E-voting Using Blockchain Technology: A Systematic Review

Mansi Ojha[1*], Praveen Kumar Mannepalli[2], Jay Prakash Maurya[3]

[1]M. Tech. Scholar, Department of Computer Science and Engineering, LNCT, Bhopal
[2]Associate Professor, Department of Computer Science and Engineering, LNCT, Bhopal
[3]Assistant Professor, Department of Computer Science and Engineering, LNCT, Bhopal

---

Abstract: - An significant part of web-based media is that it reexamines itself according to the desires and inclinations of its clients and, thus, it continually develops a few outcomes. The writing audited sets up a relationship between's web index control and its conceivable effect on the results of a specific field like political race. The clear force of search rankings can change the inclinations of the uncertain citizens. The web has been clarified as the new brain control component and has become the inconspicuous type of impact that can control the vast majority of the things we do and say. Blockchain based stages were at that point proposed by investigates to address the interoperability and protection issues identified with e-casting a ballot interaction with different difficulties actually remain. Specifically, adaptability, convenience, and availability as center specialized difficulties. The first technical challenge is storing the heterogeneous form of E-voting data in off-chain and provides the secure access control of the data via on-chain. The second challenge is describing ownership and share access control over data in emergency e-voting situations. Moreover, the lack of accessibility is an unsolved issue because formal verification of smart contract is huge with respect to time to process block of transactions in largescale. In order to address the above challenges, anE-voting framework through progressive temporal blockchain approach is studied. Analysis of reviewed articles provides a direction for future direction in related area.

Keywords: - E-voting, Blockchain, Privacy, Scalability, On-chain

1. INTRODUCTION

Democracy gains its value from the nature of the government it forms after the elections and the governance it offers to its people. Government and governance focus on getting the appreciation and cooperation of the people who are governed. Governments around the world are taking efforts to reform their public administration organizations and deliver more efficient and cost effective services, as well as better information and knowledge to their citizens. Every one of us aspires for a good and effective government in our country to ensure the safety and happiness of the people. It is true that the quality of a government naturally depends upon the ways and means of promoting and preserving the standard of life. A government has to use its power and authority to provide goods and services to the people to maintain the general welfare and basic needs of the common man. So governance is the knack of application of power, strategies, policies and projects with the aim of improving the quality and standard of life. The fundamental expectation of a citizen is minimum cost of living and maximum satisfaction in his everyday life. The assurance for high quality in governance proposed by the rulers during the elections is in turn checked by the voters.

Online voting system is a voting system by which any voter can exercise his/her voting rights from anywhere in the country. Various factors like technology, social issues and election administration are related to the arguments regarding internet voting. Electronic voting is capable of converting the process of voting simpler and more open for balloters. This is valid for web casting a ballot on the grounds that the voting forms can be projected from any PC with a web association. These techniques generously decline the democratic expense for some balloters by making many passageways from which they can cast a ballot. There is the likelihood to kill long lines at surveying stations and give better openness to people with inabilities, those experiencing ailment, those serving in the military or living abroad and those away on close to home travel and other people who think that its hard to distinguish the surveying station. Moreover web casting a ballot can bear the cost of the voters the important chance of having the option to cast a ballot whenever. Youngsters matured 18 to 30 are the uncommon populace of voters and web is the strategy for drawing in those citizens who are viewed as the hardest to reach.

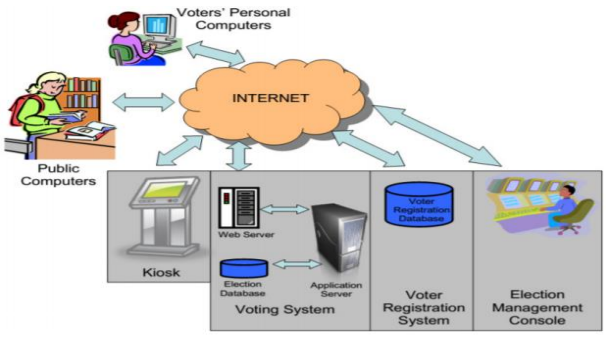

Figure 1: Basic architecture of online voting

These voters, who are generally acquainted with the innovation, are the most regular announced clients and

would probably profit the most from the augmentation of distant kinds of electronic democratic.

Most web casting a ballot action has happened in Europe with numerous nations testing some on the web or electronic voting forms. By and by, some sort of web casting a ballot is being utilized in the accompanying nations: Australia, Estonia, France and Switzerland. Norway is likewise taking an interest in on-going pilot projects. The following sections provide the detailed description of the global scenario in internet voting.

2. BLOCKCHAIN FOR E-VOTING

Blockchain is a new technology, booming in most of the industries. Blockchain was first proposed for a cryptocurrency (Nakamota, 2008). A novel element of distributed blockchain network has no central database. The blockchain information repeated over every one of the nodes in the circulated framework. The three components of the blockchain are decentralization, transparency, and immutable. All the transactions stored in the blocks. Once the block verified with peer nodes, then it is stored in the blockchain. Each block contains a list of transactions. The blocks arranged in chronological order, permission, decentralized record management system, which allows people to share the information in a trustworthy manner. It is a secure database, where it is controlled by the whole network, not by a single user. Blockchain network types are shown in table 1.

Table 1: Types of Blockchain Network

Property	Public	Private	Consortium
Management	Not Centralized	For Single Organization	For Multiple Organization
Participants	Permissionless	Permissioned	Permissioned
Centralized	No	Yes	Partial
Determination [Consensus]	For All miners	Organization participating	For Selected miner
Transaction	Long	Short	Short

Blockchain originally named from the block and chain, the list of transactions called block, which connected with the cryptography technique. Each block linked with the previous block header. Blockchain is a distributed database and managed by a peerto-peer network. It is used to store and access data. Each block contains the Block header and transactions. The block header maintains the Hash of previous block header, timestamp, nonce, and Merkle root value. The health data stored in the block cannot be changed. The primary use of blockchain is to avoid inconsistencies. Blockchain is a shared record of transactions. It empowers members in a group to share the data with the other providers without a third party involvement and monitor the transaction. Rather than store the record on a single server, it is kept up over various PCs, which makes the information incredibly difficult to play with or delete. That carefully designed qualities brand name close by a technique that ensures any information put into the blockchain is substantial and enables trust between the gathering individuals.

2.1 Properties of blockchain

The properties of blockchain are decentralization, transparent, immutable, autonomy, open-source, anonymity, and consensus.

a)Blockchain as a Data Structure:-The blockchain contains a list of the transaction and compiles as a block. The structure begins with a single block called a genesis block. As the measure of transaction increases, more blocks getting added. The previous block was linked with the current block. The chain of the block gives this type of data structure. The blockchain is ordinarily intended to be tamper-proof and irreversible.

b) Decentralized:-The decentralized peer-to-peer network; the groups of the system make it as decentralized and one of the key highlights of blockchain innovation that works splendidly. Anybody can store the asset and in the future, access the asset through the web without requiring help from the third party. Store any transaction like cryptocurrencies, documents, contracts, digital asset.etc, and in future access the transaction with the help of private key.

c) Consensus:-The Consensus is the technique in which the blockchain system can approve and trust the transactions before they add to the chain. The transaction interrupts one of the agreed rules, then that transaction will be viewed as invalid. Blockchains are deployed in an agreement based convention, which is either permissionless or permission. Public consensus implies that anybody can attempt to include transactions and participate in consensus. In Permissioned-based conventions, the nodes are to be approved and distinguished to participate in the agreement or to add transactions to the chain.

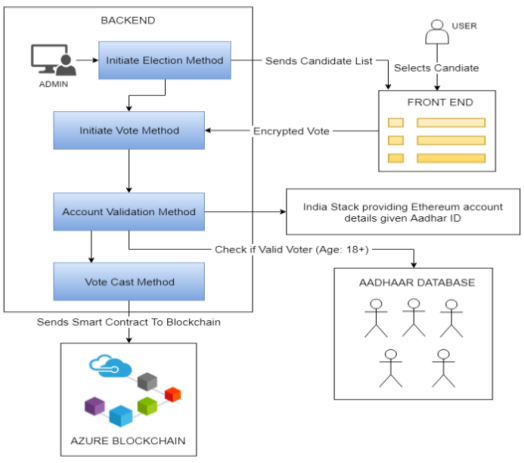

Figure 2: Framework for online voting

3. E-VOTING USING BLOCK CHAIN

Democratic is anything but an exceptional marvel even in the created nations. To improve the trust, the most un-thing that should be possible in such manner is the direction of the electronic democratic dependent on the biometric validation. This may help is taking care of half of the issues being looked by numerous nations in the constituent cycle. The e-casting ballot frameworks have been utilized by couple of nations before, for example Estonia, Ireland, and Norway, while some won't utilize it any longer to wipe out the review issues. Some facts and results have been concluded by different articles published in referenced area of e-voting using blockchain. For a good e-voting system following features must be in the suggested framework.

1. Voter's choice for a particular candidate
2. Fairness
3. Data Integrity for voters
4. Privacy/voter Anonymity
5. Robustness
6. Verifiability

This paper involves a workflow to review the articles related to the area given in figure 2.

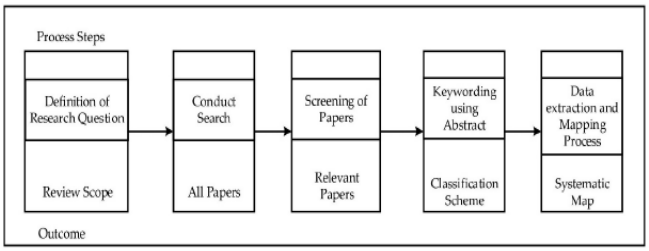

Figure 3: The Systematic Mapping Process

Research Questions that is identified on various blockchain based e-voting frameworks.

- RQ1: What are the current e-casting a ballot framework holes?
- RQ2: Can the blockchain idea improve e-casting a ballot frameworks?
- RQ3: What are the exploration themes and proposed arrangements that have been distributed in blockchain-based e-casting a ballot?
- RQ5: What are the future exploration bearings for the blockchain-based e-casting a ballot?
- RQ5: What are the future examination bearings for the blockchain-based e-casting a ballot framework?

The article search includes all publications on relevant platforms from 2010-2019 that includes keywords "Blockchain," "e-voting," "blockchain ballot" also, "blockchain casting a ballot" (Table 2). With the search.string, we distinguished articles as per the fitting measures from the streaming on the web information bases: IEEE Xplore, Arxiv, Iacr, ScienceDirect, Web of Science, Scitepress and Springer.

Table 2: Search Results

Database	Blockchain	E-voting	Ballot
Sci. Direct,	316	462	80
Arxiv.org	1178	56	7
IEEE explore	1349	290	24
Scitepress.org	57	100	5
Webofscience.com	4299	740	26
Springer.com	510	2123	2126

Relevant to our research questioners and systematic mapping process the articles trends are shown in figure 3.

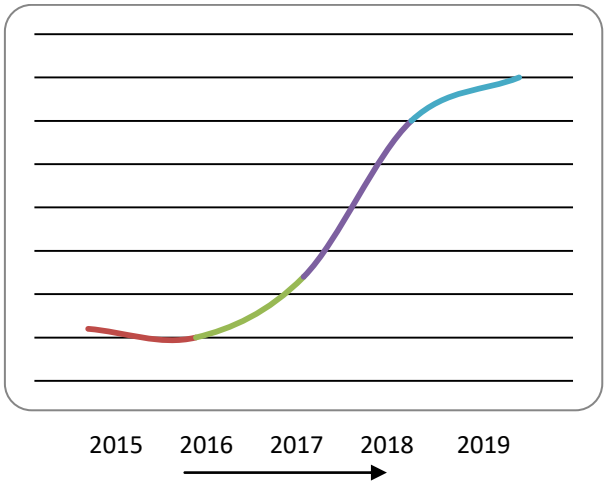

Figure 4: Year wise growth in ralted article on e-voting

The research article summary matrix based on blockchain parameter are identified as given in table 3

Table 3 Article Summary matrix

Type of blockchain	**Count**
General	11
Coin-based	4
Privacy	4
Integrity	5
Consensus	1

4. FACTS OF LITERATURE REVIEWED

Y. Stein et al. [1], has presented a model from the canton of Valais Switzerland in March 2011, where the postal democratic structures were not gotten by the residents and when the democratic structures were re-given, it was perceived that the vote of the impacted voters had quite recently been casted a polling form. Regardless of the way that Switzerland, has an e-projecting a voting form structure yet it really allows her voters to project a polling form either electronically or by post or by genuinely going to the studying station. The e-projecting a polling form system similarly needs more noteworthy

security, insurance, and straightforwardness to transform into an absolutely trustworthy plan of projecting a polling form.

B. Shehzad et al. [2], has referenced that there were discussions in the appointment of understudy's association decisions held in Austria in 2009. The sacred court of Austria considered this political decision invalid as the discretionary council was not directed and the cycle of vote and elector confirmation was discovered to be underneath the security principles.The AES keys in any case, must be made sure about and applied adequately to recuperate the encoded substance. This makes the exchange chomped increasingly slow force of electronic democratic and blockchain is undermined. To beat this test, the private blockchain is recommended.

J. Al-Muhtadi et al. [3], has communicated that the Irish government used evoting machines in 2017 general races and it was being expected to use them in 2004 EU choices. These machine were bought to a detriment of e55 million. During the audit it was tracked down that the machines are not strong and its outcome can't be trusted firmly as there were issues with the paper trail and the affirmation system. The Irish government thusly has picked to scrap the machines while this movement has cost e55 million to the Irish residents. For the relative reasons, Germany and the Netherlands have moreover decided to forever blacklist the vote based machines at political votes.

M. I. U. Laliet al. [4], give an understanding about the utilization and weaknesses of the electronic democratic machines (EVM's) both as far as programming, equipment and other related difficulties. Parshad has talked about a few occurrences where the failing of one or the other equipment or programming was accounted for a while now and again it was likewise seen that the EVM's is being used for the Election Day had altered equipment and additionally programming in expectation. It was likewise revealed that the couple of US researchers having a place with University of Michigan (tentatively) could intercede into the Indian races and could play with the numbers.

A. M. Abdullatifet al. [5], has introduced the idea of giving three polling forms to the citizen where elector will project all the voting form papers subsequent to checking. Each voting form paper contains a one of a kind identifier yet the elector stays unknown as the keys are unscrambled. At the hour of classification, the votes projected are connected and the decision found on two polling form papers is picked while the decision with one polling form paper is dismissed. The plan may not be adequately utilized if there are just two candidates or if there are number of competitors. The plan additionally has the disservice of being moderate and the human mistake increment if the votes are not precisely poled in the individual boxes.

D. Basinet al. [6], presents a business arrangement that manages a token put together framework work with respect to the blockchain innovation and in this manner guarantee the secrecy and security of the democratic framework. The arrangement is more reasonable for I-casting a ballot where the physical and biometric confirmation of the elector isn't used. The token based framework, nonetheless, limits the relevance of this democratic stage to be utilized successfully in wide ran, full fledge races where the force of the arrangement looks bargained to address the difficulties. The blockchain produced with the end goal of the electronic democratic can either be kept public or hidden. In the public blockchain, notwithstanding, the substance of the exchanges stays obvious to everyone in the blockchain. It is accordingly imperative to encode the substance of the squares by utilizing some safe calculations, for example AES to keep the substance of the square ambiguous and scrambled.

M. Pilkingtonet al. [7], has demonstrated a few worries for utilizing the blockchain for the electronic democratic. The e-casting a ballot framework requests that a blockchain is responsive and adaptable at untouched to get productive reaction to form the general outcomes. In such manner the square size must be of satisfactory size. At present, the bitcoinblockchain covers 100's of gigabytes of capacity which makes the expansion of squares and data recovery very moderate.

G. Gabisonet al. [8], is of the view that in blockchain based electronic democratic frameworks the clients make the changes dependent on the addresses and not on their personality and in the event that if there is a data spillage, the clients can produce a few locations. It is extreme for the blockchain system to guarantee value-based security since the data, everything being equal, and public keys are obvious to public. It has introduced a technique to connect client's nom de plumes the IP address of the client in any event, when the clients are behind a firewall or even behind the organization address interpretation which can help in coming to the cause of an exchange.

5. CONCLUSION & FUTURE WORK

E-voting differs immensely on worldwide. A few nations have state-supported services, and few privatized, some half and half, and still others have limited access to the mind. These varieties show the complexity of E-voting when conveyed to a large population. Security is a significant problem in E-voting service. Keeping the primary information protected and secured in the blockchain. More than 176 million E-voting records were breached, between the range of 2009 and 2017. The companies trust the distributed ledger technologies (DLTs) are the only solutions to the E-voting service information problems. Since blockchain can be used as a convention or interoperability layer, it may be useful in

helping disparate systems converse with each other. The following companies are utilizing the blockchain to help change E-voting data management. The blockchain holds enormous potential to improve and increase the value to the E-voting system, and few companies have begun testing it for E-voting.

Block;-A block is permanent data storage. Block in the blockchain is made up of block header and an arranged in approved transactions and hash pointer to the previous block. In the framework will Ethereum blockchain used for securing the E-voting records. In the decentralized network, the nodes connected with a peer-to-peer network protocol. The Smart Contract runs on the Ethereum Virtual Machine (EVM), which acts as a runtime environment. The main aim is to develop an algorithm to encourage the e-voting for the public. The module displays the classes' entity and graphical representation of voter's turn out with minimal classification error which encourages adapting the e-voting systems. The main objective will to reduce the classification error and to minimize the retrieval process in comparison with an available data set. This system helps to minimize misclassification error pruning. The secure framework will design through Progressive temporal blockchain, which enhances the security of the E-voting record. The research work focused on data integrity, authentication, confidentiality, auditability, and privacy towards achieving users' trust and acceptance of E-voting systems. The permissioned blockchain decentralized network management system which allows people to share the information in a trustworthy manner with the temporal properties.

REFERENECS

[1] Y. Stein and H. Primo, ‘‘Programmable data encryption engine for advanced encryption standard algorithm,’’ U.S. Patent 7 508 937 B2, 2009. Accessed: Aug. 1, 2018.

[2] B. Shehzad, K. M. Awan, M. I.-U. Lali, and W. Aslam, ‘‘Identification of patterns in failure of software projects,’’ J. Inf. Sci. Eng., vol. 33, no. 6, pp. 1465–1480, 2017.

[3] J. Al-Muhtadi, B. Shahzad, K. Saleem, W. Jameel, and M. A. Orgun, ‘‘Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment,’’ Health Informat. J., Apr. 2017.

[4] M. I. U. Lali, R. U. Mustafa, K. Saleem, M. S. Nawaz, T. Zia, and B. Shahzad, ‘‘Finding healthcare issues with search engine queries and social network data,’’ Int. J. Semantic Web Inf. Syst., vol. 13, no. 1, pp. 48–62, 2017.

[5] A. M. Abdullatif, B. Shahzad, and A. Hussain, ‘‘Evolution of social media in scientific research: A case of technology and healthcare professionals in Saudi Universities,’’ J. Med. Imag. Health Inform, vol. 7, no. 6, pp. 1461– 1468, 2017.

[6] D. Basin, H. Gersbach, A. Mamageishvili, L. Schmid, and O. Tejada, ‘‘Election security and economics: It's all about eve,’’ in Proc. Int. Joint Conf. Electron. Voting, 2017, pp. 1–28.

[7] M. Pilkington, ‘‘11 Blockchain technology: Principles and applications,’’ in Research Handbook on Digital Transformations. 2016, p. 225.

[8] G. Gabison, ‘‘Policy considerations for the blockchain technology public and private applications,’’ SMU Sci. Tech. Rev., vol. 19, p. 327, Sep. 2016.

[9] K. Saleem, A. Derhab, J. Al-Muhtadi, and B. Shahzad, ‘‘Humanoriented design of secure machine-to-machine communication system for e-healthcare society,’’ Comput. Hum. Behav., vol. 51, pp. 977–985, Oct. 2015.

[10] K. Saleem, A. Derhab, J. Al-Muhtadi, B. Shahzad, and M. A. Orgun, ‘‘Secure transfer of environmental data to enhance human decision accuracy,’’ Comput. Hum. Behav., vol. 51, pp. 632–639, Oct. 2015.

[11] B. Shahzad, E. Alwagait, S. Alim, and I. Resaercher, ‘‘Investigating the relationship between social media usage and students grades in Saudi Arabia: A mixed method approach,’’ in Proc. Recent Adv. Elect. Eng. Educ. Technol., 2015, pp. 211–214.

[12] B. Shahzad, ‘‘Identification of risk factors in large scale software projects: A quantitative study,’’ Int. J. Knowl. Soc. Res., vol. 5, no. 1, pp. 1–11, 2014.

[13] A. B. Shahzad and A. Said, ‘‘Application of quantitative research methods in identifying software project factors,’’ Int. J. Inf. Technol. Elect. Eng., vol. 1, no. 1, pp. 30–33, 2012.

[14] M. Volkamer, O. Spycher, and E. Dubuis, ‘‘Measures to establish trust in Internet voting,’’ in Proc. 5th Int. Conf. Theory Pract. Electron. Governance, 2011, pp. 1–6.

[15] S. Wolchok et al., ‘‘Security analysis of India's electronic voting machines,’’ in Proc. 17th ACM Conf. Comput. Commun. Secur., 2010, pp. 1–14.