International Journal of Future Generation Communication and Networking
Vol. 13, No. 1s, (2020), pp. 46- 54

Secured Online Voting System Using Blockchain Technology

Tanvi Shah[1],Sneha Kadam[2],Ankita Mane[3],Tanvi Kapdi[4] *Atharva College of Engineering*

Abstract

Social Life is one of the most benefited area by technology. Advancement in technology provides unrestricted access to diversified resources and a huge knowledge base to develop a globally connected architecture. Technology such as the Internet has proved to be a boon for innovations and crafting resources beneficial to mankind. One such groundbreaking innovation is Blockchain-an exciting technological advancement prominently

Known for its application in cryptocurrency. Blockchain offers an infinite range of applications which benefit from the concept of shared economy. With properties such as immutability, decentralized architecture, Blockchain presents itself as a potential solution in bridging the current parity between common man and its government. Elections keeps a democratic country functioning by providing its citizens the fundamental right of choosing their own government.Thus carrying out transparent elections and preventing electoral fraud is of utmost importance.

This paper aims to evaluate the application of Blockchain technology as a medium to conduct online electronic voting seamlessly and transparently.This paper analyzes the need and requirements of building an Electoral portal using the Blockchain technology and identifying the legal and technical challenges that may be faced while designing the system.

Keywords: Blockchain, e-voting, Security, Privacy, Decentralized public ledger

1. Introduction

Voting whether conducted through the traditional ballot or via electronic means forms the basis on which the democracy depends.[1] With the rise in technological impact on the youth of the country and the various anomalies faced by the current electoral process,using technology to modify the existing process is necessity of the hour.However for any new technique to take the place of current voting system,the said system needs to satisfy certain minimum criteria.Electronic Voting has taken center place in research with the intention of minimizing the cost associated in setting up the voting process,while ensuring the electoral integrity is maintained by fulfilling privacy,security and compliance requirements.[10]

The current method ,whether electronic or not has proved to be unsatisfactory with respect to transparency.It can be very difficult for the voters to be assured that the vote he/she has casted during the election reflects in the election result.Electronic voting using Direct Recording Electronic do not generate receipt on successful casting of votes.No record of election except vote count is made public by the government,which means that the voters are not assured of any external interference in case of government conducting the process of vote recounting[2].Replacing the traditional method with electronic method using Blockchain technique has the ability to prevent potential frauds that may take place during election.[10]

Blockchain technology is a distributed network of interconnected nodes.A copy of distributed ledger is assigned to each node,each of which contains a complete history of all the transactions that have been processed by the network.[1]Each transaction processed generated a hash.The hash created depends not only on the current transaction but also on the hash of the previous transaction.Thus any

ISSN: 2233-7857 IJFGCN

small change on the data will impact the hash of the transaction.[3]If a transaction is approved by a majority of nodes it is written to the block.This allows the users to remain autonomous while using the system. A basic analysis of Blockchain suggests that it provides the potential of making the voting process more secure and reliable.[5]

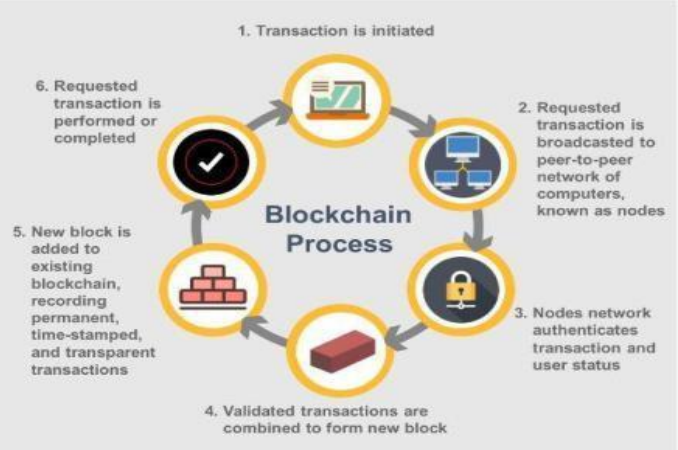

Figure 1: Overview of Blockchain Technology

1.1. Motivation

Will of people forms the basis of democracy.However is it of utmost importance to protect the anonymity of voters and allow complete privacy to cast their votes.The current methodology may sometimes fail to protect the fundamental right of privacy of the voters. The master key to build an electronic voting system is to find out a secure underlying platform which provides the required features that overcomes the drawbacks of the current system.

1.2. Scope

The scope of the system is very vast as it can be implemented in any organization where elections play a major role in electing their representatives.The system can be adapted as per the need and the number of participants using the system.The techniques and concepts used in providing a base to the system uses strong encryption techniques to provide privacy to the votes and tamper free results.

2. Literature Review

Votem[14] has presented a solution of implementing a token based system that is build on blockchain technology which ensures privacy and security of the voters are preserved.The solution is suitable for conditions where authentication of the users is not utilized. The token based system,is however limited in using it effectively in full fledge elections where the solution looks compromised to address the challenges that can be encountered. The blockchain developed can either be based on public or private blockchain platform [15], [16]. If the voting platform is developed on a public blockchian ,its contents are visible to anyone present on the blockchain.Hence it is necessary to protect the contents of the blockchain by encrypting using some secure algorithms such as AES.

There is always a concern over the authenticity of the voter which requires some measures to be taken such as biometric authentication or physical verification. A Blockchain based solution is a better alternative to the traditional ballot based voting system providing transparency and privacy to the users.The voting system deployed on the Blockchain platform has no single authority controlling it and anyone can participate in the blockchain provided they have legitimate authentication credentials.The read only and write once feature of blockchain makes it the best platform to develop an electronic voting platform.However for smooth functioning of the elections through electronic means,strong foundation rules have to be laid which cannot be misused.

ISSN: 2233-7857 IJFGCN

Ethereum attempts to build a generalized technology on which all transaction based state machine concepts may be built.It aims to provide the developer an integrated end-to-end system for building a decentralized application.Using the Ethereum platform a developer may implement a node on the Ethereum network which is then joined to the other nodes present in the network and cresate a decentralized voting system. Election security is an important societal problem that has to be taken in account which a country adopts to the Electronic voting system.When establishing that an election system is secure, one must one must take into account the diverse and adversarial environment the system may be exposed to.An adversary model is proposed which takes to account the capabilities of the Voting system and the assume the possible exploitation on the system.For election security existence of reasonably strong adversaries are taken into consideration when designing the system, for example adversaries that may compromise the client's platform but not the voting server or the postal channel [11].

In order to conduct a fair election,trust of the voters is the most important phenomenon that must be satisfied. Mistrust in the voting is not an uncommon phenomenon even in the developed countries. In order to improve the trust, the least thing that can be done in this regard is the orientation of the electronic voting based on the biometric authentication [8]. Rivest put forth the concept of providing three ballots to the voter.The voters would cast a vote across all the ballot papers.Each ballot paper is marked with a unique identifier.The voter remains anonymous as the keys are used to encrypt the vote

[12] The votes casted are then linked and the choice found on two of the ballot papers is taken into consideration with the single ballot being rejected.However this scheme proves to be inefficient if there are only two candidates participating or there is a large number of participants participating. The scheme also has the disadvantage of being slow and the human error increase if the votes are not accurately poled in the respective boxes. However, given the various advantages that Blockchain has to offer,we believe that technologies making use of distributed ledgers, such as Blockchain, find an imperative use in the Digital Governance landscape. Due to an array of functionalities offered whether in terms of security or privacy,Blockchain technology will find its major applications across the globe.

3. Design Considerations

Various factors which are considered as the key to successful designing of the system are listed as follows:

3.1 Verifiability

Each participant of the election process can verify the voting procedure and its outcome.The system provides the ability for each parties to check whether votes casted are counted correctly or not.Verifiability is typically classified as public verifiability and individual verifiability.[1]

3.2 Privacy

The main aim of this system is to protect the voters physically from prying eyes.Voters voting for any parties should not be revealed to anyone.[1]

3.3 Eligibility

This property states that only the voters eligible to cast should be allowed access to the system .Each voter should vote only once.[4]

3.4 Auditability

The whole process and data stored in blockchain can be viewed and verified at any point in time even after elections are conducted.

3.5 Transparency

The whole process is open to public.This is the most important factor for a secure e-voting system[4]

ISSN: 2233-7857 IJFGCN

4. BACKGROUND STUDY

In this section,we discuss about a brief overview of the technology, various participants and other related terns which that will help us secure the present method of voting system and design a robust and more secure system.[7]

4.1. Participants

Voters: It contains a set of all registered voters.List of voters are defined by a set V={v1,v2,v3,…,vn}where n is the list of all the registered voters.

Organizers: It contains a set of the organizing committee defined by a set O={1} and responsible for enforcing the rules and regulations for election.

Candidates: Candidates wishing to stand for election participate in the system.They are defined by a set C={c1,c2,…,cn} where n is the total number of candidates participating.

4.2. Blockchain

Blockchain was first introduced by a person or group of person under the anonymous identity of Satoshi Nakamoto.It was first implemented on a peer to peer network with no requirement of having a centralized authority.Blockchain technology was first implemented as public ledger for transactions made using bitcoin. It is an ordered data structure with data stored in blocks each containing a set of transactions.

The blockchain network works on the principle of no governing central authority. One party wishing to conduct to a transaction initiates the transaction process by creating a block. This block is verified by thousands of computers distributed across the net. The verified block is added to a chain, which is stored across the net, creating a unique record having a unique history.Each block is linked with previous block in order to maintain the chain structure of blockchain.Each block is secured by a encryption technique and hashing algorithm.The first block that forms the basis of blockchain structure is called as the Genesis block.Transactions in blocks are hashed with SHA-256 hashing function.SHA-256 is a novel hashing function which computes 64-bit words.The block data contains the encrypted votes casted by the voters.

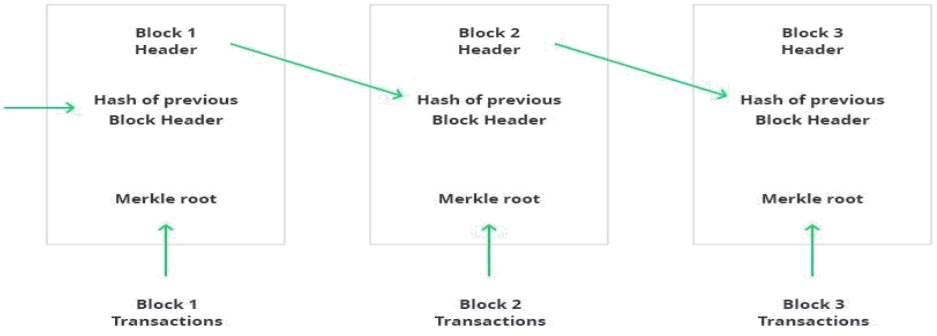

Figure 2: Blockchain Structure

A new transaction can only be added to the blockchain by consensus between participants in the system.Once new data is appended to the blockchain it cannot be erased. It is a write-once,append-many technology,making each record of the transactions verifiable and auditable. Merkle trees are created by repeatedly calculating hashing pairs of nodes until there is only one hash left. This hash is called the Merkle Root, or the Root Hash. Every leaf node in Merkle root is a hash of transactional data, and the non-leaf node is a hash of its previous hashes.

ISSN: 2233-7857 IJFGCN

5. PROPOSED SYSTEM

In order to conduct an election electronically,the parties wishing to compete must enroll themselves with the system. The election administrators create the election, register voters, decide the lifespan of the election.Voters can authenticate themselves, cast their vote and verify their vote after an election is over.

.

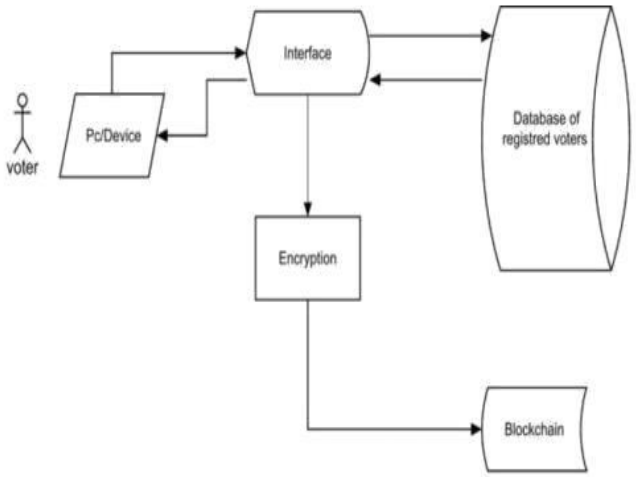

Figure 3: E-Voting System Methodology

The users are provided a user interface from where they can view the candidates, register votes, and check the reports.The website will be active only during the Election period.. The voter submits their personal credentials such as voter's name, address, identity card number, date of birth etc to the server. Once the voter credentials are verified by the application server,the voter can then proceed to view the candidates,cast votes and view results. The verification helps in the prevention of fraud. To confirm the identity of the voter,a One Time Password(OTP) is send to the contact number of the voter.On verification the voter is allowed to cast the vote.

On verification, the user can view the candidates electing the contest according to their legislature and can register their votes. These votes are flooded to the peer nodes in the form of transactions .Once all the nodes verify the transaction to be valid,these nodes are added to blockchain.The Election Commission receives the votes in form of a report.The blockchain technology ensures that the votes are tamper proof and complete privacy is ensured.
The following steps are involved when a voter wants to cast a vote:

5.1. Pre-Voting Phase Steps :

1. Voters intending to cast a vote needs to register themselves with the system.The voter can choose a password for signing which is to be used to login to the system
2. After successfully registering themselves,the voters receives access to the system.[7]

5.2. Voting Steps:

1. During the specified period of election ,the voter can login to the system using the voter Id and password.
2. The voter is then verified using the eligible voters list.
3. Once the voter is authenticated,they can cast a vote to the candidates.
4. The Election Commission uses the public key to encrypt the vote.
5. The encrypted vote is then signed by the private key of the voter.
6. The voter's information is stored in the server.This forms the first block of the blockchain.
7. Steps 3 to 6 are carried out continuously until the election period is served.

ISSN: 2233-7857 IJFGCN

5.3. Post Voting Phase Steps:

1. One the election process at each constituency,the votes are clubbed to form a complete blockchain.
2. The election Commission performs verification of the votes and generates reports of the election.

6. Implementation

The proposed system uses a web based application that is created to serve as a front end application which enables the users to interact with the system.The application is implemented in PHP language and uses MYSQL database as the backend for the application. The database is used by the Admin to store the following:

1. Information related to creation of election such as Election type, Organizer, start date, end date etc.
2. Information related to candidate details such as candidate name, age, qualification, contact no, image etc.
3. View list of candidate's registered.
4. View list of voter's registered.

The project has two major modules:

1. The Admin Module

Performs functions such as creating elections,adding candidates,displaying candidate's and voter's details,verifying hashed blocks of data and viewing results.

2. The Voters Module

This module performs two major functions of allowing the voters to cast votes and viewing graphical results instantly.

6.1. ALGORITHM

Algorithm 1 Electronic Voting System

1: **procedure** INPUT: (user Id, password, vote)

2: OUTPUT: Complete vote in the form of Blockchain
3: **BEGIN**
4: The voter registers themselves on the website with all the required information.
5. Input voter Id, choose password.
6. **if** (username == registered user) and (voter == eligible)
7. Enter password
8. **else**
9. Voter is not eligible and cannot cast vote
10. **if** (entered password == registered password)
11. Redirect to voting page
15. **else**
16. Enter Password.
17. Enter Aadhar number
12. Enter OTP received on Mobile number linked to Aadhar Card.
13. **if** (OTP entered == OTP sent)

ISSN: 2233-7857 IJFGCN

14. Cast vote.
15. **else**
16. Voter cannot cast vote.
17. Hash previous block's hash,user Id,Vote casted and nonce using SHA-256 hashing algorithm.
18. Total no of votes-$\sum^{n}i=1$ partyi, where n is the total count of registered parties.
19. **END**

6.2 Index of Functionalities

```
* @param array $transactions
* @return void
*/
function createAndDisplayBlockchain($transactions)
{
   $prev_block_hash = '0';

   // iterating to all the transactions in the array
   foreach($transactions as $transaction) {
      $result = hashCalculator($transaction, $prev_block_hash);

      dd(' /* ************************************ */ ', false);
      dd($result, false);

      // setting the last hash found: this will be sent to the next block in the
      // next iteration
      if ($result) {
         $prev_block_hash = $result['hash'];
      }
   }
}
```

Figure 4: Creating Blockchain in PHP

Function CreateAndDisplayBlockchain() takes a set of transactions and is responsible for generating and displaying the blocks present in blockchain.The functions iterates for each transaction present to calculate the hash value and the result is assigned to an array.

```
* @param array $transaction
* @param string|null $prev_block_hash
* @return array

function hashCalculator($transaction, $prev_block_hash=null)
{
   $cycles_limit = 10000000;

   for($nonce=1; $nonce<$cycles_limit; $nonce++) {
      $block = getBlockContent($transaction, $nonce, $prev_block_hash);

      // calculating the hash SHA-256 of the text block
      $hash = hash('sha256', $block);

      // checking if the block starts with three zeros
      if (substr($hash, 0, 4) === '0000') {
         return [
            'block_content' => $block,
            'hash' => $hash,
         ];
      }
   }
}
```

Figure 5: Hashing Blockchain data in PHP

The function hashcalculator() takes the array of transactions and previous transaction's hash as parameters.It performs the functionality of computing the hash value of the transactional data.A difficulty level is assigned to a variable.The difficulty level is a number that that regulates how long it takes for a miner to add block to the blockchain.The functions a SHA-256 hashing function to compute the hash value of the transaction.

ISSN: 2233-7857 IJFGCN

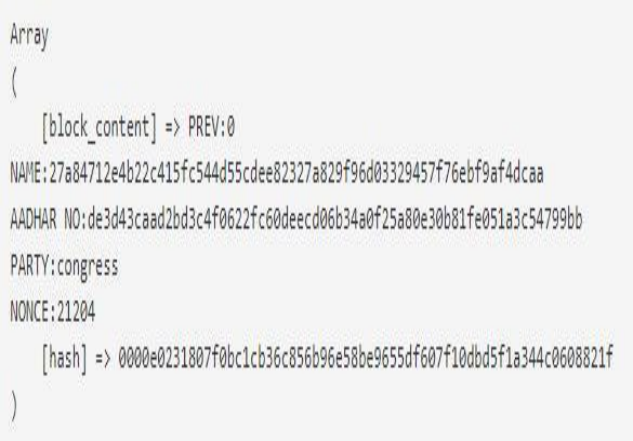

Figure 6: Example of blocks of votes

As shown in fig 6,the blockchain used in the project consists of blocks for each party.Each transactions in a block is a vote casted to a candidate by a voter.The name and aadhar number of the voter along with the the party to whom vote is casted is hashed together using SHA-256 hashing algorithm.

7. Pros and Cons

Since Blockchain is based on the concept of distributed public ledger it stores the votes highly resistant to technical failures.It allows voters to remain anonymous while casting votes. Processing time is cut down.As voting results are generated as soon as the voting process is completed .Votes can be tallied and stored on an immutable public ledger thus providing transparency between government and voters. However along with its benefits,using Blockchain technology also has a few drawbacks.In order to verify the authenticity of the vote,the noes verifying the data must be in a peer to peer network and the voting system must be connected to the network.This network may be susceptible to various cyber security attacks.[2]

8. Conclusion

E-voting, as discussed, is a crucial factor in improving the interest and participation of youth amongst the tech savy population. Recent elections have shown us how much the current election process can improve in order to provide a transparent, trustworthy and a democratic environment.Rigging of poll booth, lack of transparency, populism etc are some of the many issues that the current election process faces.Thus creating an electronic voting platform will encourage a greater turnout during election process and increased voter's confidence.

A potential solution to deal with the aforementioned issues is Blockchain based voting system.This paper explores the applicability of Blockchain based voting system and its usefulness in overcoming the drawbacks of the present system.We believe that the distributed ledger feature of Blockchain technology will help us to overcome the shortcomings of the current system.

References

1. Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis, "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy", IEEE 2018.
2. Teogenes Moura,Alexandre Gomes, "Blockchain Voting and its effect on Election Transparency and Voter Confidence",IEEE Security and Privacy(2006),Volume:4,Issue 1.
3. Nir Kshetri,Jeffrey Voas, "Blockchain-Enabled E-Voting", IDAACS 2009.

ISSN: 2233-7857 IJFGCN

4. Yi Liu,Qi Wang., “An E-voting Protocol Based on Blockchain”, ICAST 2009.
5. Weilin Zheng,Zibin Zheng 1,2, Xiangping Chen,“NutBaaS:A Blockchain-as-a-Service Platform”, IEEEAccess,2019.
6. Kanika Garg,Pavi Saraswat,Sachit Bisht , “A Comparitive Analysis on E-Voting System Using Blockchain
7. ”,IEEEAccess,2019.
8. Ashish Singh,Kakali Chatterjee, “SecEVS : Secure Electronic Voting System Using Blockchain Technology”,International Conference on Computing, Power and Communication Technologies (GUCON),2018.
9. [8].BasitShahzad,JonCrowcroft,“TrustworthyElectronicVotingUsingAdjustedBlockchain
10. Technology”,IEEEAccess,2019
11. Zou, X., Li, H., Sui, Y., Peng, W., Li, F.,”Assurable, transparent, and mutual restraining e-voting involving multiple conflicting parties.”, In:2014 IEEE Conference on Computer Communications INFOCOM ,2014
12. Friðrik Þ. Hjálmarsson, Gunnlaugur K.Hreiðarsson, Mohammad Hamdaqa, Gísli Hjálmtýsson, “A formal framework and evaluation method for network denial of service”, ResearchGate, 2018.
13. 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.
14. R. L. Rivest,‘‘The threeballot voting system,’’Tech. Rep., 2006, p. 15. [11] J. Stern. Votem—Voting for a Mobile World. Accessed: Jul. 31, 2018.
15. M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, ‘‘Strong authentication for RFID systems using the AES algorithm,’’ in Cryptographic Hardware and Embedded Systems. 2004, pp.
16. 357–370.
17. J. Stern. Votem—Voting for a Mobile World. Accessed: Jul. 31, 2018. [Online]. Available: https://votem.com/
18. M. Pilkington, ‘‘11 Blockchain technology: Principles and applications,’’ in Research Handbook on Digital
19. Transformations. 2016, p. 225.
20. G. Gabison, ‘‘Policy considerations for the blockchain technology public and private applications,’’ SMU Sci. Tech. Rev., vol. 19, p. 327, Sep.2016

ISSN: 2233-7857 IJFGCN