International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 03, March-2021

E-Voting using Blockchain

Yash Dalvi
Information Technology
Vidyavardhini's College of Engineering and TechnologyVasai, Palghar

Shivam Jaiswal
Information Technology
Vidyavardhini's College of Engineering and TechnologyVasai, Palghar

Pawan Sharma
Information Technology
Vidyavardhini's College of Engineering and Technology
Vasai, Palghar

***Abstract*—Blockchain is a distributed, digitized and consensus- based secure information storage mechanism. The present article provides an overview of using blockchain to create a secure and reliable e-voting system. The primary purpose of this review is to study the up-to-date state of blockchain-based voting research along with associated possible challenges while aiming to forecast future directions. The methodology appliedin this paper is a systematic review approach. Following an introduction to the basic structure and features of the blockchainin relation to e-voting, we provide a conceptual description of the desired blockchain-based e-voting application. Symmetrical and asymmetrical cryptography improvements play a key role in developing blockchain systems. We have extracted and reviewed multiple research papers from scientific databases that have advised the adoption of the blockchain framework to voting systems. These articles indicate that blockchain-supported voting systems may provide different solutions than traditional e-voting. We classified the main prevailing issues into the five following categories: general, integrity, coin based, privacy and consensus. As a result of this research, it was determined that blockchain systems can provide solutions to certain problems that prevail in current election systems. Using this application we try to architect a system that maintains the core and most important principles related to a voting system like: transparency, confidentiality, security, decentralization and also provides an added advantage of mobility.**

***Index Terms*—e-voting, blockchain, cryptography, security, leveldb**

I. INTRODUCTION

Voting is one of the most important pillars of any democracy. The current system for voting has a very strong base but at the same time it has a lot of lackings. The most prominent one being lack of mobility. As voting is a very crucial process and every citizen of any nation or organization is expected to participate in this activity. The voting centers being statically placed at a certain station makes it really difficult and problematic for people to stand in long queuesto cast their vote.

That's where the proposed solution comes in as a virtual alternative to conduct an election. Online voting being very easy to implement also comes with a set of drawbacks as a generic system will be filled with security loopholes. The proposed solution differs from any generic solution as it leverages the concept of blockchain technology to make the application more secure. Along with mobility this solution also aims to make the system as secure as existing offline voting systems by considering various factors of a voting system like voter confidentiality, security, transparency, etc.

II. LITERATURE SURVEY

Some distinctive work has been done in this field already which has been referred for gaining the general idea and grasp a few key concepts required for this study.We referred to conference paper [1] to gain an overall idea on how the author tried to solve a similar problem using Ethereum as a blockchain network. Research paper [8] was further referredto get a better view of how Ethereum works and whether it can be included in the study. We also referred to paper [10] to gain an idea from a study which focuses on the same problem as us. SAlso many other references that have been mentioned below are referred to understand various concepts by reviewingprevious work in the same field. After referring various related work an understanding of var- ious topics such as blockchain security, blockchain structure, various existing blockchain networks, general voting systems perks and drawbacks and many other topics was gained. It also introduced us to various consensus algorithms such as proof of work, proof of existence, etc. This review helped us to formulate our own study and contribute to similar problems.

III. METHODOLOGY

Blockchain is a system in which rather than treating every entry as an individual we treat them as a block and connect all these blocks using an interlink hence the name 'Block-Chain'. Every block consists of all the possible dataof a single entity with a timestamp and sometimes preferably a nonce. All this data inside of a block is then passed through a hashing function which creates a hash value of all the data. This hash value becomes the identity of the recent block. All the blocks of data go through the same hash function.The first block is usually auto generated as a genesis blockand then the chain follows. Every block in the blockchain contains a field containing the previous block address. This previous block address is what creates a link between anytwo blocks in a chain. As hashing functions have a property of avalanche effect, viz. even a small change in the original data will have a massive impact on its hash value, any change made to any data in a block with change its hash value

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 03, March-2021

completely which in turn will trigger a function as the new hash value will not match the value present in the previous block field of the next block, thus breaking the chain. This is the function of blockchain through which it makes data immutable.The hashing function used in this implementationis SHA-256. It is one of the strongest hashing algorithms present. In SHA-256, messages up to 2 bit (2.3 exabytes, or 2.3 billion gigabytes) are transformed into digests of size 256 bits (32 bytes).

The proposed methodology for the problem statement is multifold. The first step is user registration with all necessary information that will identify the user as a valid member ofa nation or an organization to whom the elections concern. While registering the users it is important to make sure that the user actually belongs to that organization, country to maintain reliability of the system. This can be done by verifying the user details during registration on the basis of some strong document like voter ID, nationality identification,etc.

In the next step after the user has verified his identity and eligibility to participate in the elections. The system will generate a 32 bytes (256 bits) secret key which is to be kept private and secured by the user at all costs. This secret key acts as a secondary verification of the user during votingprocedure and also as a kind of digital signature on the vote. This key helps us implement proof of existence consensusfor our vote.

The way it works is that the system will take the data stored in the database for the user and encrypt it using a symmetric key encryption algorithm, using this randomly generated secret key as the key required for encryption. Which in turn means that this encrypted message can only be decrypted back to the original data if the same key is used during the decryption process. The encryption algorithm used in the suggested solution is AES 256.

AES 256 is a symmetric key cipher. This means only one key is used for both encryption and decryption. The advantage of symmetric key encryption algorithms like AESis the encryption and decryption speed. Since symmetric key algorithms require less computational power than an asymmetric one , it's faster and more efficient to run. AES256 is considered to be one of the most secure and fast encryption algorithms of all time.

During the voting phase after the user has logged in using the credentials he used while registering, he has to select the candidate he wants to vote for. After the user confirms the candidate he wants to vote for he has to enter the secret key that was generated during registration. This secret key will be used to decrypt the encrypted text. If the result of decryptionis the same as the data that it was encrypted on previously, we can confirm that the person casting the vote right now is actually the user registered for the election and no one else using his credentials to cast a fake vote (proof of existence) and also we can confirm that the user is in his complete consciousness while making this decision. If the decrypted data does not match the previously encrypted version then it will be considered as a malicious act and the vote will not be recorded.

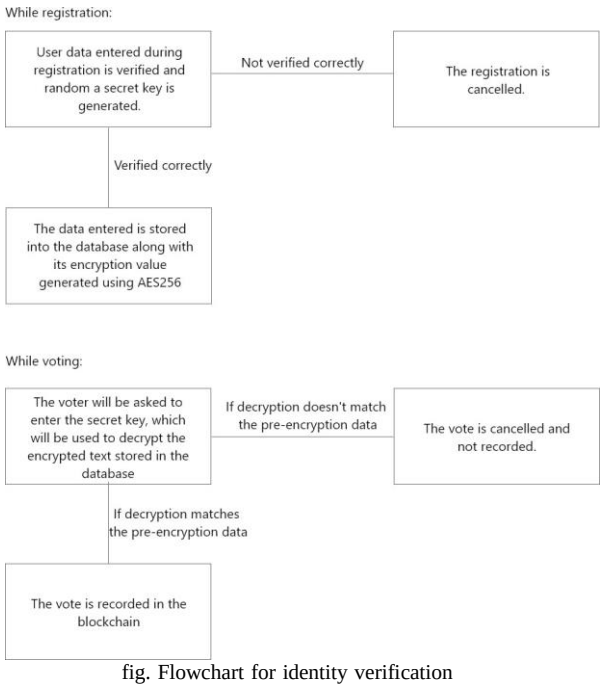

fig. Flowchart for identity verification

Once the vote has been verified, it will then be turned into a block and added to the blockchain, the transaction historyof the user will be updated to prevent the same user from casting multiple votes.

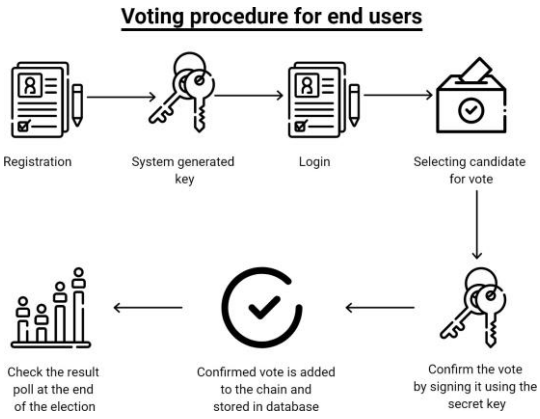

fig. Voting procedure

IV. IMPLEMENTATION

The implementation of the system is divided into 4 parts namely client side application, server side API, authentication API and database.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 03, March-2021

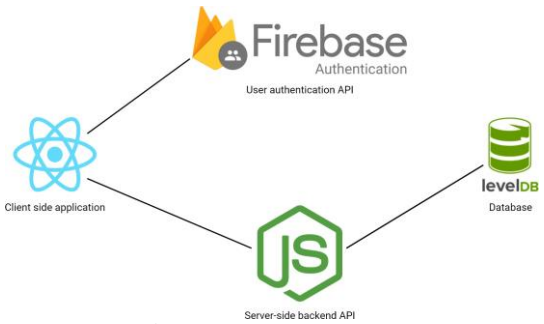

fig. Implementation

Client-side application consists of the user interface in form of a web based application through which the user will communicate with the system. It is a simple system designed to be user friendly and easy to use application. Using simple forms we can make users do certain tasks like registration, login and voting. When the user registers for the election as a voter, all the data that he enters is sent to the backend through api for verification. If the verification is successful the user is registered using the authentication API and a secret key is generated for him.

On the day of election when the user logs in his credentials are verified using the authentication API which creates a session for the users. During voting, to prove his/her identity the user is asked to enter the secret key that was generated for him. If the secret key is verified to be true using the process mentioned above in the methodology, the vote is casted and recorded in the database.

The type of database used proves to be a key factor in implementation of this methodology. The database used by us for the solution is LevelDB which is a database created by google engineers. LevelDB is also the database used in the chain of Bitcoin as it provides a key feature of immutability. If the database used is not strict against immutability it will break the system down as anyone with access to the system can modify the votes and manipulate the results.

To maintain the transparency of the voting procedure it is suggested to implement a transaction panel in the application where the user based on its identity can verify that the vote has been accurately casted to the right candidate. And at the end of the election the polls panel will display the results of the election. It is mandatory that the polls panel should not be activated before the end of the event as premature results might cause chaos in the nation and be used as a way to manipulate citizens.

V. RESULTS AND DISCUSSION

To close, our service proposal comprises a geographically distributed network comprising machines from both government and public infrastructure; this infrastructure houses two distinctly separate blockchains, one for voter information such as who has voted and the other for vote information such as what has been voted. These blockchains are held completely separately to remove any threat to link votes for certain parties back to individual voters while maintaining the ability to track who has voted and how many votes are actually present. The blockchain containing information of who has registered to vote also allows our service to ensure each voter is unique. Various other concerns related to transparency, confidentiality and reliability were also considered and the proposed solution to a huge extent maintains every aspect of a secured voting system by moving over various such challenges.

Once registered you are then allocated a vote after verification of your details has been completed. To ensure these registeredvoters are who they say they are when voting begins there is a 3 factor authentication method. Further to this we also need to ensure they are not forced to vote in a particular way so we have incorporated a double-check service where by users shall be prompted a second time to confirm their submission before the vote is sent; this also then allows us to almost eradicate accidental votes

For further advancements in the implementation with proper infrastructure and resources it is possible to implement the database on a distributed architecture to prevent it from having a central authority on the elections and decentralizing the whole process.

REFERENCES

[1] Votereum: An Ethereum-based E-voting system Linh Vo-Cao-Thuy,
Khoi Cao-Minh, Chuong Dang-Le-Bao, Tuan A. Nguyen, IEEE
[2] E. Hubbers et al., ”RIES-Internet Voting in Action”, [in Proceedingsof 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 Applica- tions (IJNSA) Vol.9, No.3, May 2017,
[4] Hsiao JH, Tso R., Chen CM., Wu ME. (2018)Decentralized E-Voting Systems Based on the Blockchain Technology. Advances in Computer Science and Ubiquitous Computing. CUTE 2017, CSA 2017. Lecture Notes in Electrical Engineering, vol 474. Springer, Singapore.,
[5] P.Y.A Ryan et al., Pret a Voter:a Voter-Verifiable Voting System[IEEE Transaction on Information Forensic and Security,vol.4,No.4,
doi:http://dx.doi.org.in/10.1109/TIFS.2009.2033233],
[6] Sos.ca.gov. (2007). Top-to-Bottom Review — California Secretary of State. Available at: http://www.sos.ca.gov/elections/voting-systems/ oversight/ top-bottom-review/.
[7] Nicholas Weaver. (2016). Secure the Vote Today. Available at:https:// www.lawfareblog.com/ secure-vote-today
[8] Vitalik Buterin. (2015). Ethereum White Paper. Available at: https:// github.com/ethereum/wiki/wiki/White-Paper.
[9] R. Hanifatunnisa and B. Rahardjo, “Blockchain based e-voting recording system design,” Proceeding 2017 11th Int. Conf. Telecommun. Syst. Serv. Appl. TSSA 2017, vol. 2018–Janua, pp. 1– 6, 2018.
[10] Y. Wu, “An E-voting System based on Blockchain and Ring Signature (Thesis),” dgalindo.es, 2017.