SECURE E-VOTING USING ADJUSTED BLOCKCHAIN TECHNOLOGY

S.A.Abrar Ahamed[1],S.Arun Karthik[2],M.Ismail Mathar[3],B.A.Prasanth[4],Dr.A.Jainul Fathima[5].

[1,2,3,4]UG Students, Department Of Information Technology, Francis Xavier Engineering College, Tirunelveli.

[5]Assistant Professor,Department Of Information Technology, Francis Xavier Engineering College, Tirunelveli.

ABSTRACT: Electronic voting refers to voting that involves the use of electronic devices to help or take care of the casting and counting of ballots. Which may also require the transfer of ballots and votes over the phone, private computing networks, or the Internet. In this paper, we suggest that blockchains have the potential to solve two of the most pressing voting issues today: ballot access and voter fraud. In this paper, a framework for E-voting system is proposed by implementing effective hashing technique. Also, blockchain concept is incorporated to achieve blocksealing concept for secure E-voting system. This paper also conclude with future work that can be incorporated to improving the system.

Keywords: Blockchain Technology; Cryptographic Algorithm; Network Security.

1. INTRODUCTION

The Electronic Voting System is used as a replacement for the paper-based voting system. Though it is a technological advancement, it has security and privacy faults. This project implements the Security in the Voting System using effective hashing techniques. The Blockchain concept is introduced in this project. The implementation of a block sealing algorithm assists in adjusting the blockchain during the polling process. The Election Commission owns the block chain and blocks unauthorized access. The framework suggested in this project deliberates the secure polling process, Implementation of the hashing algorithm, Block Chaining concept, data storage, and result declaration is finalized using the adjustable blockchain algorithm. Hence, this project can be a replacement for the E-voting system which overcomes the security and privacy flaws using adjusted blockchain technology. The

power of blockchain has been used adjustably to fit into the dynamics of the electronic voting process.In the recent past there have been several examples where it was noted that the voting process was not completely hygienic and faced several issues including transparency and fairness, and the will of people was not observed to be effectively quantified and translated in terms of formation of the governments. Such examples can be vastly found in countries like Nigeria, India, Brazil, Pakistan, and Bangladesh. Since all these countries are among the emerging democracies, it is pretty likely that in next decades they will emerge as full democracies and the vote and the voting process will earn more respect and trust over time. The disadvantages of such mistrusts are multi-fold and they include but not limited to the following national problems:

1. Political instability

2. Compromised writ of the government

3. Mistrust over the electoral process

4. Compromised governance

5. Disorder in the state institution

6. Chain of command to run state affairs

7. Economic instability

1.1 BLOCKCHAIN

Satoshi Nakamoto first suggested the idea of blockchain in 2008. Blockchain is an electronic database that requires database transmission to still be decentralized and explicit. With disseminated accounts, all exchange information (released in hubs) is packed and added to various squares., empowering checks to be utilized middle people. All the hubs at that point structure a blockchain with timestamps. The information put away in each square can be confirmed all the while and become inalterable once entered. The entire procedure is available to the general population, straightforward, and secure. The rise of Ethereum Smart Contracts in 2013 helped blockchain innovation, which became blockchain 2.0. As introduced in blockchain 1.0 was chiefly embraced by Bitcoin to tackle issues concerning digital forms of money and decentralized installments. Blockchain 2.0 concentrated on decentralizing the whole market and is utilized to change resources through savvy contracts, along these lines making an incentive through the rise of options to Bitcoin

Enter your text below:

CodingJavaScript

Generate   Clear All   ☐ Treat each line as a separate string

SHA256 Hash of your string:

7269FF2EF7399C036CD704AC9768AEFE1213DE8676A80F4E83AFCF2A35C9169E

Fig 1 Hashing

Blockchain infrastructure shapes the central framework behind the modern currency scheme. A walkthrough of the Bitcoin technology's basic building blocks is listed below. Blockchain is fundamentally a Blocks chain. Blocks are hashed using the SHA256 hashing algorithm to extract the data associated with the signature. The cost of repairing the corrupted blockchain as defined in the above step is very high. And from the beginning block to the last one we have to go to patch the chain. When the Chain becomes high, it is costly process. In the case of Distributed Blockchain, where many peers are active in the transaction and hold the Blockchain replica, it is much more difficult to restore the blocks The value of restoring the exploited blockchain as discussed in above step is really high. And from the starting block to the other one we have to go to patch the chain. When the chain becomes wide it is costly process. In the case of Distributed Blockchain, where many Peers join in the process and retain the Blockchain replica, restoring the blocks is much more costly This Project presents the idea of block forming and block sealing The implementation of a block sealing principle aims to allow the block chain flexible to satisfy the polling phase criteria. Through time, electronic voting arose as a substitution for Project based polling to reduce redundancies and in coherences. The empirical analysis provided over the past two decades shows that owing to the protection and privacy witnessed over time, it has not been as effective. This Project proposes a structure for using appropriate hazing methods to enhance security and privacy.

Therefore, creating such an electronic program

Hash Function	Hash Length	Secure
Md5	128 bit (32 symbols)	No
Ripemd 1	160 bit (40 symbols)	Yes
SHA1	160 bit (40 symbols)	No
SHA256	256 bit (64 symbols)	Yes
SHA3	256 bit (64 symbols)	No
Keccak-256	256 bit (64 symbols)	Yes

would take these options off, as several votes will be gained by this method and as these accidents arise. To boost data stability and efficiency in e-schemes, votes are processed in the block chain.

1.2 SECURE HASH ALGORITHM 256

The Secure Hash Algorithm 256 (SHA 256) is one of the most secure methods of protecting digital data. SHA 256 is a math algorithm that takes any data and produces a 256-bit (64-character) random sequence of letters and numbers (hash). A hash is a mathematical programming method that converts data into letters and numbers of a predetermined length. Since hashes are normally simpler and easier to locate, they are used to speed up the storage and retrieval of data. Hashes also rendered data unreadable, allowing the original data to be kept private. Forexample,ad3e58f21b94f32dcadca6b71df4c31a1 8179f38011551a17a80d0ff065d22c5 can be hashed and equals: ad3e58f21b94f32dcadca6b71df4c31a18179f38011

551a17a80d0ff065d22c5. The hash will be totally different if I capitalised the "b" in bitcoin, as in "I like Bitcoin":

Table 1 Why SHA-256 is secured

d988ca30eaa88c0410ad6e48a5297c0d505dcee572f 9884f1a6fa2cbc8dedc86.

The number of possible letter and number combinations provided by SHA 256 is greater than the number of grains of sand on Earth! It's almost impossible to guess the data contained inside the hash because of this. Since hashes cannot be reversed, they are often used in computer security.

Fig 2 SHA-256

2. EXISTING SYSTEM

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 the recent past there have been several examples

where it was noted that the voting process was not completely hygienic and faced several issues including transparency and fairness, and the will of people was not observed to be effectively quantified and translated in terms of formation of the governments. Since all these countries are among the emerging democracies, it is pretty likely that in next decades they will emerge as full democracies and the vote and the voting process will earn more respect and trust over time.

3. PROPOSED SYSTEM

- In this project addresses the usefulness of the polling procedure, utilizing the dynamic block chain approach to hash the utility of algorithms, block formation and sealing, data collection, and outcome declaration.

- This project seeks to explain the complexities of network security and data processing, and offers an improved description of the online voting process.
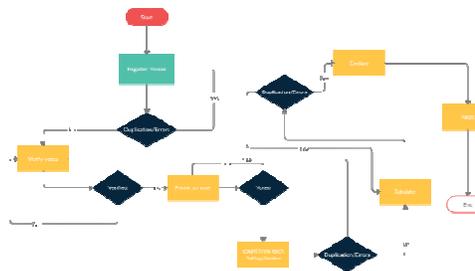

Fig 3 Entire E-Voting System

4. Conclusion

Suspicion in the voting is not an uncommon occurrence 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 expected 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 consideration by the legislatures, technologist, civil society, and the people. This project 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] Volkamer, M. Spycher, O. and Dubuis, E. (2011) 'Measures to establish trust in Internet voting', in Proc. 5th Int. Conf. Theory Pract. Electron. Governance, pp. 1–6.

[2] Bélanger , É. and Nadeau, R. (2005) 'Political trust and the vote in multiparty elections: The Canadian case,' Eur. J. Political Res., vol. 44, no. 1, pp. 121–146.

[3] Kunioka, T. and Woller, G. M. (1999) 'In (a) democracy we trust: Social and economic determinants of support for democratic procedures in Central and Eastern Europe,' J. Socio-Econ., vol. 28, no. 5, pp. 577–596.

[4] van der Meer, T. (2010) 'In what we trust? A multi-level study into trust in parliament as an evaluation of state characteristics,' Int. Rev. Administ. Sci., vol. 76, no. 3, pp. 517–536.

[5] Bevelander, P. and Pendakur, R. (2008) 'Electoral participation as a measuresocialinclusionfornatives,immigrantsanddescendantsinSweden,'Tech. Rep.,p. 33.

[6] Wolchok, S. (2010) 'Security analysis of India's electronic voting machines,' in Proc. 17th ACM Conf. Comput. Commun. Secur., pp. 1–14.

[7] Rivest,(2006) R. L. ''The threeballot voting system,'' Tech. Rep., p. 15.

[8] Pilkington, M.(2016)'11 Blockchain technology: Principles and applications,' in Research Handbook on Digital Transformations. 2016, p. 225.

[9] Gabison,G. (2016) 'Policy considerations for the blockchain technology public and private applications,' SMU Sci. Tech. Rev., vol. 19, p. 327.

[10] Stein, Y. and Primo, H. (2009) 'Programmable data encryption engine for advanced encryption standard algorithm,' U.S. Patent 7508937 B2,

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

[12] Abdullatif, A. M. Shahzad, B. and Hussain, A. (2017)'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.

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

[14] Al-Muhtadi, J. Shahzad, B. Saleem, K. Jameel, W. and Orgun, M. A.(2017)'Cybersecurityandprivacyissuesforsociallyintegratedmobilehealthcare applications operating in a multi-cloud environment,' Health Informat. J.

[15] Shahzad, B. Alwagait, E. Alim, S. and Resaercher, I. (2015)'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., pp. 211–214.

[16] Abbasi et al. R. A. (2018)'Saving lives using social media: Analysis of the role of Twitter for personal blood donation requests and dissemination,'Telematics Inform., vol. 35, no. 4, pp. 892–912.

[17] Alwagait, E. Shahzad, B. and Alim, S. (2015)'Impact of social media usage on students academic performance in Saudi Arabia,' *Comput. Hum. Behav.*, vol. 51, pp. 1092–1097, Oct. 2015.

[18] Shahzad, B. and Alwagait, E. (2014)'Does a change in weekend days have an impact on social networking activity?' *J. UCS*, vol. 20, no. 15, pp. 2068–2079.

[19] Zheng, Z. Xie, S. Dai, H.-N. Chen, X. and Wang, H.(2018) 'Blockchain challenges and

opportunities: A survey,' *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375.

[20] Johnson, D. Menezes, A. and Vanstone, S. (2001) 'The elliptic curve digital signature algorithm (ECDSA),' *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 36–63.