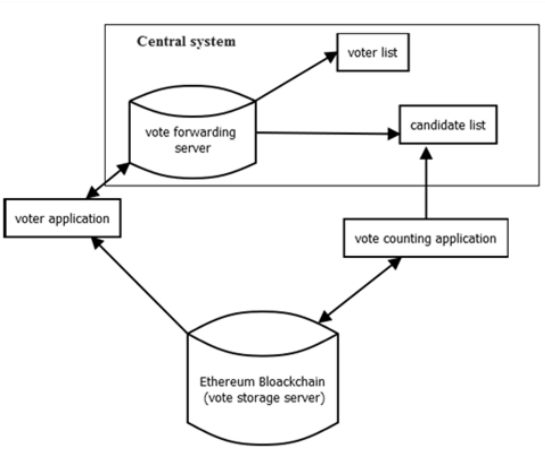

Fig. 1 Example of e-voting diagram

MOTIVATION FOR BLOCKCHAIN TECHNOLOGY

Blockchain Technology is becoming more and more evident in our day to day lives. More and more companies have started using Blockchain as an underlying network for their daily transactions. When Blockchain became popular, it was only used for handling payments using the crypto currency Bitcoin. Still, various studies have been carried upon over the years, which suggest that Blockchain can be used in many more areas.[5] Traditionally, the database is maintained by a central authority or a single organisation that has complete control of the database. It can tamper with the database and manipulate the data.[11] Usually, the authority maintaining the database is the same that has created it and will be using it. In such cases, the organisation has no motive for manipulating or falsifying its data. But in other cases involving financial matters or sensitive data like voting, it's not wise to give a single authority

or organisation total control of the database. Even if the organisation is confident of preventing any fraudulent changes to the database, it is easier for hackers to manipulate a central database. To avoid such situations, Blockchain makes the database public so that anyone can store an individual copy of a database that can always be compared to check for manipulations. However, individual copies must constantly be updated to maintain consistency. To maintain a consistent decentralised database, Blockchain utilises a consensus mechanism.

Therefore, DApps will have the following Blockchain features: 1) Strong data integrity. 2) Decentralised control and validation through consensus mechanisms. 3) Transparent run time environment.4) Public business rules running in the run-time environment. 5) High availability [5].

(A) Smart contract

Smart contracts are self-executable code written inside blockchains. These are similar to conventional business contracts that are used for code of conduct agreements between two parties. The intelligent contracts execute automatically when the defined conditions are met. Smart contracts help to carry out agreements and transactions in a trusted manner among the untrusted or unknown parties without the requirement of central authority. A smart contract is an account that is controlled by its code [9]. It is considered an autonomous agent executed by the EVM (Ethereum Virtual Machine) and is the core foundation and the main building block of any DApp [10]. Once this code is deployed on the Blockchain, the EVM will run it as long as the conditions apply. It is important to note that smart contracts, once deployed to the Blockchain network, can be publicly visited and viewed via their address with all their associated transactions (to address, from address, timestamp, etc...).[14] Triggering functions in the smart contract can be performed from any account as long as the following two conditions are met: 1) the address of the smart contract is known, 2) The function caller has sufficient Ether to trigger.

The Determinism of Smart Contract: The first challenge to address is to ensure the determinism of smart contracts. Ideally, we hope the entire voting flow can be driven by smart contract only to ensure that every step of voting, verifying and tally is done under the consensus of all voters.[12] However, since the smart contract is executed in all peers within a network, its behaviour must be deterministic to ensure different executions can always result in the same output.

(B)DApp(DECENTRALISED APPLICATION)

DApp is a "blockchain-enabled" web application running on a peer-to-peer computer network rather than a single server. It includes both the front end and back end and works independently on all nodes. Typically, other applications also use the same technology to create the front-end interface. The only critical difference is a smart contract that connects the application with a blockchain network.[18]DApps aims to alleviate these issues by distributing critical components that store data or parts of infrastructure between various peers or nodes. That's why, when designing DApp, security, cost, usability features should be considered [19]. DApp applications are required to contain some features. Such as; [10] Better performance (low latency, high throughput), Reasonable low transaction fee, Flexible maintainability, DApps should not store or

replicate user data. The point of Blockchain security is based on not having any central vulnerability. Users should use the application as the sole administrator of their independent and unique identifiers. It reduces reliance on central authorities. The application should not be too complicated and should have a simple interface. Unnecessary coding should be avoided; it increases the cost and may create a security weakness.[20]

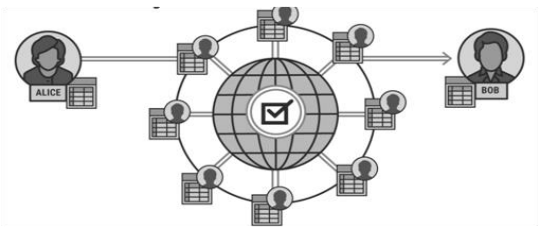

Fig. 2 Decentralized Application diagram

(C) Challenges of voting

1. Privacy: There shall be no third-party intervention of any kind regarding the election. The only voter is allowed to view their details and who voted. The only disclosed information in the election is total votes to candidates and the entire election.[22]
2. Lack of Evidence: Although privacy with anonymity can ensure safeguards against electoral fraud. There is no way to ensure that votes are being cast under the effect of bribes or any form of electoral fraud. This issue has roots from the beginning.
3. Fraud-Resistance: Each qualified voter should be able to vote precisely once, and no other persons should be able to vote. The system must verify the identity of each potential voter and determine their status but must not allow this information to become associated with their vote.[23]
4. Ease-of-Use: Elections must serve the entire public. It must be so designed that it can be used with minimal training and little technical skills.
5. Scalable: Election is a means to serve a large population. It must be flexible enough to work on a large scale also.
6. Speed: This computer-driven era must ensure that results are declared within a few hours of the election procedure ends.
7. Low Cost: Cost is one of the major for any system design. The System must be cost-efficient, having good efficiency and require the least maintenance possible.

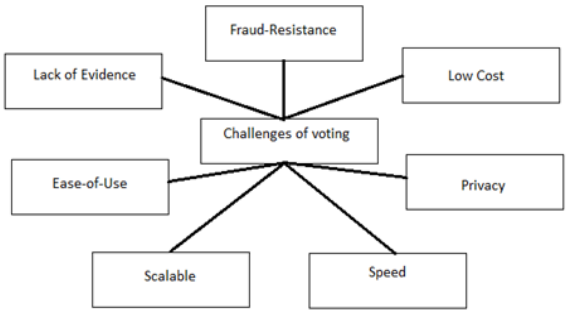

Fig. 3 challenges of e-voting system diagram

(D) Why Ethereum

Ethereum takes the lead in terms of usability, scalability, support and development and has its own set of quirks in development, security and currency; while only lacking in flexibility, which is not a problem because it is a grey area and development is not entirely focused on it. Ethereum is also backed because it uses the latest encryption technologies such as SHA 3[4], and the elliptic curve [4] is used for key generation. The programming language, solidity, used in ethereum is user friendly as it combines C++ and Javascript. Ethereum has a vast community that commits millions of transactions every week. The support provided by the community is very much

beneficial to new developers. The mode of operation in Ethereum is permission less and can work in both private and public modes, which is essential in testing.

(E)P2P Network

peer-to-peer network connection of the systems. Where one system is connected to another system using a peer-to-peer network. Blockchain is a P2P network to improve the security of e-voting. First, we design a synchronised model of voting records based on distributed ledger technology (DLT) to avoid the forgery of votes. Second, we design a user credential model based on elliptic curve cryptography to provide authentication and non-repudiation.[31]

P2P network is proposed for the essential requirements of the e-voting process. A blockchain-based e-voting system for multiple candidates has been designed on Linux platforms in the P2P network to prove and verify the scheme.

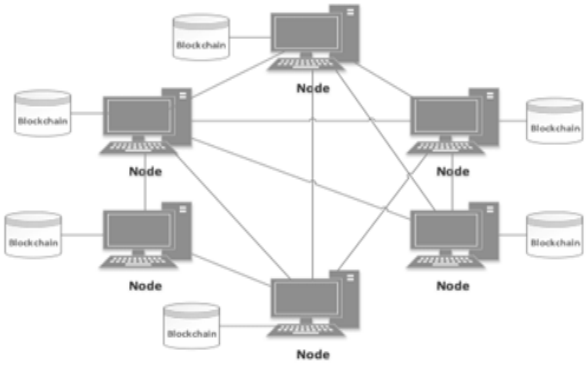

Fig. 4 Peer-to-Peer network Diagram

OVERVIEW OF METHODOLOGY

Table 1 Overview of Methodology

No.	Methodology/ Tools/ Techniques used	Define	Advantages	Disadvantages/ Limitation
1.	Solidity	Solidity is an object-oriented programming language for writing smart contracts. It is used for implementing smart contracts on various blockchain platforms, most notably, Ethereum.[31]	• including multiple level inheritance • **Application Binary Interface**	• **Transactional Operation** • **Limited expressiveness**
2.	Truffle	Truffle is a development environment, testing framework, and asset pipeline all rolled into one.[33]	• support for compiling, deploying and linking • automated contract testing	• The only "limitation" would simply be the features they may not have added yet. (means no right now)
3.	Ganache	Ganache is a personal blockchain for rapid Ethereum, and Corda distributed application development.[34]	• supporting both Ethereum and Corda technology. • graphical user interface	• grab the private key, not a public key
4.	Metamask	*MetaMask is a bridge that allows you to visit the distributed web of tomorrow in your browser today. It will enable you to run EthereumdApps right in your browser without running a full Ethereum node.[34]*	• the security level is quite good	• Still, not so easy and required good knowledge of the ETH network (metamask)
5.	Smart contracts	Smart contracts are codes of code stored on a blockchain and automatically execute when	• time-saving • safety • precision	• Data quality And mistakes

		predetermined terms and conditions are met.[38]	• Accuracy • Transparency	
6.	Hyperledger Fabric	Hyperledger Fabric is a modular blockchain framework that acts as a foundation for developing blockchain-based products, solutions, and applications using plug-and-play components aimed at private enterprises.[37]	• improvises the level of trust • very flexible and scalable • a high degree of privacy • multilateral transactions	• not a Network fault-tolerant • got minimum APIs and SDKs.
7.	Homomorphic encryption	Homomorphic encryption is a method that computes encrypted data. it uses proxy re-encryption technology to protect the selected ciphertext from being attacked.[39]	• a higher standard of data security	• incredibly slow and non-performant
8.	RabbitMQ	RabbitMQ is a messaging broker. It gives your applications a common platform to send and receive messages and your messages a safe place to live until received.	• Approximately 75% of the time, Redis takes in accepting messages. • RabbitMQ's queues are fastest when they're empty.	• RabbitMQ is probably not aware of the feature lazy queues.
9.	Linkable ring signature	A linkable ring signature allows one person in the group to sign on behalf of the group. Still, it has a tag so that an external verifier can know that a defined signer has produced the signature, but they cannot tell who the signer is.[35]	• Privacy protection	• **Signature verification is a complex process**
10.	Distributed Ledger	Distributed ledgers use independent computers (called nodes) to record, share and synchronise transactions in their respective electronic ledgers.[32]	• highly secure, transparent, immutable and tamper-proof	• Low speed in the process • Difficult to scale or to work with on a much larger scale.
11.	Biometric system	Biometrics are physical or behavioural human characteristics that can digitally identify a person to grant access to systems, devices or data.	• High security and assurance • User Experience • Non-transferrable	• **Costs** • **Data breaches** • **Tracking and data** • **False positives, bias and inaccuracy**

PROPOSED METHODOLOGY

Ensuring complete anonymity of the election process by eliminating all correlations between voters and votes without the additional storage and computational overhead of separate blockchains for voter information and vote information is required. Various existing designs for Blockchain-based e-voting systems incorporate the ability of the election administration to query the Blockchain during the election process to check if the voter ID of the current voting block already exists in the Blockchain, which introduces the possibility of inequitable misuse by accessing count of vote's information during the election. This anomaly

undermines the democratic principles and ideologies of a fair election, and thus, needs to be addressed using a better design of the blockchain implementation. Moreover, existing system designs utilise digital signatures and encryption techniques to ensure the system's reliability but do not address scalability in the design decisions. The proposed solution aims at resolving these issues in a Hyperledger Sawtooth framework implementation to ensure scalability using parallel transaction processing and using two distinct divisions in a single blockchain to ensure anonymity and fairness in the voting process.

CONCLUSIONS AND FUTURE DIRECTIONS

We proposed an approach of e-voting system using Blockchain because e-voting system has to be very secured. We were also able to remove the disadvantages of time and location constraints by allowing the users to vote from their blockchain nodes at their convenience. The entire counting process of the votes is open to all to be monitored. Thus, reducing any chances of manipulations of the votes, and the results are seen in real time. Aim to improve further the developed application for scalability problems in compliance with the generally accepted security criteria in the e-voting domain. This paper gives knowledge about different blockchain techniques, and it also provides knowledge about the work done over blockchain techniques till today.

REFERENCES

1. F.Hao, P.Y. A. Ryan, "Real-world electronic voting:" Design, analysis and, pp deployment (CRC Press,(2017)
2. F. S. Hardwick, A. Gioulis, R. N. Akram, K. Markantonakis, "E-voting with Blockchain: An e-voting protocol with decentralisation and voter privacy" International Conference on Computing and Communication Technologies. (2017)
3. Y. Liu, Q. Wang, An e-voting protocol based on Blockchain, Department of Computer Science and Engineering, Southern University of Science and Technology, Shenzhen, China(2018)
4. R. Hanifatunnisa and B. Rahardjo, "Blockchain-based e-voting recording system design," 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), Lombok, (2017).
5. Kristian Kost'al, Rastislav Bencel, Michal Ries, Ivan Kotuliak "Blockchain E-Voting Done Right: Privacy and Transparency with Public Blockchain" IEEE10th International Conference on Software Engineering and Service Science (ICSESS) (2019)
6. [6] Linh Vo-Cao-Thuy, Khoi Cao-Minh, Chuong Dang-Le-Bao, Tuan A. Nguyen “Votereum: An Ethereum-based E-voting system” IEEE RIVF International Conference on Computing and Communication Technologies (RIVF)(2019)
7. Wei-Jr Lai, Yung-chen Hsieh, Chih-Wen Hsueh, Ja-Ling Wu "DATE: A Decentralised, Anonymous, and Transparent E-voting System" IEEE International Conference on Hot Information-Centric Networking (HotICN)(2018)
8. JiazhuoLyu, Zoe L. Jiang, Xuan Wang, ZhenhaoNong, Man Ho Au, Junbin Fang "A Secure Decentralised Trustless E-Voting System Based on Smart Contract" IEEE 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering(2019)

9. K. Delmolino, M. Arnett, A. Kosiba, A. Miller, and E. Shi, "Step by step towards creating a safe, smart contract: Lessons and insights from a crypto currency lab," in International Conference on Financial Cryptography and Data Security. Springer, (2016)
10. M. Pilkington, "11 blockchain technology: principles and applications," Research Handbook on digital transformations,(2016).
11. ShitangYu, KunLu, ZhouShao, Yingcheng Gou, BoZhang"A High Performance Blockchain Platform for Intelligent Devi" IEEE International Conference on Hot Information-Centric Networking (2018).
12. Kriti Patidar, Dr Swapnil Jain "Decentralized E-Voting Portal Using Blockchain" IEEE 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)(2019)
13. NirKshetri ; Jeffrey Voas-2018 “Blockchain-Enabled E-Voting”, IEEE Software (2018)
14. Hiren M Patel, Milin M Patel, Tejas Bhatt, "Election Voting Using Blockchain Technology", International Journal of Scientific Research and Review, (2019).
15. Marathe, K. Narayanan, A. Gupta, and M. Pr, "DInEMMo: Decentralised incentivisation for enterprise marketplace models," 2018 IEEE 25th International Conference on High Performance Computing Workshops (HiPCW)(2018)
16. A. B. Kurtulmus and K. Daniel, "Trustless machine learning contracts; evaluating and exchanging machine learning models on the ether EUM blockchain," IEEE 25th International Conference on High Performance Computing Workshops (2018).
17. F. Daniel, P. Kucherbaev, C. Cappiello, B. Benatallah, and M. Allahbakhsh, “Quality control in crowd sourcing: A survey of quality attributes, assessment techniques and assurance actions,” CoRR,(2018).
18. Bin Yu, Joseph K. Liu, Amin Sakzad, Surya Nepal, Ron Steinfeld, Paul Rimba, and Man Ho Au. Platform-independent secure blockchain-based voting system. In Information Security: 21st International Conference,(2018).
19. Patrick McCorry, Siamak F Shahandashti, and FengHao. A smart contract for boardroom voting with maximum voter privacy. In International Conference on Financial Cryptography and Data Security,(2017).
20. M. Pawlak, J. Guziur, and A. Poniszewska-Mara NDA, "Voting Process with Blockchain Technology: Auditable Blockchain Voting System," Lecture Notes on Data Engineering and Communications Technologies,(2019).
21. P. McCorry, S. F. Shahandashti, and F. Hao, "A Smart Contract for Boardroom Voting with Maximum Voter Privacy," Lecture Notes in Computer Science, (2017).
22. “DAO soft fork voting on Ethpool & Ethermine”, forum.ethereum.org/discussion/7796/dao-soft-fork-voting-on-ethpoolethermine(2017)
23. Abhishek Kaudare, D Milan Hazra, Anurag Shelar, Manoj Sabnis “Implementing Electronic Voting System With Blockchain Technology” IEEE International Conference for Emerging Technology (INCET)(2020)
24. Yuxian Zhang, Yi Li, Li Fang, Ping Chen, Xinghua Dong "Privacy-protected Electronic Voting System Based on Blockchain and Trusted Execution Environment" IEEE 5th International Conference on Compute (2019)
25. R. Aroul Canessane, N.Srinivasan, Abinash Beuria, Ashwini Singh, B. Muthu Kumar” Decentralised Applications Using Ethereum Blockchain” IEEE 2019 Fifth International Conference on Science Technology

Engineering and Mathematics (ICONSTEM)(2019)

26. David Khoury, Elie F. Kfoury, Ali Kassem, HamzaHarb “Decentralized Voting Platform Based on Ethereum Blockchain" IEEE International Multidisciplinary Conference on Engineering Technology (CET). (2018)
27. Wenbin Zhang, Sheng Huang, Yuan Yuan, Yanyan Hu, Shaohua Huang, Shengjiao Cao, Anuj Chopra "A Privacy-Preserving Voting Protocol on Blockchain" IEEE 11th International Conference on Cloud Computing. (2018)
28. P. Zhang, J. White, D. C. Schmidt, and G. Lenz, "Design of Blockchain-Based Apps Using Familiar Software Patterns to Address Interoperability Challenges in Healthcare", the 24th Pattern Languages of Programming Conference, Canada, (2017).
29. M. Wohrer and U. Zdun, “Design Patterns for Smart Contracts in the Ethereum Ecosystem”, 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Canada, (2018).
30. V. Buterin, "Ethereum white paper: a next-generation smart contract & decentralised application platform," [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper, (2013).
31. Tutorials for the solidity https://www.dappuniversity.com/articles/solidity
32. Tutorials for the Blockchain https://www.dappuniversity.com/articles/blockchain-app-tutorial
33. Truffle: https://truffleframework.com
34. Ganache: https://truffleframework.com/ganach
35. E-Voting, GitHub:https://github.com/topics/e-voting
36. Ethereum project: https://ethereum.org
37. Hyperledger Fabric. www.hyperledger.org/projects/fabric Ethererum. www.ethereum.org.
38. Nodejs, [Online]. Available: https://nodejs.org/en/, 2019
39. ”What is a Digital Signature? - Definition from WhatIs.com.” Search Security. Accessed September 11, 2019. https://searchsecurity.techtarget.com/definition/digital-signature