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

Survey study on Block-chain Based E-Voting System

[1]Sonali sonavane, [2]Heramb kulkarni, [3]Himanshu Mishra, [4]shreyas Sarode, [5]Pranay Gaikwad, [6] Vyenktesh Mohite

[1]Professor, [2]Student, [3]Student, [4]Student, [5]Student, [6]Student
[1]Dept. of Comp. & IT,
[1]G. H. Raisoni Institute of Engineering & Technology, Pune, India

Abstract: The basic idea of this system is to create an Online Voting System that will help to suppress deceive of the manual voting system and also the prior versions of online voting OTP generation. We are also implementing location free voting system to the voters for whom it is not possible to come at the voting location (hometown). Here we propose a system that includes multiple layers of verification to ensure the reliability of the device which includes OTP verification with validation data. Each voter can access to the system only when being recognized and checked with the given database of enlist voters. Once the corresponding face is matched with the information provided, the voter will be allowed to proceed for choosing their preferred candidate from the panel. People can share private hyperlinks to any created poll (as long as they know the link) and people who have the link can vote and one browser can only use one vote. In terms of voter authentication, duplicate votes and non-repudiation of votes, is very weak. E-voting is being studied extensively, and many implementations are tested and even used for a while. However, very few implementations are reliable enough and are still in use. The advantages that we get while using the e-voting system would be to reduce election expenses including material, logistics and salary cost.

Index Terms **–E-Voting, OTP.**

INTRODUCTION

Elections are a crucial part of a democratic system because they allow the general population to voice their views by voting. Because of their importance to our society, ballots should be transparent and fair in order to assure participants of their legitimacy. The traditional or paper-based polling method increased people's trust in the majority voting preferences. It has contributed in the democratization of the democratic process and electoral system for electing constituencies and governments. The procedure additionally will improve the situation picking the individual that requirements to cast a ballot who will in the situation for handle the assignment for instance for the picking the pioneer in the class. As known, the Voting procedure was utilizing the tickets paper to guarantee the procedure framework. It is essential to guarantee that voter confidence does not erode. A recent research found that the traditional voting process was not entirely clean, raising various problems about justice, equality, and the people's will, all of which were not fully defined and comprehended in the system of governance. It is troublesome on the grounds that the issue which the tickets need to determine by physically computing. In physically computing, the issue that can be happen when the individual who determined the polls will miss tallying or perhaps the individual more inclination at one individual applicants. Electronic voting procedures, on the other hand, feature a single controller that controls the whole voting process. Due to the central authority's dishonesty (election commission), this methodology leads to erroneous selections, which are hard to fix using current policies and procedures. To get around the central authority, the decentralised network might be employed as a modern electronic voting approach. Blockchain is one of the technological solutions that has strong cryptographic foundations, allowing applications to take advantage of these capabilities to build security systems. A Blockchain resembles a data structure that records and distributes all transactions carried out from its inception. It is basically a distributed, decentralised database that keeps track of all germination and growing data, increasing the security of data records against illegal manipulation, tampering, and modification.

LITERATURE SURVEY

Election processes and tactics are also being influenced by advances in information technology. Researchers are striving and contributing to enhance such systems. Electronic voting is compared to traditional voting methods from several perspectives, including convenience, reduced margins of error, and speedy results [1]. The end-to-end process of registration, voting, and counting using a digital election administration platform is referred to as e-voting. Electronic voting systems strive to be as simple to use and secure as traditional voting methods while eliminating human error. Electronic voting systems may be classified into two groups. Ballots can be cast remotely as well as through closed systems in voting centers. The voters engage physically in pool site electronic voting, but the ballots are discarded and counted electronically. Remote online voting involves using a personal device to cast votes over the Internet. Voting kiosks, PCs, mobile devices are examples of various devices [2]. For more than thirty years, experts have been researching safe and practical e-voting concepts. For the first time, an anonymous communication route to encrypt the ballot in an early essay published in 1981 as Chaum. Since the 2000s, several e-voting methods have been adopted in numerous nations.

E-voting was employed in municipal and general elections in a number of nations throughout the globe. The following are a few examples: The United States of America (2000), the United Kingdom (2002), Estonia (2005), Canada (2006), and Norway (2011) [3]. Blockchain technology is basically distributed ledger data storing technology which uses hashing for encryption of data into number blocks chained and validating each other to preventing tampering to data. Because of the well-known projects in Bitcoin and Ethereum, the first things that spring to mind when thinking of blockchain are cryptocurrency and smart contracts. Bitcoin was the first cryptocurrency to employ a blockchain data structure. Ethereum introduced smart contracts, which use the power of blockchain immutability and distributed consensus to provide a crypto-currency solution equivalent to Bitcoin. Smart contracts were presented much earlier in the 1990s by Nick Szabo and are defined as "a collection of promises, specified in digital form, including protocols within which the parties fulfil on these promises." [4]. as data is stored in distributed manner and smart contracts are used to insure data integrity in bitcoin, for online voting or electronic voting, blockchain technology is introduced for providing a decentralised node, end-to-end verification, and distributed ledger [5]. The Caltech/MIT Voting Technology Project came into being in order to develop a new voting technology in order to prevent a recurrence of the problems that threatened the 2000 U. S. Presidential Elections. The report assesses the magnitude of the problems, their root causes and how technology can reduce them. They address a wide range of "What is" issues including voting procedures, voting equipment, voter registration, polling places, absentee and early voting, ballot security, cost and public finance of elections, etc. [6]. They then propose a novel "What could be" framework for voting technology (that moves away from monolithic voting structures), and propose that a process for innovation be setup. The framework is "A Modular Voting Architecture ("Frogs")" in which vote generation is performed separately from vote casting, and the "Frog" forms a permanent audit trail, the importance of which cannot be overstressed. Here, the vote generation machine can be proprietary whereas the vote casting machine must be open-source and thoroughly verified and certified for correctness and security. Finally, the report provides a set of short-term and long-term recommendations on the various issues related to voting. In "Electronic Voting", Rivets addresses some issues like the "secure platform problem" and the possibility of giving a receipt to the voter. He also provides some personal opinions on a host of issues including the striking dissimilarity between e-commerce and e-voting, the dangers of adversaries performing automated, wide-scale attacks while voting from home, the need for extreme simplicity of voting equipment, the importance of audit-trails, support for disabled voters, security problems of absentee ballots, etc [7]. The NSF Internet Voting Report addresses the feasibility of different forms of Internet voting from both the technical and social science perspectives, and defines a research agenda to pursue if Internet voting is to be viable in the future. It groups Internet voting systems into three general categories like Poll-site Internet voting: It offers the promise of greater convenience and efficiency in that voters could cast their ballots from any poll site, and the tallying process would be both fast and certain. More importantly, since election officials would control both the voting platform and the physical environment, managing the security risks of such systems is feasible [8]. Fridrik Attempt to assess the potential of distributed ledger technologies by using a case study, such as the election process and its implementation using a block-chain-based system. Framework that will improve security and lower the cost of holding national elections The Go-Ethereum Proof-of-Authority approach is being used to achieve these goals (POA) Setup of blockchain authorization. They employed the algorithm in a procedure that was based on Identity is treated as a stake, resulting in speedier transactions. They employ the terms district and boot. When an individual elector casts a vote from the district, the majority of the district nodes verify it. Any vote they agree on gets attached to the blockchain by their conforming smart contract [9]. Zhang offers a block-chain-based local voting system to aid decision-making in peer networks. It safeguards privacy and allows for detection as well a reprimand for cheating the blockchain technology employed is based on distributed consensus algorithm. Elections can be utilized as a Blockchain component of Smart Contracts and Peer to Peer transactions, two-phase validation (decryption private key, smart contract to peer network verification). The downside is that there is no guarantee that the model will function. Many haven't tried it [10]. The open vote network (OVN), the first deployment of a transparent and self-tallying internet voting system with complete user privacy utilizing Ethereum. The voting size at OVN was limited by the framework to 50–60 electors. The OVN is powerless to stop rogue miners from destroying the system. By sending an invalid vote, a fraudulent voter can get around the voting procedure. The protocol makes no guarantees about the electoral administrator's ability to withstand violence [11].

PROPOSED SYSTEM

The system was built to enable a voting application in a real-world setting, taking into consideration needs such as privacy, eligibility, convenience, receipt-free voting, and verifiability. The suggested approach strives for safe digital voting without sacrificing usability. Several requirements must be met, whether we're talking about digital or e-voting system over traditional voting system such as –

Privacy - To achieve voter confidentiality, the system makes use of the cryptographic capabilities of blockchain. More specifically, when a voter registers with the system, the blockchain generates a voter hash, which is the voter's unique identity in the blockchain and is safeguarded against misuse owing to the cryptographic hash's collision resistance characteristic. As a result, the traceability of a vote is not trivial, safeguarding the voter.

Eligibility - Only registered voters are allowed to vote, and each voter is only allowed to vote once.
To establish their eligibility, all eligible users must register using unique identifiers such as government-issued papers. In our system we have used Voter-Id card, PAN card, and Adhar card for identification and verification of user. Furthermore, our system employs OTP verification to uniquely validate voters.

Voter receipt freedom - Voters should not be able to verify to a third party that they voted a certain manner.
The proposed system allows voters to choose their preferred option and generates a cryptographic hash for each occurrence (transaction). This is necessary for verifiability, or determining if a particular vote was counted. However, having this hash does not provide you access to information about how a person voted.

Convenience -Voters must be able to vote without difficulty, and everyone who is eligible must be able to vote. The system uses a user-friendly web-based interface, and the voting process requires very little input from the user. For example user have to go through simple registration process and submit his documents.

The system is divided into two layers one for user side and one for administration side. Front-end development and user interaction. The security layer takes care of dealing with voters (to facilitate vote casting operations) and election administrators (to support election administration duties). It contains two main functions: user authentication and authorization (voters and administrators) to guarantee that system access is limited to valid users in line with present access control policies. This feature may be achieved using a variety of approaches ranging from simple username/password to more complex ones such as fingerprinting or iris recognition. As a result, these are made unique to each implementation of the suggested design. Overall, this layer is the initial point of contact for users and is in charge of confirming user credentials according to the rules.

COMPARATIVE ANALYSIS

The below table represents the analysis of various research papers. The research papers were taken in between year 2019 to 2021.We have used the various Algorithms and the Technologies like Block chain to maintain the security and Hash rate of data

Sr No.	Methodology	Advantage	Disadvantage	Accuracy
1	A Smart Contract For Boardroom Voting- The Open Vote Network (OVN) DDoS- a Byzantine fault tolerance algorithm SHA 256	Authentication Anonymity accuracy	Inability to change vote in case of user mistake	As we are unable to change vote in case of mistake so it is not that accurate at only 50%
2	DLT[]- to avoid forgery of votes hash value based on SHA-256 User credential based on ECC[Elliptic curve digital signature algorithm]	Voting ballot is marked by the voters as a signature so that no one else can find out for whom a citizen is voting.Blockchain-based e-voting system for multiple candidates has been designed on Linux platforms which solves the problem on forgery of votes during e-voting.	Size of the encrypted message. It is significantly bigger in size when compared to the most commonly used form of cryptography.	It is ECC based algorithm with generation time of 10ms and hash rate can't be calculated, so the overall speed is slow which affects accuracy of the system.
3	Hyperledger Fabric Private/local Blockchains ECC/ElGamal Shamir's Secret Sharing Cryptographic Algorithm: ECDSA	Transaction speed is 15 per scale which makes it more secure. Hash rate is 168.59 Th/s	ECDSA has high mining difficulty. Power Consumption is high.	Its generation time is upto 10ms. And can handle 3500 transaction per second but the mining difficulty is low at 55,057 so the accuracy is moderate.
4	Consensus: Mining based on PoW ElGamal encryption Security mechanism-ZK-SNARK	In this comparative study, the most consensus use in the Blockchain technology is Proof of Work (PoW) as it adopts the Ethereum.	Energy intensive. Costly and required plenty of computing power.	Generation time is upto 10ms, Hash rate is 169.59 TH/s, power consumption is moderate and no mining is required

5	Polyas- Hyperledger Fabric Private/local Blockchains	Uses AES/GCM for encryption. Main advantage is no mining is requires, power consumption is low	No built in cryptocurrency mechanism present. Need to implement own cryptocurrency Mechanism makes it complicated.	Generation time is 10 to 19ms. Transaction per second are 15, mining difficulty is high as this system is pretty accurate.

CONCLUSION

As the Blockchain is new and developing technology, it can be used in various security applications where authentication, authorization, integrity of the system comes into the picture. The purpose of this study is to review and assess existing research on blockchain-based electronic voting systems. The article addresses recent blockchain-based electronic voting research. First, the blockchain idea and its applications are discussed, followed by existing electronic voting methods. Following that, a number of flaws in existing electronic voting systems are identified. We are trying to implement am e-voting system that describes how distributed ledger is implemented in blockchain and ensuring data integrity using hashing, and securing the system using consensus algorithm.

REFERENCES

[1] Dr.Aree Ali Mohammed and Ramyar Adbolrahman Timour,Efficient E-voting Android Based System, IJARCSSE,vol.3,Issue 11,2017.

[2] A.S. Belenky and R.C. Larson, "To Queue or not to Queue?" OR/MS 27, October 2013, pp. 30-34.

[3] "An Electronic Polling Service to Support Public Awareness Using Web Technologies", Christos Bouras, Nikolaos Katris, Vassilis Triantafillou. International Journal of Computer- Aided Technologies (IJCAx) Vol.4, No.1/2, April 2017.

[4] "E-voting on Android System" paper (International Journal of Emerging Technology and Advanced Engineering) prepared by: Kirti Autade, Pallavi Ghadge, Sarika Kale, Co-authors- Prof. N. J. Kulkarni, Prof. S. S. Mujgond, February 2016.

[5] "Electronic voting," Encyclopedia of Computers and Computer History, prepared by Lorrie Faith Cranor and edited by Raul Rojas, published by Fitzroy Dearborn, 2019.

[6] "Voting – What is, what could be," Caltech/MIT Voting Technology Project (VTP) Report, July 20019.

[7] Java Cryptography an e-book by Jonathan B. Knudsen, First edition May 1998, ISBN:1-56592-402-9

[8]Chang, V.; Baudier, P.; Zhang, H.; Xu, Q.; Zhang, J.; Arami, M. How Blockchain can impact financial services–The overview,challenges and recommendations from expert interviewees. Technol. Forecast. Soc. Chang.2020,158, 120166. [CrossRef] [PubMed].

[9]Wang, B.; Sun, J.; He, Y.; Pang, D.; Lu, N. Large-scale election based on blockchain. Procedia Comput. Sci.2018,129, 234–237.[CrossRef].

[10] Ometov, A.; Bardinova, Y.; Afanasyeva, A.; Masek, P.; Zhidanov, K.; Vanurin, S.; Sayfullin, M.; Shubina, V.; Komarov, M.;Bezzateev, S. An Overview on Blockchain for Smartphones: State-of-the-Art, Consensus, Implementation, Challenges and FutureTrends. IEEE Access 2020,8, 103994–104015. [CrossRef].

[11].Tan, W.; Zhu, H.; Tan, J.; Zhao, Y.; Da Xu, L.; Guo, K. A novel service level agreement model using blockchain and smart contractfor cloud manufacturing in industry 4.0. Enterp. Inf.Syst. 2021.

[12]Wood, G. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Proj. Yellow Pap. 2014,151, 1–32.

[13]. Szabo, N. Formalizing and securing relationships on public networks. First Monday 1997,2, 9.

[14] Çabuk, U.C.; Adiguzel, E.; Karaarslan, E. A survey on feasibility and suitability of blockchain techniques for the e-voting systems.arXiv 2020, arXiv: 2002.07175.