IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Secure & Transparent E-voting with Block-Chain

Dr. Uma Rani V, Khushhal Qasimyar

Associate Professor of Computer Science and Engineering, MTech Student
School of Information Technology,
Jawaharlal Nehru Technological University, Hyderabad, Indian

Abstract: Electronic voting or e-voting have been used in various ways over the decades, along with basic advantages over paper-based systems such as increasing efficiency and reducing error. However, the E-voting schemes bring issues mainly relating to security, credibility, transparency, reliability, and functionality which remain challenges to achieve widespread adoption of such systems especially regarding improving their resilience against potential faults. Blockchain is a distinct technology of our time that has the potential to improve the overall resilience of e-voting systems. The basic principle of the blockchain is in the immutability of the records already placed in blocks and advanced cryptography is used to ensure the chaining of blocks, and providing data integrity. This study represents an effort to leverage blockchain benefits such as cryptography and transparency to achieve an efficient voting model. Moreover, we present sec-vote, a blockchain-based voting system to bring accessibility with easy access to the web portal through the internet, reliability with face recognition and OTP, transparency with blockchain, security with hashing and cryptographic algorithms, and reduce the cost of the election

Index Terms - Blockchain, cryptography, face recognition, OTP, Hashing.

I. INTRODUCTION

Elections are the basic pillar of a democratic system, allowing the public to express their opinions in the form of a vote. Due to its importance to our society, the election process must be transparent and reliable to ensure the credibility of the participants. In this case, voting methods have always been an evolving field. This evolution is primarily driven by efforts to make the system secure, verifiable, and transparent. In view of its importance, continuous efforts have been made to enhance overall efficiency and resilience of the voting system. Electronic voting or e-voting has a significant role in this. E-voting systems have come a long way since their inception as punched-card ballot in the 1960s, with their adaptation to internet technology (Gobel et al, 2015). However, in order for e-voting systems to be widely adopted, they must adhere to specific benchmark parameters. These parameters include the voter's anonymity, the vote's integrity, and non-repudiation among others.

Blockchain is an emerging technology with strong cryptographic foundations, allowing applications to take advantage of these capabilities to build secure solutions. A Blockchain is a data structure that stores and distributes all transactions that occur through its genesis. It is basically a distributed decentralized database that maintains and store a complete list of continually germinating and growing data records secured from unauthorized revision, manipulating, and tampering.

Every user can join to the blockchain network, transmit new transactions, verify transactions, and build new blocks (Rosenfeld, 2017; Kadam et al, 2015; Nakamoto, 2009). Each block is given a cryptographic hash (which can be thought of as a block's fingerprint) that is valid as long as the data in the block isn't changed. If there are any changes to the block, the cryptographic hash will change quickly, indicating that the data has changed, which might be due to malicious activity. As a result of its strong cryptographic foundations, blockchain is rapidly being utilised to prevent fraudulent transactions in a variety of domains (Nakamoto, 2009; Kraft, 2015; Narayanan et al, 2015).

Although Bitcoin is the most well-known blockchain application, researchers are eager to investigate the use of blockchain technology to facilitate applications in a variety of domains by leveraging benefits such as non-repudiation, integrity, and anonymity. In this paper, we look at how blockchain might help with e-voting

applications by ensuring voter anonymity, vote integrity, and end-to-end verification. We believe that fundamental blockchain features like self-cryptographic validation structure among transactions (via hashes) and public availability of distributed ledger of records can be used for e-voting. Due to its fundamental nature of protecting anonymity and maintaining a decentralised and publicly distributed ledger of transactions across all nodes, blockchain technology can play a crucial role in the sphere of electronic voting. As a result, blockchain technology is highly effective at dealing with the risk of using a voting token multiple times and attempts to sway the outcome's transparency.

In this research we also make use of Face recognition which is proven to be an authentic technique for online voting. We use two steps secure technique which can be used for e-voting. Firstly, the face of the voter will be captured by a web camera and sent to the database for recognition. Then we apply face recognition mechanism over the voter's image. If the image is recognized from the database, then we go to the second level of security. In the second phase, OTP send to email of voter is matched with the OTP entered by voter, then we allow the voter to cast his vote.

The rest of the paper is structured as follows: the next section is a review of related work done; in third section, we will discuss the system's methodology. Section 4 will be the explanation of how the system is implemented and result in section 5 we have a conclusion and future work.

II. LITERATURE REVIEW

2.1 Electronic Voting Machines: The Electronic Voting Machine or EVM is the most widely used voting system. Voting machines are used to store votes from each polling station, and individual voting machines are transported to a central counting centre, where their voting data is retrieved and counted.

2.2 Estonian E-Voting System: Estonia is one of the first countries to adopt the evaluation system (Madise .et.all) Since 2005, voters in Estonia can vote via the Internet. Voting is conducted by downloading and installing an application locally on the voter's PC. The system uses an asymmetric encryption scheme to encrypt all data transmitted between the client and the server, while a server owned by the central government is used to store voting data.

2.3 Washington DC Internet Vote: Washington DC's online voting system was introduced in 2010 to allow absentee voters to vote online. The system is based on an open-source application developed by TrustTheVote Foundation using the Ruby on Rails framework. Voting is done through a PDF form that is securely uploaded to the server. A MySQL database is used to store votes on the server, and multiple firewalls are configured to reduce the size of the attack surface. After the election, the ballots will be moved to computers that are not connected to the Internet and will then be counted. This system didn't see mainstream use due to several security vulnerabilities found by (Wolchok et. al.).

2.4 Azaria et. al. The use of blockchain as a scalable and secure data storage for patient-provider relationships has been shown to enable better data exchange and collaboration in healthcare applications (Asaria et .all 2016). Lee et. al. have used a blockchain for building BIDaaS or "Blockchain ID as a Service" (Lee .et .all) that serves as a way of generating virtual IDs for user verification of online transactions. The ID provider maintains a private blockchain, and the provider's partners have read access to the chain to verify the ID generated by the user (Tse et. Al.). used a blockchain to store data such as the circulation, quantity and origin of food (Tse .et.Al 2017) in order to improve the transparency of the food supply chain. Zhang et. al. have shown that the Hyperledger fabric can be used to enable secure handling of data for the Internet of Things devices (Zhang et .al 2015). Guo et. al. have found that using blockchain technology has helped banks in significantly reducing their transaction fees(Guo .et .Al 2018).

Hence, literature contains a number of applications where blockchain technology has been well suited for different use cases. These applications differ in the data stored inside the blocks, the way the mining takes place, and the mechanisms used to reach consensus

III. METHODOLOGY

Our proposed system we utilize the benefit of private blockchain which only authorize users can enter the network and cate its vote. A private blockchain is an invitation-only blockchain. The blockchain is governed by a single entity. The participating parties require permission to read, write, or audit the blockchain. The blockchain can have multiple layers of data access to keep certain pieces of data confidential.

The organizer which in our proposed system is admin is responsible for collecting the list of the eligible nominee based on the desired condition (if any). He will add the nominees in the system. The voters are responsible to register themselves to the system. In registering phase user will enter email and photo along other credential for authentication.

In our proposed system we have Tow Module first authentication module which is achieved using face recognition and OTP verification and second Block creation and joining of it to the Blockchain. We will start our elaboration with authentication which include face recognition and OTP verification ,next we will discussed how blocks are created and joined to the Blockchain.

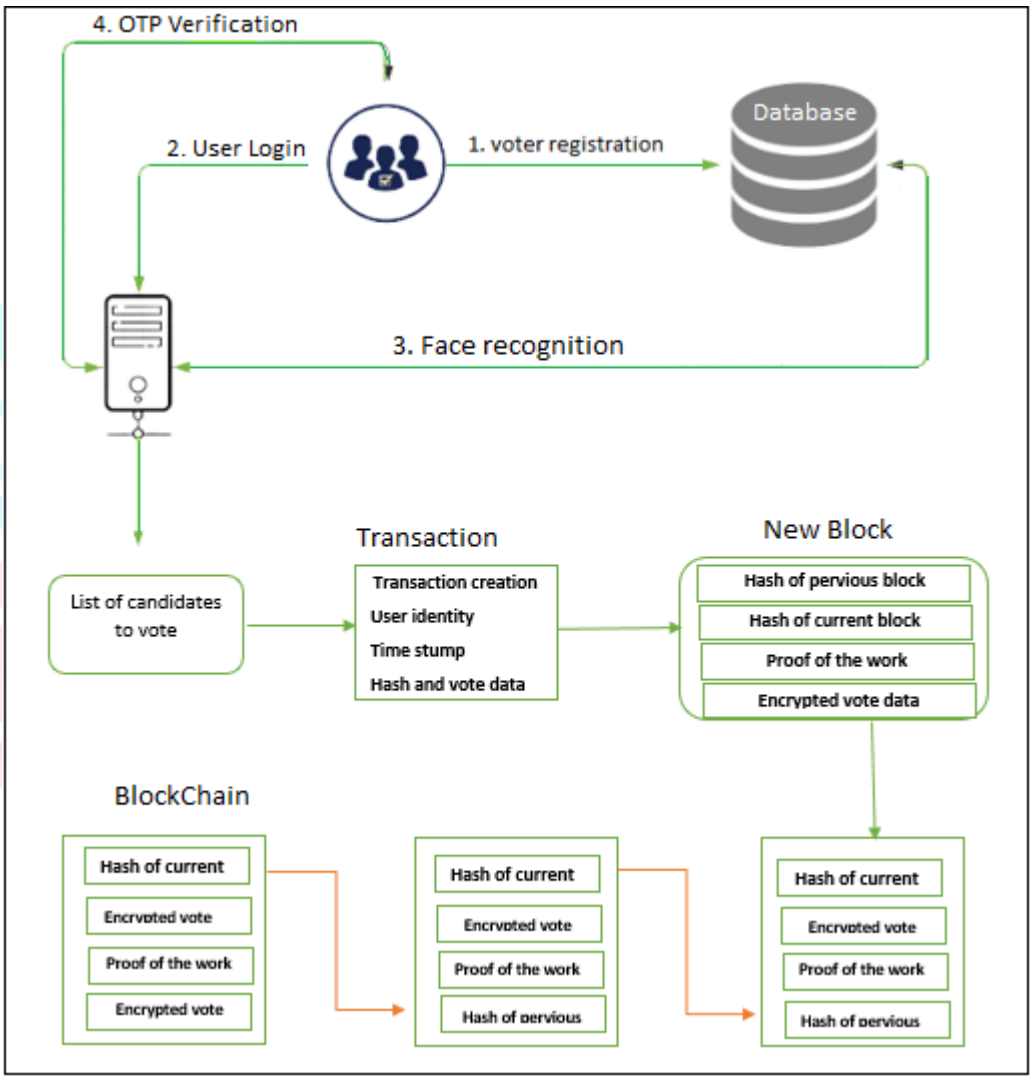

Figure 1 System Architecture

3.1 Authentication Module

Authentication is important because it allows organizations to secure their networks by allowing only authenticated users (or processes) to access its protected resources, which may include computer systems. , networks, databases, websites, and other network-based applications or services.

In our proposed system authentication can be done using in three levels. Its start with generating username and password while registering for voting. After successfully registration and login the system will capture its photo using webcam and authenticate user face recognition library which built dlib stat-of-art face recognition. At after face recognition it will send OTP to voter email. After successful authentication the user will be provided the interface to vote. A short review of face recognition using face recognition library.

3.1.1 Face Recognition

Face recognition is the process or method of recognizing human faces based on your photos and videos. These systems are widely used, especially law enforcement agencies. The face recognition starts with storing voter image in database while registration for voting. system will load the image from database find and locate face in image. The next step is face feature extraction which also called face landmarks which is used for face comparing and recognition and the final step is encoding these features and store it . when voter goes for voting system will capture its photo and redo the above steps for new image also. The last part of face recognition is comparing the faces, if it's found any match in known faces it will identify voter and proceed for OTP verification. the system will we utilize the power of face recognition library of python base on dlib stat-of-art library of C++ to recognize voter face and make authentication process fast and reliable.

3.1.2 OTP Verification

A one-time PIN code is a code that is only valid for login sessions or transactions using a mobile phone. It is commonly used for two-factor or 2FA authentication to provide users with an extra layer of security when using ATM or trying to log in to the service from a different computer. There are many ways to provide one-time passwords and PIN codes, of which the two most common and secure ways are through proprietary emails and mobile phones. Since mobile phones are ubiquitous and most of them meet the hardware requirements necessary to successfully process OTP, using mobile phones and email to deliver OTP is a logical step. In this work, I use an email-based OTP architecture and send it after voter facial recognition as a multi-factor authentication mechanism.

3.2 Block Creation and Validation Module

E-Voting second module is start with providing authorization to voter to cast his vote. The voter access list of candidates to vote for it. The system will ensure that the voter does not already voted and then process of creation of new block will started which include transaction creation, block creation and validation and joining blocks to blockchain. it will be discussed in one by one in short review.

3.2.1 Structure of Each Transaction:

We make use of vote data as transaction and after the validation of transaction we will store it in block and then the block will joint to the blockchain. Each transaction contains the following fields:

1) User identity: Name and personal identification number of voters
2) Timestamp: the time that vote has been casted
3) Vote data: the chosen candidate
4) Hash of entire vote: Sha256 hash of entire transaction

3.2.2 Block Creation and Validation

Each block contains the following:

1) Hash of the previous block
2) Transaction: Encrypted vote
3) Block Number
4) Prof of the work
5) Hash of current Block

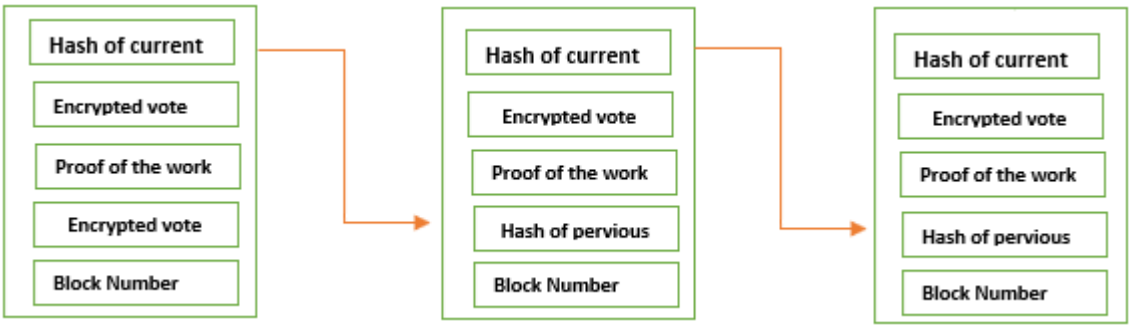

Figure 2: Blockchain

Hash of previous block is used for integrity of the block chain which is achieved using SHA256 This is a one-way algorithm that takes random-sized input data (known as a key) and change it onto values of fixed sizes (hash value). We also use block number to make each block unique in order to guarantee that duplications do not occur. The transaction will be encrypted using AES (Advanced Encryption Standard) algorithm which one of the widely adopted encryption standard.

On our purposed system we use proof of work for user to rich into a consensus on a single chronological history of the chain in the specific order in which the transactions were made. To solve this, we use the following mechanism.

3.2.3 Proof-of-Work Mechanism for Blockchain

The proof-of-work mechanism makes it progressively more difficult to accomplish the work required to create a new block. This means that someone who alter a previous block would have to redo the work of this block and all of the blocks that follow it. The proof-of-work system needs scanning for a value that starts with a specific number of zero bits when hashed. This value is accepted as a nonce value. The number of leading zero bits is known as the difficulty. The average work needs to create a block increases exponentially with the number of leading zero bits, and therefore, by increasing the difficulty with each new block, we can adequately prevent users from altering previous blocks, since it is practically impossible to reperform the following blocks and catch up to others.

IV. EXPERIMENT AND RESULTS

The test implementation of our system is done in a class with 20 voters. The authentication and block creation and validation module are developed using python programming language and Django framework. A web portal for voting is build using HTML, CSS, and JavaScript.

4.1 Web Portal

The web portal is used for voting and viewing vote results. The web portal provides specific views for both admin and voters. The admin views are as follows:

1) add candidate: Candidate details are gathered before the voting process begins and registered by admin.
2) View candidates: Candidate dashboard shows the candidate details and also information on the voter demographics for votes received by the candidate.
3) Vote Results: The results view shows when election completed.

The portal requires voters to register before voting. Voter identity is verified using a PID number, Face recognition, and their authenticity is verified using a One-Time Password sent to their email address. Hence, voters are given two views, as follows

1) Cast Vote: Voter details are collected and verified before a vote can be cast.
2) Vote acceptance status: when the vote accepted the system will provide the hash of its vote to the voter.

4.2 Results

The main objective of evaluation was to assess the performance of the system to identify any considerations with regards to its application in a real world scenario. The experimentation consisted of multiple steps i.e. conducting multiple transactions, verification of transactions, mining transactions into blockchain, time taken for face recognition.

The experiment is done on pc with following specification

- Intel core i3 Processor
- Physical memory 8 GB DDR3
- 750 GB HDD Storage

A test run was made directly at system by starting from face recognition. An outcome of this is demonstrated by Fig. 3. The test shows the amount of time required to encode the images and show the similarities found in the database. We have applied the 20 images and it take 19.76 seconds to encode and 1.16 seconds to recognize the person. The result will be different if the system runs on different system with high specification.

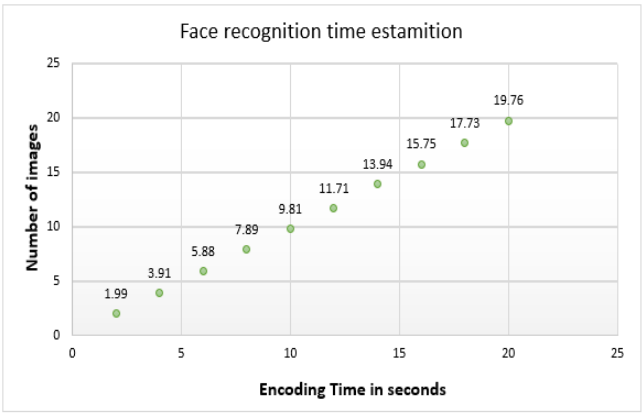

Figure 3: Face recognition Time

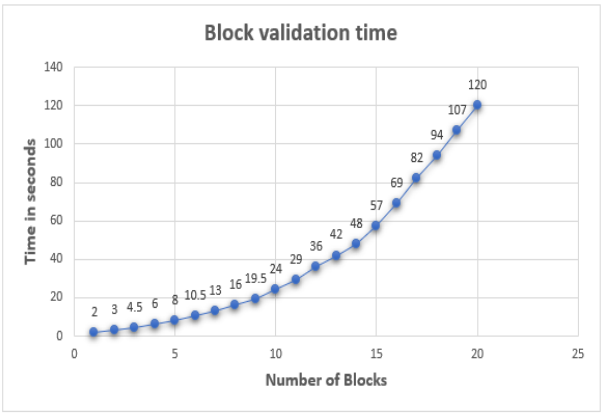

Figure 4: Block Validation Estimation

The blockchain network is run also in same machine with 50 MB LAN connection and only one node as miner. Figure 4 shows the amount time of time required to create transaction validate by miner and add block to the blockchain network. The maximum time required to validate a transaction is 120 seconds which is acceptable for having only one miner and the time will decrease when we have multiple miners.

V. CONCLUSION AND FUTURE WORK

In this study, we use private blockchain to improve the overall resilience of e-voting systems such as security credibility transparency reliability, and functionality. Although we can see slight differences in network times, they are so negligible that public blockchain has more advantages in such an electoral system due to its openness of data and that anyone can watch them in real-time. A private blockchain is a bit faster, but it reduces the credibility of the whole system by being partially centralized because it only runs where the authority wants it. This project leverages the benefit of private blockchain in case of time efficiency and uses python advanced face recognition library based on dlib state-of-art machine learning and deep learning library with the help of OTP verification code for authentication. Data integrity is achieved through the use of hashing algorithm, confidentially and transparency are ensured using encryption algorithm.

The future work of the system is to provide a mechanism to be accessed and used using mobile phones and trained a deep learning module for fast and quick face recognition.

REFERENCES

[1] Lee, Jong-Hyouk. ”BIDaaS: blockchain based ID as a service.” IEEE Access 6 (2018): 2274- 2278.
[2] Madise, lle, and Tarvi Martens. ”E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world.” Electronic voting 86, no. 2006 (2006).
[3] Wolchok, Scott, Eric Wustrow, J. Alex Halderman, Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, and Rop Gonggrijp. ”Security analysis of India’s electronic voting machines.” In Proceedings of the 17th ACM conference on Computer and com- munications security, pp. 1-14. ACM, 2010.
[4] Wolchok, Scott, Eric Wustrow, Dawn Isabel, and J. Alex Halderman. ”Attacking the Washington, DC Internet voting system.” In Interna- tional Conference on Financial Cryptography and Data Security, pp. 114-128. Springer, Berlin, Heidelberg, 2012
[5] Zhang, Yu, and Jiangtao Wen. ”An IoT electric business model based on the protocol of bitcoin.” In Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on, pp. 184-191. IEEE, 2015.
[6] Tse, Daniel, Bowen Zhang, Yuchen Yang, Chenli Cheng, and Haoran Mu. ”Blockchain application in food supply information security.” In Industrial Engineering and Engineering Management (IEEM), 2017 IEEE International Conference on, pp. 1357-1361. IEEE, 2017
[7] Guo, Ye, and Chen Liang. ”Blockchain application and outlook in the banking industry.” Financial Innovation 2, no. 1 (2016): 24.
[8] Gobel, J., Keeler, H. P., Krzesinski, A.E. and Taylor, P.G. (2015). Bitcoin Blockchain Dynamics: the Selfish-Mine Strategy in the Presence of Propagation Delay, May 2015.
[9] Nakamoto., S. (2009) Bitcoin: A peer-to-peer electronic cash system, 2009 [Online]. Available: http://bitcoins.info/bitcoin-a-peer-to-peer-electroniccash-system-satoshi-nakamoto. Last accessed: December 2017.

[10] Narayanan, A., Bonneau, J., Felten, E., Miller, A. and Gold, S. (2015) Bitcoin and Cryptocurrency Technologies, Chapter 2 and 3, Draft October 2015.
[11] Rosenfeld. M. (2017). Analysis of hashrate-based double-spending. [Online]. Available: http://arxiv.org/abs/1402.2009 last accessed: December 2017.
[12] Azaria, Asaph, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. ”Medrec: Using blockchain for medical data access and permission management.” In Open and Big Data (OBD), International Conference on, pp. 25-30. IEEE, 2016.
[13] N. Kshetri and J. Voas, “Blockchain-Enabled E-Voting,” IEEE Software,vol. 35, pp. 95-99, jul 2018.
[14] Archit Pandey, Mohit Bhasi, K. Chandrasekaran “VoteChain: A Blockchain Based E-Voting System” 978-1-7281-3694-3/19/$31.00 ©2019 IEEE
[15] Kristian Kost’al, Rastislav Bencel, Michal Ries, Ivan Kotuliak, PP 983-986 ©2018 IEEE
[16] B. Singhal, G. Dhameja, and P. S. Panda, “How Blockchain Works,” inBeginning Blockchain, pp. 31-148, Berkeley, CA: Apress, 2018.
[17] S. Landers, “Netvote: A Decentralized Voting Platform - Netvote Project- Medium,” 2018.
[18] Ajit Kulkarni, (2018), "How To Choose Between Public And PermissionedBlockchain For Your Project", Chronicled, 2018.