Blockchain-Enabled E-Voting

Omkar Mangalgiri, Azhar Bekinalkar, Akash Bharsakle, Prof S.N.Shelke

Department of Computer Engineering, Sinhgad Academy of Engineering, Pune

Abstract: This paper gives an implementation of the a robust e-voting scheme which will help to maintain the privacy of voter identity using block chain technology by providing security to voter's personal information. Here the block chain technology for decentralized voting data storage is used. By using this system we can avoid voter identification fraud.

Keywords: E-Voting, Blockchain Technology, Voter Identification, Decentralized Voting, Consensus Algorithm.

1. Introduction

In today's digital world, various systems are interrelating with one another for data exchange. Each relation in between the system is secure and trustworthy. The blockchain is a novel technology provides a cost-effective, consistent, and protected the system for performing and recording any transaction with no need for a middleman. The Blockchain is a concept build to provide distributed and decentralized ledger like functionality for public [2].

E-Voting is a popular concept in the public sector. This includes punched cards, optical scan voting systems etc. But in this system, the voter identification is the main issue because it is difficult to maintain the huge amount of voter's personal data. Most government elections are carried out physically using sealed paper ballots so there are many chances of fraud voting. They misuse the voter identification. The existing system does not find out such voter identification fraud.

To avoid this type of identification fraud Freya Sheer Hardwick et al.[1] proposes the use of blockchain to build such a voting system in which no such kind of fraud will be possible and she also explains all the benefits as well as setbacks of the system.

Again Emre Yavuz et al. [4] provides the idea to solve the fundamental problems faced by the legacy e-voting system through the use of Ethereum network and structure of blockchain. The idea of the security methodology and blockchain which uses unalterable hash chains and to make it more adjustable to be used in polls and elections. A blockchain-based e-voting system that uses "permission blockchain" to facilitate liquid democracy [5]. Liquid democracy is a concept in which the voter has the right, to evaluate his vote was cast in terms of a specific governmental proposal or a bill at any given moment, which give the domain-specific knowledge to the people for better authority of final decisions, which should lead to overall better governance.

Nir Kshetriet al.[6] uses a digital-currency analogy, explains blockchain-enabled e-voting in which every user has some wallet credential. The credentials are just like coins, and a single coin can be used for voting once only.

This paper can overcome the drawbacks by providing top-level security in E-Voting system. With the help of this system, the voter can register their identity information and it is stored with the help of blockchain technology. The election officer can verify the voter identity information. If they are valid voter then the election officer cast the ballot to the particular user. A ballot is cast to the both verified and register ID of the authorized voter. After assigning the ballot to the voter, the voter can vote and submit their ballot to the blockchain based ballot box. The ballot box contains the collection of voter ballot. It provides the security to all submitted ballot. The election officer can announce the final voting result. The voter can verify their vote through the blockchain.

2. PROPOSED SYSTEM

A. System Architecture

Mostly, all the government elections are conducted using the traditional paper ballot system which involves many types of fraud issues such as identity fraud, use of manpower to exploit the people and alter their votes. To avoid such kind of cases we propose a system through the use of blockchain to ensure proper voting environment for the public.

So the main motivation of our in this proposed system is to provide a secure voting environment. The proposed system delivers a dependable and secure e-voting scheme using blockchain. Blockchain-based E-Voting System that works in a decentralized environment based on consensus algorithm. Figure 1 shows the architecture of the proposed system followed by the details working of the system.

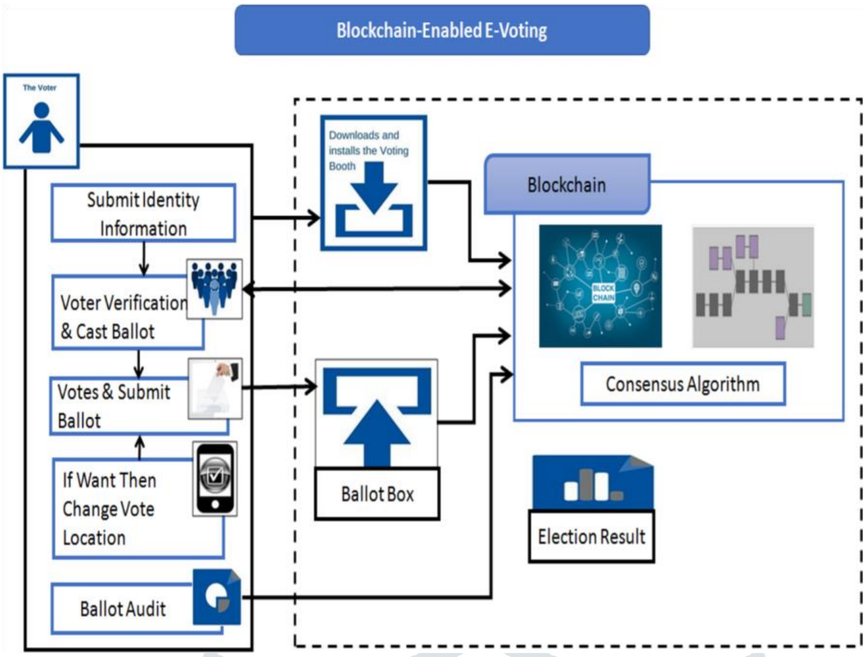

Blockchain-Enabled E-Voting
The Voter
Submit Identity Information
Voter Verification & Cast Ballot
Votes & Submit Ballot
If Want Then Change Vote Location
Ballot Audit
Downloads and installs the Voting Booth
Blockchain
BLOCK CHAIN
Consensus Algorithm
Ballot Box
Election Result

Figure 1.System Architecture

1. **Voter Identity:**

The voter should be registered for voting by giving personal identity information. It is a unique identification of any voter.

2. **Voter Verification:**

The voter is verified by the Election Officer. The officer should be verifying the voter's personal information and their register data. The voter has been authorized to cast a ballot by both the ID verifier and registrar.

3. **Ballot Submission:**

After giving the votes by the voter their ballot is submitted to a secure blockchain based ballot box while retaining anonymity and ballot secrecy. Ballot box contains the collection of voter ballot.

4. **Ballot Audit:**

The voter can use their vote account to go into the ballot box and verify themselves. The voter can even audit each ballot box for confirmation of the accurate election results. All retaining privacy and top-level security.

5. **Election Result:**

Through the ballot box, count final voting result. With help of consensus algorithm, the final election result generated.

B. System Flowchart

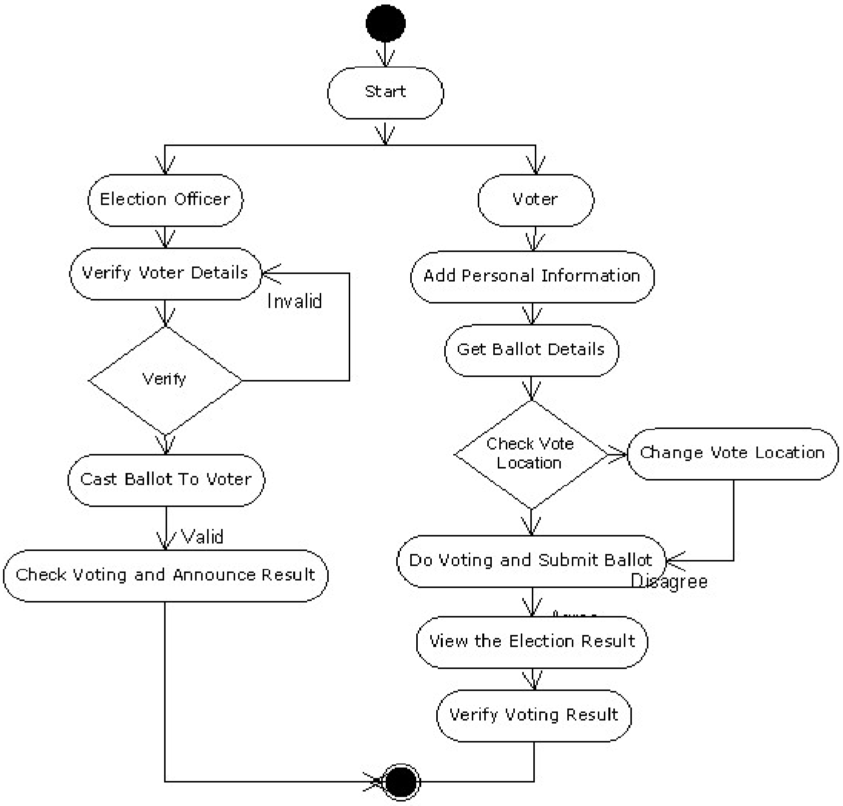


Figure 2.System Flow

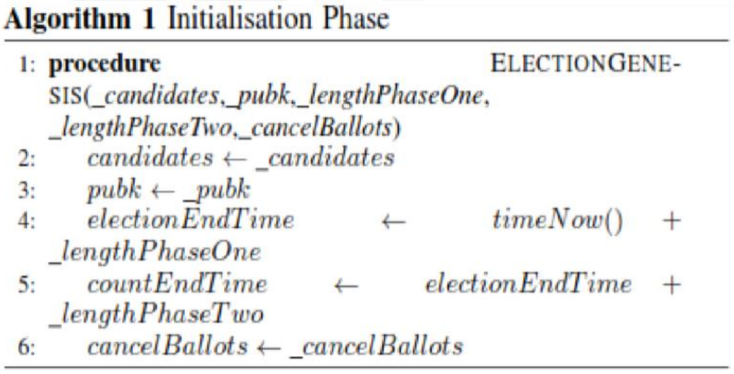
I. ALGORITHMS USED

1. Consensus Algorithm:

In Consensus algorithm work in both decentralized and consortium way. Ethereum used as decentralized/ permission less consensus algorithm. Ethereum [1] [3] is a widely recognized and popular technology. The protocols with similar goals are also available but we had implemented comparative protocols on Ethereum to ensure better results.

1) Initialization Phase:

In the starting phase of election an initial contract has to be put up on the blockchain.(Algorithm 1).

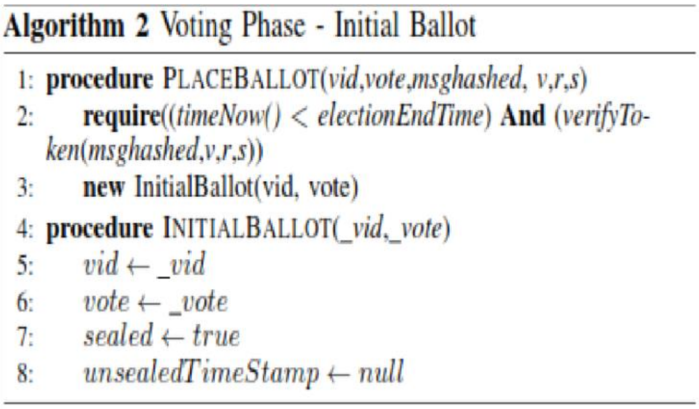


Algorithm 1 Initialisation Phase

```
procedure ELECTIONGENESIS(_candidates,_pubk,_lengthPhaseOne, _lengthPhaseTwo,_cancelBallots)
    $candidates \leftarrow \_candidates$
    $pubk \leftarrow \_pubk$
    $electionEndTime \leftarrow timeNow() + \_lengthPhaseOne$
    $countEndTime \leftarrow electionEndTime + \_lengthPhaseTwo$
    $cancelBallots \leftarrow \_cancelBallots$
```

2) Voting Phase (Initial Ballot):

For the user to cast his vote, it is compulsory for the user to first contact with the CA and get his credentials authorised and the CA will assign a token for his election.

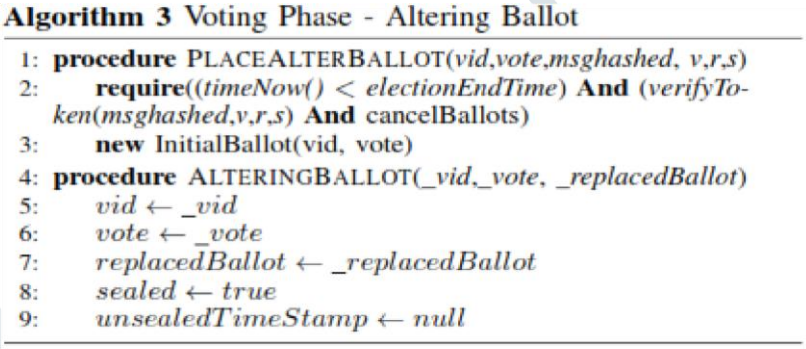


Algorithm 2 Voting Phase - Initial Ballot

```
procedure PLACEBALLOT(vid,vote,msghashed, v,r,s)
    require((timeNow() < electionEndTime) And (verifyToken(msghashed,v,r,s))
    new InitialBallot(vid, vote)
procedure INITIALBALLOT(_vid,_vote)
    vid ← _vid
    vote ← _vote
    sealed ← true
    unsealedTimeStamp ← null
```

3) Voting Phase (Altering Ballot):

The procedure for altering ballot is almost same as the procedure of getting the initial ballot.

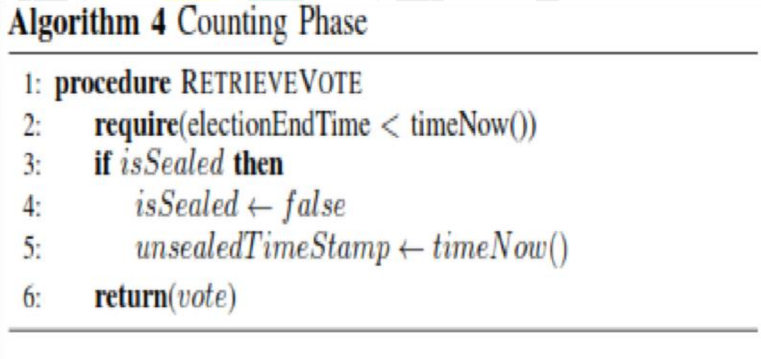


Algorithm 3 Voting Phase - Altering Ballot

```
procedure PLACEALTERBALLOT(vid,vote,msghashed, v,r,s)
    require((timeNow() < electionEndTime) And (verifyToken(msghashed,v,r,s) And cancelBallots)
    new InitialBallot(vid, vote)
procedure ALTERINGBALLOT(_vid,_vote, _replacedBallot)
    vid ← _vid
    vote ← _vote
    replacedBallot ← _replacedBallot
    sealed ← true
    unsealedTimeStamp ← null
```

4) Counting Phase:

After the elections are conducted, the votes are counted after the end date of election.

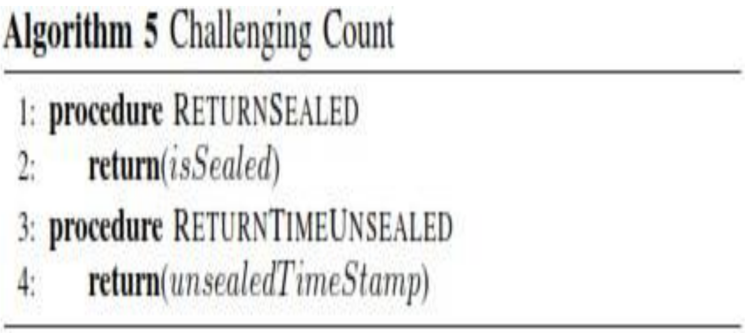


Algorithm 4 Counting Phase

```
procedure RETRIEVEVOTE
    require(electionEndTime < timeNow())
    if isSealed then
        isSealed ← false
        unsealedTimeStamp ← timeNow()
    return(vote)
```

5) Challenging Count:

Blockchain nodes have the capability to verify the upcoming nodes on the chain.



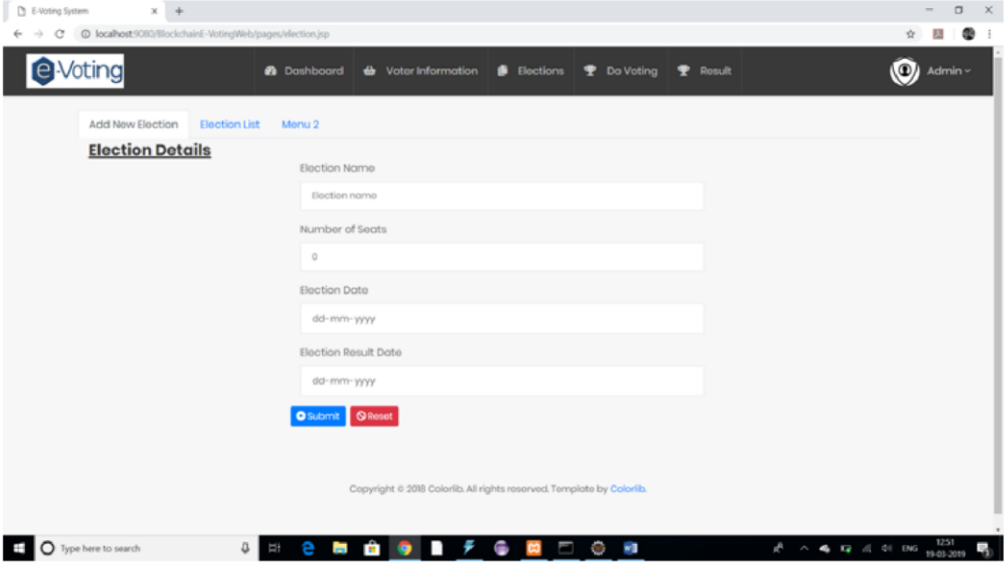
Algorithm 5 Challenging Count

```
procedure RETURNSEALED
    return(isSealed)
procedure RETURNTIMEUNSEALED
    return(unsealedTimeStamp)
```

II. EXPERIMENTAL RESULT

The main purpose of the system is to provide security to voter’s personal information using block chain technology to provide top level security.

The systems GUI was designed in JSP for the server and for the android application the GUI design in XML. Core Technologies used were Ajax, JQUERY, JSP, etc. The overall development was done in the eclipse IDE and for DB we used MY SQL GUI browser. Admin can add the election details like Name, Election Result Date, Election Date and Number of seats.



Election Details

Election Name: Election name

Number of Seats: 0

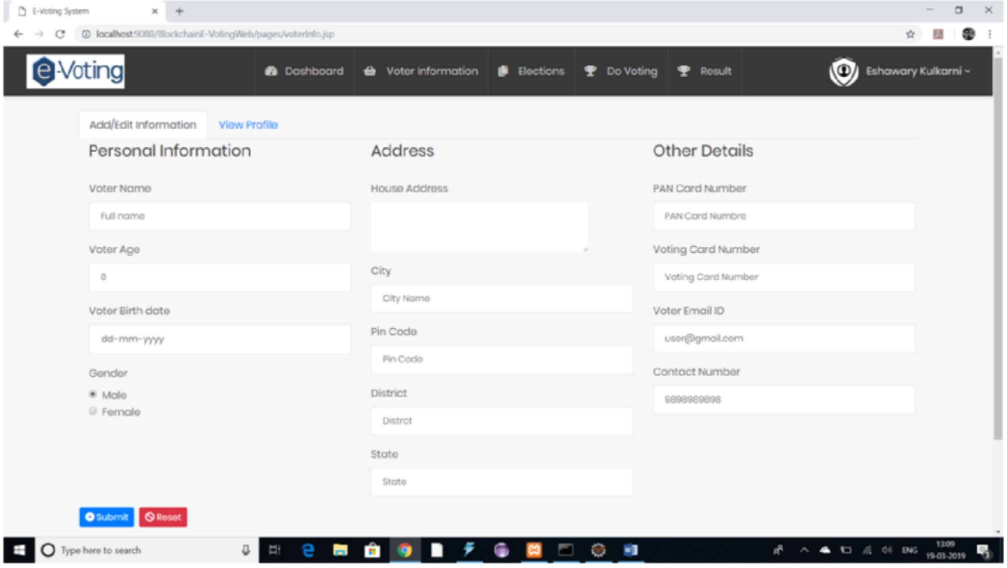
Election Date: dd-mm-yyyy

Election Result Date: dd-mm-yyyy

Copyright © 2018 Colorlib. All rights reserved. Template by Colorlib.

Figure 3. Election Details

Voter should be registered themselves for voting by giving personal identity information given in below figure.



Personal Information

Voter Name: Full name

Voter Age: 0

Voter Birth date: dd-mm-yyyy

Gender: ● Male ○ Female

Address

House Address:

City: City Name

Pin Code: Pin Code

District: Distrct

State: State

Other Details

PAN Card Number: PAN Card Numbre

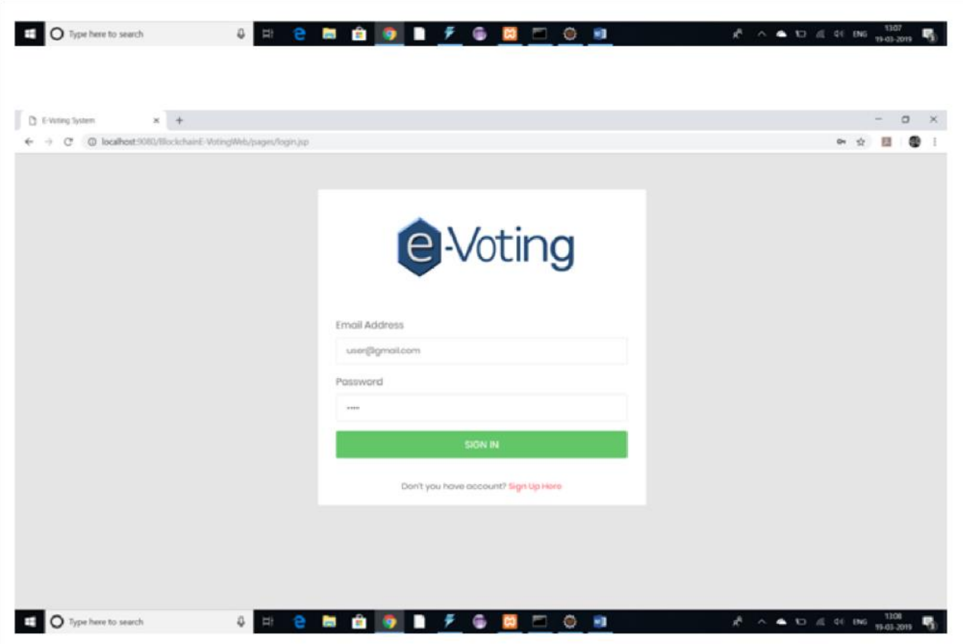
Voting Card Number: Voting Card Number

Voter Email ID: user@gmail.com

Contact Number: 9898989898

Figure 4.Voter Registration

User should have login to the system with Id and password.



Email Address

user@gmail.com

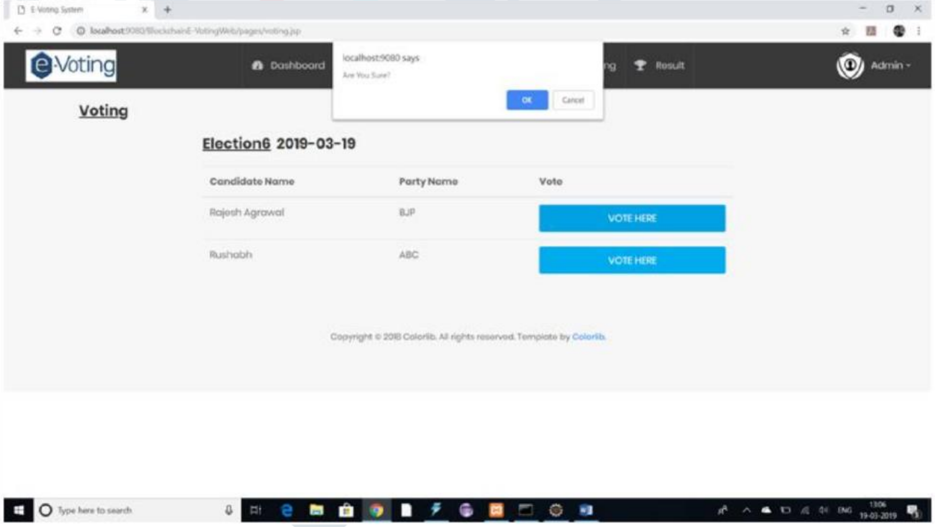
Password

****

Don't you have account? Sign Up Here

Figure 5. Login

After the voter has been authorized to cast a ballot by both the ID verifier and registrar he can submit the vote for particular candidate.



localhost:9080 says

Are You Sure?

Voting

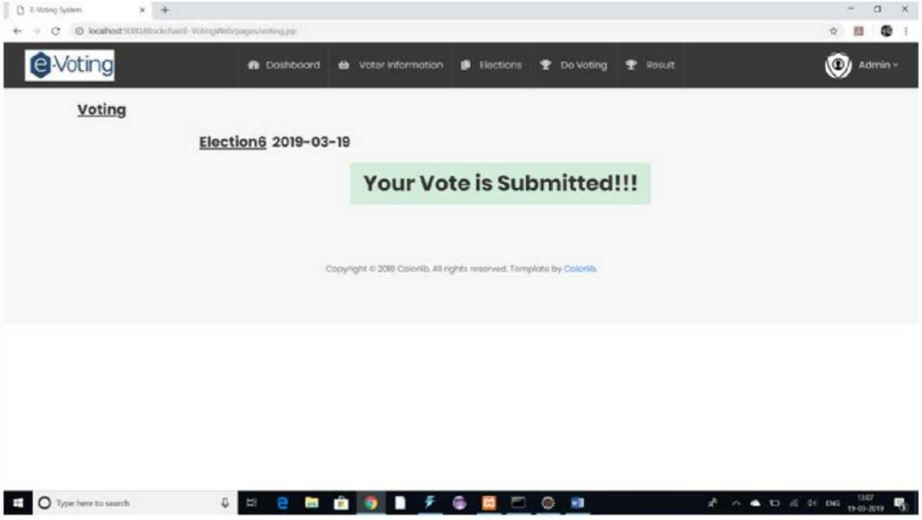
Election6 2019-03-19

Candidate Name	Party Name	Vote
Rajesh Agrawal	BJP	VOTE HERE
Rushabh	ABC	VOTE HERE

Copyright © 2018 Colorlib. All rights reserved. Template by Colorlib.

Figure 6.Voting

After giving the votes by the voter their ballot are submitted to a secure block chain based ballot box.



Voting

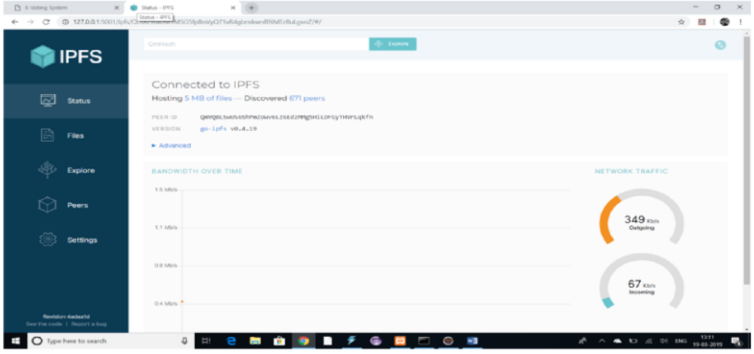
Election6 2019-03-19

Your Vote is Submitted!!!

Copyright © 2018 Colorlib. All rights reserved. Template by Colorlib.

Figure 7.VotingSubmission

IPFS Dashboard:



Connected to IPFS

Hosting 5 MB of files — Discovered 671 peers

PEER ID QmVQBL5wU5s5hPmZoWv6LZ6EdzMMgSHiLDFGyTHVrLqkfn

VERSION go-ipfs v0.4.19

Figure 8.IPFS Dashboard

III. CONCLUSION

Here we have developed a system which provides a security to the voter information and voting details with blockchain technology in voting system. With the help of the system we can also track the voting history from the initial stage to the end of election. With the use of this system election officer can verify the voter details and cast the ballot. The proposed system can access only the authorized user and it can use a blockchain based consensus algorithm for accessing the data. So, in future we implement the system with the fingerprint authentication and blockchain technology.

REFERENCES

1. Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, Konstantinos Markantonakis, “EVoting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy”, 2018.
2. “State of blockchain q1 2016: Blockchain funding overtakes bitcoin,” 2016. . Available: http://www.coindesk.com/state-of-blockchain-q1-2016/.
3. Mattoli, V., Mazzolai, B., Mondini, A., Zampolli, S., & Dario, P., Flexible tag datalogger for food logistics. Sensors and Actuators A: Physical. 2010, 162(2), 316-323.
4. Emre Yavuz, Ali KaanKoç, Umut Can, Çabuk, GökhanDalkılıç, “Towards Secure E-Voting Using Ethereum Blockchain”, 6th International Symposium on Digital Forensic and Security (ISDFS), IEEE, 2018.
5. Si Chen, Rui Shi, Zhuangyu Ren, Jiaqi Yan, Yani Shi, Jinyu Zhang, “A Blockchain-based Supply Chain Quality Management Framework”, 14th, IEEE International Conference on e-Business Engineering, 2017.
6. Bin Yu , Joseph Liu 1 , Amin Sakzad , Surya Nepal , Ron Steinfeld , Paul Rimba , and Man Ho Au "Platform-independent Secure Blockchain-BasedVoting System".