Implementing Electronic Voting System Using Block chain

Anirudh Grover, Kedar Apet , Aabhas Fulzele , Rishabh Agarwal
Students, Dept. of Computer Engineering
Maharashtra Institute of Technology, Pune

Mrs S.J. Rajput
Asst. Professor, Dept. of Computer Engineering ,
Maharashtra Institute of Technology, Pune.

Abstract: ***Traditional elections satisfy neither citizens nor political authorities in recent years. They are not fully secure since it is easy to attack votes. It threatens also privacy and transparency of voters. Additionally, it takes too much time to count the votes. Electronic voting (e-voting) is an electronic means for casting and counting votes. It is an efficient and cost-effective way of conducting a voting procedure. However, it's been challenging to develop an online voting system that can satisfy the legal requirements of a democratic country. The main concerns are the security of networking and privacy of communication for e-voting have been grown.***

In this paper, an empirical review has been performed to understand issues faced by a voting system besides with Blockchain-based solution as a better alternative for providing a more transparent and error-free voting system. All the related papers are have been studied here along with an abstract view of the proposed system that we are going to implement. The proposed system provides high security to voter's personal information using the IPFS decentralized file sharing platform.

Keywords: Blockchain Technology, e Voting System, Cryptocurrency, Transparency, Efficiency, Inter-Planetary File System (IPFS) protocol, Election Officer, Blockchain as a Service.

I. BACKGROUND

Blockchain technology is an emergent and disruptive technology, which as the potential to improve the way individuals and organizations interact and operate, ultimately influencing almost all facets of our daily lives Nowadays, besides the financial sector in which the blockchain concept was born, we are witnessing0 substantial efforts made by many organizations, from distinct economic sectors, which are using blockchain technology to develop very innovative applications.

Voting plays a significant role in a democratic Society. The issue with the current ballot system is that it can be easily manipulated and looks to eliminate the aspect of trust from an election. Building a more secure and transparent electronic voting that can satisfy the legal requirements of a democratic country has been a challenge for a long time for many researchers. The current e-voting implementations face several problems like poor privacy protection of voting behavior. Such problems led to a situation where the current e-voting systems are not any safer. This paper presents different approaches that potentially enhanced the electronic voting system features by applying blockchain technology in an appropriated manner.

II. INTRODUCTION

The blockchain technology is presented as a game-changer for many of the existing and emerging technologies/services. One potential application of blockchain can be found in e-voting schemes. It is an alternative solution for the traditional paper ballot voting. It is cryptographically secured, transparent, public ledger technology that can remove the trust gap between central authority and voters, thus providing the more democratic and portable voting solution. The solution is far better as compared to other solution because, it is a decentralized system; contain the results in the form of bit-coins, having different locations.

- **Blockchain Technology**

Blockchain is an emerging technology that has drawn considerable interest by providing benefits such as decentralization, persistence, anonymity, and auditability. It holds immense promise for a variety of applications, including financial services, real estate, supply chain management, health care, academia cryptocurrency, and more.

Blockchain can be described as a distributed data structure that is replicated and shared among the members of a network, whose purpose is to record every transaction done. Each transaction is batched into time stamped blocks and each block is identified by its cryptographic hash. Each block stores the hash of the previous one, creating a link between the blocks or, as the name implies, a chain of blocks, thus generating a transparent and immutable history of records whose veracity is provided by a consensus protocol

Blocks are composed of a list of transactions recorded over a given period and a header. The header contains: the previous Hash, which is the result of encrypting all data found on the previous block header; the nonce, which is a value adjusted by miners so

that the hash of the block generated will be lower or equal to the current target of the network; finally, the Merkle tree root, which summarizes all the transactions in the block, making it possible to verify if a transaction is included or not.

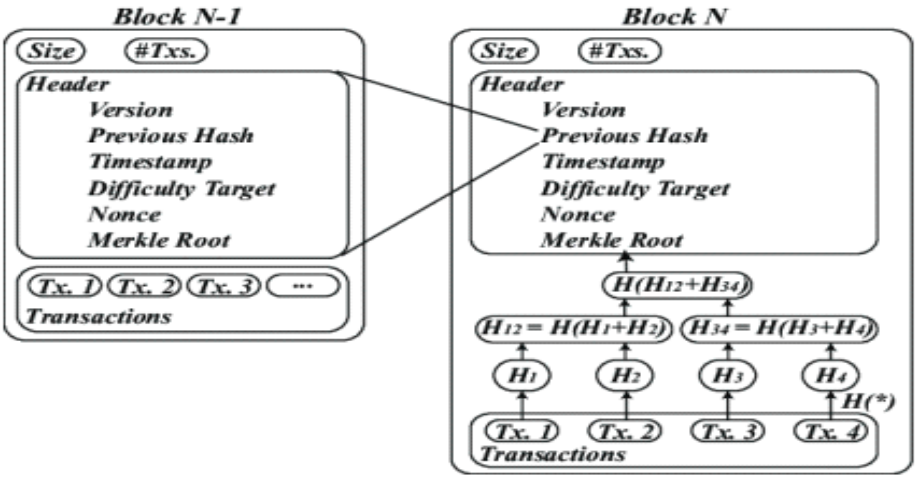

Figure 1: Structure of a Block

- ## Blockchain for Electronic Voting Systems

Voting is a very crucial activity for any institution or organization that needs to elect a certain entity for a certain role. Historically, the most common way to vote, still largely used nowadays, is through a paper based system. Of course, this is not the safest nor the most convenient or economical method to support the voting process. Electronic voting systems might be the solution to the disadvantages mentioned above. The first electronic voting system was introduced in the early eighties.

- **Requirements of Electronic-voting Systems**

The adequacy and security parameters of a voting system it is necessary to evaluate following core requirements

Requirement	Description
Authenticity	Only users with the right to vote should be able to cast a vote
Transparency	Voting systems should be clear and transmit accuracy, precision, and security to voter
Anonymity	It should not be possible to associate a vote to a voter
Integrity	Votes should not be able to be modified or destroyed
Availability	Voting systems should be always available during the voting period
Verifiability	Anyone should be able to independently verify that all votes have been correctly counted

- **Benefits of Blockchain regarding E-voting Systems**

Blockchain has the potential to improve electronic voting systems by solving some of their major limitations and issues.

- **Authenticity:** Every user of the network is identified by a public key, which can only be accessed by its own private key. Assuming that every voter will keep its own private key secret, then the authenticity requirement is fulfilled.
- **Transparency:** identically to the Auditability and Certifiability requirement, transparency is one of the blockchain properties, and every application implemented in the blockchain inherits this same property.
- **Anonymity:** since every user is identified by a public key and the stored vote is encrypted, it is impossible to associate a voter with a vote.
- **Integrity:** since the hash pointer provides the blockchain with tamper-evident properties, every stored vote has the same properties, meaning that it can't be adulterated.
- **Availability:** since blockchain is a distributed network, as long as the network has the required number of nodes to achieve consensus, the voting system will be always available.
- **Verifiability:** since the blockchain is transparent to every node of the network, everyone could confirm that the number of votes casted and counted is the same.

III. LITERATURE REVIEW

Fridrik P and his team evaluates an application of blockchain as a service to implement distributed electronic voting systems based on blockchain that uses "permissioned blockchain", and review of existing blockchain frameworks suited for constructing blockchain-based e-voting system.

Author proposed proposes the E-voting model to evaluate the application of blockchain as a service to implement distributed electronic voting systems. Taban Habibu presents an electronic voting system (E-Voting)(Zibin Zheng) to be applied to Muni University student's electoral body. Several security measures were integrated into the E-Voting system in order to achieve an enhanced, speedy and accurate performance. A computer software application was developed using PHP (Hypertext Processor) programming language and MYSQL, a relational database management system in designing the database; tested and found to have produced the expected results.

Gunnlaugur K. Hreidarsson proposes a novel electronic voting system based on blockchain by evaluating the potential of distributed ledger technologies through the description of a case study; namely, the process of an election, and the implementation of a blockchain-based application, which improves the security and decreases the cost of hosting a nationwide election.

Author in [12] proposed Blockchain-enabled e-voting (BEV) could reduce voter fraud and increase voter access. Eligible voters cast a ballot anonymously using a computer or smartphone. BEV uses an encrypted key and tamper-proof personal IDs. The blockchain's audit trail ensures that no vote has been changed or removed and that no fraudulent and illegitimate votes have been added. In this system to address voter tampering, blockchains generate cryptographically secure voting records. Votes are recorded accurately, permanently, securely, and transparently. So, no one can modify or manipulate votes.

Authors implemented the blockchain technology in digital e-voting system to solve the security issues in the university campus to find the best suitable candidate. This model not only conducts the voting procedure without human intervention but also provides security against all the major attacks. When the university administration wants to elect one student leader from the contestants. Each college starts the voting process. Each vote under one college creates one block and each block joins together to make a blockchain. After completion of the voting, the blockchain of each college under one zone join together to make a zone level blockchain. Now, each zone level blockchain joins together to make a university-level blockchain. Now, we get a complete blockchain. The committee will consider this single blockchain for the vote count.

Paolo Ceravolo proposed an e-Vote-as-a-Service based on Blockchain using a cloud-based approach. Even if a number of cloud providers such as IBM and Oracle are offering ready-to-use blockchain installation on the cloud with a fee based on the number of transactions, the challenge of a dynamic and on-demand system configuration and optimization based on end-users business requirements remains. The presented approach allows the end-users to specify functional and non-functional requirements of services and the Cloud infrastructure where services are deployed on-demand to optimize costs and service performance.

IV. PROPOSED SYSTEM

The proposed system provides a reliable and secure e-voting scheme using blockchain. Blockchain-based E-Voting System that works in a decentralized environment based on IPFS protocol.

In the proposed system initially, the Voter should be registered themselves for voting by giving personal identity information. It is a adhaar card number that will going to be used for identification of any voter. Then the voter is added and verified by the Election Officer. The officer should be verifying the voter's personal information and their registration data.

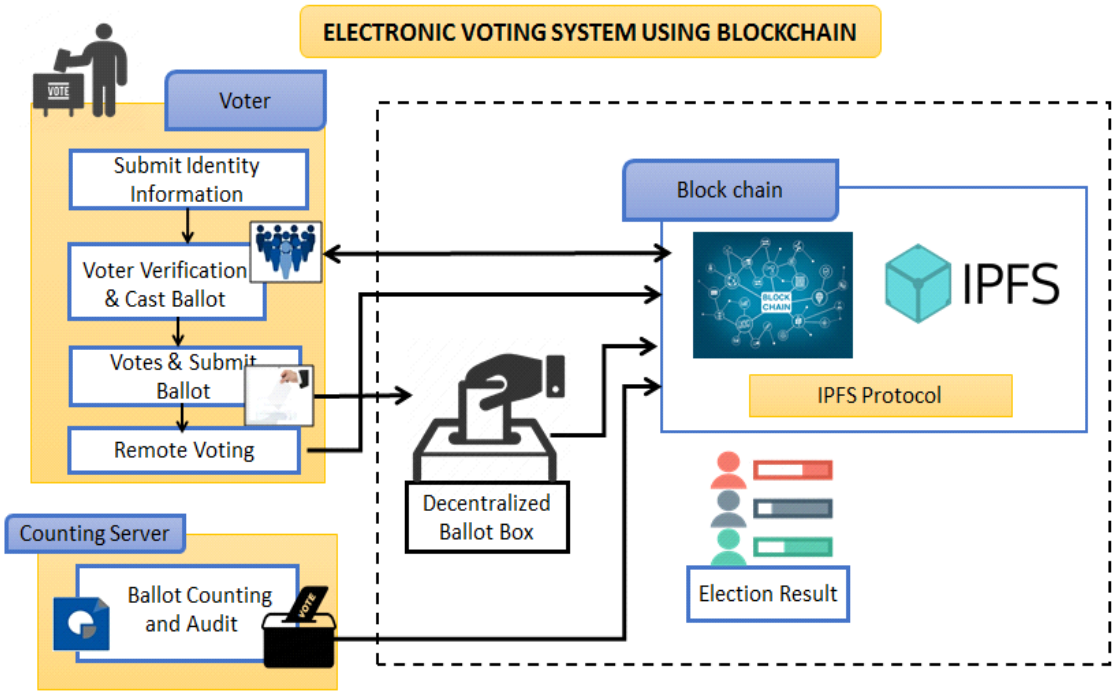

Figure: - System Architecture

1. Voter Identity:
Voter should be registered themselves for voting by giving personal identity information. It is unique identification of any voter.

2. Voter Verification:
Voter is verified by the Election Officer. 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. Remote Voting :
The voter can do the remote voting according to their respective regions they belong from their current location.

4. Ballot Submission:
After giving the e-voting by the voter the ballot are submitted to a secure block chain based ballot box, while retaining anonymity and ballot secrecy. Ballot box contains the collection of voter ballot.

5. Ballot Audit:
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.

6. Election Result:
Through the ballot box, count final voting result. With help of Inter-Planetary File System (IPFS) protocol the final election result generated.

V. ALGORITHM USED

- **<u>The Inter-Planetary File System (IPFS)</u>**
- **Aim:-**
  - The Inter-Planetary File System, IPFS is a decentralized file sharing platform that identifies files through their content.
  - When a file is uploaded to IPFS, it is split into chunks, each containing at most 256 kilobytes of data and/or links to other chunks.
  - Every chunk is identified by a ryptographic hash, also named content identifier that is computed from its content.
- **Identifier:-**
  Node IDs: - Public Key Hash. Routing in DHT, based on:
  1. Other peer's network addresses.
  2. Object names.
- **DHT: S/Kademlia:**
  It stores two different types of information.
  1. First, whenever a file is uploaded through a node, the latter registers itself as a provider of the files chunks.

2. Second, the DHT contains information on how to connect to a node with a specific identifier, for example by providing an IP-address.

- **Block exchange:-**
  1. Like BitTorrent, but not exchange not limited to blocks in a torrent.
  2. Incentivizing cooperation (different strategies: tit-fortat, currency-based etc.).
  3. Per-node ledger for accounting transfers that is exchanged when nodes connect.
- **Object Merkle directed acyclic graph (DAG):-**
  1. Because of the Merkle DAG, an entire file can be identified by just using the root hash.
  2. On top of DHT/block exchange.
  3. Objects are immutable.
  4. Generalization of Git data structure.
- **File sharing:-**
  IPFS integrates both the use of complex Merkle-Linked structure with the data address ability of P2P file sharing systems. The content is distributed over a peer-to-peer network.

VI. RESULT AND ANALYSIS

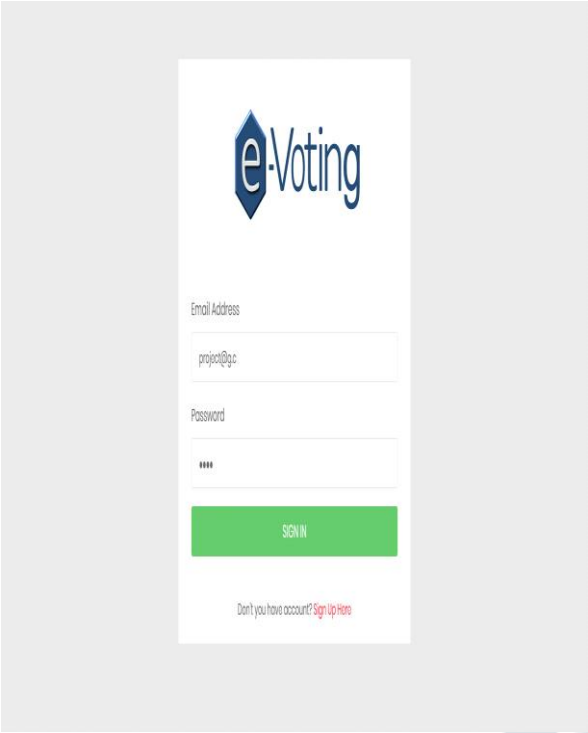

Figure: Login Page

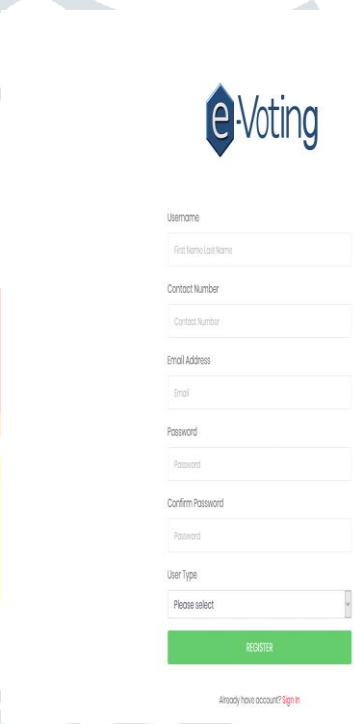

Figure: Registration Page

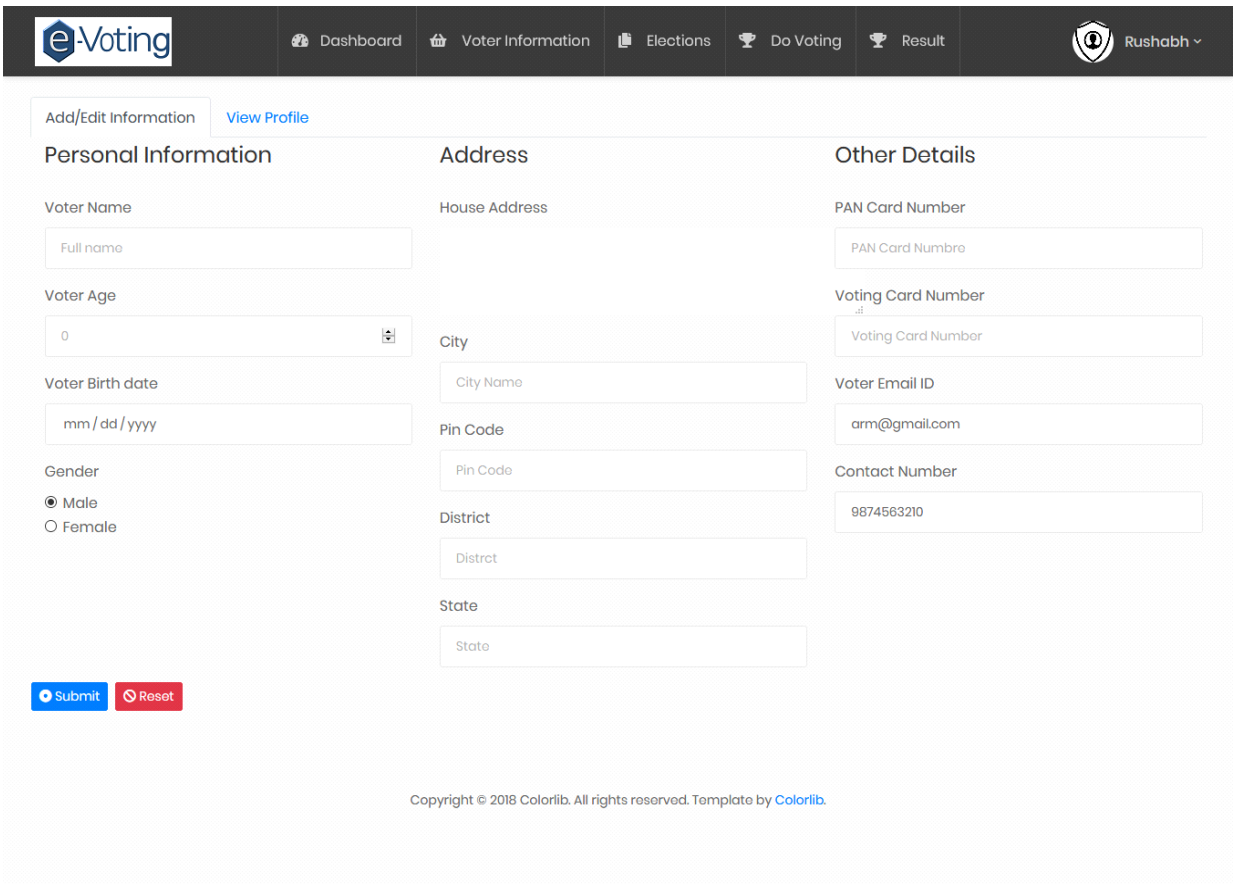

Figure: Personal Information

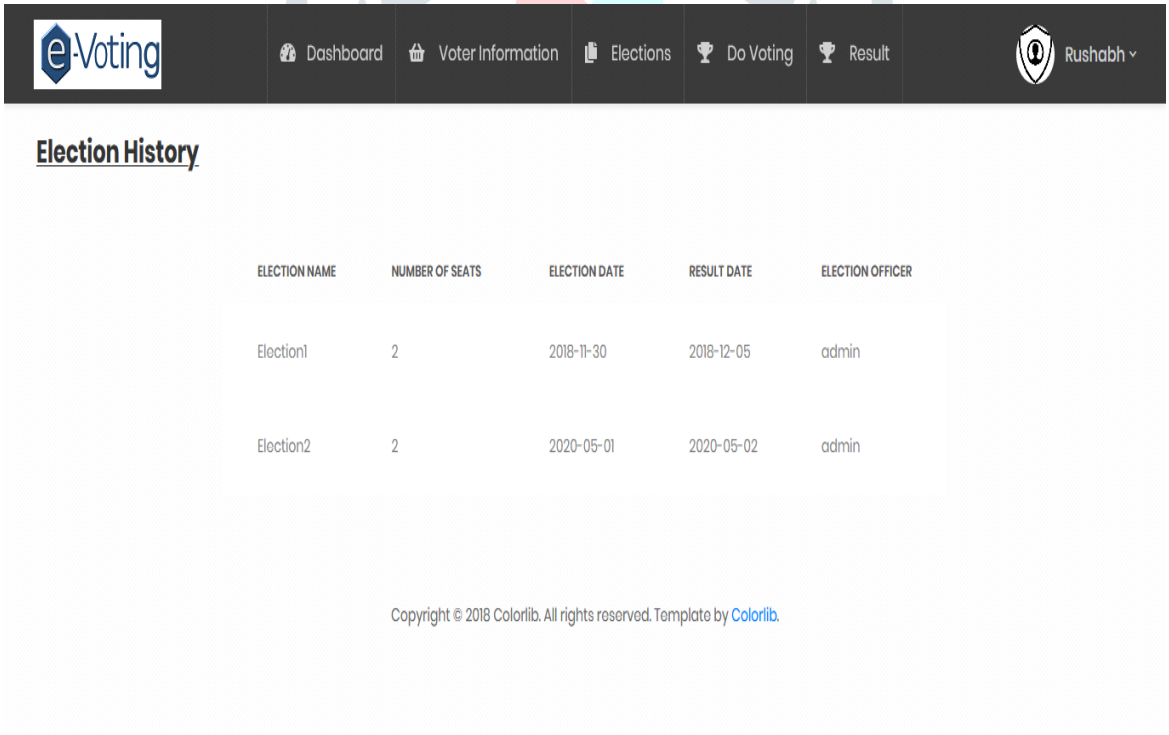

Figure: Election History

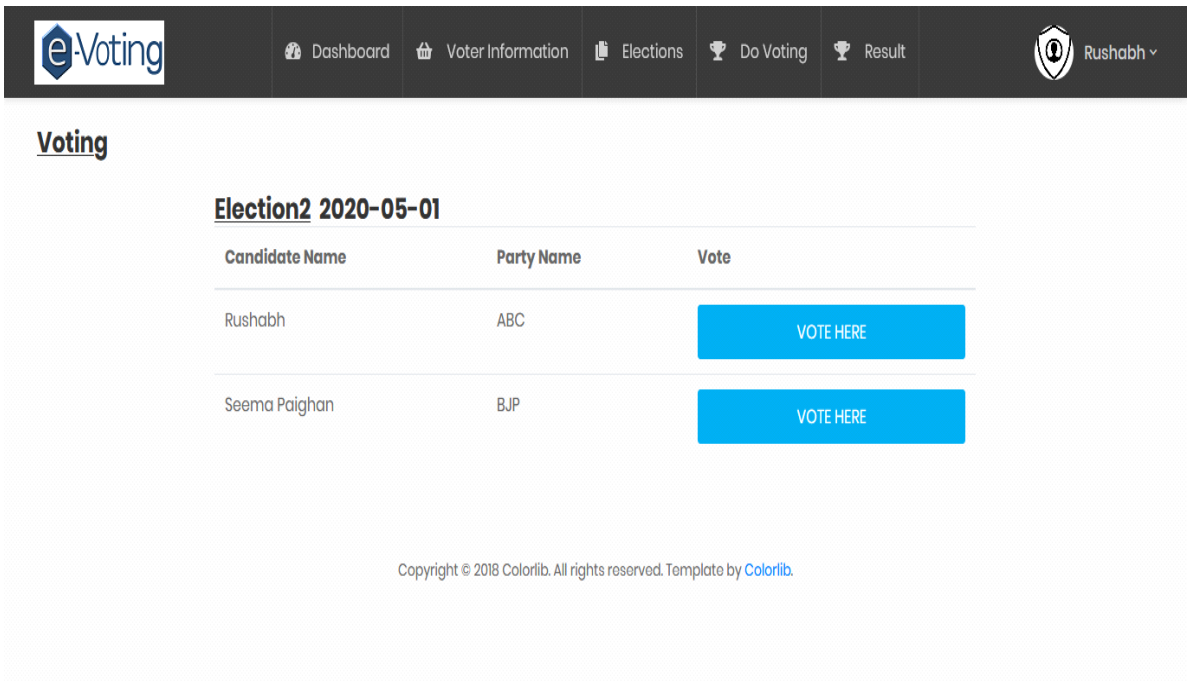

Figure: Voting Details

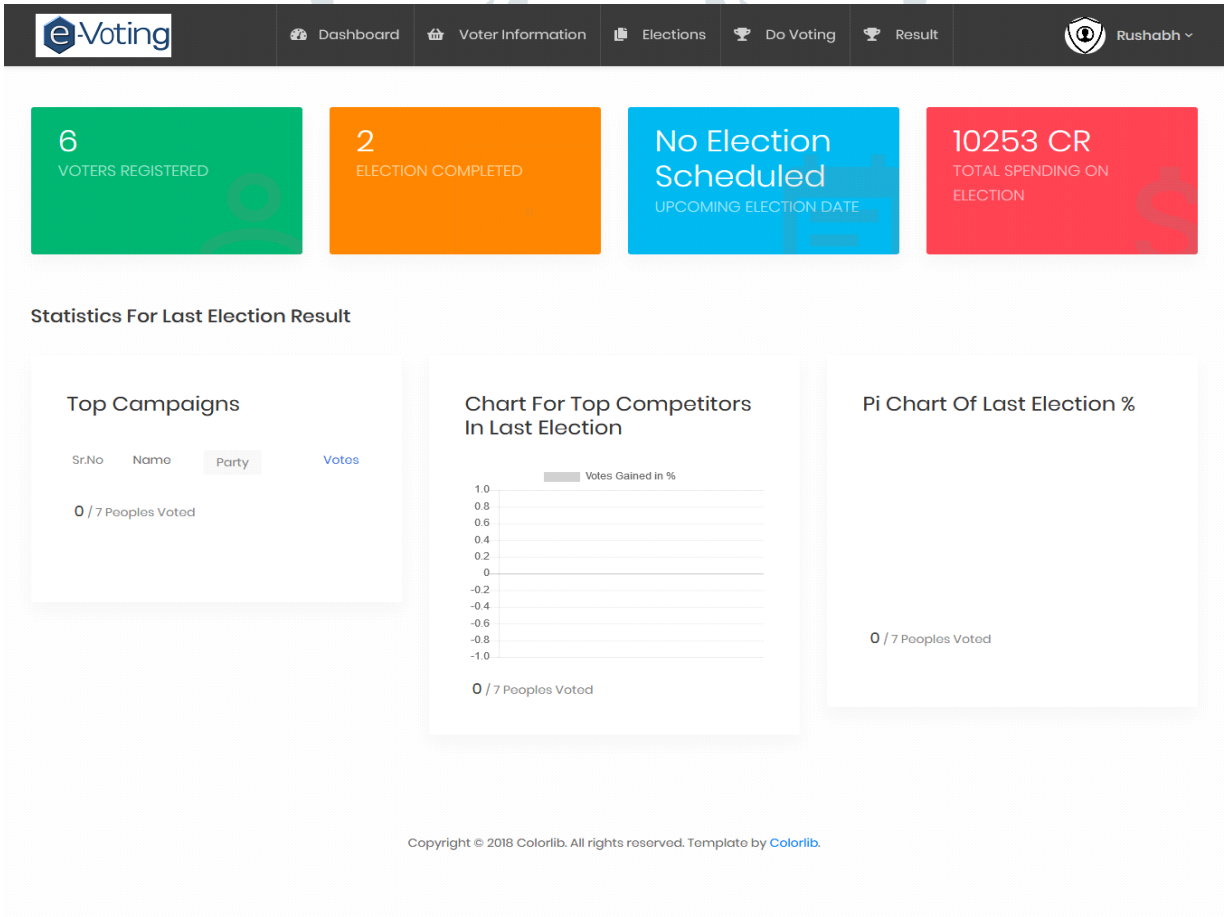

Figure: Statistics for last election Results

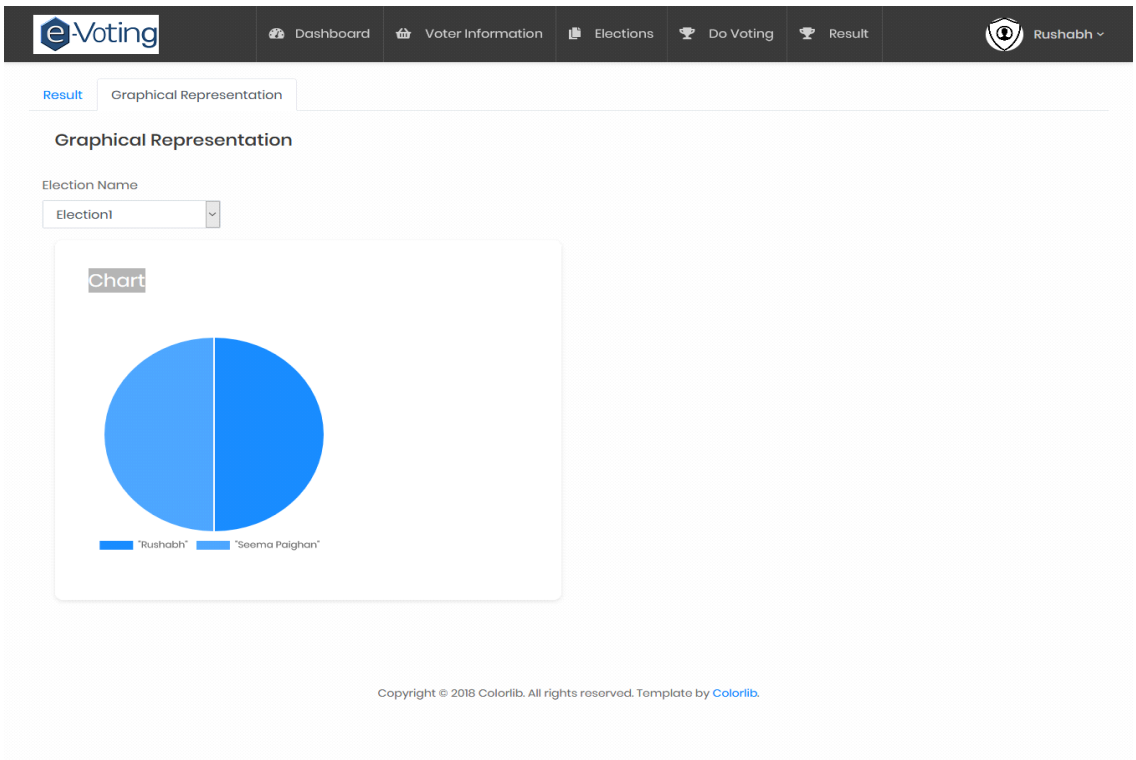

Figure: Graphical Representation

VII. CONCLUSION

Blockchain has shown its potential for converting the traditional industry into advanced one with its key characteristics like decentralization, persistency, anonymity, and auditability.

Here we present a comprehensive system on the blockchain technology used by researchers in the field of e-voting systems. Extensive research has been done on electronic voting systems that enable voters to vote at their convenience using a mobile phone, computer or any other electronic device. Still, none of these technologies have been incorporated on a larger scale due to inherent security threats/concerns that these systems might pose to the integrity of the voting process. In this paper, we discuss electronic voting system using blockchain, a secure and robust system that ensures the anonymity of the voter, transparency in the process, and robust functioning.

REFERENCES

[1] Rumeysa Bulut, Alperen Kantarcı, SafaKeskin,Şerif Bahtiyar,"Blockchain-Based Electronic Voting System for Elections in Turkey".
[2] Fridrik Þ. Hjalmarsson, Gunnlaugur K. Hreiðarsson"Blockchain-Based E-Voting System".
[3] Mrs. HarshaV.Patil1, Mrs. KanchanG.Rathi2, Mrs.MalatiV.Tribhuwan,"A Study on Decentralized E-Voting System Using Blockchain Technology",International Research Journal of Engineering and Technology(IRJET) Volume: 05 Issue: 11| Nov2018. Clement Chan Zheng Wei, Chuah Chai Wen,"Blockchain-Based Electronic Voting Protocol ",INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION ,2018.
[4] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis,"E-Voting with Blockchain: An E-Voting Protocolwith Decentralisation and Voter Privacy".
[5] Taban Habibu,Konde Sharif,Sebwato Nicholas,"Design and Implementation of Electronic Voting System",DOI: 10.14445/22492593/IJCOT-V45P301, August 2017.
[6] Zibin Zheng and Shaoan Xie ,Hong-Ning Dai ,Xiangping Chen, Huaimin Wang ,"Blockchain challenges and opportunities: a survey", Int. J. Web and Grid Services, Vol. 14, No. 4, 2018.
[7] Wei-Tek Tsai, Libo Feng, Hui Zhang ,Yue You, Li Wang, Yao Zhong ,"Intellectual-Property Blockchain-based Protection Model for Microfilms ", 2017 IEEE Symposium on Service-Oriented System Engineering .
[8] Suhan Jiang, Yubin Duan, Jie Wu, "A Client-biased Cooperative Search Scheme inBlockchain-based Data Markets", 2019 IEEE.
[9] Merlinda Andoni,Valentin Robu David Flynn, Simone Abram, Dale Geach, David Jenkins, Peter McCallum, Andrew Peacock, "Blockchain technology in the energy sector: A systematic review ofchallenges and opportunities",Elsevier 2018.
[10] Fridrik Þ. Hjálmarsson ; Gunnlaugur K. Hreidarsson ; Mohammad Hamdaqa ; Gísli Hjálmtýsson "Blockchain-Based E-Voting System", 2018 IEEE 11th International Conference on Cloud Computing (CLOUD).

[11] Nir Kshetri ; Jeffrey Voas ,"Blockchain-Enabled E-Voting", IEEE Software (Volume: 35 , Issue: 4 , July/August 2018) (Nir Kshetri et al., 2018, Ashish Singh et al.,2018)

[12] Ashish Singh ; Kakali Chatterjee ,"SecEVS : Secure Electronic Voting System Using Blockchain Technology", 2018 International Conference on Computing, Power and Communication Technologies (GUCON).

[13] Scott Wolchok, Eric Wustrow, Dawn Isabel, and J AlexHalderman. Attacking the washington, dc internet voting system. In International Conference on Financial Cryptography and Data Security, pages 114–128. Springer,2012.

[14] Emanuele Bellini ; Paolo Ceravolo ; Ernesto Damiani ,"Blockchain-Based E-Vote-as-a-Service", 2019 IEEE 12th International Conference on Cloud Computing (CLOUD).

[15] Rahul Rakhe1, Rahul Kale1, Pritish Bisht1, Prof. K.S.Balbudhe ,"E-Voting System using Blockchain Technology for Distributed Environment", International Journal of Innovative Research in Science, Engineering and Technology,Vol. 8, Issue 5, May 2019.