Trustworthy Electronic Voting Using Adjusted Blockchain Technology

Ms. Amala CR[1], Mr. Dinesh Kumar [2], Mr. Akarsh CR[3]
[1]Dept of CSE
[2]Assistant Professor
[3]Dept of EEE
[1, 2, 3]CMS College of Engineering and Technology

Abstract- *This paper suggests a framework by using effective hashing techniques to ensure the security of the data. The concept of block creation and block sealing is introduced in this paper. The introduction of a block sealing concept helps in making the blockchain adjustable to meet the need of the polling process. The use of consortium blockchain is suggested, which ensures that the blockchain is owned by a governing body (e.g., election commission), and no unauthorized access can be made from outside. The framework proposed in this paper discusses the effectiveness of the polling process, hashing algorithms' utility, block creation and sealing, data accumulation, and result declaration by using the adjustable blockchain method. This paper claims to apprehend the security and data management challenges in blockchain and provides an improved manifestation of the electronic voting process.*

Keywords- Blockchain voting, e-voting, Electronic voting.

I. INTRODUCTION

Over the years, 'vote' has emerged as a tool for representing the will of the people when a selection is to be made among the available choices. The voting tool has helped improving the trust of people over the selection they make by a vote of majority. This has certainly helped in democratization of the voting process and the value of voting system to elect the parliaments and governments. In 2018, there are 167 countries out of little over 200 who have some kind of democracy; full, flawed, or hybrid etc. Since the trust of people is increasing in democracies it is important that they don't lose their trust on vote and voting system. By virtue of the emerging trust on the democratic institutions, the voting system emerged as a platform to help people to elect their representatives, who consequently form the governments. The power of representation empowers the people with a trust that the government shall take care of the national security, national issues like health and education policies, international relations and taxation for the benefit of the people.

In order to make the voting process more effective the institutions like 'Election Commission' came into existence in different parliamentary democracies. The institutions, along with setting up the process and legislation for conducting the elections, formed the voting districts, electoral process, and the balloting systems to help in conduct of transparent, free and fair elections. The concept of secret voting was introduced since the beginning of the voting system. Since the trust on democratic systems is increasing it is important to uphold that the trust on voting should not decrease. In therecent past there have been several examples where it was noted that the voting process was not completely hygienic and faced several issues including transparency, fairness and the will of people was not observed to be effectively quantified and translated in terms of formation of the governments.

II. PROPOSED SYSTEM

The voters name must exist in the voting list to enable himself to visit the polling station for the purpose of voting. It is the responsibility of the voter himself to ensure that once he attained the age of eighteen years, his name should be present in the voting list. This can be done by consulting the respective offices. Eg. National Database and Registration Authority (NADRA) in Pakistan. The voting lists are published few weeks earlier than the elections. The individual having his name in the voting list is eligible to vote and presents his original identity to the polling staff. Before casting the vote, the voter has to be authenticated by the biometric system. The record of the voter is checked with the help of NADRA's Database. Once the voter has passed the authentications check, he is brought to voting screen to vote. From the voting machine the names and the respective party symbols of each candidate are displayed and the voter can vote according to his will. The confirmation screen seeks the confirmation of the voter and records the vote casted by the voter. The voter can vote only once, and once the vote is casted in voting record is marked "as voted", which restrict the voters from voting again. The name of the voter can be blocked or eliminated from the list of eligible voters list for

the current elections, once he has casted the vote. The polling process continues until the voting time ends or all the voters in the voting list have casted their votes.

III. MODULES

A. POLLING PROCESS

The electronic voting system is executed in a way that it deploys many individuals at different levels. In order to develop an effective block creation system, it is important to understand the actual execution on ground. In the conduct of the elections, the election commission and the NADRA (National Database and Registration Authority) have a big role to play. NADRA is the national registration authority in Pakistan and is responsible for the registration and issuance of identity documents to the citizens of Pakistan. The NADRA is responsible to ensure that each citizen of the country has its record available and the biometrics of each individual are also available

The biometric authentication is used in the voter's authentication on the polling day. The election commission is responsible for making theelectoral lists available which are verifiable from the base records. The authenticated voters can vote according to the provision provided to them and the usage of technology is made to get the vote recorded and tabulated accordingly. It is also the responsibility of the election commission to declare the results when polling station wise and constituency wise tabulation has been made.
The casting of vote is a procedural step that includes the following.

a) The voters name must exist in the voting list to enable himself to visit the polling station For the purpose of voting. It is the responsibility of the voter himself to ensure that once he attained the age of eighteen years, his name should be present in the voting list. This can be done by consulting the respective offices, e.g. National Database and Registration Authority (NADRA) in Pakistan. The voting lists are published few weeks earlier than the elections. The individual having his name in the voting list is eligible to vote and presents his original identity to the polling staff. Before casting the vote, the voter has to be authenticated by the biometric system. The record of the voter is checked with the help of NADRA's database.
b) Once the voter has passed the authentications check, he is brought to voting screen to vote. From the voting machine the names and respective party symbols of each candidate are displayedand the voter can vote according to his will. The confirmation screen seeks the confirmation of the voter and records the vote casted by the voter.
c) The voter can vote only once, and once the vote is casted is voting record is marked as ''voted'', which restricts the voters from voting again. The name of the voter can be blocked or eliminated from the list of eligible voters list for the current elections, once he has casted thevote.
d) The polling process continues until the voting time ends or all the voters in the voting list have casted their votes. The results of the polling station are declared and the votes attained by each candidate are listed.
e) The process is repeated for all the polling stations in the constituency and the collective result of all the polling stations forms the result for that specific constituency. Likewise, the results for all the constituencies are collected to form the results of the national election.

B. BLOCKCHAIN

Blockchain has three different types, i.e. public blockchain, private blockchain, and consortium blockchain. Bitcoin and Ethereum are the examples of public blockchain, anyone and from anywhere can join them and can get relieved at the time of his will. This is proofed by the complex mathematical functions. The private blockchain is the internal-public ledger of the company and the joining on that blockchain is granted by the company owning that blockchain. The block construction and mining speed is far better in the private blockchain as compared to public blockchain due to the limited nodes. The consortium blockchain however exists among the companies or group of companies and instead of the consensus the principles of memberships are designated to govern the blockchain transactions more effectively. This research uses consortium blockchain as the blockchain is to be governed by a national authority in the country.

C. HASHING

Hashing is the process of changing the arbitrary and variable size input to a fixed size output. There are different functions that perform hashing of different level. MD5 algorithm is widely used for hashing purposes and it provides a 128 nit or 32 symbols long hash value. MD5 is the latest algorithm in the series while before that Md2, Md3, and Md4 also existed [40]. The algorithm was designed to be used as a cryptographic hashing algorithm but it faces some problems that reduce the production of unique hash value and hence it faces some vulnerabilities. Race Integrity Primitive Evaluation Message Digest (RIPEMD) is a family of hash function developed by Hans Dobbertin in 1996. This algorithm was designed to replace the MD5 as a more secure alternative. It has few variations that have emerged over time including

RIPEMD-128, RIPEMD-160, RIPEMD256, and RIPEMD-320 SHA (Secure Hashing Algorithm) is another cryptographic hash function that yields 160 bit hash value consisting of 40 hexadecimal characters. The algorithm could not resist the collusion attacks against it and its usage has declined after 2005. In this time several new algorithms have also been proposed, including SHA 3, and SHA 256. The SHA 2set of algorithms is designed by the US's Nation

Security Agency. SHA 256 and SHA 512 are new hash functions that do not have collusion problems and deemed secure otherwise, at least as yet. Keccak is a family of algorithms designed by designed by Guido Bertoni, Joan Daemen, Michaël Peeters. The flexibility of the algorithm, in contrast to its other counterparts, is that it accepts any length of input and yields an arbitrary length of output, while all other algorithms produce a fixed length output.

D. PROOFS

In Proof of work deals with the mining/creation of the blocks in such a way that it can be proved that a significant effort has been made for the resolution of the mathematical problem introduced for the creation of a block in theblock chain. The mathematical complexity is increased on the creation of every new block so make the creation of the block complex and a rewarding scenario. The increasing complexity is introduced with the help of the hash functions, and the nonce value. In Proof of Stake revolves around the identification of the stakes in the blockchain. The holders of assets are subject to have more priority in the creation of the blocks. The likelihood of that only few creators of the blocks may control the entire blockchain by virtue of the assets that they have, can't be ignored. The holders of assets are subject to have more priority in the creation of the blocks. The likelihood of that only few creators of the blocks may control the entire blockchain by virtue of the assets that they have, can't be ignored. This concept is applicable in the consortium blockchain or the private blockchain where the holding companies may need an administrative access to the blockchain. Proof of Burn n deals with the burning of the coins that are gained over a period of time. This burning process works as a fuel for the creation of new blocks. This proof of burn concept ensures that the individuals don't become powerful enough by increasing their stakes in the network. The burn process is recorded by sending the coins / proof of work to an arbitrary address, that may be designated by the network itself.

IV. CONCLUSION

Mistrust in the voting is not an uncommon phenomenon even in the developed countries. The electronic voting, however, has emerged as an alternative but still not being practiced at a large scale. The electronic voting is anticipated to have a great future yet the past is not that glorious. In some countries e-voting is not an option while few are in a process to eliminate the security, verifiability, and anonymity concerns. There are issues that require immensely deep con- sideration by the legislatures, technologist, civil society, and the people. This research has proposed a framework based on the adjustable blockchain that can apprehend the problems in the polling process, selection of the suitable hash algorithm, selection of adjustments in the blockchain, process of voting data management, and the security and authentication of the voting process. The power of blockchain has been used adjustably to fit into the dynamics of the electronic voting process.

REFERENCES

[1] 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

[2] N.Y aser, N. Mahsud, and I. A. Chaudhry, ''Effects of exposure to electronic media political content on voters' voting behavior,'' Berkeley J. Soc. Sci., vol. 1, no.4,pp.1–22,2011.

[3] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, ''Consortium blockchain for secure energy trading in industrial Internet of Things,'' IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3690– 3700, Aug. 2018.

[4] Y. Zhang, R. Deng, X. Liu, and D. Zheng, ''Outsourcing service fair payment based on blockchain and its applications in cloud computing,'' IEEE Trans. Services Comput., to be published.

[5] Alonso, M. Gasco10, D. Y. M. del Blanco, J. A. H. Alonso, J. Barrat, and H. A. Moreton,''E-voting system evaluation based on the council of Europe recommendations: Helios voting,'' IEEE Trans. Emerg. Topics Comput., Nov. 2018. doi:10.1109/TETC.2018.2881891.

[6] Y. Zhang, R. H. Deng, J. Shu, K. Yang, and D. Zheng, ''TKSE: Trust- worthy keyword search over encrypted data with two-side verifiability via blockchain,'' IEEE Access, vol. 6, pp. 31077– 31087, 2018.

[7] B. Shahzad, ''Quantification of productivity of the brands on social media with respect to their responsiveness,'' IEEE Access, vol. 7, no. 1, pp 9531–9539, Jan. 2019