International Journal of Advanced Science and Technology
Vol.118 (2018), pp.13-22
http://dx.doi.org/10.14257/ijast.2018.118.02

Secure Electronic Voting System using Blockchain Technology

D. Dwijesh Kumar[1], D. V. Chandini[1], B. Dinesh Reddy[1], Debnath Bhattacharyya[1] and Tai-hoon Kim[2*]

[1]Computer Science and Engineering Department, Vignan's Institute of Information and Technology, Visakhapatnam-530049, India
[2]Department of Convergence Security, Sungshin Women's University, Bomun-ro 34da-gil, Seongbuk-gu, Seoul, Korea
{dwijesh.daka,chandini2996,dinesh4net}@gmail.com, debnathb@gmail.com
**taihoonn@daum.net*

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 the result is made public everyone can agree upon the final count. This system is simply 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 easier by allowing the voter to vote at his/her location and also reducing the effort put by staff members.

Keywords: *Blockchain, trust, transparency, digitalization, anonymity, security, verification, privacy, accuracy*

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 key 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 the 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 digital voting system. Estonia was the first country to implement this and still continuing it. In the recent election conducted in Estonia about 30.5% of all votes were casted through online. In order to

Received (January 15, 2018), Review Result (April 17, 2018), Accepted (April 23, 2018)
* Corresponding Author

ISSN: 2005-4238 IJAST

provide a better platform for voting we have researched some of the existing systems particularly Estonia[1] and understood their flaws and have come up with a better solution. Estonia provided national ID for each citizen which acted as the main system for voting process. This card helps in the unique identification 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 number 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 casting of 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 a number of 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 appropriate party or not and this can lead to any changes of the casted vote done by 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 a by letting the voter choose a 6 digit PIN. The voter thenlogins the system using the ID and PIN. Upon successful authentication, each voter receives a 12 digit receipt number. In order 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 casted gets stored in the votesblockchain. In this system once the vote is casted, 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 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 have expanded and hardened the security of relational databases. But the major constraint that they suffer from is the 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 Santoshi Nakamoto [7] in the year 2008. He proposed an entirely new system for the exchange of most popular crypto currency called Bitcoin. This technology runs in a decentralized platform where each node can communicate with the other and each node holds a copy of ledger that contains all transactions.

3.1. Algorithm

As shown in Figure 1, 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 transaction and linked with the previous block hash value in order to establish a chain of blocks.

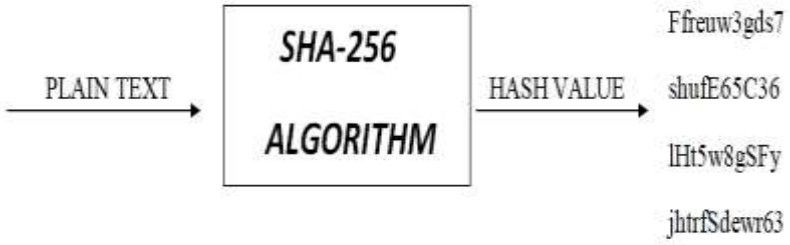

Figure 1. Representation of SHA-256 Algorithm

In our system, 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 (key, value) pairs.

3.2. Steps

a. Initially everyone has to register with their basic details and a PIN is assigned to each voter.

b. Login includes two step verifications, first one with their basic details and the next with the PIN assigned during registration.

c. Voter is then directed to voting page, where he can confirm and cast the vote and after casting another new PIN gets generated.

d. Later, 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 greater risk of tampering of votes. Several research projects say that, in order 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 basic details and a password. Each voter is also assigned with an PIN, which he/she has to remember. The PIN and the password given are used in the login process to ensure high-end authentication.

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

Integrity: The integrity property confirms the elections to take place in a fair and honest way. Each voter can 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 is applicable 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 correct party or not.

5. Proposed System

In our design, we have extended the current process and have come up with new features to meet user expectations at higher level and to provide accurate and fair results, where everyone can agree upon. In order 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 details of all the users.

In our model we have developed an android application which runs using blockchain technology behind it. With this application, every voter who wishes to vote needs to download the app during the election period. This system replaced the earlier system of going to polling station and standing in the queues for long time and created an entirely new platform where voters can vote at their own place in an easy way. The application has a user friendly interface where initially when the voter opens the application it instructs the user about the steps to be followed as shown in Figure 2.

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 basic details in order to register *i.e.*, name, voter_id, National Identification Number (NID), contact number, password and confirm password and this registration page also includes a PIN. During the registration process, the user needs to remember the password given and the PIN assignedfor the further login process. When the user enters all the details and clicks the registration button, all the registration details are sent to the database for verification, validation and upon which the details getsuccesfully stored in the database. Only if the user details do not exist in the database and his/her details are valid then they are allowed to register.

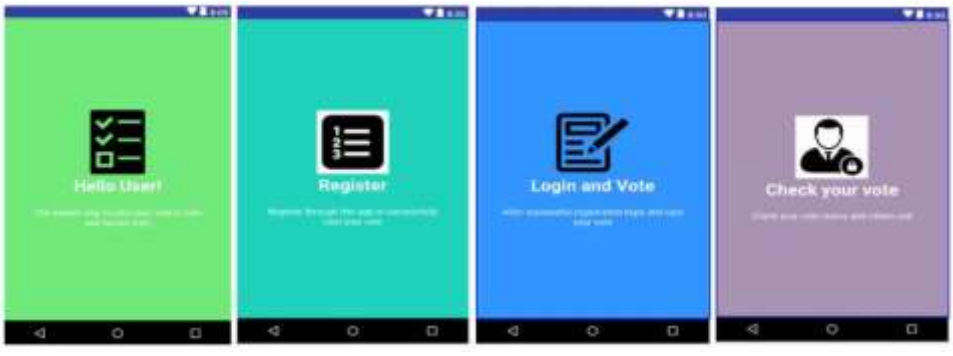

Figure 2. Instructions for New User

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 verification 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 entered 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 VOTERS blockchain, the user details gets displayed on the screen *i.e.*, his respective voter_id and PIN along with the navigation buttons to other page *i.e.*, PROCEED_TO_VOTE and CHECK_STATUS. The entire process of registration, login, and validate_id is shown in Figure 3.

Figure 3. Registration and Log In Process

5.1. Voters Blockchain

The two fields *i.e.*, PIN and voter_id are sent to the VOTERS blockchain as (key, value) pair and are stored in a block as shown in figure 4 and. After registration follows the login process which includes two step verification in order to ensure stronger authentication. This login step can be only done by the users who have already registered.

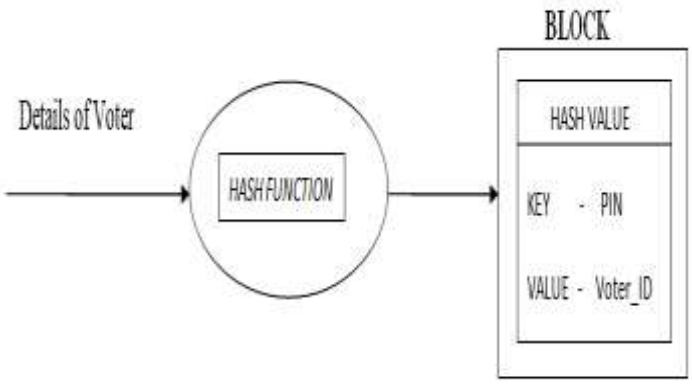

Figure 4. Representation of BLOCK in Voters Blockchain

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 gets successfully casted as shown in the Figure 5. When the user casts his vote, another new PIN gets generated which is specific for each user.

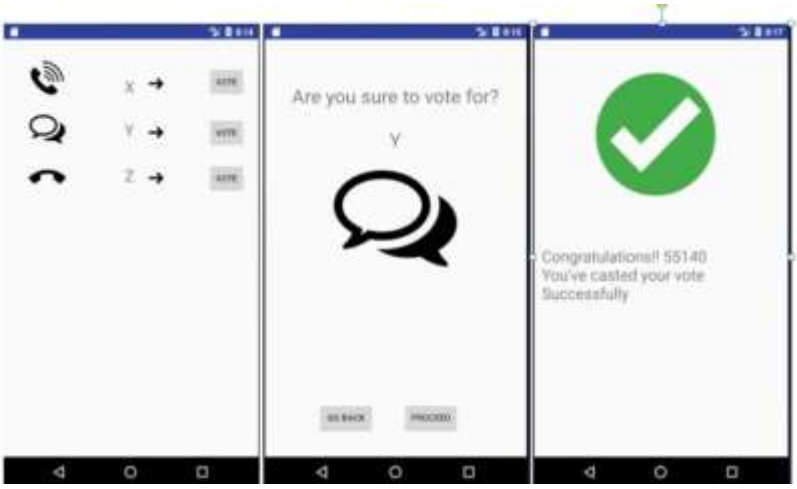

Figure 5. Voting Process

Once the vote gets casted the details gets updated in the database and he is not allowed to vote again. This application also ensures the voters to not to submit a blank vote. If the users tries to login and vote again, the message shown in the Figure 6 gets displayed. Therefore, this property in the system does not allow duplication of votes.

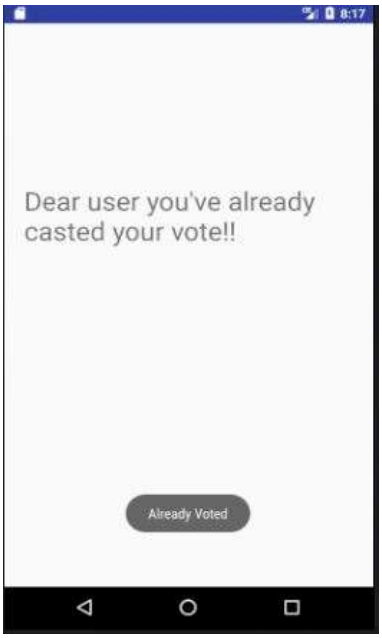

Figure 6. Non-acceptance of Vote by Same User

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. When the user clicks on the check voting status button, it navigates to a new page and 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 as shown in the Figure 7. 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 hold by the other person.

Figure 7. Verification of Votes by User

5.3. Votes Block Chain

As another new PIN gets generated after the casting of vote. The new PIN along with the respective value of vote of each voter is successfully sent to the to the database as well as to the VOTES blockchain as (key,value) pair. The representation of block in the VOTERS blockchain is represented in the Figure 8.

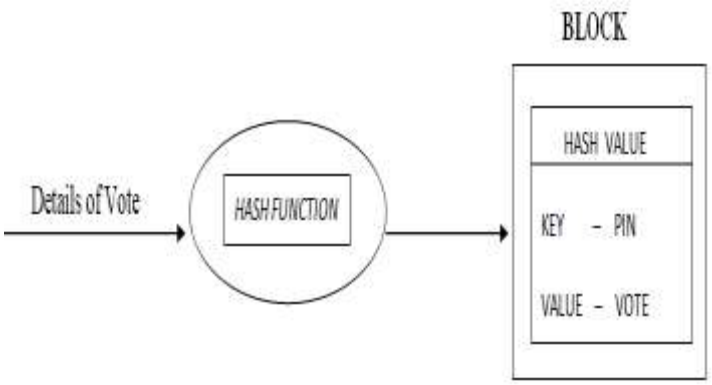

Figure 8. Representation of BLOCK in Votes Blockchain

6. Results

In this model only the admin has 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 the each logo a query runs behind to count all the votes of the respective party and displays the count below the logo. This way the accurate result can be out for each party.

Figure 9. Count of Votes by Admin

7. Stages of e-Voting System

a. 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 the vote. This PIN acts as a key to the database.[6]

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

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

d. 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 block gets created as shown in Figure 10.

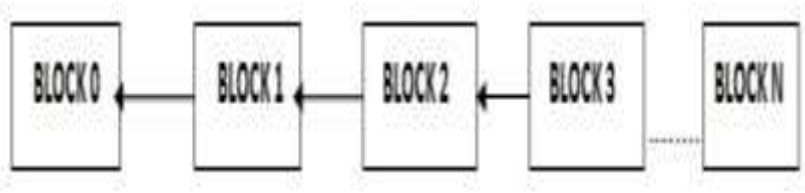

Figure 10. Representation of Blocks in Blockchain

8. Conclusion

With the implementation of leading technology blockchain in this model, we can ensure the voting process to take place in secure and accurate way. With the inclusion ofPIN in this model, it assures the voting to take place in a completely anonymous way. The main important 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 voting process highly secure and also easier for the voters to vote at their own place. This model acts as a step towards digitalization and thereby reduces the effort put by staff members and voters.

References

[1] D. Springall, "Security analysis of the Estonian internet voting system", Proceedings of the 2014 ACMSIGSAC Conference on Computer and Communications Security, ACM, **(2014)**.
[2] M. Kovic, "Blockchain for the people: Blockchain technology as the basis for a secure and reliable e-voting system", **(2017)**.
[3] A. Essex, "Internet Voting in Canada: A Cyber Security Perspective", Online Voting Roundtable, Centre for e-Democracy, **(2016)**.
[4] A. B. Ayed, "A conceptual secure Blockchain-based electronic voting system", International Journal of Network Security & Its Applications, vol. 9, no. 3, **(2017)**.
[5] G. L. Villarreal, "Blockchain (no todo lo que brillaes Bitcoin)".
[6] C. Meter, "Design of Distributed Voting Systems", arXiv preprint arXiv:1702.02566, **(2017)**.
[7] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", **(2008)**.
[8] V. Cortier, G. Fuchsbauer and D. Galindo, "BeleniosRF: A Strongly Receipt-Free Electronic Voting Scheme", IACR Cryptology ePrint Archive 2015, **(2015)**, pp. 629.
[9] A. A. Abu Aziz, H. N. Qunoo and A. A. Abu Samra, "Using homomorphic cryptographic solutions on E-voting Systems", **(2018)**.
[10] E. A. Quaglia and B. Smyth, "A short introduction to secrecy and verifiability for elections", arXiv preprint arXiv: 1702.03168, **(2017)**.

