Irish Interdisciplinary Journal of Science & Research (IIJSR)
Vol.6, Iss.2, Pages 81-86, April-June 2022

E-Voting using Blockchain Technology

R.Madhanachithran[1], Sasikala R[2], Shalini A[3] & Vinitha R[4]

[1]*Assistant Professor, Department of Information Technology, Vivekanandha College of Technology for Women.*
[2-4]*Student, Department of Information Technology, Vivekanandha College of Technology for Women.*

DOI: http://doi.org/10.46759/IIJSR.2022.6211

Article Received: 15 March 2022 *Article Accepted: 22 May 2022* *Article Published: 16 June 2022*

ABSTRACT

Blockchain is a decentralized, digital, and consensus-based secure information storage system. This article gives an overview of how to use the blockchain to construct a secure and trustworthy electronic voting system. The main goal of this paper is to investigate the most recent state of blockchain-based voting research while attempting to foresee the accompanying potential issues future developments. This paper's technique is as follows: a methodical approach to review and following an overview of the blockchain's core structure and properties in relation. We present a conceptual definition of e-voting. Desired e-voting application based on blockchain symmetrical improvements in asymmetrical cryptography are also important. We gathered and examined a number of research papers from scientific databases that advocated for the use of the blockchain architecture in voting systems. These articles suggested that blockchain-based voting systems may offer alternatives to standard e-voting. The most pressing challenges were divided into five categories: general, integrity, coin-based, privacy, and consensus. As a consequence of this study, it was discovered that blockchain systems can help solve some of the issues that now plague election systems. We are attempting to design a system that respects the essential and most significant aspects of a voting system, such as transparency, secrecy, security, and decentralisation, while also providing the extra benefit of mobility.

1. Introduction

One of the most crucial pillars of any democracy is voting. The existing voting mechanism has a lot of flaws. Strong foundation, yet it suffers from numerous flaws. The most noticeable is a lack of mobility. As voting is a highly important procedure that every citizen of any country should participate in. This is expected to involve a nation or organisation. The voting centres are at a fixed location. Certain stations make it extremely challenging and problematic for people to line for hours in order to vote. That's where the proposed idea as a workaround comes in. Elections can be conducted virtually. Because online voting is so simple to set up, it has a number of problems, such as a generic system becoming overrun with spam and flaws in security. The recommended solution is unique. Any general solution since it makes use of the concept of the application will benefit from blockchain Technology. This solution includes mobility as well as intends to make the system as safe as an offline system voting methods that take into account a variety of criteria voting system features such as voter secrecy and security.

A blockchain could be a public ledger that is distributed, immutable, and indisputable. The four primary elements of this innovative technology are as follows:

1. The ledger can be found in a variety of places: No Maintenance of the distributed ledger has a single point of failure.

2. A UN agency with distributed administration will add new transactions to the database ledger.

3. Any "new block" to the ledger that is proposed should refer to prior version of the ledger, creating a link.

4. Before a proposed new block of entries becomes a permanent part of the ledger, a majority of the network nodes must agree. These technological possibilities use modern cryptography to provide a level of security

equivalent to or greater than any previously notable data. Several countries, including the United States, consider Blockchain technology to be the finest tool for producing the new popular democratic voting process. The use of blockchain as a service to construct an associate degree electronic ballot (e-voting) system is evaluated in this research.

The system then makes the following unique contributions:

1. Investigate existing blockchain frameworks for building blockchain-based e-voting systems;

2. Suggest a blockchain-based e-voting system that alters liquid democracy using "permissioned blockchain."

2. Methodology

Blockchain is a system that treats each entry as a block and connects all of these blocks through an interlink, hence the name 'Block-Chain.' Every block contains all of the potential data for a single entity, together with a timestamp and, in rare cases, a nonce. All of the data in a block is then sent through a hashing function, which generates a hash value for everything. This hash value becomes the recent block's identity. The same hash function is applied to all data blocks. The genesis block is normally generated automatically, followed by the chain. A field in every block of the blockchain contains the preceding block address. This preceding block address is what connects any two blocks in a chain together. Avalanche effect is a characteristic of hashing functions i.e., even a minor modification in the original data has an impact. Any modification to its hash value has a tremendous impact.

Any data in a block will totally change its hash value, triggering a function since the new hash value will not match the value in the previous block field of the following block, effectively breaking the chain. This is the role of blockchain: it makes data unchangeable. SHA-256 is the hashing function utilised in this implementation. It is one of the most powerful hashing algorithms available.SHA-256 converts messages of up to 2 bits (2.3 billion gigabytes) into 256-bit digests (32 bytes).

The problem statement methodology proposed is multifaceted. The initial stage is user registration, which includes all required information to identify the user as a user. It is necessary to register the users. It's critical to ensure that the user belongs, maintain the reliability of that organisation. This can be accomplished by confirming the user's information on the basis of a strong document during registration, voter identification, nationality identification, and so on.

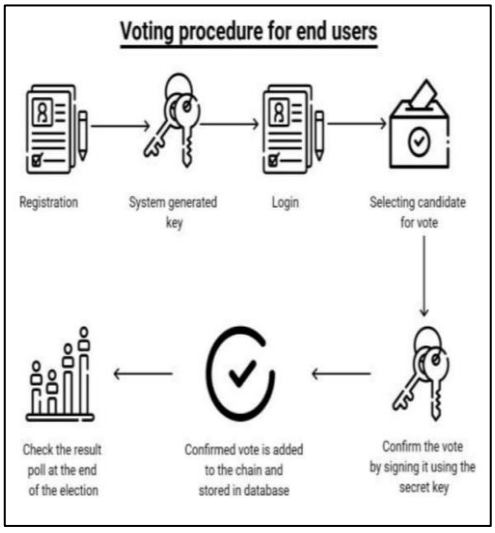
After the user has validated his identity and ability to vote in the elections, the user will proceed to the next step. The system will generate a secret key of 32 bytes (256 bits) that will be used to be kept private and secure at all times by the user. This secret key serves as a backup to the primary verification. User during the voting process and as a form of digital currency signature on a ballot. This key assists us with implementation. For our vote, we need confirmation of existent consensus.

The system encrypts the data stored in the database for the user using a symmetric key encryption algorithm, with this randomly generated secret key serving as the encryption key. As a result, this encrypted message can only be decrypted back to the original contents if the same key is used. AES 256 is the encryption algorithm utilised in the offered method.

AES 256 is a symmetric key encryption algorithm. This means that for both encryption and decryption, only one key is used. The encryption and decryption speed is similar to AES. Since, Asymmetric key algorithms are less computationally intensive. It has more power than an asymmetric one, and it is faster and more efficient, run efficiently AES256 is regarded as one of the most secure encryption algorithms. The most secure and quick encryption methods ever devised.

After logging in with the credentials he used to register, the user must select the candidate for whom he wishes to vote during the voting phase. After the user has confirmed the candidate for whom he wishes to vote, he must enter the secret key that was generated throughout the voting process registration. This code will be decrypted using this secret key. Text is encrypted. If the decryption result is the same, we can decrypt the data that was previously encrypted, check that the person who is currently voting is actually, the user voted in the election and no one else did.

The vote will be made into a block and put to the blockchain once it has been verified, and the user's transaction history will be changed to prevent the same user from casting numerous votes.



3. Proposed System

In India, this is the current voting method. Electronic ballet is used to cast votes under this system. We vote in a hardware machine in this game. This is a collection of counters and cash registers. This voting technique is straightforward and straightforward. For electoral commissions, it has advantages like as mobility, security, and flexibility. However, in today's environment, everyone is so busy that they don't have time to vote. This paper takes a look at the electronic voting process from a different angle. This includes, but is not limited to, identifying the polling process and the actual voting process employed on election day.

4. Related Works

Some notable work has already been done in this topic, and it has been referenced to in order to get a general notion and grasp a few important concepts needed for this study. To get a general understanding of how the author attempted to tackle a comparable problem utilising Ethereum as a blockchain network, we looked the research papers [1-3].

To gain a better understanding of how Ethereum operates and whether it can be included in the study, researchers turned to research paper [4]. We also looked at paper [5] for inspiration from a study that tackled the same issue as us. Many other references, including those listed below, are used to better grasp specific topics by reading past work in the field. Following the referral of different connected works, a comprehension of a variety of subjects, including blockchain security and blockchain structure, current blockchain networks, and general information. Benefits and downsides of voting methods, among other things topics was acquired.

5. Existing System

In India, this is the current voting method. Electronic ballet is used to cast votes under this system. We vote in a hardware machine in this game. This is a collection of counters and cash registers.

This voting technique is straightforward and straightforward. For electoral commissions, it has advantages like as mobility, security, and flexibility. However, in today's environment, everyone is so busy that they don't have time to vote.

This paper takes a look at the electronic voting process from a different angle. This includes, but is not limited to, identifying the polling process and the actual voting process employed on election day.

6. Results and Discussions

This is the home page, which is made up of many parties.

Figure 1. Home page

This page enables the administrator to log in (Admin).

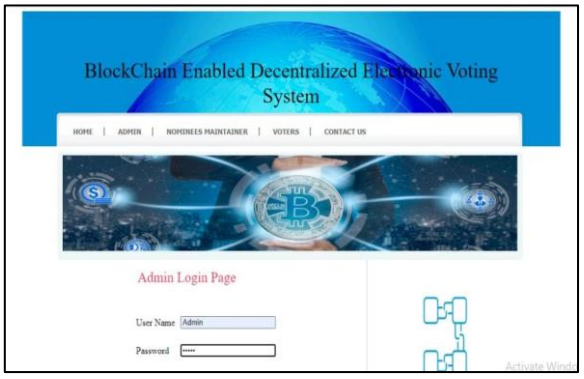


Figure 2. Admin Login

This page allows you to search for, add, and update new candidates.

Figure 3. Candidate management page

A new candidate can register on this page.

Figure 4. Candidate Registration Page

This page enables the voter to log in.

Figure 5. Voter login page

A new voter can register on this page.

Figure 6. Voter Registration Page

7. Conclusion

Based on blockchain block generation and sealing, we built an effective approach for generating a block for each vote. Each candidate's votes can be counted using the sealed blocks. Only a voter can access his or her data and who voted for them in our proposed system, which overcomes the disadvantage of votes being cast through EVM. There is no way to guarantee that votes are cast in some sort of electoral fraud. Despite the fact that blockchains are quite secure when it comes to securing data stored on them, the biggest issue arises when clients fail to protect their private credentials. This means that private keys are always at risk of being stolen. As a company or undertaking, you must educate clients on how to preserve their private keys.

Declarations

Source of Funding

This research did not receive any grant from funding agencies in the public or not-for-profit sectors.

Consent for publication

Authors declare that they consented for the publication of this research work.

References

[1] Linh Vo-Cao-Thuy, Khoi Cao-Minh, Chuong Dang-Le-Bao, Tuan A. Nguyen, "Votereum: An Ethereum-based E-voting system", IEEE.

[2] E. Hubbers et al., "RIES-Internet Voting in Action", in Proceedings of the 29th Annual International Computer Software and Application Conference, IEEE Computer Society, Washington DC, USA, pp.417-424, 2005. http://dx.doi.org/10.1109/COMPSAC.2005.132.

[3] Ayed, A.B. (2017). "A Conceptual Secure Blockchain Based Electronic Voting System". International Journal of Network Security Its Applications, Vol.9, No.3, May 2017.

[4] Vitalik Buterin. (2015). "Ethereum White Paper", Available at: https:// github.com/ethereum/wiki/wiki/ White-Paper.

[5] Y. Wu, "An E-voting System based on Blockchain and Ring Signature (Thesis)," dgalindo.es, 2017.