E-Matdaan: A Blockchain based Decentralized E-Voting System

Shreyas Tandon
Department of Computer Science & Engineering
Motilal Nehru National Institute of Technology Allahabad
Prayagraj, India
s.tandon.512@gmail.com

Niharika Singh
Department of Computer Science & Engineering
Motilal Nehru National Institute of Technology Allahabad
Prayagraj, India
niharika.singh9914@gmail.com

Shivani Porwal
Department of Computer Science & Engineering
Motilal Nehru National Institute of Technology Allahabad
Prayagraj, India
porwalshivani@gmail.com

Satiram
Department of Computer Science & Engineering
Motilal Nehru National Institute of Technology Allahabad
Prayagraj, India
satiram4020@gmail.com

Ashish Kumar Maurya
Department of Computer Science & Engineering
Motilal Nehru National Institute of Technology Allahabad
Prayagraj, India
ashishmaurya@mnnit.ac.in

2022 IEEE Students Conference on Engineering and Systems (SCES) | 978-1-6654-8072-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/SCES55490.2022.9887759

***Abstract*— In current times, electronic voting systems are used for conducting elections but E-voting system has many problems like transparency, credibility, security functionality and reliability and also the complete process is quite slow. Most of these drawbacks can be removed by using Blockchain based E-voting system. Blockchain is a shared, immutable record that allows for the recording of transactions and the tracking of benefits in a network. Blockchain is an immutable and shared record that provides the method of recording transactions and tracking benefits in a network. In this paper, we propose and implement a blockchain based E-voting system using proof of work as the consensus algorithm. We feel this field has a lot of potential and scope of improvement in near future.**

Keywords*— *blockchain, E-voting, peer to peer, elections, decentralized, proof of work, consensus

I. INTRODUCTION

As a democratic country, India's democratic principles are based on elections. Voting is a constitutional right that we are privileged to have. But for elections to fulfill their critical function, they must be free and fair. Various countries like Ghana, Kenya and Nigeria have used technology to varied degrees in their election management and processes [1]. Elections are very essential thing to maintain the democratic nature of the country but evolution of Internet continuously challenging the voting process. [2].

A. Motivation

When comparing with the old method of pen and paper voting, e-voting cut election costs and provided some convenience, but it was deemed unreliable since anyone with physical access to the system might impede the mechanism and alter the votes. E-voting has advantage over ballot paper as it manages all the information automatically while in ballot paper all things are managed manually. The main advantages are cost effectiveness, computerized generation of results, immediate comprehensive reporting methods, and instant storing and display of results [3]. Also, a central system is necessary to control the whole process, from e-voting through electoral outcomes and tracking the results. Voters are not fully safe because their votes can be readily targeted. It also poses a serious threat to voting rights and openness. The conventional voting system also incurs costs for human resources, ballot distribution, and security measures. Every country in this world spends a huge amount of money to conduct elections [4]. The modern voting system which used the electronic voting machines, has set aside the old-fashioned way of voting, which is a very time consuming procedure requiring strenuous and burdening efforts, resulting in a wide range of error and miscalculations [5]. Researchers have argued that blockchain is the technology of the future and in the following years, it will cause havoc in a variety of businesses, with elections in democracy being one of the major areas that blockchain will transform [6].

In this paper, we implement an E-voting system which uses blockchain as an underlying technology to store votes. The blockchain is created from scratch. This implemented blockchain lies over P2P network such that each node carries a copy of the chain. Votes after getting validated and digitally signed get stored on the chain. The proposed method also follows Proof of Work consensus algorithm while mining new blocks.

The rest of the paper is structured as follows: the next section provides with the preliminary knowledge required to understand the proposed work and discusses some similar works proposed by other authors and what gaps are there in their researches; Section 3 specifies the work proposed in this paper and how its system is designed; Section 4 shows the actual implementation of the E-voting system with an example of how the system works; finally Section 5 concludes the study by summarizing current progress and future work plans.

II. PRELIMINARIES AND RELATED WORK

In this section, we discuss some preliminaries and related work.

A. Preliminaries

We go through some of the fundamental concepts behind blockchain technology in this subsection.

978-1-6654-8072-7/22/$31.00 ©2022 IEEE

1) Blockchain: In 2008, a person (or group of people) going by the moniker Satoshi Nakamoto popularised the blockchain to serve as the public transaction log for the cryptocurrency bitcoin. "Blockchain is a shared, immutable ledger for recording transactions, tracking assests and building trust" [7]. Every miner maintains the same ledger, ensuring consistency across all blockchain nodes. The records already put in blocks are unchangeable and this is the fundamental notion of blockchain. Network nodes communicate on a peer-to-peer network. Each block in the blockchain stores hash of its precedent block. The hash of the block is produced considering the contents of the block and the hash of its preceding block. Data in the blocks in the blockchain is represented as transactions between two or more users. Blockchain involves many important concepts from cryptography [8] to distributed systems [9]-[12].

2) Cryptographic Hash Function: It takes an arbitrary/random quantity of data and produces an encrypted text of fixed-size output known as hash. The same hash is generated every time the algorithm is applied on that data. For example- SHA-256 (Secure hashing algorithm) is a proprietary cryptographic hashing algorithm that generates a 256-bit value [8].

3) Public Key Cryptographic: It is often known as asymmetric cryptography that includes the use of key pairs. Each pair consists of a public key and a private key. The public key is known to everyone but the private key is known only to the key owner as it is the confidential part of the algorithm. The algorithms used in cryptography use one-way functions ie., we can generate public key from private key but not private key from public key. This key pair is used to encrypt and decrypt the data [8].

4) Elliptic Curve Cryptographic (ECC): It is a kind of public key encryption that utilizes the algebraic structure of elliptic curves over finite fields to encrypt data [8]. ECC is one of the most used digital signature implementation methods in cryptocurrencies. It is a standard for encryption that will be embraced by most online apps in the future due to its shorter key length and efficiency.

B. Related Works

The E-voting technology is a significant improvement over the traditional ballot paper method. It has grown in popularity in many nations. Several countries are incorporating e-voting technology into their electoral processes. Although it has various benefits such as improved voter turnout, auditability, cheap cost, accessible and convenient elections, and so on, it also has a number of significant obstacles and issues. In this part, we present many e-voting systems that promise to deliver Blockchain-based e-voting.

In [2], the authors emphasized the hazards and potential of blockchain based E-voting systems. When the blockchain is accessed by peers, the transaction data resides on the blockchain is most susceptible. The reason for this is the credentials needed to access a shared distributed ledger and how security flaws could disclose these credentials at endpoints. Citizens must be eligible and so confirmed before casting a vote, which can be done with biometric solutions, but these solutions are not that safe and can easily be stolen or biased.

In [4], the authors proposed an early stage implementation of blockchain-based voting system. The merits and demerits of using blockchain as an e-voting system were also mentioned. The system proposed in this paper did not have a proof of work implementation. The data is sent over a P2P network in the JSON format and one block contains only 1 transaction. The node has two interfaces to communicate. For controlling the node, such as publishing transactions, an HTTP interface is used. For peer-to-peer communication with other nodes, a WebSocket interface is employed.

In [5], the authors proposed a system that made use of a number of tools, including NPM, ganache, truffle, and Metamask. A user must have some Ethereum as a currency to create an account. The user must pay a transaction charge called gas in order to write the transaction to the blockchain. After the casting of votes, a group of nodes called miners add transactions to the chain. They compete with each other using their computational power to mine a new block and validate the transactions. The miners who succeed in this transaction are given rewards for creating blocks. Instead of nodes, authors used ganache software for mining purposes.

In [6], the authors presented a permissionless blockchain architecture based on the Ethereum blockchain technology. The paper mentioned two type of nodes: Full nodes and light nodes. Full nodes are political party nodes and election commission nodes. On the other hand, light nodes are polling station nodes that initiate transactions such as reporting results. The study used a public blockchain, and the results were made public. Transparency is therefore provided. Fungible tokens were utilized in this suggested design to show vote counting at every polling station, and these tokens were created at the polling station to symbolize the vote count that was moved from one collation centre to the EC main office. The total vote count is reflected on the blockchain as fungible tokens at the time of ballot counting. Hence, by using tokens collation is prevented which was earlier there at constituency and EC collation centres.

In [13], the authors focused primarily on using the Aadhar's Virtual ID, which allows service providers to perform verification. To ensure integrity, the voter's biometric data is collected from the Aadhar database and converted to a digital signature by comparing fingerprint data on the local device. The Virtual ID is Aadhar's temporary ID and it replaces the Unique ID number(UID) and enables us to validate and verify the user's statistical profile. In [14], the authors aimed at considering blockchain based system as a service. Rather than using this system as a product, they aimed at using its Blockchain-based "eVote-as-a-Service" was built on an architecture that selects, deploys, and executes an e-Voting service dynamically. End users are allowed to select their requirements based on their organization/constituency's size and features and hence can set-up a straightforward and secure voting service utilizing a pay-per-use configurable methodology, welcoming on costs during the restricted time period of an election.

In [15], the authors used the blockchain in the electronic-voting systems to provide data security and eliminate fraud while computing election results. They provided a solution showing how the voting process can be made tamper-proof with the use of fingerprint verification and voting tokens. These card shape voting tokens are one time use and provided to the voters after successful fingerprint verification. In [16], the authors focused on crucial issues such as vote secrecy, and

end-to-end verification. Solving these issues makes the voting system efficient and also maintains the integrity of the process of voting. The authors used Multichain, an open source blockchain technology, to create their solution. To ensure the secrecy and integrity of a vote, the system produces a robust hash for each vote transaction founded on voter's data and then it sent to the voter over encrypted channel for verification. They created the system using Java EE and MySQL at the backend to store voters' and candidates' information. In [17], the authors tested and implemented e-voting as a smart contract for the Ethereum network. the Ethereum blockchain is used as a storage for recording votes and ballots utilized in election process.

The above mentioned researches have given a slight idea of how blockchain can be used for an e-voting system but a proper implementation of the same is missing.

III. Proposed Work

Our work is a blockchain-based solution for reducing the inconvenient aspects of traditional elections. Blockchain has emerged as an intriguing technology for a variety of applications due to its unique properties that exceed other technologies. As the fundamental function of this system, the e-voting process necessitates qualities such as security, anonymity, privacy and verifiability. It is critical that the technology involved be reliable in order to address these difficulties. It is found that the Blockchain technology adequately handles all such defies. The goal of this effort is to build a decentralized rather than centralized e-voting system using blockchain technology, which ensures voter identity security, data transfer privacy, and verifiability through a transparent and open voting process. Blockchain provides transparency, security, anonymity and a huge time reduction in the processing of election results. In our proposed framework, the votes of the citizens of the constituency/organization are stored as transactions on the blockchain after getting digitally signed. The transactions stored on the blockchain are immutable and only valid users are allowed to cast votes, hence providing transparency and security to a large extent.

The complete system of the proposed work, as mentioned in Fig 1, works as follows: The users interact with the client side application running on a node.js server, created with the help of HTML and CSS. The users enter their details and cast votes on the application. The user's response is then sent to the backend with the help of Express.js. The node then validates the user, digitally sign the transaction and try to mine a new block containing user's vote as a transaction. All the other nodes verify the block and after consensus the block is added to the chain.

IV. Implementation and Results

This section discusses in detail how the E-voting system is implemented with blockchain at the backend.

A. Technologies used

1. Node.js: It is an open source environment which provides server platform to run JavaScript code.
2. Express.js: Express.js, or just Express, is a Node.js back end web application framework. It is envisioned to develop the APIs and web applications.
3. JavaScript: it is a lightweight programming language. It is generally utilized for the development of applications that are network-centric.
4. HTML: Stands for Hyper Text Markup Language; used for designing webpages and web applications.

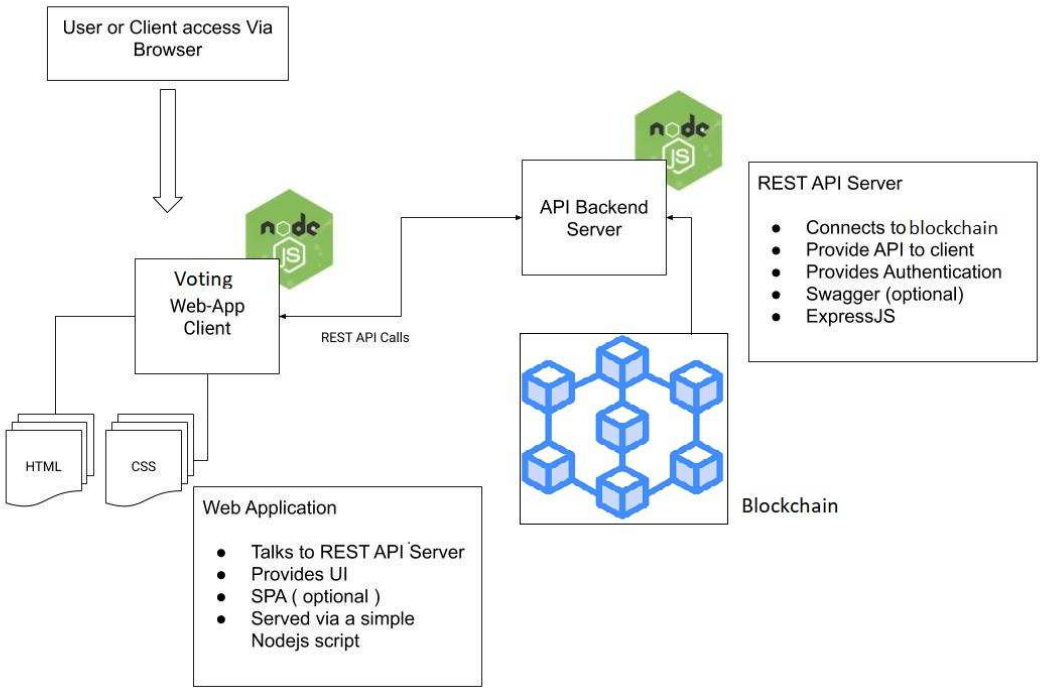

Fig. 1. System design of proposed work

B. Consensus Algorithm

1) Issue: Modern machines can add transactions and blocks at breakneck speed, but we don't want people creating hundreds of thousands of blocks per second and spamming our blockchain. There is also a security vulnerability; you can change the contents of a block and then just recalculate the hashes for all subsequent blocks, resulting in a legal chain despite the fact that you tampered with it.

2) Solution Implementation: To solve these issues, block chains have something that is called consensus With this approach, you must demonstrate that you used a significant amount of computational power to create a block. This is also known as mining. We need a system that requires a lot of computational power; this is achieved if the hash of a block must begin with a specific number of zeroes. We are implementing a variation of the existing Proof of Work (PoW) algorithm. We decide to simply try a lot of variations and hope to get lucky with a hash that has a sufficient number of zeroes in front of it because we can't alter the outcome of a hash function. This is also known as the difficulty, and it is regulated such that there is a constant supply of fresh blocks. Currently, our work has dynamic difficulty. It gets updated depending on the mining rate of the previous block. The difficulty of the previous block is used, and the difficulty is adjusted based on this difficulty and the timestamp. We aim to make the hash of the current block start with a specific number of zeroes. For this reason, we have added a nonce to the block, whose value can be changed to meet the hash requirement.

The algorithm for block mining works as follows:

1. The nonce variable is initialised with 0
2. A loop is started in which the nonce is increased by 1 in every iteration
3. In each iteration, the difficulty for the new block is adjusted based on the mining time of previous block
4. If previous block took more time than difficulty is reduced by 1, else it is increased by 1
5. Then, the hash of the new block is calculated and it is checked if the hash starts with the number of zeroes equal to the difficulty
6. This process repeates until the required hash is found
7. When the required hash is found the loop is terminated and block is mined and broadcasted to the peers.

C. Digital Signature on Transactions

It should be mandatory for a transaction to be signed with the public and private key of the voter so that we can cast vote from a valid account only if we have the private key of it.

1) Generating key pair: The elliptic curve that we are using is secp256k1. This is the algorithm that is also the basis of Bitcoin wallets. When a user wants to generate a public key from their private key, they multiply it by the Generator Point, which is a defined point on the secp256k1 curve.

2) Anonymity: To sign the transaction, firstly the SHA256 hash of the transaction is generated and it is this hash that is signed using the user's private key. From user's private key, its public key can be generated. Before signing of the transaction it is checked if the public key equals the fromAddress or not. We can only vote from the account that we have the private key for and because the private key is linked to the public key, this means that the fromAddress in our transaction has to equal your public key. If the public key is not equal to the fromAddress then the transaction stands invalid.

D. Peer to Peer Network

P2P networks are an important component of blockchain technology, as they support a decentralized ledger of transactions. To implement P2P, WebSocket in JS is used. This module connects different sockets to one another and is used for sending and syncing the blockchain. Every time a new peer is added, it is provided with the latest version of blockchain from existing peers. Whenever a miner mines a new block, the block is sent to all the peers currently active. The peers validate is the block is authentic and accordingly add it to the chain, else reject it.

E. Example

We consider 3 nodes connected on the network, each doing a different task. Firstly, to connect a node to the network, it should know about its peers that are already on the network. Fig 2 shows how 3 nodes are connected on the network by specifying their peers and ports.

Now, the node at Port 3001 votes for its favorite candidate by entering the correct Aadhar number and private key, as mentioned in Fig 3. After validation, this creates a transaction in the transaction pool.

Node 2 at port 3002 now mines a new block by using its computational resources as shown in Fig 4. The transactions are then stored on the block and the new chain is shared with the other nodes. The other nodes check if the incoming chain is valid and longer than their current chain and then replace their chain with the incoming chain accordingly.

After mining a new block, the respective node adds a new block to its chain and broadcasts the updated chain to its peers. The peer nodes replace their chain with the new chain after validation the incoming chain as shown in Fig 5.

F. Results

The above subsection shows how the E-voting system works at the backend and the frontend. In this work, we have achieved the following results.

The above subsection shows how the E-voting system works at the backend and the frontend. In this work, we have achieved the following results.

1) Security: We have implemented several checkpoints to ensure security in our e-voting system. We are making it mandatory for a transaction to be signed with the public and private key, in which the private key is only known to the user. The hash of this transaction is digitally signed by the user. In the case where public key is not equal to the formAddress the user is not able to sign the transaction, if there is no signature or the signature length is zero then the transaction is invalid. Another checkpoint to make sure that the transaction is valid and secure is to extract the public key from the fromAddress and see if the transaction has been signed with that key or not.

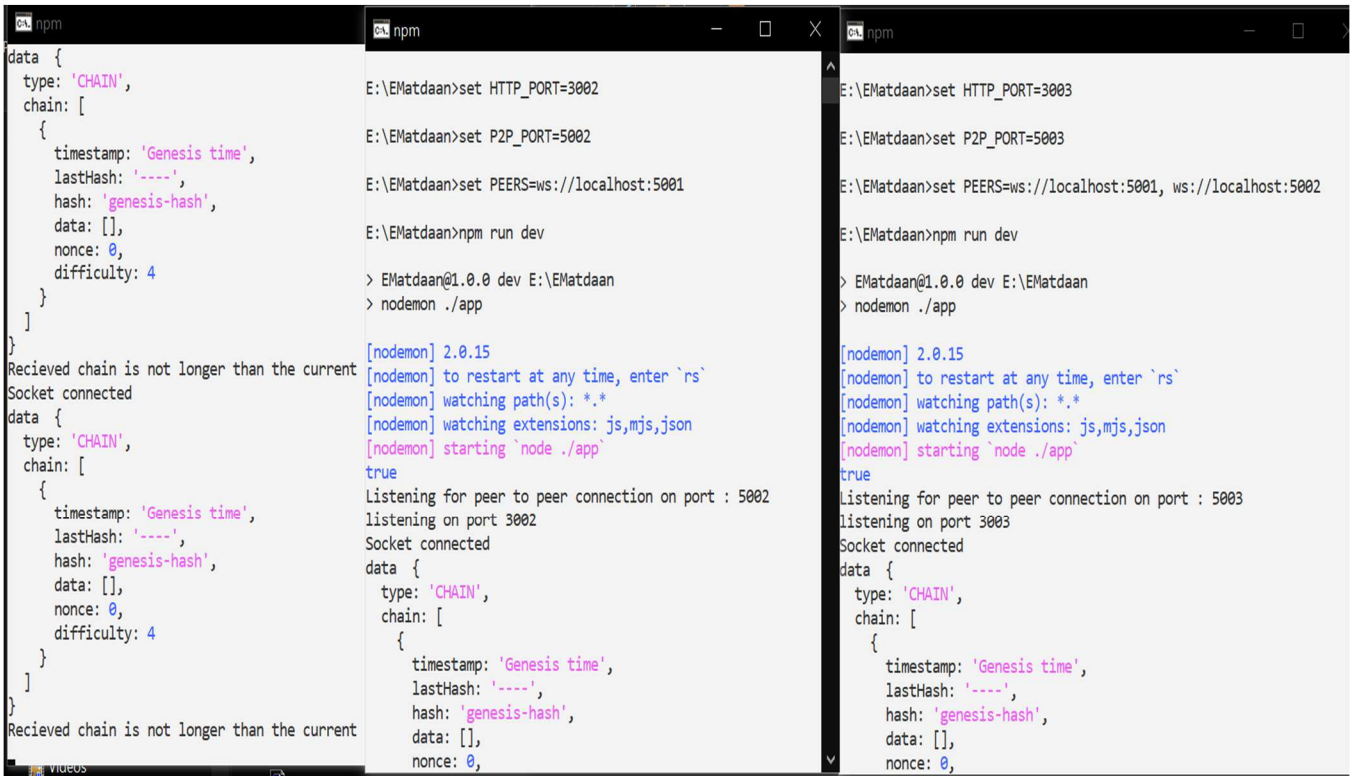

Fig. 2. Commands to add nodes on the network

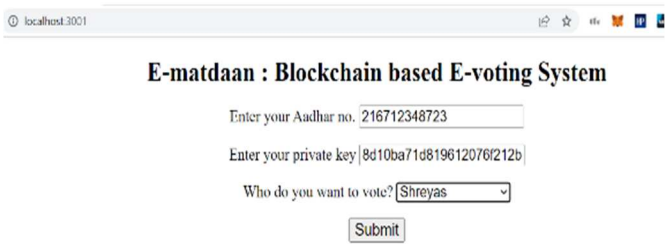

Fig. 3. User voting for his preffered candidate

2) Anonymity: Which voters have voted for which candidate is not known to anyone except the voter himself in the implemented system. The users vote transactions are stored with their key pair as the id. Without user's private key it is impossible to map who the user is. Hence, the system provides anonymity and safety to the users.

3) Transparency: The voting results can be viewed in real time as shown in Fig 6. The results get updated every time a new block is mined. Hence, providing transparency in the system.

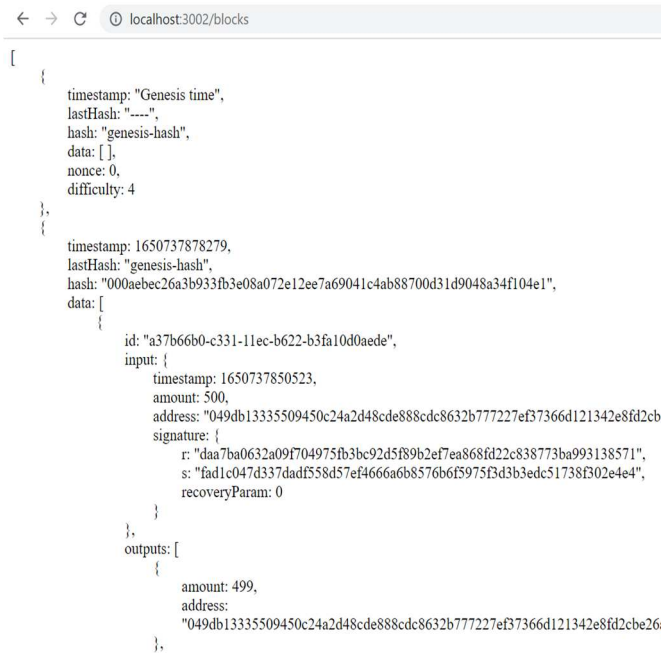

Fig. 4. Miner mining a new block

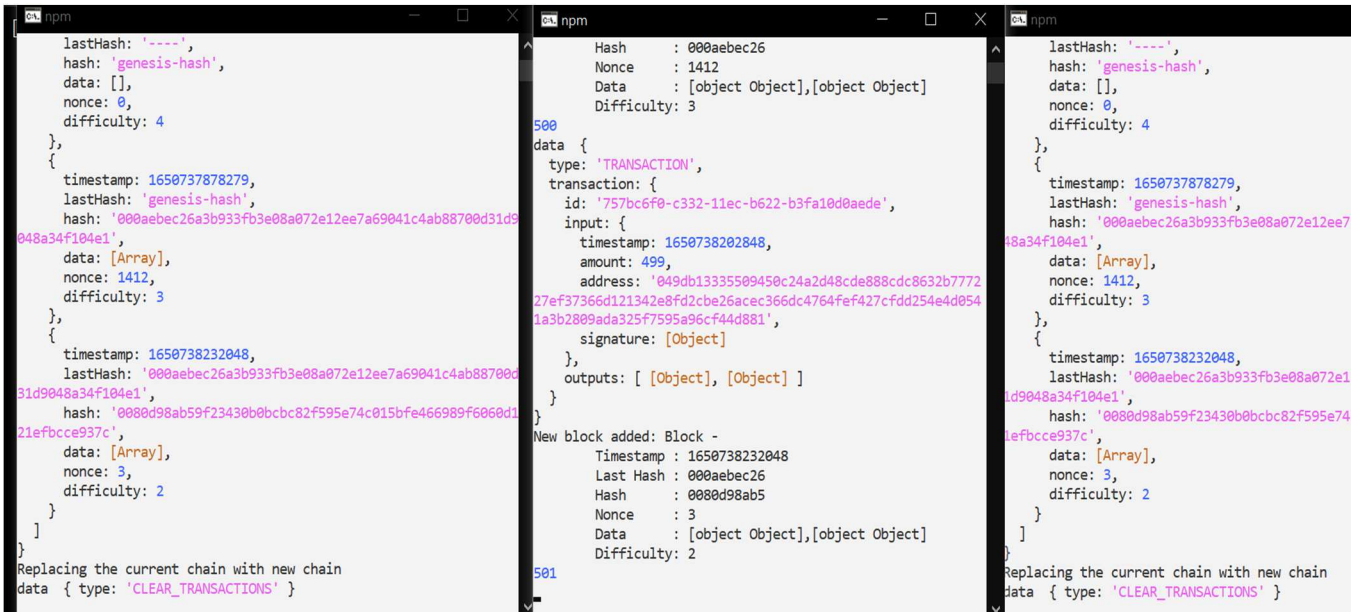

Fig. 5. New block is added and broadcasted to other nodes

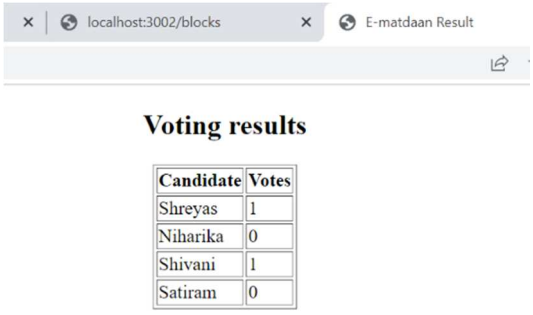

Fig. 6. Interface of voting results

V. CONCLUSION

Learning about the vast drawbacks of the traditional voting systems, a system which is secure, decentralized and transparent is the need of the hour. We have successfully implemented a voting system where the votes are stored on a blockchain in a decentralized manner. This system allows users to login using their Aadhar number and cast vote using their private key. The valid votes are recorded as transactions and stored in the transaction pool. Whenever a miner mines a block, the transactions in the pool get stored in the block. The results portal has also been implemented successfully where live results of the voting are shown with complete transparency. Till now, we have implemented the E-voting system with a maximum of 4 nodes on the network. In future, we plan to extend this to a large number of nodes. Also, we plan to link the work with the UIDAI database so that Aadhar verification process is made more efficient.

REFERENCES

[1] S. A. Adeshina and A. Ojo, "Maintaining Voting Integrity using Blockchain," 2019 15th International Conference on Electronics, Computer and Computation (ICECCO), Abuja, Nigeria, 2019, pp. 1-5.

[2] Y. Abuidris, A. Hassan, A. Hadabi and I. Elfadul, "Risks and Opportunities of Blockchain Based on E-Voting Systems," 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, Chengdu, China, 2019, pp. 365-368.

[3] S. Bistarelli, I. Mercanti, P. Santancini, and F. Santini. “End-to-end voting with non-permissioned and permissioned ledgers,” Journal of grid computing, Vol. 17, No. 1, pp. 97-118, 2019

[4] C. K. Adiputra, R. Hjort and H. Sato, "A Proposal of Blockchain-Based Electronic Voting System," 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 2018, pp. 22-27. S. M. Khan, A. Arahad, G. Mushtaq, A. Khalique, and T. Husein, “Implementation of decentralized blockchain e-voting,” In EAI Endorsed Transactions on Smart Cities, Vol. 4, No. 10, p.e4, 2020.

[5] S. Agbesi and G. Asante, "Electronic Voting Recording System Based on Blockchain Technology," 2019 12th CMI Conference on Cybersecurity and Privacy (CMI), Copenhagen, Denmark, 2019, pp. 1-8.

[6] https://www.ibm.com/in-en/topics/what-is-blockchain

[7] W. Stallings, “Cryptography and Network Security”, 4/E. Pearson Education India, 2006.

[8] A.K. Maurya, and A.K. Tripathi, “Performance comparison of heft, lookahead, ceft and peft scheduling algorithms for heterogeneous computing systems,” 2017 7th International Conference on Computer and Communication Technology,ACM, November 2017, pp. 128-132.

[9] A.K. Maurya, and A.K. Tripathi, “On benchmarking task scheduling algorithms for heterogeneous computing systems,” The Journal of Supercomputing, Vol. 74, No. 7, pp. 3039-3070, 2018.

[10] A.K. Maurya, and A.K. Tripathi, “ECP: a novel clustering-based technique to schedule precedence constrained tasks on multiprocessor computing systems,” Computing, Vol. 101, No. 8, pp.1015-1039, 2019.

[11] A.K. Maurya, and A.K. Tripathi, “An edge priority-based clustering algorithm for multiprocessor environments,” Concurrency and Computation: Practice and Experience, Vol. 31, No. 11, p.e5060, 2019.

[12] T. M. Roopak and R. Sumathi, "Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology," 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India, 2020, pp. 71-75.

[13] E. Bellini, P. Ceravolo and E. Damiani, "Blockchain-Based E-Vote-as-a-Service," 2019 IEEE 12th International Conference on Cloud Computing (CLOUD), Milan, Italy, 2019, pp. 484-486.

[14] E. Febriyanto, Triyono, N. Rahayu, K. Pangaribuan and P. A. Sunarya, "Using Blockchain Data Security Management for E-Voting Systems," 2020 8th International Conference on Cyber and IT Service Management (CITSM), Pangkal, Indonesia, 2020, pp. 1-4.

[15] K.M. Khan, J. Arshad, and M.M. Khan, “Secure digital voting system based on blockchain technology,” International Journal of Electronic Government Research (IJEGR), Vo. 14, No. 1, pp. 53-62, 2018.

[16] E. Yavuz, A. K. Koç, U. C. Çabuk and G. Dalkılıç, "Towards secure e-voting using ethereum blockchain," 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 2018, pp. 1-7.