International Journal of Smart Home
Vol.14, No.2 (2020), pp.31-38
http://dx.doi.org/10.21742/ijsh.2020.14.2.04

Secure Electronic Voting System using Blockchain Technology

D.Dwijesh Kumar[1], D.V. Chandini[2], and Dinesh Reddy[3]

Vignan's Institute of Information and Technology, Visakhapatnam, India
[1]dwijesh.daka@gmail.com, [2]chandini2996@gmail.com, [3]dinesh4net@gmail.com

Abstract

The Secure Electronic Voting System using Blockchain Technology is ensured to make the current voting process to take place in an honest, accurate and highly secure way. This system stores the details of the voters and votes in two separate blockchains, which provides transparency into election results by allowing voters to independently audit the ballot box while protecting each voter's right to privacy. All the details of the voters get stored into one Blockchain, and this guarantees greater security by providing a PIN confirmed before the vote is taken into consideration. By casting votes as transactions, we can create another blockchain which keeps track of the tallies of the votes. This way, everyone can count the votes themselves, they can verify that no votes were changed or removed, and no illegitimate votes were added and as a result, is made public everyone can agree upon the final count. This system is only taking the current process of voting in an election and bringing that process entirely online, in an attempt to make it highly secure and also more accessible by allowing the voter to vote at his/her location and also reducing the effort put by staff members.

Keywords: *Blockchain, Electronic voting, Privacy, SHA-256 algorithm*

1. Introduction

With the advancement of digitalization in every sector of our modern life, the e-voting can transform immense changes in the current voting system. In the elections conducted offline, the results are not accurate and fair. The power in the hands of central administrators plays a crucial role in manipulating changes in the casted votes and declaring the unfair results. The proposed model mainly aims to ensure high-end security and brings an out the willingness for each voter to vote. The most common threat that all the e-services suffer from is security. The online voting platform can resolve this issue with the implementation of blockchain technology in it. The evolution of blockchain technology can shift the authority and trust away from the central actors.

2. Existing system

Currently, there are many countries which are in use of the digital voting system. Estonia was the first country to implement this and to continue it. In the recent election conducted in Estonia, about 30.5% of all votes were cast online. To provide a better platform for voting, we have researched some of the existing systems, notably Estonia [1] and understood their flaws and have come up with a better solution. Estonia provided national ID for each citizen who acted as the central system for the voting process. This card helps in the unique identification

Article history:
Received (July 15, 2020), Review Result (August 19, 2020), Accepted (September 20, 2020)

Print ISSN: 1975-4094, eISSN: 2383-725X IJSH

of the voter. The voting process starts with accessing the voting website on the connected computer, and the voter needs to enter their card into a card reader. Then, it asks for their PIN and checks whether they are eligible to vote and only after successful authentication they can cast their vote. In this process, the voters can cast their vote any number of times until four days before Election Day. The users can also use their mobile phone for the casting of the vote if there is no card reader for computer. This model makes use of three servers, i.e., VFS (Vote Forwarding Server), VSS (Vote Storage Server) and VCS (Vote Counting Server).

Initially, when a voter submits their vote, it is passed through the publicly accessible VFS and VSS (where the vote in encrypted and stored until the election period is over). All the votes in the VSS are cleared from the identifying information and then transferred to the VCS by a DVD. This VCS is isolated from all the networks, this server decrypts and counts all the votes followed by providing the results. Many researchers have studied this process and identified several security risks [2]. The centralized feature in this system enables any attackers or third parties to make changes in the database [3]. This model also allows the voter to vote any number of times in the available four days. In this model, the voter cannot check whether his vote has gone to the appropriate party or not, and this can lead to any changes of the casted vote done by the third party. Therefore, the users cannot agree with the final count.

We have also come across the New South Wales iVoteSystem [4], and have extended their process. This system creates a solution by letting the voter choose a 6 digits PIN. The voter theologians the system using the ID and PIN. Upon successful authentication, each voter receives a 12 digits receipt number. To check the vote, the voter has to give his ID, PIN, receipt number, and this is an optional choice.

Another system, Team Plymouth Pioneers [5] created a solution using Blockchain. This process follows by creating two blockchains, one for storing the voter's details (Voter's Blockchain) and the other for storing vote details (Votes blockchain). Authentication for the voter to vote is done using the voter’s Blockchain, and the vote cast gets stored in the votes Blockchain. In this system, once the vote is cast, the details of the respective voter from the voter's Blockchain are deleted.

Another solution to this system is given by creating a scenario where voting for a candidate is related to a transaction in the bitcoin protocol. In this, each voter who wishes to vote sends a BallotCoin to the wallet of the desired party and amount of BallotCoins in the wallet of each candidate gives the result. This way, valid votes are only stored in the Blockchain [6].

3. Blockchain

Well-funded research by many companies has expanded and hardened the security of relational databases. But the major constraint that they suffer from is TRUST. They put the task of storing, updating entries in the hands of one or few entities, which we have to trust. Blockchain has created a new trend in the TRUST in business. The blockchain protocol is a means of logging and verifying records that is transparent and distributed among users. Usually, the credentials are recorded, managed, and checked by a central authority. The implementation of blockchain technology would empower users to do these tasks themselves, by allowing them to hold a copy of the ledger. Blockchain technology was first introduced by SantoshiNakamoto [7] in the year 2008. He proposed an entirely new system for the exchange of most popular cryptocurrency called Bitcoin. This technology runs in a decentralized platform where each node can communicate with the other, and each node holds a copy of the ledger that contains all transactions.

3.1. Algorithm

The blockchain system uses the SHA-256 algorithm for encryption of all the details within the block. This algorithm takes plain text as input and generates a 256-bit binary value as output. The SHA-256 is strictly one way, i.e., the input can only undergo the process of encryption but not decryption. This unidirectional feature of the Blockchain enables any distrusted parties to make manipulations in the database and rejects the members in the network who wish to do so.

Each block in the Blockchain holds a hash value in its header. This hash value is generated using the SHA-256 algorithm. The blocks in the Blockchain are created whenever a valid transaction occurs. Each block is updated with the details of the transaction and linked with the previous block hash value to establish a chain of blocks.

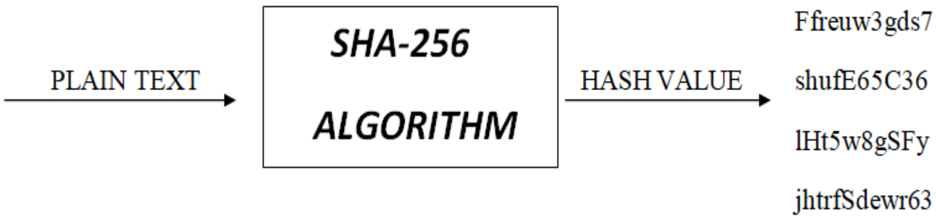


Figure 1. Representation of SHA-256 Algorithm

In our system, the casting of vote by the voter is considered as a transaction, and the Blockchain gets updated with the voter details as well as the respective vote. The details which are to be sent into the Blockchain are inserted as (principal, value) pairs.

3.2. Steps

(1) Initially, everyone has to register with their necessary details, and a PIN is assigned to each voter.

(2) Login includes two-step verifications, first one with their necessary details and the next with the PIN assigned during registration.

(3) The voter is then directed to the voting page, where he can confirm and cast a vote and after casting another new PIN gets generated.

(4) Later, the voter can check whether his vote has gone to correct party or not and he can also view other polls with their respective new PIN.

4. Security properties of e-voting system

The risk of tampering with traditional voting is usually low [8]. But when it comes to e-voting, the situation is quite different. E-voting without strict security measures can result in a higher risk of tampering of votes. Several research projects say that to build a system that supports high-end security in the e-voting platform; the following properties are to be taken into consideration [9].

Authentication: This property ensures that only registered people are allowed to vote. In our system, the registration process includes the voters to register with their details and each voter is assigned with an ID, which he/she has to remember. This ID is used in further verification.

Anonymity: Anonymity is an essential aspect of the voting system. This is included to make sure that no one knows for whom anyone else has voted. With the inclusion of ID assigned to each voter in our system, anonymity is wholly assured.

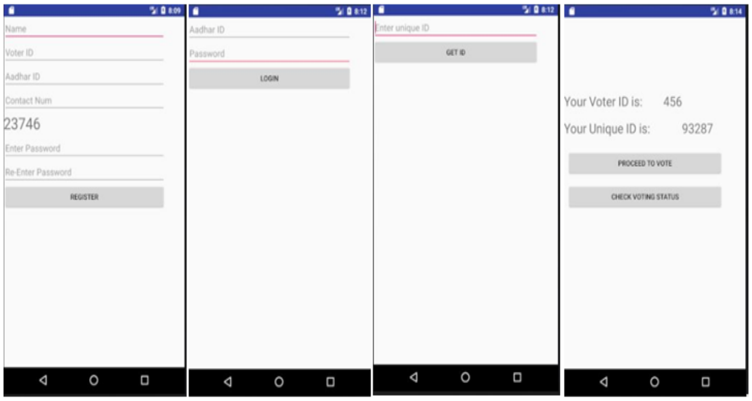
Integrity: The integrity property confirms the elections to take place fairly and honestly. Each voter can make check that his/her vote is not manipulated. Therefore, accuracy in the final results is the main aim of integrity.

Verifiability: The property of verifiability applies both to the system and the individual. The system must make sure all the votes are counted correctly [10]. Each individual should verify whether their vote has gone to the correct party or not.

5. Proposed system

In our design, we have extended the current process. We have come up with new features to meet user expectations at a higher level and to provide accurate and fair results, where everyone can agree upon. To ensure complete authenticity and security, this model makes use of two blockchains. One is the VOTERS blockchain that stores the details of the user and authenticates them. The other is the VOTES Blockchain which stores the vote and NID of all the users.

In our model, we have developed an android application which runs using blockchain technology behind it, and every voter who wishes to vote needs to download the app during the election period. This model includes the first step with Registration. This registration process is open for one week before elections, and people who have registered can only vote. The users have to give their necessary details to register, i.e., name, National Identification Number (NID), voter_id, phone number, password and confirm the password and this registration page includes a PIN which the user has to remember for the further login process. Only if the user is new and valid, he is allowed to register. The two fields, i.e., PIN and voter_id are sent to the VOTERS blockchain as (key, value) pair and all the registration details are sent to the database and after registration follows the login process which includes two-step verification to ensure stronger authentication. This step can be only done by users who have already registered. The first step of verification includes the users to login using the NID and the password given during the registration. These details are sent to the database and checked and after identification of the credentials and the user is directed to the next second step of verification, i.e., VALIDATE_ID page which includes only one field where he has to enter his PIN provided during registration. The PIN given by the user in the page enables to retrieve details from the Blockchain. Upon the successful match of PIN given by the user and the key present in the Blockchain, the user details get displayed on the screen, i.e., his respective voter_id and PIN along with the navigation buttons to another page, i.e., PROCEED_TO_VOTE and CHECK_STATUS.



23746

Your Voter ID is: 456

Your Unique ID is: 93287

Figure 2. Registration and log in process

5.1. Voters blockchain

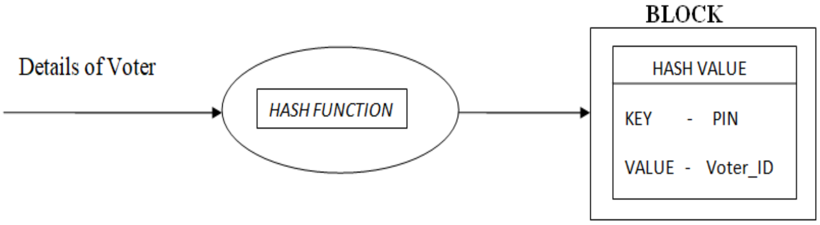
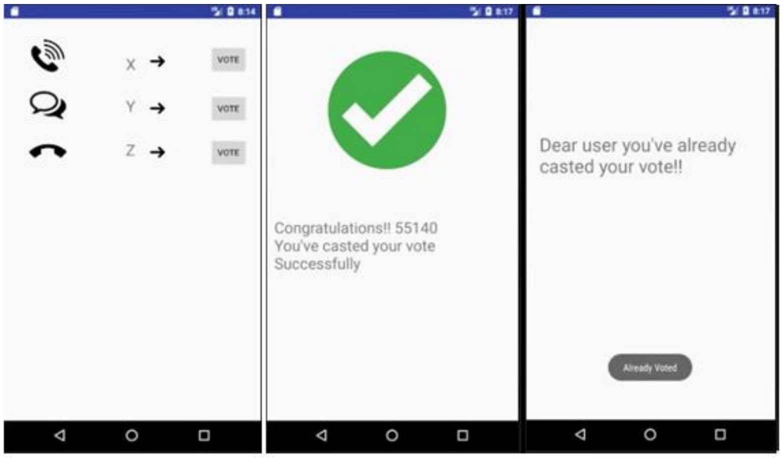


Figure 3. Representation of BLOCK in voters blockchain

5.2. Voting process

When the user clicks on the PROCEED TO VOTE button a list of all eligible parties get displayed, where the user can choose any one party of his choice. Later he is asked to confirm his vote, and if he is sure he can proceed by clicking OK, and if not, he can go back and choose the other party. After confirmation, the votes get successfully cast. When the user casts his vote, another new PIN gets generated which is specific for each user. The new PIN, along with the respective vote of each voter, is successfully sent to the VOTES Blockchain and also to the database. Once the vote gets to cast the details gets updated in the database, and he is not allowed to vote again. This application also ensures the voters not to submit a blank vote.

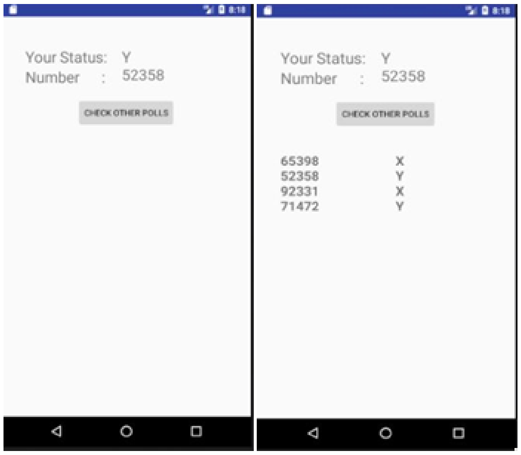
After the casting of vote, when the user navigates to CHECK_STATUS page, he can check whether his vote has gone to appropriate party or not. This feature in the model brings out a sense of willingness for each voter to vote as the user can check his vote and make sure it is not manipulated. This page displays the user their new PIN and respective vote and also a button to check other polls. When the user clicks on the button, a list of newly generated number and the corresponding votes of all the voters gets displayed. With the implementation of this feature in the model enables the user to act as an admin and access the database details. This newly generated number ensures the property of anonymity to the fullest where no user can know the number being held by the other person.



Congratulations!! 55140
You've casted your vote
Successfully

Dear user you've already
casted your vote!!

Figure 4. Voting process



Your Status: Y
Number : 52358

Your Status: Y
Number : 52358

```
65398        X
52358        Y
92331        X
71472        Y
```

Figure 5. Verification of votes by user

5.3. Votes blockchain

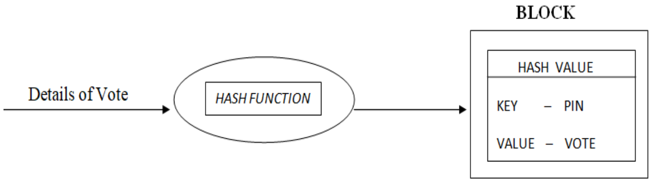
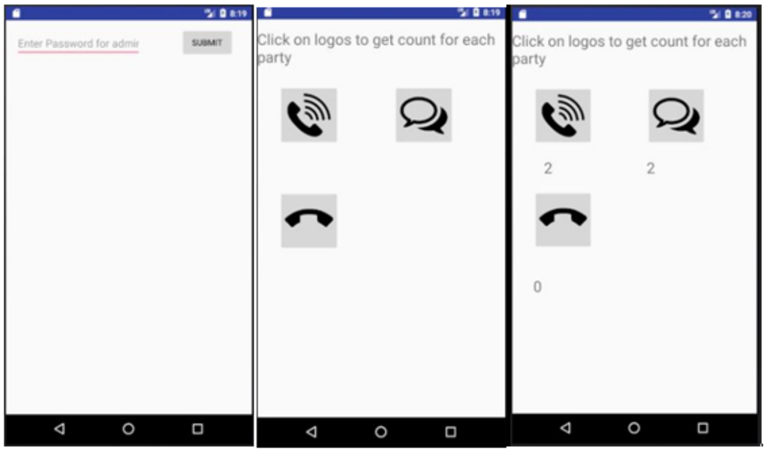


Figure 6. Representation of BLOCK in votes blockchain

6. Results

In this model, only the admin has the right to view the result. When the admin gives his respective password, all the logos of the eligible parties get displayed on the screen. When the admin clicks on each logo, a query runs behind to count all the votes of the respective party and displays it below the logo. This way, the accurate result can be out for each party.



Enter Password for admir

Click on logos to get count for each party

Click on logos to get count for each party

Figure 7. Count of votes by admin

7. Stages of e-voting system

Voter Eligibility: Voter is allowed to register with this national identification number, voter_ID and other personal details. Upon validation, the voter is provided with a PIN. The PIN, along with the Voter_ID of each is sent to the Blockchain. The PIN has to be given for login purpose and to cast a vote. This PIN acts as a key to the database [6].

Casting a vote: After successful login, the user is directed to an interface where he can view all the eligible parties and choose to vote for one party and confirm his vote.

Encryption of vote: The vote is then sent to the Blockchain, where it encrypted using the Secure Hash Algorithm-256. New gets generated after the submission of the vote. The new PIN, along with the votes, is stored into a block in the Blockchain.

Adding the vote to Blockchain: Each block gets created when the user votes successfully. These blocks are linked to the previously formed ones, and a chain of the block gets created.

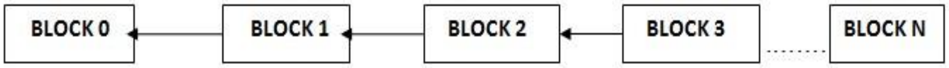


Figure 8. Representation of blocks in blockchain

8. Conclusion

With the implementation of leading technology blockchain in this model, we can ensure the voting process to take place securely and accurately. With the inclusion of PIN in this model, it assures the voting to take place in a completely anonymous way. The essential central aspect of the proposed model is that the user can check whether his vote has gone to appropriate party or not and can also view other polls while protecting others privacy to the fullest. This model creates a new trend in the existing system where the results are accurate, fair and honest, and everyone can agree with the final count. The implementation of this model is an effort to make the voting process highly secure and also more comfortable for the voters to vote at their place. This model acts as a step towards digitalization and thereby reduces the effort put by staff members and voters.

References

[1] Springall Drew, et al. “Security analysis of the estonian internet voting system,” Proceedings of the 2014 ACMSIGSAC Conference on Computer and Communications Security, ACM, (**2014)**

[2] Kovic Marko, “Blockchain for the people: Blockchain technology as the basis for a secure and reliable e-voting system,” **(2017)**

[3] Essex Aleksander, “Internet voting in Canada: a cyber security perspective,” Online Voting Roundtable, Centre for e-Democracy, **(2016)**

[4] Ayed Ahmed Ben, “A conceptual secure Blockchain-based electronic voting system,” International Journal of Network Security & Its Applications 9.3, **(2017)**

[5] Villarreal and Gonzalo Luján, “Blockchain (no todo lo que brilliant Bitcoin).

[6] Meter, Christian, “Design of distributed voting systems,” arXiv preprint arXiv:1702.02566, **(2017)**

[7] Nakamoto and Satoshi, “Bitcoin: A peer-to-peer electronic cash system,” **(2008)**

[8] Cortier, Véronique, Georg Fuchsbauer, and David Galindo, “BeleniosRF: A strongly receipt-free electronic voting scheme,” IACR Cryptology ePrint Archive, **(2015)**

[9] Aziz, Ahmed A. Abu, Hasan N. Qunoo, and Aiman A. Abu Samra, “Using homomorphic cryptographic solutions on E-voting Systems,” **(2018)**

[10] Quaglia, Elizabeth A., and Ben Smyth, “A short introduction to secrecy and verifiability for elections,” arXiv preprint arXiv:1702.03168, **(2017)**