International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 01 | Jan 2019 www.irjet.net p-ISSN: 2395-0072

E-VOTING SYSTEM USING BLOCKCHAIN

Dr. Prasath N[1], Joshwa Daniel Raj P[2], Kabesh K[3], Karthikeyan M[4]

[1]Associate Professor, Dept. of Computer Science and Engineering, KPRIET, Tamilnadu, India
[2,3,4]Student, Dept. of computer science and Engineering, KPRIET, Tamilnadu, India

---

Abstract - In our social life the internet which plays a major role. Internet has been a rich ground for innovation and creativity. Distributed ledger technologies is an exciting technological advancement in the information technology world. Cryptocurrency and its underlying technologies has been gaining popularity for transaction management. Transaction information is maintained in the blockchain, which can be used to audit the integrity of the transaction. The block chain technology is presented instead of many of the existing and emerging technologies/services so, a decentralized architecture such as blockchain can be used to run and support a casting a ballot plot that is open, reasonable, and free. In this paper, we propose the block chain which acts as a ballot box in the potential new e-voting protocol. This design to the system has been designed to obey the fundamental e-voting properties and it offer a degree of decentralization and allow the voter to update his/her vote.

Key Words: E-voting, blockchain, SHA, blockchain safety.

1. INTRODUCTION

For last several years many of the government having the interest on e-voting systems. This interest, however, has been followed closely by alert this security issues. While some methods for creating transparent voting system protocols have been proposed, these methods are both costly and have not been implemented on a large scale. As more of a population uses the Internet regularly, electronic and remote voting becomes an incentive for greater participation in democracy The computer security field has for a decade studied the possibilities of electronic voting systems, with the goal of minimizing the cost of having a national election, while fulfilling and increasing the security conditions of an election. Replacing the traditional pen and paper scheme with a new election system is critical to limit fraud and having the voting process traceable and verifiable.

In this work we discuss criteria of electronic voting, and how blockchain may be used as a transparent, cost- effective method to manage and verify transactions in large-scale voting. Where the system Monitor and verify the transaction. The section gives background into the underlying technologies that will be used in the proposed electronic voting system.

2. E-VOTING

Electronic voting system or e-voting uses electronic means to either aid or take care of casting and counting votes have been studied in both the commercial and the academic world.

All together for an e-voting a ballot system to be regarded secure certain formally-expressed properties must hold.

• Fairness:

No early results should be obtainable before the finish of the casting a ballot procedure; this gives the affirmation that the rest of the voters won't be influenced in their vote.

• Eligibility:

This property expressed that only eligible voters should be permitted to make their vote and they should do so only once. The premise of this property is verification, since voters need to demonstrate their identity before being considered eligible or not.

• Privacy:

The manner in which that an individual voter casted a vote should not be revealed to anyone. This property in non-electronic voting plans is guaranteed by physically protecting the voter from prying eyes.

• Verifiability:

This property guaranties that all gatherings included can check whether their votes have been counted or not. Normally two types of verifiability are defined, individual and all-inclusive verifiability. Individual verifiability enables an individual voter to check that one's vote has been counted. All-inclusive verifiability necessitates that anybody can check that the election result is the one distributed.

• Coercion-resistance:

A coarser should not be able to recognize whether a constrained voter casted a ballot the manner in which they were told to. It is inside the extent of the paper to consider a convention that has the previously mentioned properties. Be that as it may, Coercion resistance won't be effectively

sought after since it was regarded unrealistic to be accomplished simply with mechanical methods in a remote e-vote a ballot convention. The convention does anyway have the property of Forgiveness that can be seen as a flimsier thought of the compulsion opposition property.

• Forgiveness:

The ability of a voter to modify ones vote after it has been cast. This property connects to compulsion opposition since it gives a pressured voter the alternative of changing ones votes at a later stage so as to reflect one's actual conclusion.

3. BACK GROUND

3.1The blockchain:

The blockchain is composed of time stamps which show at what time block was added. A block that contains transactions happening at a specific time is similar to a time-stamped binary file. The hash estimation of the past block and the present block will be the contribution of the hash estimation of the following block. Each hash estimation of a block is determined from the hash estimation of the past block, and transactions are recorded in the block. Since the hash of the previous block is utilized to produce the hash value of the next block, the next block is "chained" with its earlier block, reinforcing the integrity of all the past blocks that came before. Every foremost block contains information about the hash of earlier blocks. The technology under goes through four main features:

A. No single point of failure in the maintenance of the distributed ledger
B. There is distributed control over who can append new transactions to the ledger.
C. Any proposed "new block" to the ledger must reference the previous version of the ledger, creating an immutable chain from where the blockchain gets its name, and thus preventing tampering with the integrity of previous entries.
D. A majority of the network nodes must reach a consensus before a proposed new block of entries becomes a permanent part of the ledger.

E. This paper evaluates the use of blockchain as a service to implement an electronic voting (e-voting) system. The paper makes the following original contributions:

(i) Research existing blockchain frameworks suited for constructing block chain based e-voting system,

(ii) Propose a blockchain-based e voting system that uses "permissioned blockchain" to enable *liquid democracy*.

(Fig :1)

3.2 Public and private key and bitcoin address

For addressing and exchange marking the Bitcoin utilizes open and private keys. A Bitcoin private key is an arbitrary CAST 256 bits. Clients utilize this key to sign their exchanges each time they exchange Bitcoin. The client will is randomly create the private key. Since the key has 2^(256) bits of test space People in general key is a (x, y) match coming about because of the secp256k1 condition increased by the generator (G). This generator is settled in Bitcoin frameworks. This implies open key uniqueness isn't ensured by the generator (G), yet is ensured by the uniqueness of the private key. Utilizing SHA256 and RIPEMD160 hashing calculations people in general key is delivered. The general population key is Base58Check encoded to create the Bitcoin address. Since this location is created from a private key that contains no mystery data, delivers can be known to people in general.

3.3 Block chain safety

In a Bitcoin framework, to make it hard to manufacture setting in blocks, a random numbers called a nonce is introduced to every block. A nonce is a self-assertive number utilized just once to help confirm the hash. So as to create a unique mark - i.e., a hash of the block - miners utilize the header of the block which is a predetermined set of data. This set of data represents all transactions contained in the block, the date, time some other information which can be settled at whatever point a specific period time has passed. Miners do this to endeavor to approve their verification of work. These header segments and nonce will be put into a hash capacity to produce a block hash.

To add to the calculation is trouble, there is a condition that the block hash should be smaller than some given value. This implies the block hash should begin with a specific number of zeros (in light of trouble). When we take a particular nonce found by a miner and the current block header, these two values should produce the unique finger impression for the block hash. Fingerprints are 64 hexadecimal digits. Expect that the initial 15 digits of a hash ought to be zeros, so multiple times 4 bits (i.e., 60 bits) toward the start of the hash ought to be zero. The likelihood that comparing 60 bits are zero is low, around 2 - 60. The

current Bitcoin organize requires 17 zeros toward the start, so 68 bits must be zeros.

It requires huge compute power to work until the nonce that produced the hash value satisfies the condition based on difficulty. We can estimate how much hash is required before the right hash is found. The Bitcoin has a hash rate of around 1200 quadrillion (1,200P) hashes/s at this time, despite everything it takes 10 minutes overall to discover the nonce. So 1200 hash times 10 mins on average is how many hash activities the mineworker needs. There is no similar way to find this hash value because there is no (known) back door in the hash function The best way to locate the correct nonce is by performing many hash activities Since finding a particular nonce at each block is troublesome, attackers who try to forge the block-chain ledger need to find the corresponding nonce to the changed transactions.

4. PROPOSED METHOD

Neumann proposed electronic voting criteria that include:

- System integrity
- Data integrity and reliability
- Voter anonymity and data confidentiality
- Operator authentication

As shown, the generation of addresses does not depend on personally identifiable information (PII), rather permits transparent tracking of transactions. These transactions are verifiable, open to people in general and are hard to forge. Block-chains, at that point, can ensure data integrity and reliability, voter anonymity, data privacy and – in any event for the block chain – framework trustworthiness. Administrator validation, be that as it may, is as yet required.

Client validation is important to guarantee that the individual casting a ballot has a directly to cast a ballot. Once verified, a vote from one user must be tracked to one candidate. In this section we give a block chain based casting a ballot framework with government-based authentication frameworks

4.1 Organization Trusted third party, Voters, and Block-chain:

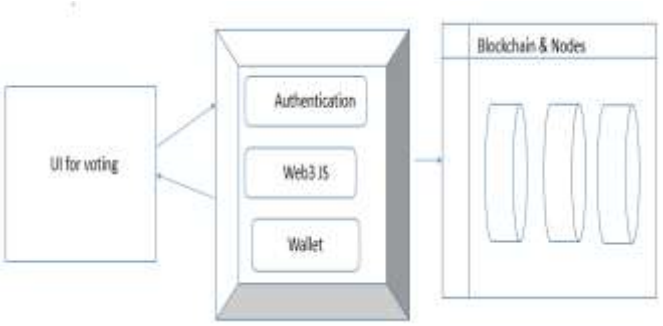
There are four sections that are engaged with this electronic casting a ballot demonstrate. A verification association alludes to any foundation that holds a voter enlistment rundown, for example, the National Election Committee or privately owned businesses. Electronic casting a ballot framework might be utilized for presidential elections, stockholder's meetings, and so on. Just the National Election Committee will have the list of voters in their country. Both Bitcoin and the proposed casting a ballot framework are available to anybody to make any transactions, however the casting a ballot framework limits voters to just the individuals who have directly to cast a ballot in their very own organization. As expressed, this implies confirmation for a client is required the first is that a verification organization ought to validate the voters, however ought not have the capacity to discover who the voter voted in favor of. The second is that since the authentication organization has the voters list, they can potentially manipulate the number of voters in their nation. The third potential issue is that a validation association could possibly give most of nonce mining. Assuming this is the case, they can possibly fashion the block chain record in the manner in which that they need.

In our proposed method, we keep vote transactions in the block-chain. To manage block chain there are many ways and we introduce two ways that are useful for voting purposes. They are,

- Operating independent block-chain funded by the organization.
- Using current Bitcoin block-chain.

4.2 Declaration of a vote:

More over in the voting system, there are individuals who can and cannot vote, so voters must be authenticated by an organization. We introduce declaration to solve this step. A voter declares a vote by sending a secret message hash to the validating organization. We accept that the verifying association has effectively enrolled a voter and gives a login to their record for verification. The voter at that point enlists their their secret message hash to the organization. This hash should be unique to each voter because this factor is going to be used as an authentication of votes in the block- chain. At the point when the message hash is sent to the organization holding the list of voters, in the event that the person is confirmed to have a vote, then they link using connect the message hash with the voter's ID . There are few IDs that can be utilized when voter's login with their account. The reason voters can't simply register the address derived from their own private key is that the location will be composed on each transaction that will be open to the public later in the block-chain. At this point when this address is enrolled to the organization, at that point they can recognize a vote as blocks being stamped The data produced from a voter's private key, for example, an open key, open key hash, or address, ought not be enrolled to the organization, else they will realize who votes in favor of whom. Since all transaction are put away in an open block chain, when you give the organization your open key as an ID, they can know which client voted in favor of whom. That is the reason the secret message hash is required to be one of a kind, which is additionally autonomous to the general population key utilized as an ID.



4.3 Casting a vote:

The number of votes is characterized as the number of transactions made to a candidate's address. Candidates will give their addresses fixed and open to the public to receive transactions from voters. An individual who runs an election will essentially produce their private key, and open up their address which can be considered as a container of votes. At that point voters make a transaction to the address of hopefuls.

4.4 Confirming votes

We propose a model to verify voters who have the directly to cast a ballot and to guarantee secret casting a ballot. The layers among voters and the verifying organization are made out of two sections. One is the third party, and the anther one is block-chain. At the point when individuals who need to cast a ballot complete the statement to cast a ballot -when their secret message hash has been connected with their ID, (such as an SSN) that only the organization has - they need to make contact with the trusted third party. Voters give the confided in third party their secret message hash and the believed third party will inquire as to whether they get a similar secret message hash from a voter. In the event that the organization answers 'yes,' it implies that an individual who sent the hash value is enrolled as a legitimate voter who completed the revelation to cast a ballot. At that point the believed outsider like trusted third party perceives this individual as an appropriate voter. The believed outsider spares the voter's open key hash once they affirm they are a substantial voter through correspondence with the organization. Eventually, the trusted third party will have will have the rundown of affirmed open key hashes and the addresses which are affirmed to be enlisted in the organization. By utilizing this enrolled address, transactions which are made by an invalid voter won't be tallied however will be evacuated when casting a ballot is finished. The casting a ballot convention.

5. CONCLUSIONS

The idea of adapting digital voting systems to make the public electoral process cheaper, faster and easier, is a compelling one in modern society. Making the electoral process cheap and quick, normalizes it in the eyes of the voters, removes a certain power barrier between the voter and the elected official and puts a certain amount of pressure on the elected official. It also opens the door for a more direct form of democracy, allowing voters to express their will on individual bills and propositions.

In this paper, we introduced an electronic voting system that uses the Block-chain as a ledger of transactions, where authenticating and filtering are done by the authenticating organization and a trusted third party. The Bitcoin protocol still can't seem have failed, and the block-chain open ledger has cannot been forged since it appeared in 2009. Further, the transparency of the block-chain enables all the more evaluating and comprehension of elections. These qualities are a portion of the prerequisites of a voting system. These attributes originate from a decentralized system, and can convey progressively popularity based procedures to election, particularly to coordinate election system. The proposed protocol changes the paradigm that we confide in a solitary organization such as a government or a company. In current election systems, voters must believe the vote records given by the casting a ballot organization and it is difficult, if not impossible, for a single voter to prove that there is no fraud. Then again, in the proposed strategy, the organization's solitary employment is to send an answer dependent on the constituent move they have, which is a tremendously limited activity scope than previously. With the proposed system, voters need to recognize their entitlement to cast a ballot by substantiating themselves to both verifying organization and the TTP. At that point, by distributing the two sides of the program, voters realize that the given vote is extraordinarily approved and auditable.

REFERENCES

1) A. B. Ayed, "A conceptual secure blockchain-based electronic voting system," International Journal of Network Security & Its Applications, vol. 9, no. 3, 2017.
2) Auðkenni.is (2018). [Online] Available at: https://www.audkenni.is/en/
3) Ayed, Ahmed Ben. "A conceptual secure Blockchain-based electronic voting system." International Journal of Network Security & Its Applications 93 (2017).
4) Fujioka, A., Okamoto, T., Ohta, K.: A practical secret voting scheme for large scale elections. In: International Workshop on the Theory and Application of Cryptographic Techniques. pp. 244–251. Springer (1992)
5) Gentry, C.: A fully homomorphic encryption scheme. Stanford University (2009)
6) Hjalmarsson, Friorik P., et al. "Blockchain-Based E-Voting System." 2018 IEEE 11th International Conference on Cloud Computing (CLOUD). IEEE, 2018.

7) Hanifatunnisa, Rifa, and Budi Rahardjo. "Blockchain based e-voting recording system design." Telecommunication Systems Services and Applications (TSSA), 2017 11th International Conference on. IEEE, 2017.
8) Hsiao, Jen-Ho, et al. "Decentralized E-Voting Systems Based on the Blockchain Technology." Advances in Computer Science and Ubiquitous Computing. Springer, Singapore, 2017. 305-309.
9) Juels,A.,Catalano,D.,Jakobsson,M.:Coercion-resistantelectronicelections.In:Proceedings of the 2005 ACM workshop on Privacy in the electronic society. pp. 61–70. ACM (2005)
10) Katz, J., Myers, S., Ostrovsky, R.: Cryptographic counters and applications to electronic voting. Advances in Cryptology Eurocrypt 2001 pp. 78–92 (2001)
11) Kiayias, A., Yung, M.: Self-tallying elections and perfect ballot secrecy. In: Public Key Cryptography. vol. 2274, pp. 141–158. Springer (2002)
12) Kshetri, Nir, and Jeffrey Voas. "Blockchain-enabled e-voting." IEEE Software 35.4 (2018): 95-99.
13) Kohno, T., Stubblefield, A., Rubin, A. D., & Wallach, D. S. (2004). Analysis of an electronic voting system (pp. 27–40).
14) N Mendoza - Conference for E-Democracy and Open …, 2015 - books.google.com
15) Neumann, P. G. (1993). Security Criteria for Electronic Voting. Baltimore, Maryland.
16) Rubin, A. D. (2002). Security Considerations for Remote Electronic Voting. Commun. ACM, 45(12), 39–44.
17) New York, NY, USA: ACM, 2017, pp. 574–575. [Online]. Available: http://doi.acm.org/10.1145/3085228.3085263
18) Osgood, Ryan. "The Future of Democracy: Blockchain Voting'." COMP116: Information Security (2016).
19) Pawlak, Michał, Jakub Guziur, and Aneta Poniszewska-Marańda. "Voting process with blockchain technology: auditable blockchain voting system." International Conference on Intelligent Networking and Collaborative Systems. Springer, Cham, 2018.
20) Vincent Gramoli. (2018). On the Danger of Private Blockchains. [Online] Abailable at: https://www.zurich.ibm.com/dccl/papers/gramoli_dccl.pdf
21) Liu, J.K., Wong, D.S.: Linkable ring signatures: Security models and new schemes. In: International Conference on Computational Science and Its Applications. pp. 614–623. Springer (2005)
22) McCorry, P., Shahandashti, S.F., Hao, F.: A smart contract for boardroom voting with maximum voter privacy. IACR Cryptology ePrint Archive 2017, 110 (2017)
23) Murphy, T.I.: hyperledger whitepaper, https://docs.google.com/document/d/1Z4M_qwILLRehPbVRUsJ3OF8Iir-gqS-ZYe7W-LE9gnE/edit#heading= h.m6iml6hqrnm2
24) Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008)
25) Neff, C.A.: A verifiable secret shuffle and its application to e-voting. In: Proceedings of the 8th ACM conference on Computer and Communications Security. pp. 116–125. ACM (2001)
26) Nsw election result could be challenged over ivote security flaw (2015), https: //www.theguardian.com/australia-news/2015/mar/23/nsw-election-result-could-bechallenged-over-ivote-security-flaw
27) Okamoto,T.:Receipt-freeelectronicvotingschemesforlargescaleelections.In:International Workshop on Security Protocols. pp. 25–35. Springer (1997)
28) Perrin, C.: Use md5 hashes to verify software downloads (2007), https:// www.techrepublic.com/blog/it-security/use-md5-hashes-to-verify-software-downloads/
29) Ryan, P.Y.: Prêt à voter with paillier encryption. Mathematical and Computer Modelling 48(9), 1646–1662 (2008)
30) Tarasov, P., Tewari, H.: Internet voting using zcash. Cryptology ePrint Archive, Report 2017/585 (2017), http://eprint.iacr.org/2017/585
31) Theguardian: Why machines are bad at counting votes (2009), https:// www.theguardian.com/technology/2009/apr/30/e-voting-electronic-polling-systems
32) Wüst, Karl, and Arthur Gervais. "Do you need a Blockchain?." 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). IEEE, 2018.