International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 4 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT1195424

Design and Implementation a Smart E-Voting Model : Decentralization Using Blockchain

Shantanu Bindewari[1], Prof. Jayesh Surana[2]

[1]M. Tech Scholar, Information Security, Shri Vaishnav Vidhyapeeth Vishwavidyalaya, Indore, Madhya Pradesh, India

[2]Assistant Professor, Information Security, Shri Vaishnav Vidhyapeeth Vishwavidyalaya, Indore, Madhya Pradesh, India

ABSTRACT

The transparency of the block-chain allows more auditing and considerate of elections. These attributes are particular of the necessities of a voting system. These features derive from decentralized network, and can bring additional democratic processes to elections, particularly to direct election systems. For e-voting to develop further open, transparent, and independently auditable, a possible resolution would be base it on blockchain technology. In this research work to proposed technique for voting system using blockchain. The blockchain will be publicly provable and distributed in a method that no one will be intelligent to corrupt it. In this research work proposed a blockchain-based model with Consensus Protocol and SHA256 hash algorithm related with the priorities of the ballot-privacy, verifiability, suitability, extensiveness, uniqueness, sturdiness, and coercion- resistance.

Keywords: Blockchain, Smart Contracts, Voting, Privacy.

I. INTRODUCTION

Numerous start-up corporations have recently begun to promote Internet voting systems, but with a novel twist – using a blockchain as the container for voted ballots conveyed over the Internet from the voter's private device. Blockchains are a moderately innovative system category a diminutive akin to a distributed database. Proponents of blockchain voting promote it as ainnovatoryinvention providing strong security guarantees that permit truly secure online elections. Internet voting has been deliberate by computer security researchers for over twenty years. Cyber security experts generally agree that no technology, with blockchains, can sufficiently secure an online public election. Elections have distinctive security and privacy requirements essentially dissimilar from and much added stringent than those in other applications, such as e-commerce. They are exclusively vulnerable because anyone on Earth can attack them, and a successful cyberattack strength go completely undetected, subsequent in the wrong people elected with no evidence that anything was amiss. There are numerous foundational computer security problems that necessity be solved earlier we can safely behaviour elections online, and we are not close to resolving any of them.

The use of Existing blockchains does not even address these problems. Here are just a few: through the existing approach No reliable voter identification: There is no proper way to understand exact vote remotely with the internet. Completely known and proposed approaches have grave weaknesses, and

Existing blockchains do not address the problem at all. Malware: There are lots of possibility that the voter's device is infected by virus or counterfeit app. It may lead to alteration in votes before they even conveyed. It is also possible that it might silently dispose the ballot or will send the voter's name and vote selections to a third party. It may result in pressure, revenge, vote buying and selling or pre counting of votes. Existing Blockchains cannot able to detect malware. Denial of service attacks: A server can be overwhelmed with fake traffic from a botnet so that actual ballots cannot get through. Blockchains as planned for elections usage multiple redundant servers, but they proposal no extra protection in contradiction of denial of service attacks beyond what is possible with a conventional system having the similar aggregate message capacity. Penetration attacks: No servers, counting blockchain servers, are protected to remote penetration and secret takeover by resolute sophisticated attackers. Online voting systems, counting blockchain systems, do not permit for the kind of true, voter-verified paper ballot backup that is essential for a meaningful recount, audit, or statistical spot check. Thus, the greatest powerful and common-sense tools we have for protection in contradiction of cyberattack are unavailable. This research paper is containing a block chain-based model with consensus protocol and SHA256 hash algorithm integrated with preferences of ballot privacy, verifiability, suitability, extensiveness, robustness and especial. The main of this system is to maintain reliability in election process and ensure privacy of voters. Second part of this paper explores the integrity issue in section. The third section of paper provide an outline of proposed methodology and forth part of paper discuss the block chain technology that is used in storing record ballots.it also help in understanding the morality and privacy of system. Lastly paper contain concluding remarks.

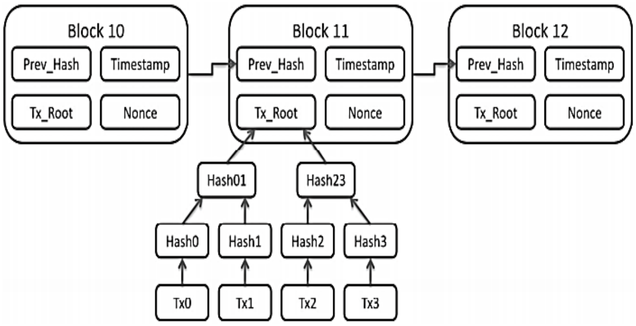


Figure 1: An example of Blockchain [6].

II. RELATED WORK

McCorry, P. et al [1] In this research, they have attainable smart agreement application that focuses on open vote network and work on Ethereum. The official Ethereum requires to test with forty stimulated voters before starting implementation procedures. Cost incurred approx. $0.73 per voter in optimistically use on the smallest setup for elections in the application. This voting protocol helps in preventing higher cost as it ensures maximum voters privacy and easily verifiable. It is prime implementation of decentralised internet voting on block chain.

Saveen A. et al [2]in this article author discuss possible application domains and the basic characteristics of block chain technology. The main focuses on the application inside SUP manufacturing business. It also constructs a hypothetical vision for planning manufacturing supply chain for the block chain. It also contains the detail information from manufacturing to recycling for the production of cardboard boxes and the part of supply chain.

Springall, D., et al [4] proposed that there are certain architectural limitation and procedural gaps that endanger the authenticity of elections in I voting system. It also gives validate information about attackers and their procedure for attacking election servers, agents that makes changes in election results or damage the legitimacy of election system. It includes various finding that define the practical barriers arises in internet voting in contemporary world. It describes the concept by various example from Estonia and other countries and impact of adopting such system and security research country.

Guy Zyskind et al [5] It is connected with banking, ecommerce services and other online services. It is important to ensure the authenticity of result which make voting services extremely difficult.it require to check precise detail to get unbiased results and therefore require very strong ballot. As designer require certain exchange it is important to create trustable central server for counting of votes. Therefore, it is important to make complete procedural control over the process to reduce risk. Even after the control the problem is still resolved. The risk of bias voting is expanding due to increase in propagation of state sponsored attacks in election procedures.

III. PROPOSED METHODOLOGY

Nowadays large portion of society do not trust their government [1]. Election is one of the most important events in modern way of democracy. The main problem with today's voting system is that the ballot can easily manipulated by people. Nowadays people are power hungry and therefore there are lots of possibility in current voting system that it can be bias [2]. The system proposed in this paper ensure that the election should execute with more security and remove any kind of trust issue occur regarding the system. It uses various technology that provides guarantee features such as transparency, security, and auditability in the block chain for ensuring transparency and security in voting process. It uses client server architecture for building trust in voting process. It ensures the accomplishment of privacy for voters

The consensus algorithm used in two kind proof based and vote based consensus algorithm that emphasis on survey in Block chain. It has two nodes the former node focuses to provide the detail proof in order to get right in adding work and generating rewards. Whereas the latter nodes help in conversation through message in order to make a deal that revolve around the block or transactions that further added to ledger. We similarly make evaluations amongst these two types based on particular of their highlighted characteristics, which explains the advantages and drawbacks of each category. It could be detected that moreover the original public Blockchain with proof-based consent algorithms, the afresh developed consortium and private Blockchain has considerable potential with vote-based ones at this time. The smart system of building is considerably less as associated to the cost of running a ballot-based system. There are considerable social benefits to expending the system as well such an easier and quicker voting process which will lead to advanced voter turnout. This system can be applied for a larger number of countries as the internet diffusion in the world increases. We might certainly see a future where each country has implemented a system similar to ours. Despite being a novel technology, a few organizations and start-ups have already started investigating with blockchain voting. This section will deliberate dissimilar implementations for blockchain voting systems that have been proposed and use those to originate to an outcome around the best, greatest realistic implementation method. Proposed smart model based on our fusion based algorithm complete eight design thoughts when generating their system:

Step 1. Persons strength check that their vote was calculated (but cannot see their neighbour's vote)

Step 2. The scheme should not permit coerce voting

Step 3. The system must whichever produce or hide temporary consequences, as desired

Step 4. The system necessity permit for voter abstinence

Step 5. Not each voter has access to the internet

Step 6. Merely citizens can vote

Step 7. The greatest practical system needs the smallest amount of behaviour alliteration for voters

The proposed algorithm is made of three elements-

- Voters (Vi),
- RA (Registration Authority),
- EA (Election Authority) and

Fusion (Consensus Protocol and SHA256 hash algorithm) Address Pool. Voters (VOTi): There should be a set of list of voters. Each voter is called as VI. Candidate (Ci): The candidates must be a set of list. For each candidate to vote can be defined as Ci. Registration Authority (RA): The voters must sign up as a register in the present voting system at first. The voter must except their public keys (PKi) and Fusion (Consensus Protocol and SHA256 hash algorithm) into this system and the scheme transfer it to the database. For the RA, it delivers the candidate (Ci) to the voters. Election Authority (EA): The election authority is accountable for adding the votes. The EA has its individual Fusion (Consensus Protocol and SHA256 hash algorithm). When the voting has been finished, the EA should start including the votes and transfer the consequence to the voting system. Fusion (Consensus Protocol and SHA256 hash algorithm) Address Pool: The Fusion (Consensus Protocol and SHA256 hash algorithm) address pool is a list of completely fusion algorithm addresses produced from the EA system randomly by using ECC algorithm. The private key SKAi of every address will store into the EA system. Public supervision: To construct this smart model, particular of the content must be public and be supervised under anybody as the open-audit part. Anyone can check its extensiveness and validity. Completely public keys of the voter PK, the EA's Fusion (Consensus Protocol and SHA256 hash algorithm) address AEA and the sets of (σ, sha256(σ)) should be public finished the inner API of the system deprived of any permission. The current ballot system is presented to have huge number of issues which can lead to widespread political unrest in a country. It is vital for a democracy to have apparent voting system that necessity have the least quantity of problems for a voter to vote. The proposed system not only handles voter privacy and auditability but correspondingly provides a transparent system for verification of the election. The proposed system is publicised to be extremely cost effective as compared to other countries and can be implemented with existing infrastructure owned by a nation. Keeping completely these factors in mind the proposed system is a complete solution that contents completely the necessities requested by the client. Our implemented system, block chain-based Vote, delivers a secure and private-voting system that is similarly effort Lesly accessible. Block chain-based Vote is a dummy scale voting system that utilizes smart contracts in SHA256 Encryption to accomplish our goals. Our system also permits for dissimilar types of ballots: users have the freedom to produce polls or elections as well as have the option to select who can vote on their ballot. SHA256delivers voter privacy on completely our ballots by encrypting each vote, fusion tallying, and revealing the vote count using Paillier cryptosystem decryption process. To preserve data integrity, completely ballot and voting data is publicly accessible as part of the smart contracts or blockchain in our system. Congruent to the objectives of smart cities, this application of a block chain-based voting system

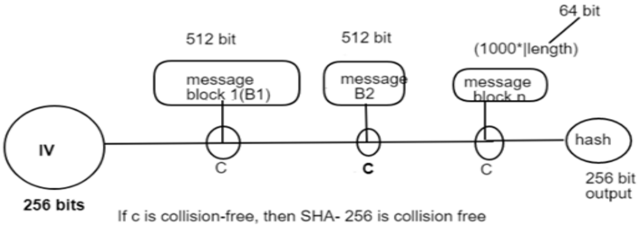


Figure 2: SHA256 hash algorithm

```
Proposed algorithm, Pseudo Code
Input
Input hashing
Plain Data = "input the plan data";
Read the data using the function of WL("Raw data: {0}", plainData);
Hashed Data =      Calculate Sha256Hash(plainData);
WL("Hash {0}", hashed Data);
WL(ComputeSha256Hash("input the plan data")
Applying the function for reading the line using RL ();
Compute Sha256Hash(rawData)
Compute the Using (SHA256 sha256Hash = SHA256. Create())
Bytes        =        sha256Hash.ComputeHash (Encoding.UTF8.GetBytes(rawData));
Applying the loop
for (inti = 0; i<bytes.Length; i++)
applying the for appending the string (bytes[i].ToString("x2"));
return returning  the stringing
```

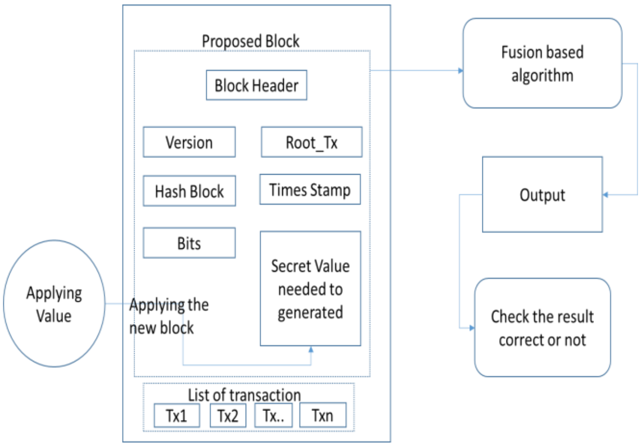


Figure 4: Proposed frame format

It has proposed a proof-based consensus that contain different variant which are basically made of two major variants PoW, PoS and their hybrid form.

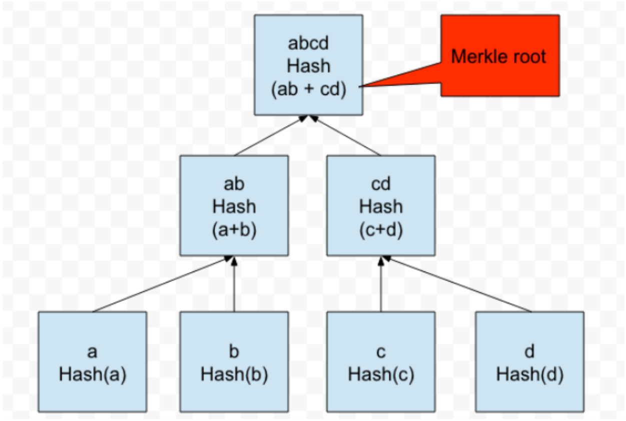
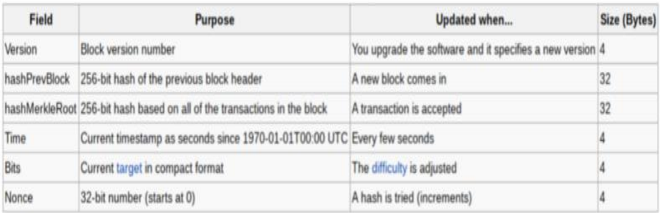


Figure 5 : Hash algorithm calculation

Basically the concept is that from various nodes joining the network the nod which perform adequate proof will be adjoin to new block in the chain and receive advantage in proof-based consensus algorithm.



Field	Purpose	Updated when...	Size (Bytes)
Version	Block version number	You upgrade the software and it specifies a new version	4
hashPrevBlock	256-bit hash of the previous block header	A new block comes in	32
hashMerkleRoot	256-bit hash based on all of the transactions in the block	A transaction is accepted	32
Time	Current timestamp as seconds since 1970-01-01T00:00 UTC	Every few seconds	4
Bits	Current target in compact format	The difficulty is adjusted	4
Nonce	32-bit number (starts at 0)	A hash is tried (increments)	4

Table 1: frame format chart

IV.CONCLUSION

This research paper aims at exploring the basic perspective about e-voting and block chain by determining fusion address algorithm and OP RETURN. Later various phrases are planned in the block chain protocol. It contain detail discussion over the definition and process of separate phrases. It labelled the transitional software development viewpoint in the same way as it label smart model development process. It contain block chain transaction process and detail analysis of contrivance of the voting system. In the end it contain the estimation about the performance and possible security risk in the protocol. The main benefit of smart model is that it help in ensuring the authenticity of electronic voting by broadcasting each ballot in the block chain from the time voting starts.

V. REFERENCES

[1]. McCorry, P., Shahandashti, S. F., &Hao, F. (2017). A Smart Contract for Boardroom Voting

with Maximum Voter Privacy. Lecture Notes in Computer Science, 357–375.doi:10.1007/978-3-319-70972-7_20.

[2]. Saveen A. Abeyratne ,Radmehr P. Monfared2(2016) .Blockchain Ready Manufacturing Supply Chain Using Distributed LedgerIJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308.

[3]. S. Bogart and K. Rice,(2015) "The Blockchain Report: Welcome to the Internet of Value," 2015. October 21, 2015.

[4]. Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., &Halderman, J. A. (2014). Security Analysis of the Estonian Internet Voting System. Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security - CCS '14. doi:10.1145/2660267.2660315.

[5]. Guy Zyskind, Oz Nathan, Alex Pentland" Enigma: Decentralized Computation Platform with Guaranteed Privacy" Submitted on 10 Jun 2015.

[6]. Bitcoin Stack Exchange, "Can someone explain how the Bitcoin Blockchain works?," 2017 [Online]. Available: https://bitcoin.stackexchange.com/questions/12427/can-someone-explain-how-thebitcoinblockchain-works.

[7]. Atzori, M. (2015). Blockchain technology and decentralized governance: Is the state still necessary? Buterin, V. (2015). On public and private blockchains. Ethereum Blog, 7. Buterin, V. et al. (2013).

[8]. Ethereum white paper. Ernest, A. K. (2014). The key to unlocking the black box: Why the world needs a transparent voting dac.

[9]. Dorri, A., Kanhere, S. S., Jurdak, R., and Gauravaram, P. (2017). Blockchain for iot security and privacy: The case study of a smart home. In Pervasive ComputingandCommunicationsWorkshops(PerCom Workshops), 2017 IEEE International Conference on, pages 618–623. IEEE.

[10]. Kappos, G., Yousaf, H., Maller, M., and Meiklejohn, S. (2018). An empirical analysis of anonymity in zcash. arXiv preprint arXiv:1805.03180.

[11]. R. Anane, R. Freeland, and G. Theodoropoulos, "E-voting requirements and implementation," in The 9th IEEE CEC/EEE 2007. IEEE, 2007, pp. 382–392.

[12]. T. Moura and A. Gomes, "Blockchain voting and its effects on election transparency and voter confidence," in Proceedings of the 18th Annual International Conference on Digital Government Research, ser. dg.o '17. New York, NY, USA: ACM, 2017, pp. 574–575. [Online]. Available: http://doi.acm.org/10.1145/3085228.3085263.

[13]. A. B. Ayed, "A conceptual secure blockchain-based electronic voting system," International Journal of Network Security & Its Applications, vol. 9, no. 3, 2017.

Cite this article as :

Shantanu bindewari, Prof.Jayesh Surana, "Design and Implementation a Smart E-Voting Model : Decentralization Using Blockchain", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 4, pp. 109-114, July-August 2019. Available at doi : https://doi.org/10.32628/CSEIT1195424
Journal URL : http://ijsrcseit.com/CSEIT1195424