Blockchain Based Secure Voting System Using Iot

Dr.R.Suganya[1], A.Sureshkumar[2], P.Alaguvathana[3], Ms.S.Priyadharshini[4], K. Jeevanantham[5]

[1,2,3,4]Assistant Professor,[5]Student, Department of Information Technology
Sri Krishna College Of Technology, Coimbatore, Tamilnadu, India.
(r.suganya@skct.edu.in, a.sureshkumar@skct.edu.in, alaguvathana.p@skct.edu.in)

Abstract

As there are many revolutionary technologies in the voting system, nowadays people can record their vote by online from their remote places, which saves time and energy. On the other perspective, important aspect that has to be considered is security in online processing system. Block chain technology helps in maintaining the security against cyber-attacks in this application. This system provides distributed architecture of storing the data and this distributed architecture system stores the data among different servers. When the voting is made by the people after their biometric confirmation, the block chain technology helps in converting the votes into the hash value and save them to their corresponding database, where the reliability of the data is maintained. This technology provides transparency in the voting system and apart from the vote count the anonymity of the people will be maintained. This ensures the privacy of the voters. So the proposed system establishes the secured voting system which makes the electronic voting system easily accessible.

Keywords: *E-Voting System, Blockchain, IoT*

1. INTRODUCTION

In the world of democracy peoples have the fullest rights to decide and select an efficient leader to lead them. That decision is finalized by the process of election. The election is done by voting for the candidates who have opted to join in the election. The person who gets the most votes will win the election and he is decided to be the leader by the people, like Abraham Lincoln said “of the people, by the people, for the people”.

To maintain the integrity nowadays election commission is formed. In the starting, the election is done by voting to a candidate by the paper and then many vote rigging has been done in this method. But a same person has voted for more than one time and day by day this was increased dramatically in the election process. To avoid this, election commission has made a great change in the voting process by introducing an E-Voting machine.

This machine consists of multiple buttons and each of the buttons is allocated for the separate candidate’s symbol. When the voters press the button for a candidate, the vote count will be saved in the voting machine. It consists of a memory storage module which stores the data and finally the votes are counted by adding the votes in the machines storage unit. But also in this process, some peoples have done vote rigging by attempting to vote more than one time, and also by hacking the storage module in the voting machine.

To over through all this types of problems we are proposing a system with more security, easy for voting and vote counting which set free time and money for next generation voting process. In this system block chain technology is implemented to provide security against the modifying the voting count through hacking, and the fingerprint module is used to evade the multiple appearances of the voters [1][4].

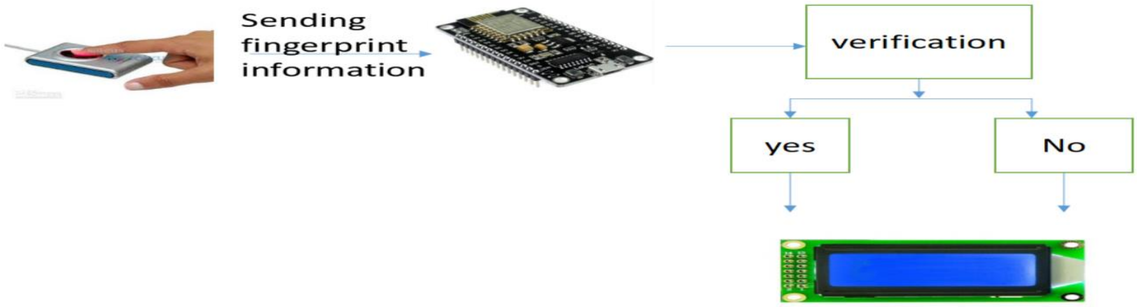


Fig.1 Fingerprint Analyze Module

In this process, the voter's fingerprint is first verified and then they will be processed to the voting process. After the voting process, the vote will be counted and updated into the server then the updated server will save the votes in the separate blockchain. A separate block is created for each candidate and each candidate's vote will be saved in corresponding blocks. Then the data are saved in many different data servers for the backup process. Then the votes will be displayed on the main server and will be monitored. In case of any fraudulent this data will be recovered from the backup data and then voting process is continued.

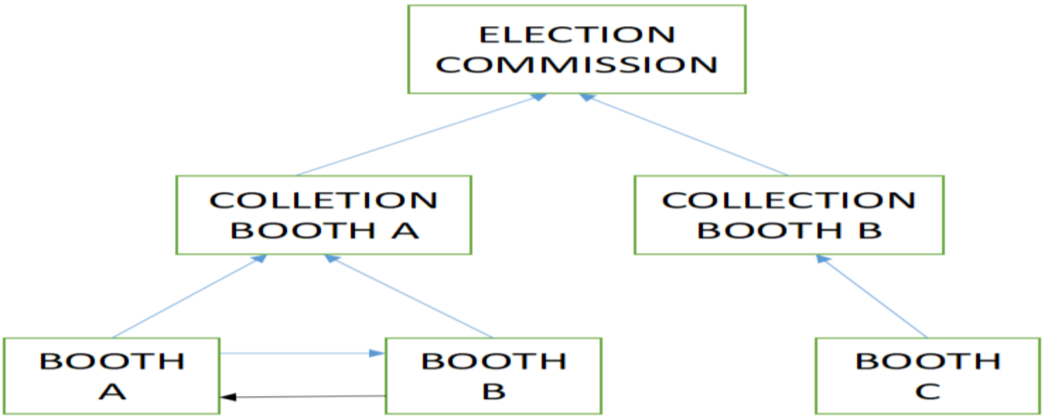


Fig.2 Voting Process Module

The field of blockchain has been drastically improving [14][15] since its introduction in 2008. Initially, blockchain was introduced to build cryptocurrencies. Now research has been going on in this technology to provide security. The main aim is to eliminate the need for a central trusted third party. It uses decentralized systems wherein the data are distributed among the servers. Blockchain technology is grounded on distributed ledger technical knowledge which may be used in financial, real estate, logistics, election, and survey. The distributed ledger mechanism consists of several nodes where each node is connected to every other network and each node has an entire copy of the blockchain. Generally it is a p2p network [16][17]. When any new transaction is added to the current copy, the block is broadcasted to all nodes. So, when the attackers try to change the data of the vote count that can be identified easily. If the majority of the nodes vote for the same copy, then the data is true. Blockchain technology uses cryptographic hashing functions like MD5, SHA 256, etc. The basic block structure of blockchain involves block number, data, nonce, block hash, previous block hash where the very first block is named as genesis block and the nonce value is used to add leading zeros. A large number of zeros means more confidentiality. The transactions are stored in a tree-like structure and the data is modified as hash value grounded on blockchain methodology. When the attacker tries to change the data in a particular server, the data from the other server is crosschecked and verified. If any changes in the data among the servers in the decentralized system, it is confirmed that the attack has been done.

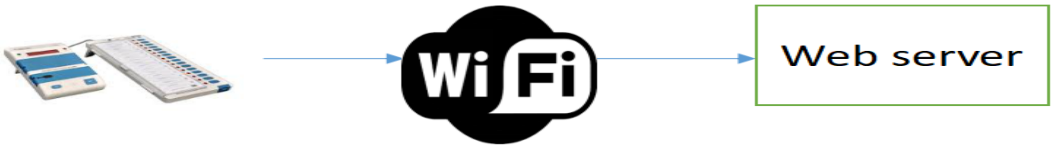


Fig.3 Server module

2. RELATED WORKS

The voter authentication mentioned in this study [2] helps in authenticating the voter with enhanced accuracy. This system provides the execution time of the process that makes the voter to vote easily without spending much time .The bilinear pairing in this study establishes a security mechanism which reduces the size of data storage [18]. The main thing is that it ensures the anonymity of voters.

Vishal, rishabh and vibhu [3] has proposed the online voting system using aadhar. This study helps in the use of unique identification of a person in the voting mechanism.`The study of decentralisation and voter privacy [5] enhances the decentralized mechanism of storing the data that improves the transparency. The block chain highly helps in keeping the privacy of the voters.The study proposed by fridrik , hjalmarsson, gunnlaugur [6] helps in evaluating the difference between the existing voting system and the block chain voting system. The different implementation of block chain in bit coins like ethereum will also be used to build the smart contracts enabling secure election.

The block chain based voting in this system [7][8] proposed by sagarshah et.al & Kashif et.al ensures the block chain implementation using distributed ledger technology that allows the p2p network in identifying the suspected nodes [9][10]. This procedure consists of four modules which include the use of the fingerprint sensor, NODEMCU, vote machine, display, web server and vote monitoring components.

The first module includes the identification and analysis of the finger print of the voter and then the voting process is continued by the voting machine and then the votes are encrypted as a hash value and stored. This voting is secured by block chain technology. This vote will be monitored by the main server and the multiple copies of this data are stored in the multiple secure servers in different areas, to avoid any cyber-attack and this helps in providing a secure voting process.

3. METHODLOGIES

The general module of this system consists of an fingerprint module which is attached to the NODEMCU and to an LCD display. the second part consists of the voting machine which is linked to the server

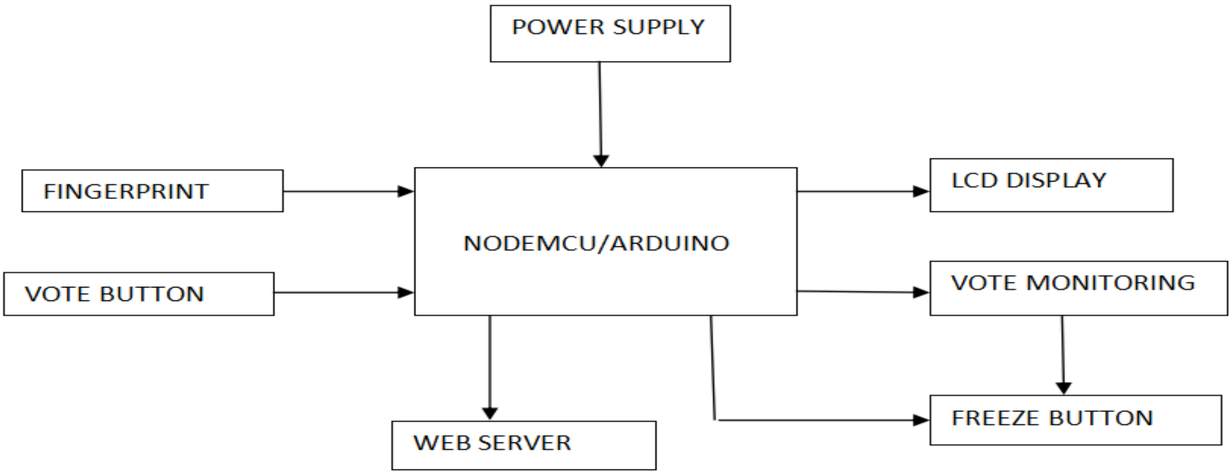


Fig.4 Block Diagram

(1) **Inviting to vote:** The user will have to log in to the polling system using his identifications. In our arrangement, the E-Voting system will use his finger print information presents in Aadhar card, and the voting confirmation details are provided back to registered voters by the local authorities. The procedure will check all data entered and, if matched with a valid voter, the user will be authorized to cast a vote. This E-Voting system won't allow members to create their individual identities and record to vote.

(2) **Casting a vote:** Voters can have two choices; vote for one of their favorite applicants or make it as protest vote. Voting can be done by a simple sophisticated user interface.

(3) **Encryption of votes:** After the user casts his vote, the system will produce information that holds the voter identification number, the name of the voter and hash value of the preceding vote. Like this, each input will be exclusive and also guarantee the unique encrypted output. The data associated with each vote will be encrypted using SHA-256, which is one of the hash functions, will be saved in the block header of each vote cast. This type of hashing votes is impossible for reverse engineer and therefore there are no ways to retrieve the voters' information.

(4) **Moving the vote to Blockchain:** A separate block is generated based on the candidate nominated, the data is saved in the respective Blockchain and every block gets connected to it's the earlier vote.

4. VOTING PROCESS

Voting is the process of electing the candidates. Generally in a democratic nation election plays a major role in choosing the right person. The voters are allowed for the voting process once for an election. To maintain the integrity in this election, the voter are only allowed to vote after their biometric and basic information is verified. The voters can vote to their beloved candidate by pressing the corresponding button of their beloved candidate's symbol once. The vote count of the corresponding candidate is updated to the main sever and then converted into hash value and stored in block which forms block chain.

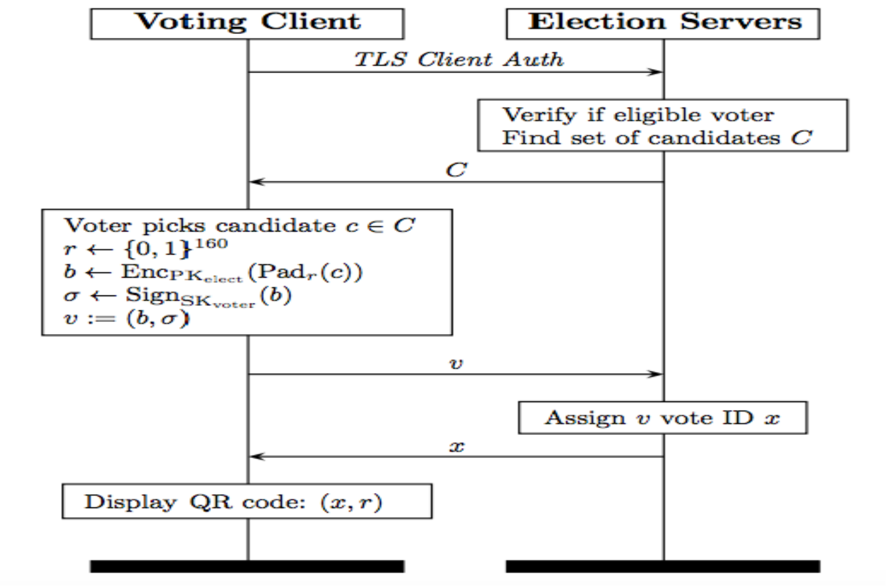

Voting Client
Election Servers
TLS Client Auth
Verify if eligible voter
Find set of candidates C
C
Voter picks candidate $c \in C$
$r \leftarrow \{0,1\}^{160}$
$b \leftarrow \mathrm{Enc}_{PK_{elect}}(\mathrm{Pad}_r(c))$
$\sigma \leftarrow \mathrm{Sign}_{SK_{voter}}(b)$
$v := (b, \sigma)$
v
Assign v vote ID x
x
Display QR code: (x, r)

Fig.5 Voting Cycle

Citizens were able to cast their vote using only the internet connection and an Aadhar card. The Aaddhar ID to be used in this system should be designed to run on an Java platform and to be protected with 2048 bit PIN [11]. It should be able to generate signatures using SHA1/SHA2 [12] and the card is simply used for authentication and encryption. The voter has to authenticate using this ID, and if the voter is qualified to vote, the candidates list will be showed and a voting can be done. Then vote will be encoded using the voting's public key and signed with the voter private key. Once the voting is done, it will be sent to a storage server which is controlled by the blockchain [13]. If the voter presses the button multiple times, only the last pressing will be considered as a valid one. This is done to prevent vote buying.

5. BLOCKCHAIN CREATION & FRAUDULENT IDENTIFICATION

Block chain is the chain like link of blocks that contains information and it is decentralized one. It is generally used for secure transmission between the source and destination without any intermediate. It also is used to transfer money and confidential information. Once the information or data is added inside a block chain, it is hard to change.

5.1 GENESIS BLOCK

This is the very first block in the block chain. When a new block chain is created the genesis block should be created immediately.

```
class BlockChain
{   public function __construct()
{
$this->chain = [$this->createGenesisBlock()];
$this->difficulty = 3;
  }
private function createGenesisBlock()
 {
 return new Block(0, strtotime("2018-01-01"), "Genesis Block");
 }
```

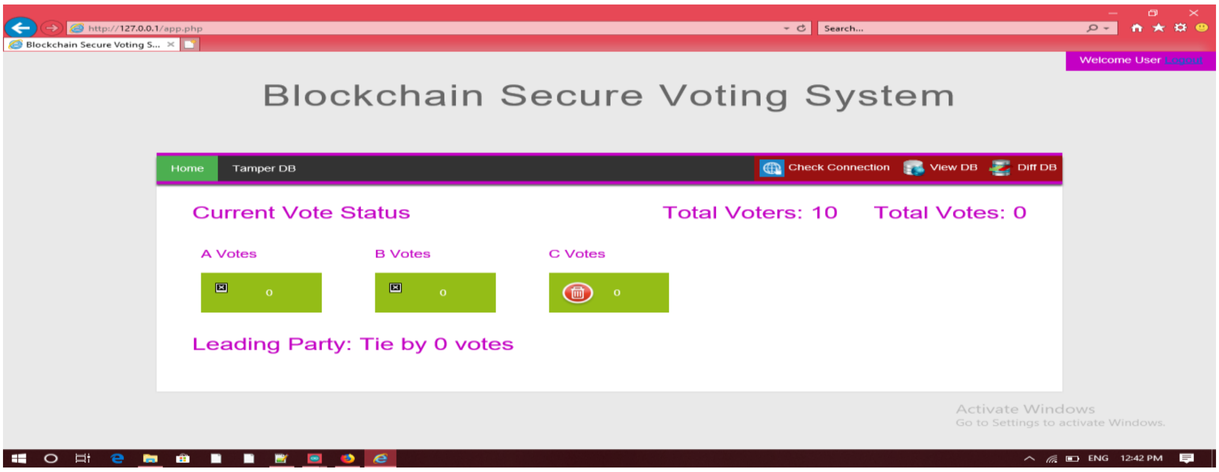
5.2 ADDING NEW BLOCKS

Before adding the new block we should know the last block in the chain, so that only we can able to attach more blocks. For identifying the last block we are using getLastBlock() function.

```
 public function getLastBlock()
 {
 return $this->chain[count($this->chain)-1];
  }
```

For adding the new block we are using the push function to insert the block. The newly created block has the hash value of the foregoing block.

```
public function push($block)
 {
$block->previousHash = $this->getLastBlock()->hash;
$this->mine($block);
array_push($this->chain, $block);
 }
```



Blockchain Secure Voting System

Current Vote Status Total Voters: 10 Total Votes: 0

A Votes 0

B Votes 0

C Votes 0

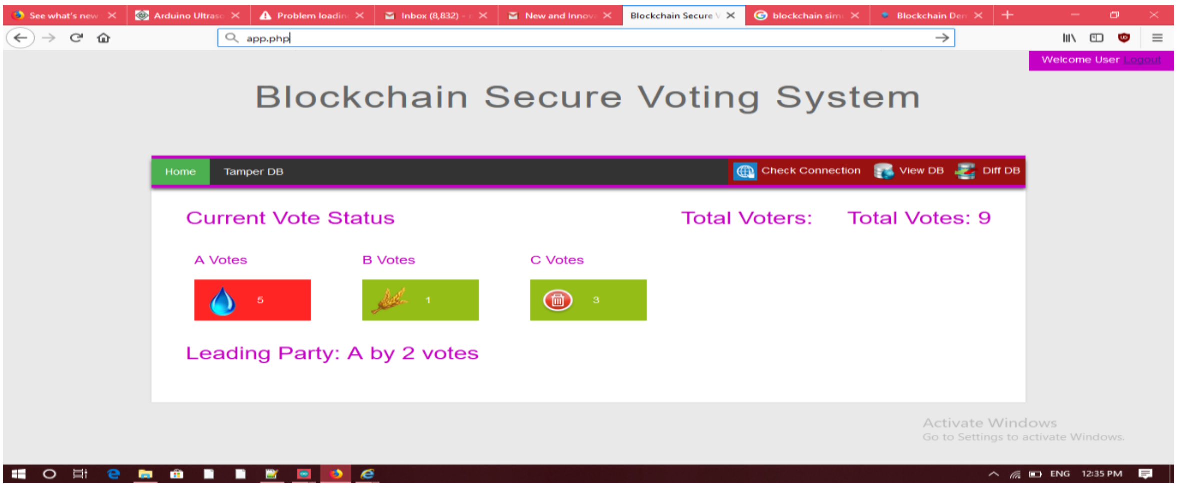
Leading Party: Tie by 0 votes

Fig.6 Adding blocks to chain

5.3 VALIDATING THE BLOCKS

The blocks are validated and attached to the block chain by using the mine function.

```
 public function mine($block)
{
while (substr($block->hash, 0, $this->difficulty) !== str_repeat("0", $this->difficulty)) {
$block->nonce++;
$block->hash = $block->calculateHash();
}
```



Blockchain Secure Voting System

Current Vote Status

Total Voters:

Total Votes: 9

A Votes	B Votes	C Votes
5	1	3

Leading Party: A by 2 votes

Fig.7 Validating the block

5.4 FRAUDULENT IDENTIFICATION

The vote count is being updated simultaneously on the server and the corresponding hash value of the count is being stored. The hash value of the present count is provided to the next hash by using the block chain. If there is any change in the values of the vote count, the hash value will change and it is reflected to the entire chain. If the chain breaks, the notification will be sent to the admin and the process of voting in the particular area will be stopped. After the recovery process, the voting progress will take place.

Generation of hash value

Data 1

Previous hash : 0

Hash: 000dc75a315c77a1f9c98fb6247d03dd18ac52632d7dc6a9920261d8109b37cf

Data 20,000

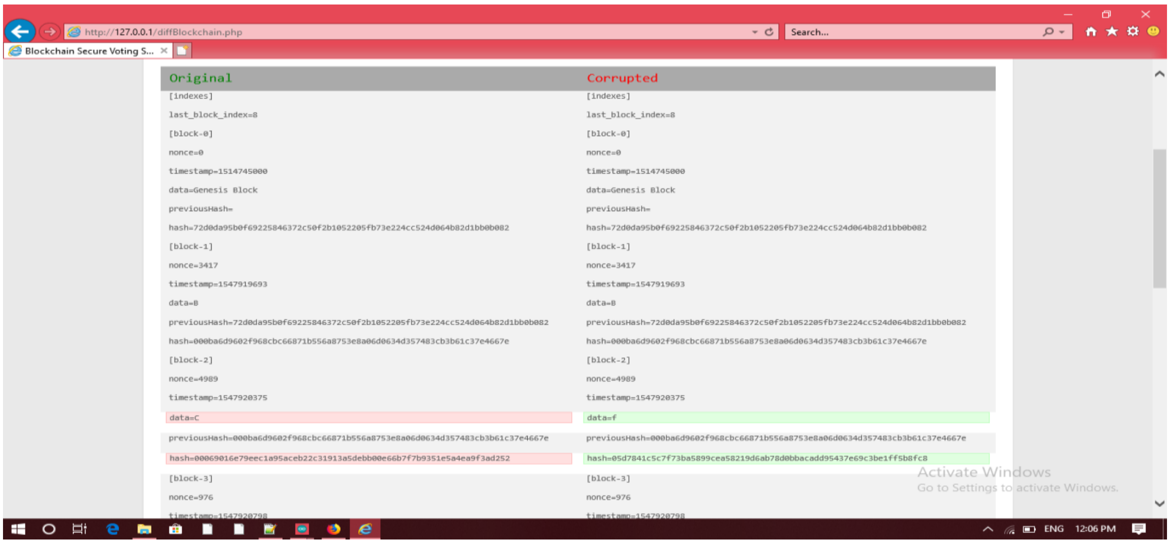
Previous hash : 000dc75a315c77a1f9c98fb6247d03dd18ac52632d7dc6a9920261d8109b37cf

Hash : 000756bbee63cb615c36e5ef8f5059a46af0c9626851948df5e3e412d2b1db66

If anybody tries to change the data, the hash value will change. While validating , the block has different values and it will collapse the entire chain.

Data 2,000

Previous hash: ba6cfadb243205194ea738248c6d10c212865263b1b6dd453f650b3ecf8d7669


http://127.0.0.1/diffBlockchain.php
Blockchain Secure Voting S...
Search...
Activate Windows
Go to Settings to activate Windows.
ENG
12:06 PM

```
Original
[indexes]
last_block_index=8
[block-0]
nonce=0
timestamp=1514745000
data=Genesis Block
previousHash=
hash=72d0da95b0f69225846372c50f2b1052205fb73e224cc524d064b82d1bb0b082
[block-1]
nonce=3417
timestamp=1547919693
data=B
previousHash=72d0da95b0f69225846372c50f2b1052205fb73e224cc524d064b82d1bb0b082
hash=000ba6d9602f968cbc66871b556a8753e8a06d0634d357483cb3b61c37e4667e
[block-2]
nonce=4989
timestamp=1547920375
data=C
previousHash=000ba6d9602f968cbc66871b556a8753e8a06d0634d357483cb3b61c37e4667e
hash=00069016e79eec1a95aceb22c31913a5debb00e66b7f7b9351e5a4ea9f3ad252
[block-3]
nonce=976
timestamp=1547920798
```

```
Corrupted
[indexes]
last_block_index=8
[block-0]
nonce=0
timestamp=1514745000
data=Genesis Block
previousHash=
hash=72d0da95b0f69225846372c50f2b1052205fb73e224cc524d064b82d1bb0b082
[block-1]
nonce=3417
timestamp=1547919693
data=B
previousHash=72d0da95b0f69225846372c50f2b1052205fb73e224cc524d064b82d1bb0b082
hash=000ba6d9602f968cbc66871b556a8753e8a06d0634d357483cb3b61c37e4667e
[block-2]
nonce=4989
timestamp=1547920375
data=f
previousHash=000ba6d9602f968cbc66871b556a8753e8a06d0634d357483cb3b61c37e4667e
hash=05d7841c5c7f73ba5899cea58219d6ab78d0bbacadd95437e69c3be1ff5b8fc8
[block-3]
nonce=976
timestamp=1547920798
```

Fig.8 Fraud Identification

6. CONCLUSION

The proposed system is successful in providing security for the votes that can change the entire life of the people. The proposed system uses block chain and hashing methodology to provide the anonymity of the voter. The security of the vote count is much higher than the conventional technology and also it reduces the time in vote counting. This can be easily implemented in the polls, which also reduces the man power. Block chain technology is now booming in various applications like logistics, real estate, certificate verification and smart city applications. The efficiency and reliability of the proposed system is well higher than the existing technologies.

The presence of the distributed system in block chain technology provides transparency. The centralized system in the conventional technology can be replaced by the distributed ledger technology which can prevent the attackers from modifying the result of an election. Thus by using this system, democracy can be maintained. In future both IoT and block chain can pave the way for new technologies that make our transactions more secured and connected everywhere.

In this proposed system, we are planning to merge the fingerprint module and the voting machine into a single component. So that we can directly verify the ID using fingerprint while voting in the voting machine, which decreases the time consumption.

References

[1]. Rahil Rezwan ; Huzaifa Ahmed ; M. R. N. Biplob ; S. M. Shuvo ; Md. Abdur Rahman., "Biometrically secured electronic voting machine" , IEEE Region 10 Humanitarian Technology Conference, 2017

[2]. Himanshu Agarwal ; G. N. Pandey. "Online voting system for India based on AADHAAR ID" Paper available at: https://ieeexplore.ieee.org/document/6756265

[3]. Vishal ; Vibhu Chinmay ; RisabhGarg; PoonamYadav "Online voting system linked with AADHAR" 3rd International Conference on Computing for Sustainable Global Development (INDIACom) Paper available at : https://ieeexplore.ieee.org/document/7724864

[4] Jameer Basha A Palanisamy V Purusothaman T ," Efficient multimodal biometric authentication using fast fingerprint verification and enhanced iris features" , Journal of Computer Science, 2011, vol 7, issues 5, pp 698 – 706.

[5] Gautam Srivastava, Ashutosh Dhar Dwivedi and Rajani Singh A Decentralized Voting Scheme using Blockchain Technology A Decentralized Voting Scheme using Blockchain Technology**,** Paper available at : www.insticc.org/Primoris/Resources/PaperPdf.ashx?idPaper=68819

[6] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson.” Blockchain-Based E-Voting System”,Paper available at :https://skemman.is/bitstream/1946/31161/1/Research-Paper-BBEVS.pdf

[7]. Sagarshah , Qaishkanchwala , huaiqian mi . “Blockchain voting system”, Paper available at: https://www.economist.com/sites/default/files/northeastern.pdf

[8]. Kashif Mehboob Khan, Junaid Arshad, Muhammad Mubashir Khan, “Secure Digital Voting System based on Blockchain Technology” Paper Available at : https://pdfs.semanticscholar.org/c1f0/b096f9ce1b17bea2d39ee760aaede9829d29.pdf

[9]. Gaby G. Dagher, Praneeth Babu ,Marella, Matea Milojkovic, and Jordan Mohler. BroncoVote: Secure Voting System using Ethereum’s Blockchain, Paper Available at: https://www.scitepress.org/papers/2018/66097/66097.pdf

[10] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system

[11] Ethereum Blog. (2018). On Public and Private Blockchains - Ethereum Blog. Available at: https://blog.ethereum.org/2015/08/07/ on-public-and-private-blockchains

[12] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis:E- Voting with blockchain: An E-Voting Protocol, Paper Available at:https://arxiv.org/pdf/1805.10258.pdf

[13] Nir Kshetri and Jeffrey Voa . Blockchain-Enabled E-Voting”, Paper Available at : https://www.researchgate.net/publication/326239528Blockchain-Enabled_E-Voting

[14] Rockwell, M. (2017) Bitcongress - Process for block voting and law, Paper Available at : http://bitcongress.org/ last accessed: December 2017

[15] D. Ashok Kumar ; T. Ummal Sariba Begum .,“Electronic voting machine “,Paper Available at:https://ieeexplore.ieee.org/document/6208285

[16] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos MarkantonakisE-Voting with Blockchain: An E-Voting Protocolwith Decentralisation and Voter Privacy Paper Available at:https://arxiv.org/pdf/1805.10258.pdf

[17]. Punithavathani D.S., Sankaranarayanan, ” IPv4/IPv6 transition mechanisms”, European Journal of Scientific Research, vol 34, issue 1,2009, pp 110-124.

[18] Sivaram Kumar V., Thansekhar M.R., Saravanan R., Miruna Joe Amali S.,” Solving multi-objective vehicle routing problem with time windows by FAGA”, Procedia Engineering, vol 97,2014, pp 2176-2185.