BEE – Blockchain Enabled Election System

Aditya Mahatpure [1], Rashmi Jain [2], Srividya Avadhani [3], Mrunal Gandhare [4], Arnav Laturkar [5], Mukul Singh Kushwah [6]

[1] UG Student, Department of Computer Science & Engineering, S. B. Jain Institute of Technology, Management & Research, Nagpur, Maharashtra, India
[2] Professor, Department of Computer Science & Engineering, S. B. Jain Institute of Technology, Management & Research, Nagpur, Maharashtra, India
[3] UG Student, Department of Computer Science & Engineering, S. B. Jain Institute of Technology, Management & Research, Nagpur, Maharashtra, India
[4] UG Student, Department of Computer Science & Engineering, S. B. Jain Institute of Technology, Management & Research, Nagpur, Maharashtra, India
[5] UG Student, Department of Computer Science & Engineering, S. B. Jain Institute of Technology, Management & Research, Nagpur, Maharashtra, India
[6] UG Student, Department of Computer Science & Engineering, S. B. Jain Institute of Technology, Management & Research, Nagpur, Maharashtra, India

---

Abstract - *Election is an important event in democratic countries however massive sections of society don't trust their election system because of different frauds involved which is major concern. Vote tampering, wrong calculation of votes and other frauds pollute the efficiency of voting environment. Online voting can be a breakthrough to deal with such issues. It has great potential to decrease costs involved and increase number of voters. Despite these benefits, online voting solutions have to be dealt with great caution because they might introduce unforeseen threats as technologies are unpredictable. Blockchain is a type of cryptographic technology that has nodes and ledger. The ledger exists in many different locations, no single point of and distributed management that will append new transactions to the ledger hence maintain security. Also, majority of the network nodes must reach a consensus before an appending the transaction to ledger making it tamper proof. Blockchain offers decentralized solution for e-voting. This technology is a suitable alternative for general voting solutions. The project presents an effort to leverage benefits of blockchain to achieve an effective e-voting system along with its implementation to achieve an end-to-end verifiable e-voting scheme.*

Key Words*: *Keywords: Online voting, Blockchain, security, verifiable e- voting scheme.

1. INTRODUCTION

Online voting may be a trend that's gaining momentum in modern society and encompasses a potential to eliminate the requirement of printing ballot papers or polling stations. However, there are many styles of threats so it has to be addressed great caution. the main focus of the project is to form a safer, transparent, immutable, and reliable web application – BEE (Blockchain Enabled Election System), for elections at institutional level using blockchain.

Elections are fundamental pillar of a democratic system enabling the final public to specific their views within the sort of a vote. because of their significance to our society, the election process should be transparent and reliable so on ensure participants of its credibility. Blockchain is one among the emerging technologies with strong cryptographic foundations enabling applications to leverage these abilities to realize resilient security solutions. It may well be a distributed, immutable, incontrovertible, public ledger; offers a decentralized node for online voting. it's an appealing alternative thanks to security. This new technology works through three main features:

- The ledger exists in many alternative locations: No single point of failure within the maintenance of the distributed ledger.
- There is distributed management that may append new transactions to the ledger.
- A majority of the network nodes must reach a consensus before a proposed new block of entries becomes a permanent a part of the ledger.

2. LITERATURE SURVEY

Stuart Haber and W. Scott Stornetta created the so-called Black Chain in 1991. His previous work was working on a chain of cryptographically secure blocks so that no one could manipulate the timestamps of documents. In 1992, they upgraded their system to include Merkel trees that increase efficiency by launching more document collection in the same block. However, in 2008 Blackchain history began to gain relevance, thanks to the work of an individual or group called Satoshi Nakamoto. Satoshi Nakamoto has been identified as the mindset behind blockchain technology. Little is known about Nakamoto because people believe it was the person or group of people who worked on Bitcoin, the first application of digital ledger technology. Nakamoto first created the blockchain in 2008, from which the technology evolved and entered into many applications beyond cryptocurrencies. Satoshi Nakamoto released the first white paper on technology in 2009. In the White Paper, he explained how technology is well-equipped to enhance digital confidence according to the decentralization theme, which means no one is in control of anything.

Electronic voting is a voting technique in which votes are recorded or counted using electronic devices. Electronic voting is generally defined as voting that is supported by certain electronic hardware and software. Such regulators should be able to support / enforce various functions from the electoral system to vote storage. Several articles have recently been published highlighting the security and privacy issues of blockchain-based electronic voting systems. Lai et al. Suggested a decentralized anonymous transparent electronic voting system (DATE) that required a minimum of trust between participants. They hope that the current DATE voting system will be conducive to mass electronic elections. Unfortunately, their proposed

system is not robust enough to protect against DoS attacks, as there is no third party authority over the scheme responsible for auditing votes after the election process. Due to the limitations of the platform this system is only suitable for small scales. Although the use of ring signatures protects the privacy of individual voters, it is difficult for multiple signatories to manage and coordinate. They also use the PoW consensus, which has significant flaws such as power consumption: miners' "supercomputers" monitor millions of calculations per second, which is happening worldwide. Because this setting requires high computational power, it is expensive and consumes energy. [1]

On a small scale, blockchain-based systems have sought to address issues of anonymity, privacy and security in elections. However, several additional issues were highlighted. Proof of labor, for example, is a mathematically vast and challenging task that requires enormous energy to complete. Third-party involvement is another issue that could affect end-to-end verification, as there is a significant risk of data tampering, leakage and incorrect table results. Large-scale, building and ceiling blocks delay the voting process. [2]

A blockchain-based anti-quantum electronic voting protocol with an audit function has also been proposed. They also modified the code-based Niederreiter algorithm to make it more resistant to quantum attacks. Key Generation Center (KGC) is a non-certified crypto system that acts as a regulator. This will not only identify voter anonymity but also facilitate audit performance. However, considering his system, the security and efficiency benefits of small-scale elections, even if the number of voters is small, are significant. If the number is high, some capacity is reduced to provide better protection. Yi introduced the blockchain-based electronic voting scheme (BES), which provides ways to improve electronic voting security on peer-to-peer networks using blockchain technology. BES is based on Distributed Ledger (DLT), which can be used to prevent voter error. The system has been tested and built on Linux systems on the P2P network. In this technique, counter-measurement attacks have become an important issue. This method requires the involvement of responsible third parties and is not suitable for centralized use in systems with multiple agents. The distributed process, i.e. the use of secure multipart computers, can solve the problem. [3]

Block-based e-Voting Architecture (BEA) has rigorously experimented with approved and unlicensed blockchain architectures through a variety of scenarios, including voting population, block size, block generation rate and block transaction speed. Their experiments have found fascinating results on how these parameters affect the overall scalability and reliability of electronic voting models, including the interchangeability between different parameters and measures of security and performance. In his scheme, the electoral process requires a voter address and a candidate address. These addresses are used to cast ballots for candidates from voters. Mining Group updates major blockchain ledger to track votes and vote status. Voting status will not be verified until the Minor Lead Ledger is updated. The ballot is then cast with a voting machine at the polling station. However, some flaws were found in this model. It does not have the regulatory power to prohibit invalid voters from casting their vote and this is not protected by quantum attachment. Their design is inaccurate and ignores voter integrity. [4] Overall, we propose to improve the system:

- Website GUI has been improved and optimized for new usage

- Email Verification makes it better and removes the problem of fake votes in the system.

3. WORK DONE

The aim of our project is to create an electronic voting system using a blockchain. By using blockchain, the voting process can be made more secure, transparent, consistent, and credible. The blockchain-based online voting system can overcome common errors in the online voting system as it is based on the decentralization system. There will be a certain number of nodes connected to the main ledger, the vote will be limited to one voter and is calculated if the majority of nodes confirm the fact that a particular vote has not been registered on any of the nodes previously.

3.1 System Architecture

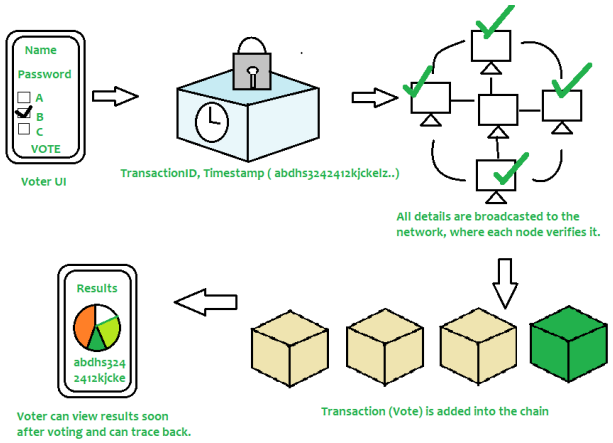

Fig. 1. System Architecture of BEE

Voter UI is responsible for voter interaction and controller. Transaction Management is a key component of architecture where operations are mapped to blockchain transaction to be mined. This mapping also contains information provided to voters for verification. This data is then used to create a cryptographic hash and contribute to the creation of a transaction ID. Verification of such information is assumed to benefit from User Engagement. Several real-world node scenarios are involved in the mining system so that these transactions end up in a series. Ledger Sync Layer aligns the Multichain ladder with a specific application website using some of the existing website technologies. Featured votes are recorded in the data tables at the back of the site. Voters are able to track their votes using the unique identifier provided as soon as their vote is mined and added to the blockchain. Voter security considerations are based on block-chain technologies that use cryptographic hashes to secure final communications. Voting results are also stored on the application website with a view to conducting audits and any other activities over time.

3.2 Modules

The system is divided into two modules - Election Management Module (Server Side) and Voter & Candidate Management (User Side)

Module 1 - Election Management (Server Side) manages the election life cycle. Many trusted institutions and companies have registered for this role. The electoral commissioner will determine the nature of the election and create the aforementioned election, prepare the votes, register voters, determine the life of the election and allocate polling stations. Election officials make notes. This geographical app works with a smart election creation contractor, in which the administrator defines a list of candidates and constituencies. Election counting is done in an instant on smart contracts. Each smart ballot contract creates its own corresponding position in its final position. Once the election is over, the final result of each smart contract is published.

Module 2 - Voter & Candidate Management (User Side) is the part when an election is held the election administrators must specify a deciding list of eligible voters. This requires part of the government's identity verification service to securely verify and authorize the right people. As mentioned earlier, each voter receives the ID of his or her vote. Each voter can go to the website for confirmation. The voter can therefore see his or her vote on the blockchain, which ensures that it is calculated and calculated correctly.

3.3 Flowchart

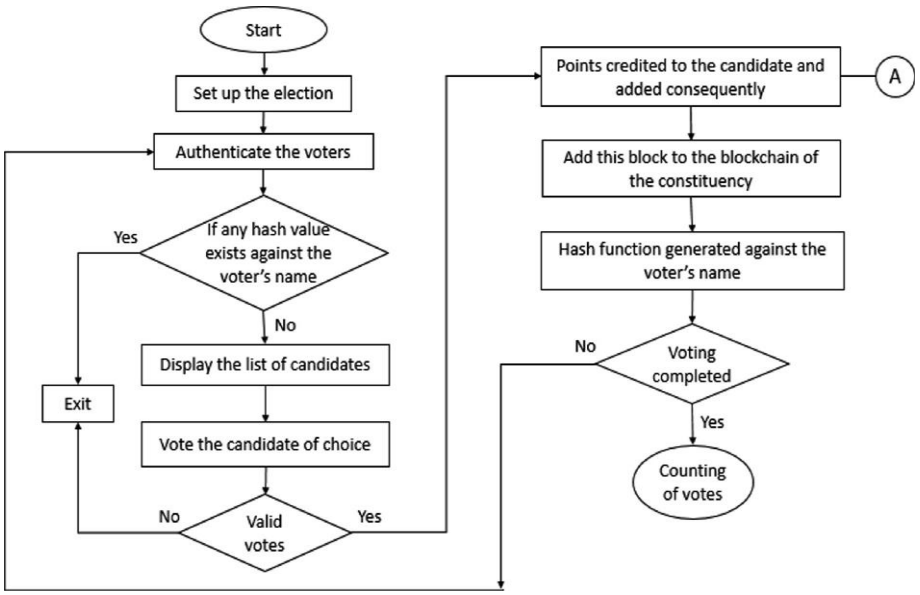

Fig. 2. Flowchart of BEE

Usually, the voter enters the system after successful login, the voter is then given a list of available elections and then candidates for voting. Conversely, login fails, any additional access will be denied. After a successful vote, more miners are dug to ensure that valid and certified votes are included in the public register. Voter security considerations are based on blockchain technology that uses cryptographic hashes to secure final verification. Successful vote is considered a transaction

within the blockchain voting application. Therefore, voting is added as a new block (behind successful mines) to the blockchain as well as recording in the data tables behind the website. The system guarantees only the property of one person, one vote (democracy) of the voting system. After the end of voting, the results are calculated.

4. DISCUSSION OF RESULTS

End users will not see much difference between a blockchain-based voting system and an electronic voting system. On the other hand, voting on a blockchain will be a fully encrypted and stored piece of data on a blockchain network that is distributed on a single server. The blockchain consensus process confirms each encrypted vote, and the public records each vote on distributed copies of the blockchain block. The Center will monitor how votes are recorded and recorded, but this information will not be limited to policy. The blockchain voting system is separate and fully open, yet ensures that voters are safe. This means that anyone can count the votes by voting via electronic blockchain, but no one knows who voted for who. Ordinary electronic voting and blockchain-based electronic voting applies to organizational ideas in stages.

The current Blockchain-based Electronic Voting Systems applied to the following businesses and organizations, established but developed mainly over the past five years, are improving the voting sector. They all share a strong blockchain network vision to highlight performance. Blockchain-based voting systems currently have growth problems. However, their systems do not work well at the national level to control millions of jobs. Our system's screenshots are as follows:

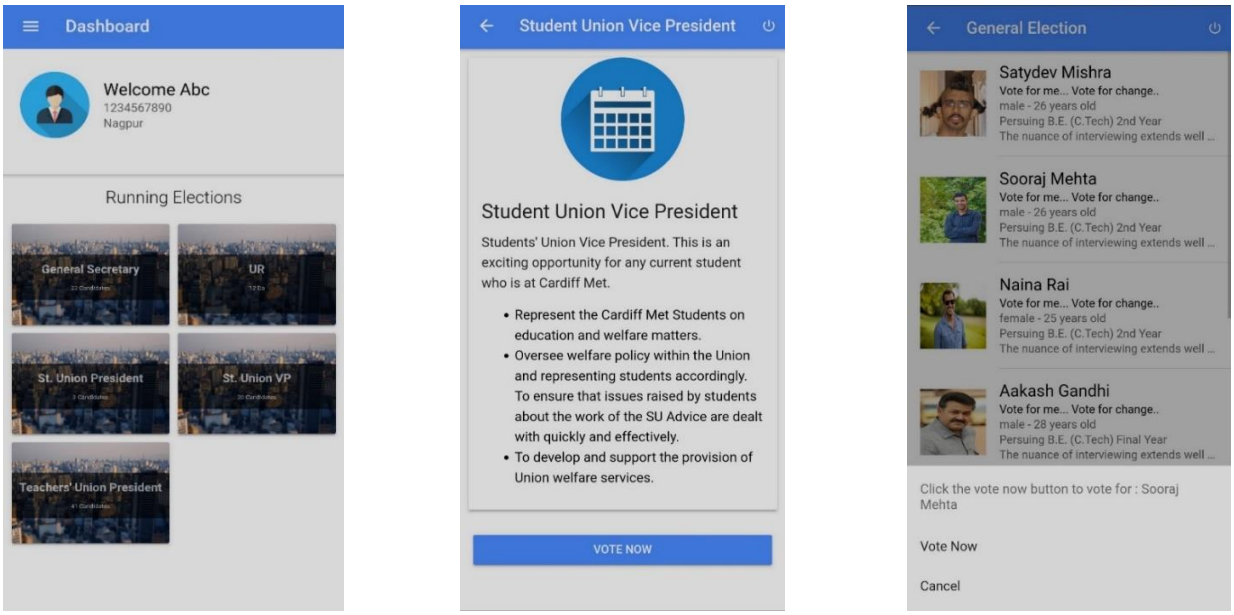

Fig. 3. Screenshots of BEE

5. ANALYSIS

Blockchain is an attractive alternative to conventional electronic voting systems with features such as segregation, non-disclosure, and security protection. Used to hold both boardroom and public voting. There are a few implementations of the blockchain voting system, however, some challenges remain in the system that need to be addressed. First, the lack of a simple Graphical User Interface (GUI) makes it difficult for people with limited computer experience to use a website and vote with one hand. This creates a privacy issue, which is an important factor in any voting system. Second, users of blockchain voting systems are generally anonymous which makes it difficult to confirm or identify the user who is voting. This anonymity of users leaves the system vulnerable to various illegal activities.

To address these issues our website features an easy-to-use GUI with guidance notes that help the user find his or her way to the website. These notes will be provided in the form of warning boxes that will appear when a user clicks a question mark next to all the buttons on a web page. In addition, we have used an additional verification layer that sends email to the user containing the OTP and the query the user has already given their response while registering on the website, this will help to identify users more effectively. So, after looking at and analyzing all the research papers and work we found some things we could add to. To address existing problems, our website features an easy-to-use GUI with guide notes that help the user find his or her way to the website. These notes will be provided in the form of warning boxes that will appear when a user clicks a question mark next to all the buttons on a web page. In addition, we have used an additional verification layer that sends email to the user containing the OTP and the query the user has already given their response while registering on the website, this will help to identify users more effectively. Overall, we propose to improve the system by:

• Website GUI Improved and customized for new user.

• Email Verification makes it better and removes the problem of fake votes in the system.

6. CONCLUSION

Electronic voting has been used in varying forms since 1970s with fundamental benefits over paper-based systems such as increased efficiency and reduced errors. With the extraordinary growth in the use of blockchain technologies, a number of initiatives have been made to explore the feasibility of using blockchain to aid an effective solution to e- voting. This paper has presented one such effort which leverages benefits of blockchain to achieve an effective solution to e-voting.

REFERENCES

1. Lai, W.J.; Hsieh, Y.C.; Hsueh, C.W.; Wu, J.L. Date: A decentralized, anonymous, and transparent e-voting system. In Proceedings (August 2018)

2. Shahzad, B.; Crowcroft, J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology (2019)

3. Gao, S.; Zheng, D.; Guo, R.; Jing, C.; Hu, C. An Anti- Quantum E-Voting Protocol in Blockchain with Audit Function. (2019)

4. Khan, K.M.; Arshad, J.; Khan, M.M. Investigating performance constraints for blockchain based secure e-voting system. (2020)