E-voting using block chain Technology

Prof. Pallavi Shejwal[1], Aditya Gaikwad[2], Mayur Jadhav[3], Nikhil Nanaware[4], Noormohammed Shikalgar[5]

[1]Assistant Professor, [2,3,4,5]BE Students
Department of Information Technology,
BSIOTR, Pune, Maharashtra, India

***Abstract*: Increasing digital technology has revolutionized the life of people. Unlike the electoral system, there are many conventional uses of paper in its implementation. The aspect of security and transparency is a threat from still widespread election with the conventional system (offline). General elections still use a centralized system, where in one organization manages it. Some of the problems that can occur in traditional electoral systems is with the organization that has full control over the database and system. It is possible to tamper with the database of considerable opportunities. Block chain technology is one of solutions; because it embraces a decentralized system and the entire database are owned by many users. Block chain itself has been used in the Bitcoin system known as the decentralized Bank system. By adopting block chain in the distribution of databases on e-voting systems one can reduce the cheating sources of database manipulation. This project aims to implement voting result using block chain algorithm from every place of election. Unlike Bitcoin with its Proof of Work, this will be a method based on a predetermined turn on the system for each node in the built of block chain.**

***Keywords*: Security and Protection, Hardware, Online Information Services**

1. INTRODUCTION

Lately, electronic voting systems have begun being used in many countries. Estonia was the first in the world to adopt an electronic voting system for its national elections [1]. Soon after, electronic voting was adopted by Switzerland for its state-wide elections [2], and by Norway for its council election [3]. For an electronic voting system to compete with the traditional ballot system, it has to support the same criteria the traditional system supports, such as security and anonymity. An e-Voting system has to have heightened security in order make sure it is available to voters but protected against outside influences changing votes from being cast, or keep a voter's ballot from being tampered with. Many electronic voting systems rely on Tor to hide the identity of voters [4]. However, this technique does not provide total anonymity or integrity since many intelligence agencies around the world control different parts of the Internet which can allow them to identify or intercept votes.

2. LITERATURE SURVEY

Increasingly digital technology in the present helped many people lives. Unlike the electoral system, there are many conventional uses of paper in its implementation. The aspect of security and transparency is a threat from still widespread election with the conventional system (offline).Block chain technology is one of solutions, because it embracesa decentralized system and the entire database are owned by many users.[1]

Bit coin introduces a revolutionary decentralized consensus mechanism. However, Bit coin-derived consensus mechanisms applied to public block chain are inadequate for the deployment scenarios of budding consortium block chain. We propose a new consensus algorithm, Proof of Vote (POV).The former guarantees the separation of voting right and executive right, which enhance the independence of bulter's role, so does the internal control system within the consortium. As for the latter, under the circumstance that at least Nc/2+1 commissioners are working effectively, our analysis shows that POV can guarantee the security, transaction? [2]

There is no doubt that the revolutionary concept of the blockchain, which is the underlying technology behind the famous crypto currency Bitcoin and its successors, is triggering the start of a new era in the Internet and the online services. In this work, we have implemented and tested a sample e-voting application as a smart contract for the Ethereum network using the Ethereum wallets and the Solidity language.[3]

Block chain was first introduced by Satoshi Nakamoto (a pseudonym) , who proposed a peer to-peer payment system that allows cash transactions through the Internet without relying on trust or the need for a financial institution. Block chain is secure by design, and an example of a system with a high byzantine failure tolerance.[4].

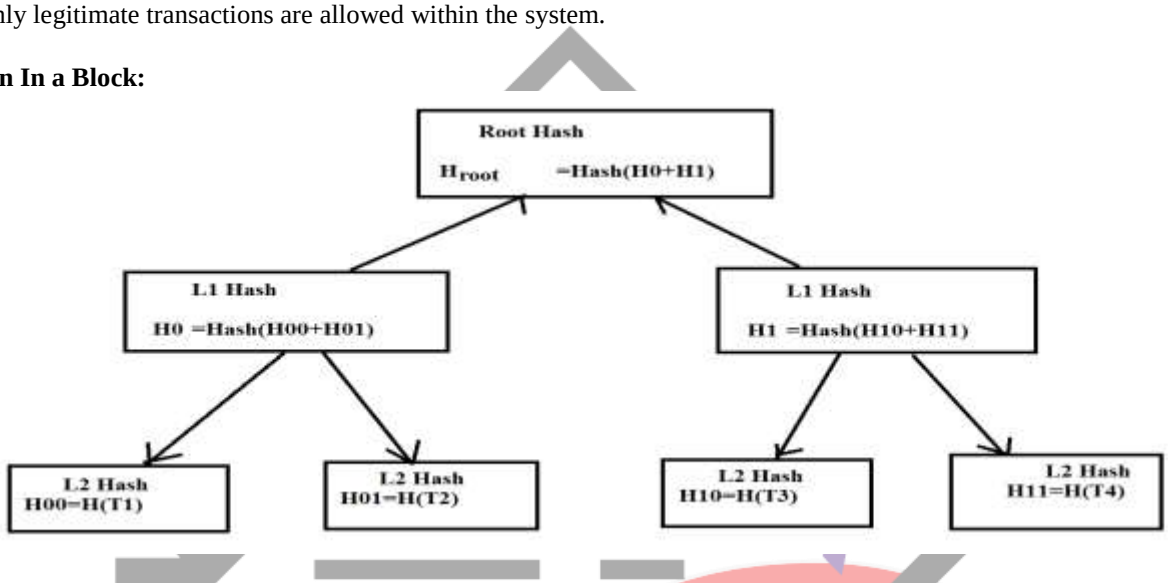
Proof of stake protocol of block verification does not rely on excessive computations. It has been implemented for Ethereum and certain altcoins. Instead of splitting blocks across proportionally to the relative hash rates of miners (i.e. their mining power), proof-of-stake protocols split stake blocks proportionally to the current wealth of miners. The idea behind Proof of Stake is that it may be more difficult for miners to acquire sufficiently large amount of digital currency than to acquire sufficiently powerful computing equipment.[5]

3. RELATED WORK

2.1 Open Block Chain: A blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree. Each block includes the cryptographic hash of the prior block in the blockchain, linking the two. The linked blocks form a chain. This iterative process confirms the integrity of the previous block, all the way back to the original genesis block. Blockchain technology aims at creating a decentralized environment where no third party is in control of the transactions and data. It is used in several domains due to its benefits in distributed data storage and the possibility of audit trails.

2.2 Closed Block Chain: A private network that maintains a shared record of transactions. The network is accessible only to those who have permission and transactions can be edited by administrators. Permission Block chain inversely proportional to the previous type, operated by known entities such as consortium block chains, where consortium members or stakeholders in a particular business context operate a Block chain permission network. This Block chain permission system has means to identify nodes that can control and update data together, and often has ways to control who can issue transactions. Private block chain is a special block chain permitted by one entity, where there is only one domain trust. The widely known Block chain technology currently exists in the Bitcoin system which is the public ledger of all transactions. Bitcoin is a decentralized, peer-to-peer digital payments system based on the first public key cryptography. Bitcoin uses a consensus protocol called PoW (Proof of Work) based on crypto currency to ensure only legitimate transactions are allowed within the system.

Transaction In a Block:

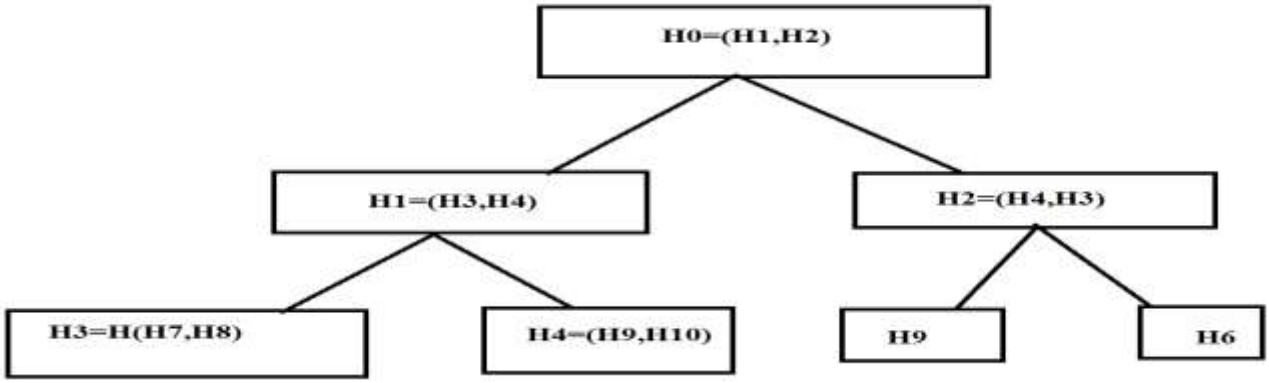


2.3 Cryptography: is used to preserve privacy and transparency at the same time, economic incentives are used to encourage desired behaviour of network actors who do not trust or know each other, nor have any legally binding agreements with each other. Cryptography is the practice and study of techniques for secure communication in the presence of third parties. Cryptography literature often uses the name Alice "A" for the sender, Bob "B" for the intended recipient, and Eve "Eavesdropper" for the adversary. There are two kinds of cryptosystems: symmetric and asymmetric.

1. Symmetric Cryptography: Two parties agree on a secret key (private key) and use the same key for encryption and decryption. The problem with this approach is that this method does not scale. If you wanted to communicate privately with somebody you would need to physically meet and agree on a secret key. In the world of modern communications, where we need to coordinate with many actors, such methods would not be feasible. Furthermore. Data manipulation in symmetric systems is faster than asymmetric systems as they generally use shorter key lengths. On the other hand, encrypting files and messages with asymmetric algorithms might not always be practical. The main reason is performance. Symmetric key cryptography is much faster and handles better the encryption of big files and databases, therefore, is still widely used.

2. **Asymmetric Cryptography (Public Key Cryptography):** Asymmetric systems use a public key to encrypt a message and a private key to decrypt it. Use of asymmetric systems enhances the security of communication. Private keys should be kept secret and a public key could be freely distributed between parties. In an asymmetric encryption scenario, two parties would distribute their public keys and allow anyone to encrypt messages using their public keys. Because of how a key pair mathematically works it is impossible to decrypt a message which got encrypted with a public key.

2.4 Merkle tree : In cryptography and computer science, a **hash tree** or **Merkle tree** is a tree in which every leaf node is labeled with the hash of a data block and every non-leaf node is labeled with the cryptographic hash of the labels of its child nodes. Hash trees allow efficient and secure verification of the contents of large data structures. Hash trees are a generalization of hash lists and hash chains.



2.5 Role Of Miner: This process begins when the voting process at each node has been completed. Before the election process begins, each node generates a private key and a public key. Public key of each node sent to all nodes listed in the election process, so each node has a public key list of all nodes. When the election occurs, each node gathers the election results from each voter. When the selection process is completed, the nodes will wait their turn to create the block. Upon arrival of the block on each node, then done verification to determine whether the block is valid. Once valid, then the database added with the data in the block.

2.5 E-voting System: E-voting currently widely used by some countries in the world, for example in Estonia. The country has been using the e-voting system since 2005 and in 2007 conducted online voting and was the first country in the world to conduct online voting. Since then, a legally binding online voting system has been implemented in various other organizations and countries such as the Austrian Federation of Students, Switzerland, the Netherlands, Norway, and so on . But it still has considerable security issues and the selection is often canceled. Although getting a lot of attention, online voting system is still not widely done in various countries around the world. The traditional voting system has several problems encountered when managed by an organization that has full control over the system and database, therefore the organization can tamper with the database, and when the database changes the traces can be easily eliminated. The solution is to make the database public, the database owned by many users, which is useful to compare if there are any discrepancies. The solution to the e-voting system is compatible with using blockchain technology. Blockchain technology allows in support of e-voting applications. Each voter's vote serves as a transaction that can be created into blockchain that can work to track voice counting. In this way, everyone can approve the final calculation because of the open blockchain audit trail, the vote count can be verified that no data is altered or deleted nor is there any unauthorized data entered in the blockchain.

4. Proposed System

The block chain technology used mostly works the same as the block chain technology contained in the E-voting system and focuses on database recording. The nodes involved in Block chain that have been used by Bitcoin are independently random and not counted. However, in this e-voting system a block chain permission is used, for nodes to be made the opposite of the Bitcoin system and the Node in question is a place of general election because the place of elections must be registered before the commencement of implementation, it must be clear the amount and the identity. This method aims to maintain data integrity, which is protected from manipulations that should not happen in the election process.

This process begins when the voting process at each node has been completed. Before the election process begins, each node generates a private key and a public key. Public key of each node sent to all nodes listed in the election process, so each node has a public key list of all nodes. When the election occurs, each node gathers the election results from each voter. When the selection process is completed, the nodes will wait their turn to create the block. Upon arrival of the block on each node, then done verification to determine whether the block is valid. Once valid, then the database added with the data in the block. After the database update, the node will check whether the node ID that was brought as a token is his or not. If the node gets a turn, it will create and submit a block that has been filled in digital signature to broadcast to all nodes by using turn rules in block chain creation to avoid collision and ensure that all nodes into block chain. The submitted block contains the id node, the next id node as used as the token, timestamp, voting result, hash of the previous node, and the digital signature of the node.

Modules:

User

Block chain

Visual Cryptography

Admin

Architecture Diagram:

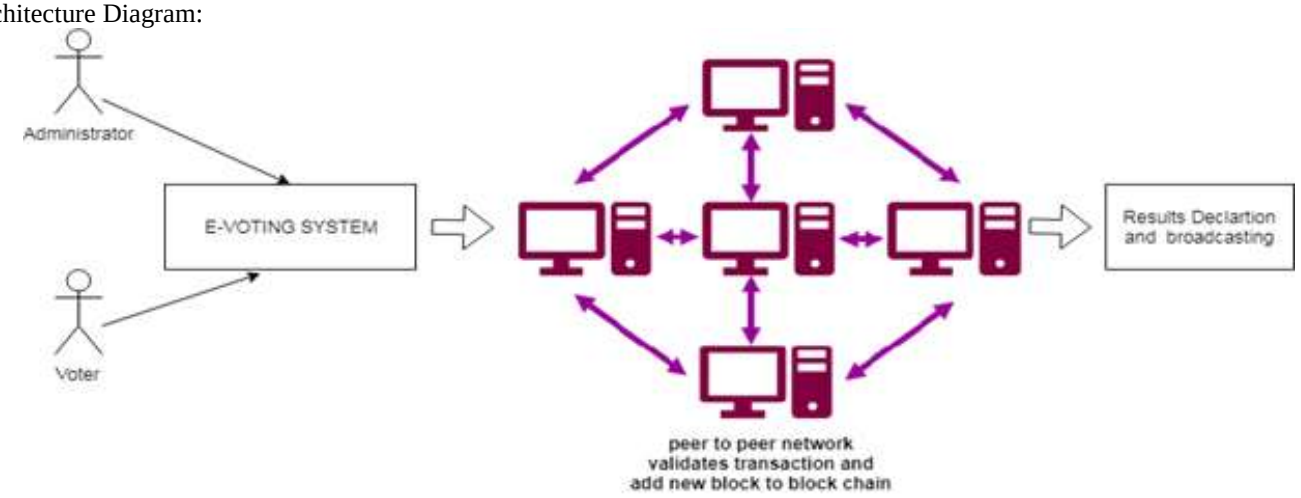


Fig. 1: System Architecture

5. ALGORIHM

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer.
Such a technique thus would be lucrative for defense and security.

2 OUT OF 2 SCHEME

- Black and white image: each pixel divided in 2 sub-pixels
- Choose the next pixel; if white, then randomly choose one of the two rows for white.
- If black, then randomly choose between one of the two rows for black.
- Also we are dealing with pixels sequentially; in groups these pixels could give us a better result.

1. There is a ***(k,k)*** scheme with $m=2^{k-1}$, $\alpha=2^{-k+1}$ and $r=(2^{k-1}!)$.

We can construct a **(5,5)** sharing, with **16** sub pixels per secret pixel and, using the permutations of **16** sharing matrices.

1. In any ***(k,k)*** scheme, $m \geq 2^{k-1}$ and $\alpha \leq 2^{1-k}$.
2. For any n and k, there is a ***(k,n)*** Visual Cryptography scheme with $m=\log n\ 2^{O(k \log k)}$, $\alpha=2^{\Omega(k)}$.

6. RESULTS

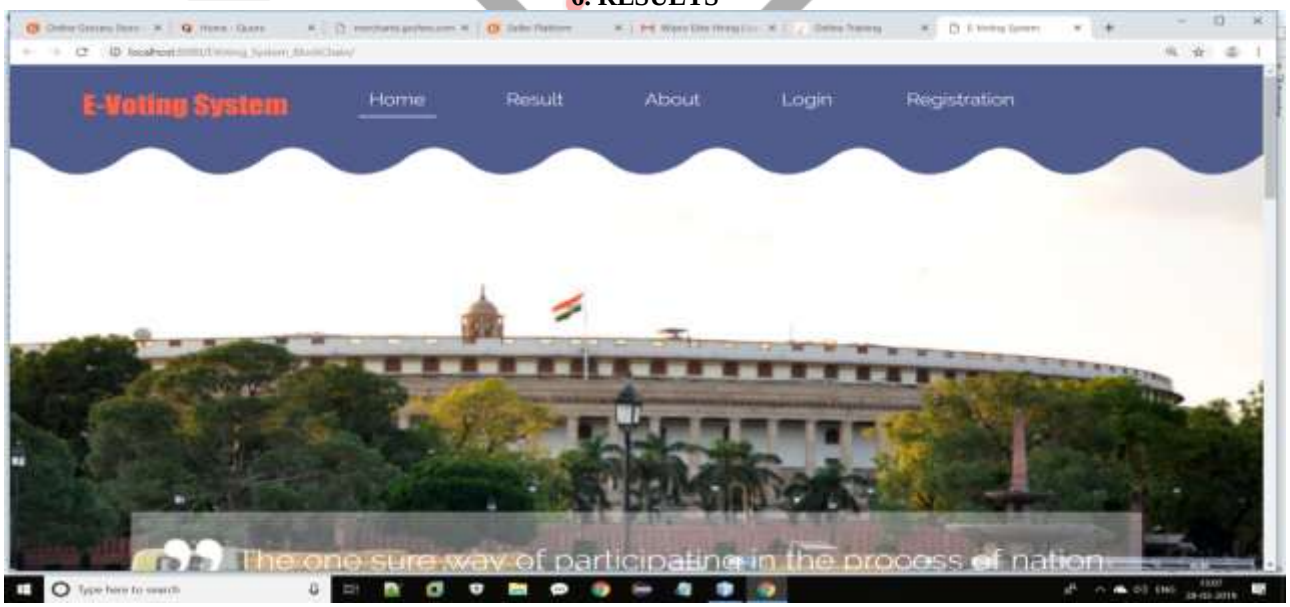


Fig. 1: Home Page

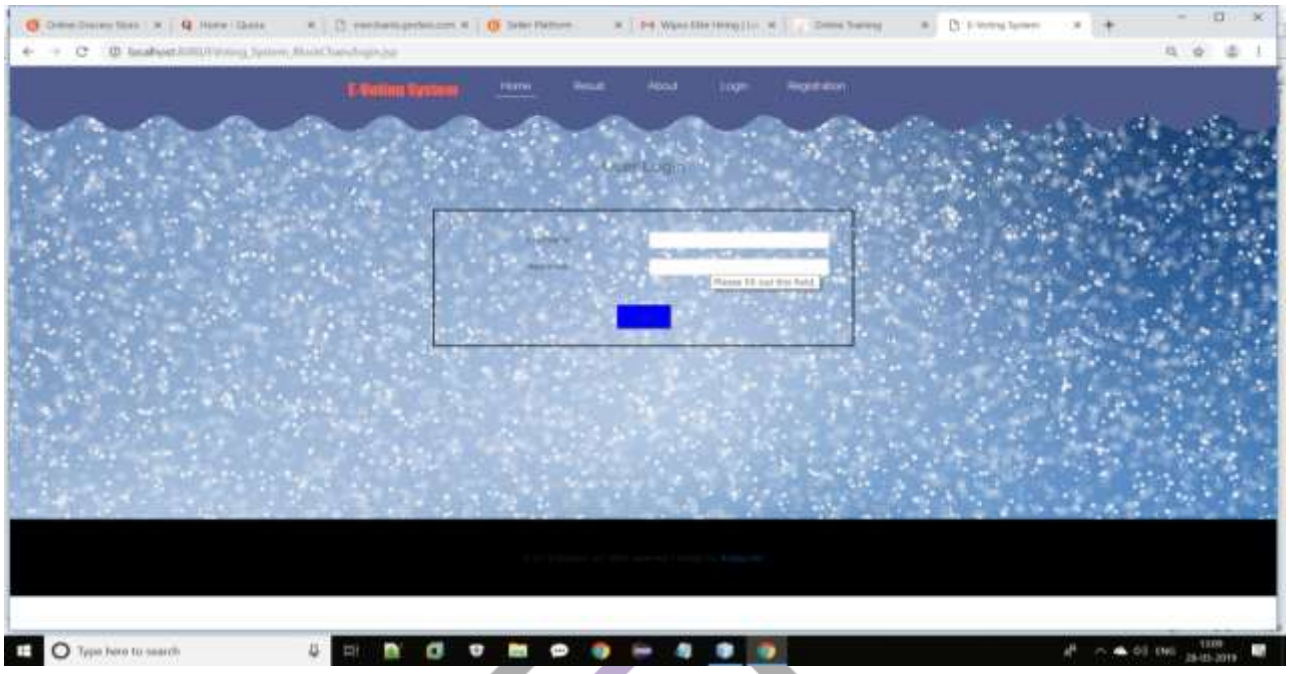


Fig. 2: Login Page

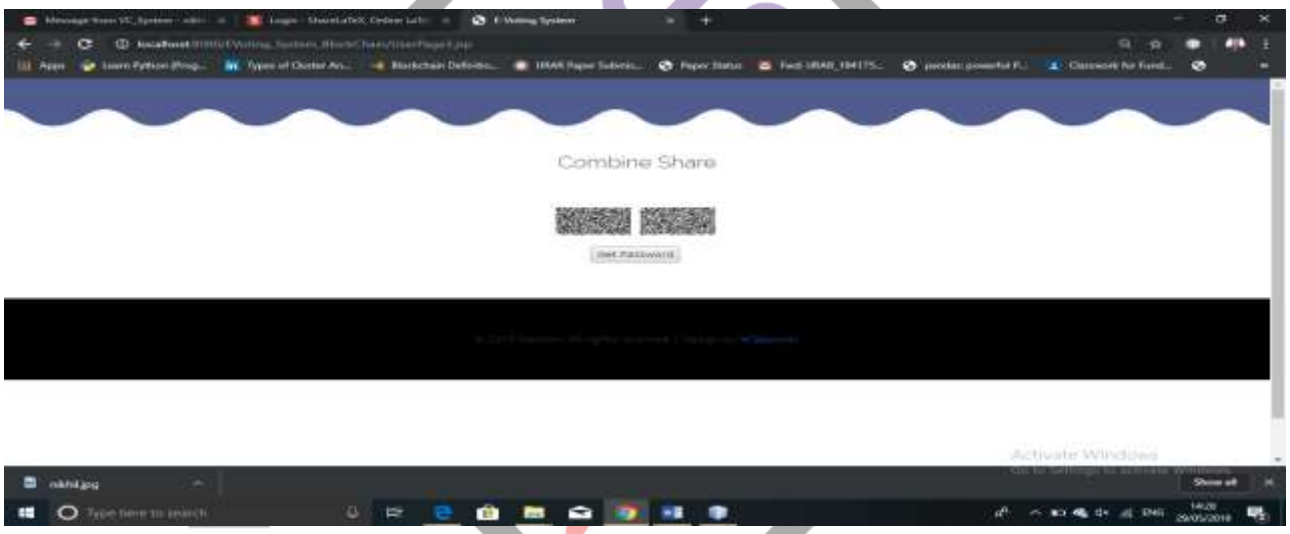


Fig3.Visual Cryptography.

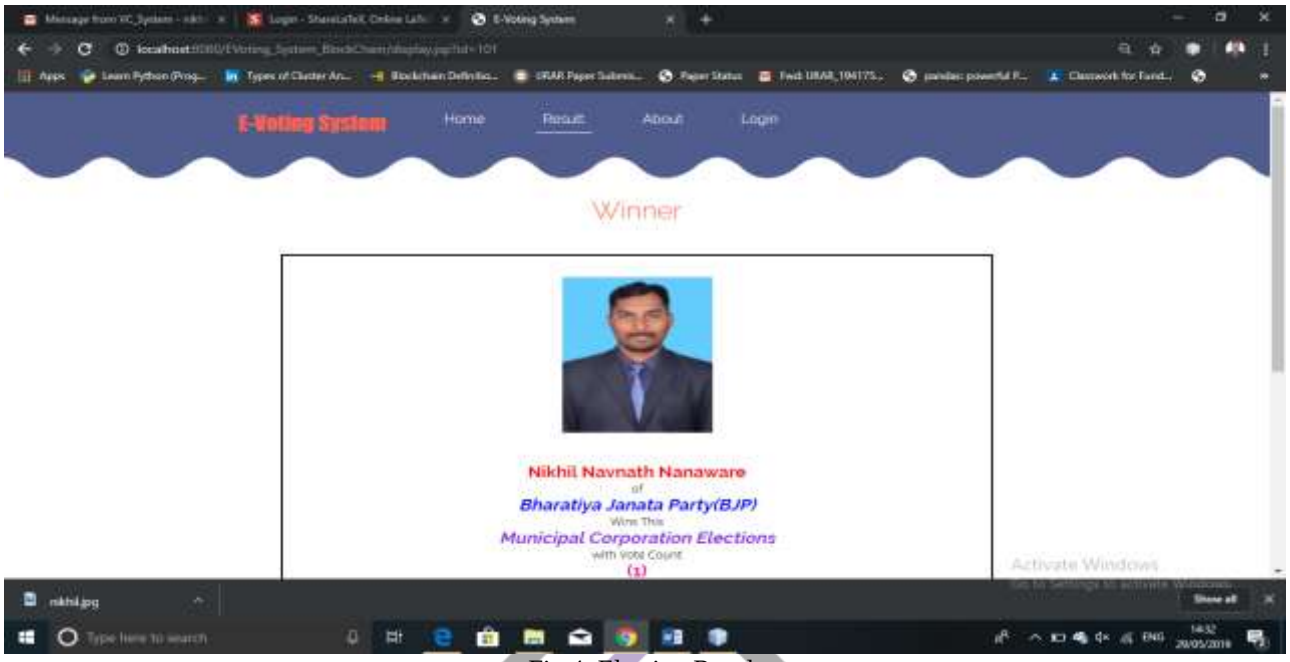


Fig.4: Election Result

7. APPLICATIONS

- This system is also used for corporate companies to conduct their elections for different posts such as the presidential election, manager election etc.
- Online social network
- Online banking
- Notary

8. CONCLUSION AND FUTURE WORK

A nation with less voting percentage will struggle to develop as choosing a right leader for the nation is very essential. Our proposed system designed to provide a secure data and a trustworthy E-voting amongst the people of the democracy. Block chain itself has been used in the Bitcoin system known as the decentralized Bank system. By adopting block chain in the distribution of databases on e-voting systems one can reduce the cheating sources of database manipulation. This project aims to implement voting result using block chain algorithm from every place of election.

REFERENCES

[1] Ahmed Ben Ayed,"A Conceptual Secure Block Chain-Based Electronic Voting System",2017 IEEE International Journal of network &Its Applications(IJNSA),03 May 2017.

[2] .Rifa Hanifatunnisa, Budi Rahardjo," Blockchain Based E-Voting Recording System Design",IEEE 2017.

[3] Kejiao Li, Hui Li,Hanxu Hou, Kedan Li,Yongle Chen," Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain", 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems.

[4] Ali Kaan Koç, Emre Yavuz, Umut Can Çabuk, Gökhan Dalkilic," Towards Secure E-Voting Using Ethereum Blockchain",2018 IEEE.

[5] Supriya Thakur Aras, Vrushali Kulkarni," Blockchain and Its Applications – A Detailed Survey", International Journal of Computer Applications (0975 – 8887) Volume 180 – No.3, December 2017.

[6] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram,Konstantinos Markantonakis," E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy",IEEE 2018,03 July 2018.

[7] Kashif Mehboob Khan, Junaid Arshad, Muhammad Mubashir Khan," Secure Digital Voting System based on Blockchain Technology",IEEE 2017.

[8] Huaiqing Wang, Kun Chen and Dongming Xu. 2016. A maturity model for blockchain adoption. Financial Innovation, Springer, Open Access, DOI 10.1186/s40854-016-0031-z

[9] Buterin, Vitalik. 2015, On Public and Private Blockchains. [Online] https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[10] Zyskind et. al. 2015. Decentralizing Privacy: Using Block chain to Protect Personal Data, 2015 IEEE Securityand Privacy Workshops (SPW), San Jose, CA, USA, July 2015 [Online].Available: http://dx.doi.org/10.1109/SPW.2015 Jianliang Meng, Junwei Zhang,Haoquan Zhao, "Overview of the Speech Recognition Technology", 2012 Fourth International Conference on Computational and Information Sciences.