International Journal of Future Generation Communication and Networking
Vol. 13, No. 3, (2020), pp. 3130–3135

Survey on E-Voting System Using Visual Cryptography & Block Chain

Ashwini S Solankar
PG Student, Department of Computer Engineering
JSPM's Rajashri Shahu College of Engineering
shinde17ashwini@gmail.com

Abstract

Voting is process were collective decision is done for a place of authority. Decades back, this process was paper based were individual person would secretly vote on paper and put the closed paper in ballot, then collective votes were counted for majority. Drawbacks faced by this process were waste of paper and was expensive. Earlier the voting process was applied through internet, claiming it as E-voting. E-Voting process must maintain data integrity and protection from manipulations of vote casted. To obtain this aim, we are proposing a method which is used in election process. Herein a voter is assigned with each node, one image is distributed in two sub-images which are generated as private key and public key. Thus, using Visual Cryptography for verification. Then nodes wait their turn to create the block, all information is stored in these blocks after verification. Thus, Security and data Integrity is maintained for casted vote with help of Visual Cryptography and Block chain Technology.

Keywords: *Security and Protection, Visual Cryptography, Internet Voting System, Voter Password, Visual secret sharing.*

1. Introduction

With digitization in millennial years, electronic voting systems have been used in many countries for their general elections as well. In 2005, Estonia become the first country to have general public election nationwide through e-voting. The same was adapted by various European countries like Switzerland and Norway. A major issue faced for these elections was maintain its spree with traditional ballot system to give voter with privacy of vote and maintain integrity of vote after casted. The main challenge was that the vote must not be tampered and changed under any influence. However, this technique was not able to provide with total animosity and many agencies were able to identify and intercept the casted. Blockchain is secure and safe way for same system to make more reliable and trustworthy.

2. Literature Survey

Innovation in digital technology has helped new millennial generation with many new things. Traditional Use of Paper for electoral process is changed with advent of digital technology. More conventional method through technology is implemented. But as the change is implemented more threat towards security and data integrity of casted vote is considered in this conventional method which is done when Offline. The system which can allow decentralize system to come together with entire database which is owned by many users as well maintain data integrity for system can be embraced by Block chain technology as one of the solutions.[1]

ISSN: 2233-7857 IJFGCN

Amongst the young tech savvy generation there is lack of casting vote, this E-voting is a perfect solution for same-voting Block-Chain technology is one of the solutions for e-voting to become more transparent and open. Block Chain technology can be used in various fields but now Block chain technology is not in in its full potential.[2]
Since 1970's electronic voting is used as it gives benefits over the use of paper-based system in accuracy and reduced errors. With advent of block chain technologies, major initiatives are taken to check the feasibility of same in use of e-voting. The proposed approach is used with Multi-chain and in-depth evaluation of approach [3].

3. Related Work

[1] Online payments can be sent from one person to another person with the use of electronic cash or digital currency. In this transaction interference of any bank portal or financial institution is negligible, this is done with help of Digital Signature. But this Digital Signature can be used more then once which allows lost of a trusted third party and problem of double spending arises. The work proposed is a solution to the double-spending problem wherein the network is used where node to node transaction are timestamped by hashing and thus chain of transaction is hash based to form a record. This record is proof of work and termed as Blockchain. Blockchain also included sequence of events as proof of work which comes from largest pool of computing. Thus, to undo theses record becomes difficult to attacker. Peer to peer network with record of transaction and sequence of events in hash form create suitable Blockchain which prevents double spending issue for digital currency thus making transaction fast and trustworthy with less interference of financial institute.

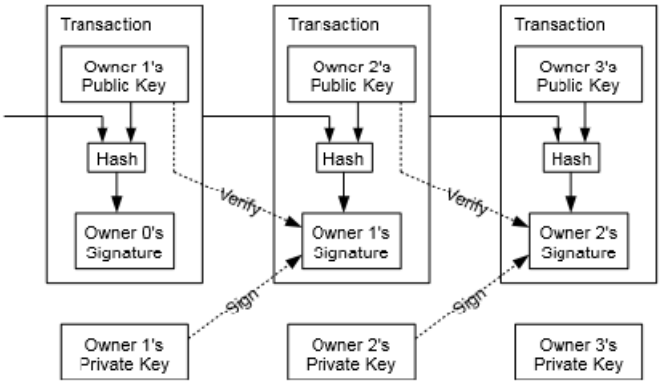

Figure1.Peer To Peer Network with Record Of Transaction

[2] The security of documents in this digital world has become new paradigm. Digital documents cover large number of paper work such as Digital signature, legal papers regarding property, will of person, etc. The authors have considered security of these legal documents through smart contracts. Smart contracts are documents with terms of agreement written in lines of code by entities involved in transaction. The contract is being executed and controlled by lines of code present in it and through network. Smart contract involves four basic things a) Terminology in which they are defined. b) Automation it involves c) Execution of agreement decided upon d) Semantics. Semantic framework is basic foundation for smart contracts, there operational and automatic aspects work side to semantics.

ISSN: 2233-7857 IJFGCN

Templates formed for smart contracts identify the further work and common standard code used for same. Blockchain form secure transit to timestamp and mark the transaction on legal level.

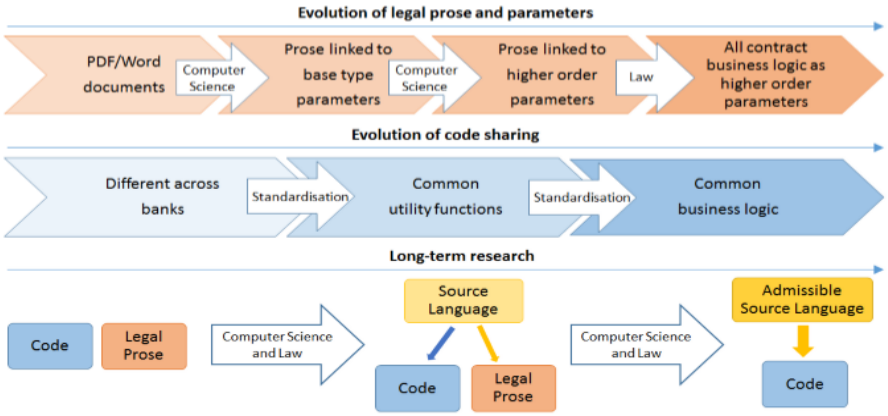

Figure 2.Evolution Of Legal Prose And Parameters

[3] Estonia was the first country to use e-voting for general elections through internet in 2005. In this system every citizen of country was provided with ID card with digital signature which holds their authentication as well as public key for security. Card was provided with remote e-voting and advance voting system wherein the citizen was able to re-vote till he finalized his vote. The system gained popularity as well as trust by giving privacy to the voters. Below figure shows the casting of vote for e-voting with pubic key and private key.

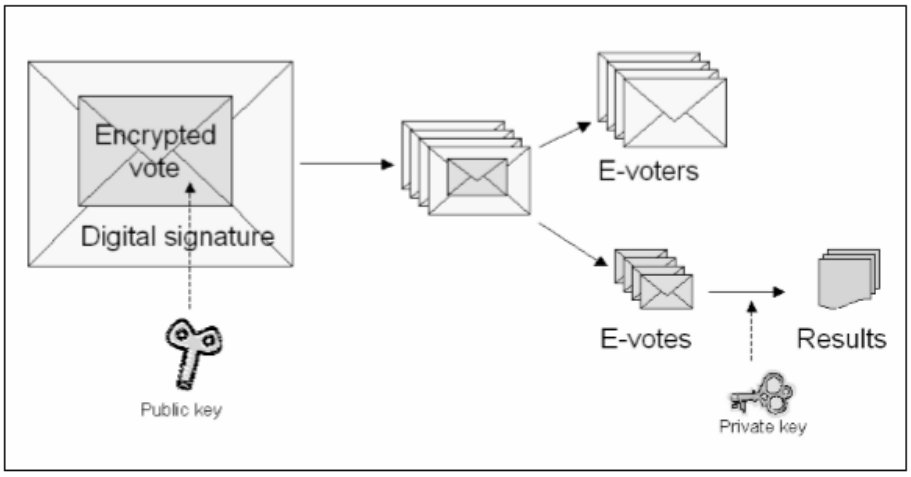

Figure 3.Casting Of Vote For E-voting With Their Keys

[4] The Internet of Things have many devices connected to each other over internet. These devices communicate with each other to give information regarding physical values or some analytics about surrounding. Machine to machine communication where two or more machines share values and information to establish a log for analysation and monitoring is represented as M2M. The logs established should identify the machine as well keep the information accurate and maintain security and privacy. This privacy maintaining issue over reputation over decentralized system is termed as M2M-REP (Machine to Machine Reputation) which keeps the log of global reputation and feedback in encrypted form.

ISSN: 2233-7857 IJFGCN

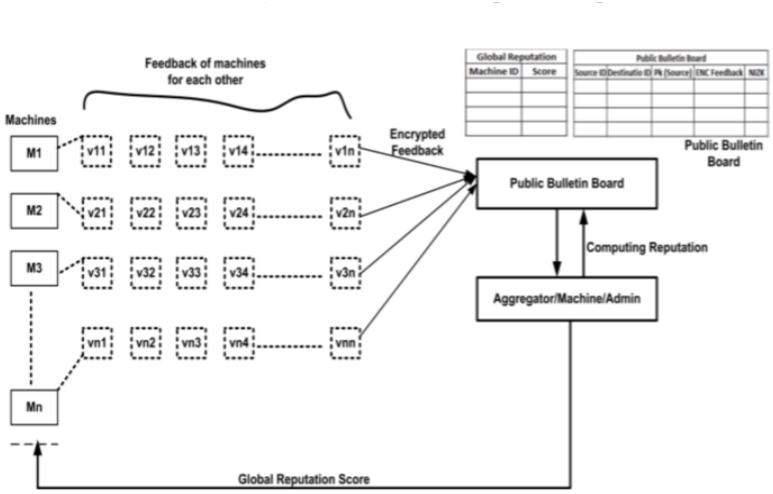

Figure 4. Machine To Machine Reputation

4. Conclusion And Future Work

The survey has been done through the way where Blockchain is used for online transaction, maintaining smart contracts and blockchains use in M2M-REP for machine to machine communication. Considering the security provided by blockchain, consideration of same for voting system is approach for this system where same security and integrity has to be maintained, Internet based voting become reliable and ensures more participation with help of blockchain. This is obtained through low cost and integrity for each vote is assured. The proposed system uses visual cryptography to provide mutual authentication for voters and election servers, Blockchain technology serves for data integrity and security.

5. Acknowledgments

I am deeply grateful to my project guide Prof. S. B. Javheri for his guidance in the field of Network Security.

6. References

1. Ahmed Ben Ayed, “A Conceptual Secure Block Chain-Based Electronic Voting System”,2017 IEEE International Journal of network &Its Applications(IJNSA),03 May 2017.[1]
2. RifaHanifatunnisa, Budi Rahardjo, “Block-chain Based E-Voting Recording System Design”,IEEE 2017.[2]
3. Kejiao Li, HuiLi,HanxuHou, KedanLi,Yongle Chen, “Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Block-chain”, 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems.[3]
4. Ali KaanKoç, EmreYavuz, Umut Can Cabuk, GokhanDalkilic, “Towards Secure E-Voting Using EthereumBlockchain”,2018 IEEE.[4]
5. Supriya Thakur Aras, VrushaliKulkarni, “Block-chain and Its Applications – A Detailed Survey”, International Journal of Computer Applications (0975 – 8887) Volume 180 – No.3, December 2017.[5]

ISSN: 2233-7857 IJFGCN

6. Freya Sheer Hardwick, ApostolosGioulis, Raja NaeemAkram,KonstantinosMarkantonakis, "E-Voting with Block-chain: An E-Voting Protocolwith Decentralisation and Voter Privacy",IEEE 2018,03 July 2018.[6]
7. KashifMehboob Khan, JunaidArshad, Muhammad Mubashir Khan," Secure Digital Voting System based on Block-chainTechnology",IEEE 2017.[7]
8. Huaiqing Wang, Kun Chen and DongmingXu. 2016. A maturity model for block-chain adoption. Financial Innovation, Springer, Open Access, DOI 10.1186/s40854-016-0031-z[8]
9. Buterin, Vitalik. 2015, On Public and Private Block-chains. [Online]https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/[9]
10. Zyskindet. al. 2015. Decentralizing Privacy: Using Block chain to Protect Personal Data, 2015 IEEE Securityand Privacy Workshops (SPW), San Jose, CA, USA, July 2015 [Online].Available: http://dx.doi.org/10.1109/SPW.2015 JianliangMeng, JunweiZhang,Haoquan Zhao, "Overview of the Speech Recognition Technology", 2012 Fourth International Conference on Computational and Information Sciences.[10]
11. Carlo Blundo, University of Salerno, Alfredo De Santis and Douglas R Stinson (1998), "On the contrast in visual cryptography scheme"pp. 1-28 [11]
12. Thomas Monoth, BabuAnto P (2009), "Achieving optimal Contrast in Visual Cryptography schemes without pixel expansion". International Journal of Recent Trends in Engineering, Vol 1, No 1, pp. 468-471. [12]
13. A B Rajendra and H S Sheshadri (2012), Study on Visual Secret Sharing Schemes Using Biometric Authentication Techniques, AJCST, Vol 1, pp.157-160. [13]
14. Anusha MN and Srinivas B K (2012), "Remote Voting System for Corporate Companies using Visual Cryptography," vol. 2, pp. 250–251. [14]
15. Pallavi V Chavan, Mohammad Atique, and Anjali R Mahajan, (2011) "An Intelligent System for Secured Authentication using Hierarchical Visual Cryptography-Review", ACCE Int J. on Network Security, vol. 02, No. 04.pp. 7-9 [15]
16. RajendraBasavegowda, SheshadriSeenappa(2013) "Electronic Medical Report Security Using Visual Secret Sharing Scheme", IEEE UKSim 15th International Conference on Computer Modeling and Simulation Proceedings, pp, 78-83 [16]
17. Hussein Khalid Abd-alrazzq1, Mohammad S. Ibrahim2 and Omar Abdurrahman Dawood (2012), "Secure Internet Voting System based on Public Key Kerberos", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, pp. 428-434. [17]
18. AdhikariAvishek and Bimol Roy (2007) "Applications of Partially Balanced Incomplete Block Designs in Developing (2, n) Visual Cryptographic Schemes". IEICE Trans. Fundamentals, Vol.E90–A, No.5 ,pp. 949-951 [18]
19. Marek R. Ogiela, UrszulaOgiela(2009) "Linguistic Cryptographic Threshold Schemes", International Journal of Future Generation Communication and Networking.Vol.2, No.1,pp. 33-40 [19]
20. Carlo Blundo, University of Salerno, Alfredo De Santis and Douglas R Stinson (1998), "On the contrast in visual cryptography scheme".pp. 1-28 [20]
21. Thomas Monoth, BabuAnto P (2009), "Achieving optimal Contrast in Visual Cryptography schemes without pixel expansion". International Journal of Recent Trends in Engineering, Vol 1, No 1, pp. 468-471. [21]
22. A B Rajendra and H S Sheshadri (2012), Study on Visual Secret Sharing Schemes Using Biometric Authentication Techniques, AJCST, Vol 1, pp.157-160. [22]
23. Anusha MN and Srinivas B K (2012), "Remote Voting System for Corporate Companies using Visual Cryptography," vol. 2, pp. 250–251. [23]

ISSN: 2233-7857 IJFGCN

24. Pallavi V Chavan, Mohammad Atique, and Anjali R Mahajan, (2011) "An Intelligent System for Secured Authentication using Hierarchical Visual Cryptography-Review", ACCE Int J. on Network Security, vol. 02, No. 04.pp. 7-9 [24]
25. 2014 "Electronic Medical Report Security Using Visual Secret Sharing Scheme", IEEE UKSim 15th International Conference on Computer Modeling and Simulation Proceedings, pp, 78-83 [25]

ISSN: 2233-7857 IJFGCN