IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol. 9, Issue.9, September 2021 E-ISSN: 2347-2693

Blockchain Based Secure Online Voting System

C. Gouthami[1], G. Vidyulatha[2*], K. Bhavani[3], G. Akhila[4]

[1,2,3,4]Department of Computer Science and Engineering, Sree Dattha Institute of Engineering and Science, Jawaharlal Nehru technology of University, Hyderabad, INDIA

[*]*Corresponding Author: vidyu.thunder@gmail.com, Mob: 8074586578*

DOI: https://doi.org/10.26438/ijcse/v9i9.7074 | Available online at: www.ijcseonline.org

Received: 02/Sept/2021, Accepted: 20/Sept/2021, Published: 30/Sept/2021

Abstract—"Large sections of society today do not trust their government or election transparency. The issue with the current EVM system is that it can be easily manipulated by power-hungry organizations. Blockchain is a disruptive technology of current era and promises to improve the overall resilience of e-voting systems. This project presents an effort to leverage benefits of blockchain such as cryptographic foundations and transparency to achieve an effective scheme for e-voting. The proposed scheme conforms to the fundamental requirements for e-voting schemes and achieves end-to-end verifiability. We can achieve this e-voting scheme along with its implementation using Multichain platform. This project presents an effort to leverage benefits of blockchain such as cryptographic foundations and transparency to achieve an effective scheme for e-voting.

This requires minimum requirements needed by a voter is a smartphone or a computer with a webcam and an internet connection. This private key public key wallet for users can completely eliminate chances of double voting. This will also lead to minimum involvement of human engagement and we can rely on a trusted software architecture. More number of voters would be able to participate in elections.

Keywords— Block chain, EVM, Power Hungry, Resilence, Cryptography, Multichain, Decentrolised

I. Introduction

Blockchain is a list of records called blocks that store data publicly and in chronological order. The information is encrypted using cryptography to ensure that the privacy of the user is not compromised and data cannot be altered. Information on a Blockchain network is not controlled by a centralized authority, unlike modern financial institutions. The participants of the network maintain the data, and they hold the democratic authority to approve any transaction which can happen on a Blockchain network. Therefore, a typical Blockchain network is a public Blockchain**[1]**.

A distributed ledger system is a peer-to-peer network of nodes independent of each other, where each node is connected to a few others (not necessarily to all). Each node has a copy of the distributed ledger that stores the data, and an interface for users or other nodes to connect. Additionally, to the peer-to-peer network[6], a distributed ledger (DL) has a decentralized identity management[5], transactions and consensus protocols.

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 [2]. This project has presented one such effort which leverages benefits of blockchain such as cryptographic foundations and transparency to achieve an effective solution to e-voting. The proposed approach has been implemented with Multichain and in-depth evaluation of approach highlights its effectiveness with respect to achieving fundamental requirements for an e-voting scheme. Blockchain will ensures the Integrity, Security, end to end verifiability, Immutability, Decentralized system.

II. LITERATURE SURVEY

2.1 ELECTIONS (DEFINITION, TYPES AND HISTORY):

An election is a formal decision-making process by which a population or society chooses an individual to hold a political office. Elections have been the usual mechanism by which modern representative democracy operates that predates to as early as the 17th Century. Elections are conducted both by public entities such as the government as well as private and business organizations, for example, choosing representatives for the Board of Directors of a company, professional club leadership and even, used in voluntary associations.

2.3 PAPER-BALLOT VOTING SYSTEMS:

The paper-based voting system can be described as the traditional means of voting that has been in used over the ages. It is also the default method of conducting elections.

TYPES:

In most democratic political systems, there are several types or categories of elections that are held which corresponds to the different layers of public governance or

geographical jurisdiction. Common types of election categories thus include
→ Presidential Elections
→ Parliamentary Elections
→ Governorship Elections
→Local Government Electronics[4]

2.2 VOTING SYSTEMS:
There are two (2) categories under which voting systems can be classified, namely
- Traditional or Paper – Ballot Voting Systems
- Electronic Voting Systems.

2.3 PAPER-BALLOT VOTING SYSTEMS:
The paper-based voting system can be described as the traditional means of voting that has been in used over the ages. It is also the default method of conducting elections. It operates by issuing paper ballots to eligible voters who present themselves at the polling unit on the day of the election. The voter is authenticated by searching for and ticking his or her name on the voters register for that particular polling unit. Indelible ink is used to mark an authenticated voter by dropping the ink on the voter’s left thumb fingernail.

The voter is then expected to proceed to a secret booth to vote a candidate by pressing his right thumb into an ink stamp and placing the inked fingerprint in front of the chosen candidate on the ballot paper given and subsequently required to drop the ballot paper into a ballot box placed in an open place within the polling unit

Fig-2.1: PAPER-BALLOT VOTING

Fig-2.2: INK-STAMP OF EXISITING VOTING
BLOCKCHAIN BASED SECURE ONLINE VOTING SYSTEM

2.4 ELECTRONIC VOTING SYSTEMS:
The Council of Europe recommendations defined electronic voting (e-Voting) as “The use of electronic means in at least the casting of the vote” (Krimmer, et al., 2007). Electronic voting [3]is a term encompassing several different types of voting, embracing both electronic means of casting a vote and electronic means of counting votes. Electronic voting systems are complex distributed systems, whose components range from general-purpose PCs to optical scanners and touch-screen devices, each running some combination of commercial off-the-shelf components, proprietary firmware, or full-fledged operating systems.

Fig-2.3: ELECTRONIC VOTING SYSTEM

2.5 STATISTICS:
The YSR Congress Party claimed that about 59 lakh entries in the voter’s lists are false in Andhra Pradesh.
Booth capturing reported at Pithua and Bakehana areas that fall under Sagar constituency.
Fresh polling is being held at six polling booths in Arunachal East Parliamentary seat and 13 in Arunachal West Parliamentary seat.
EVMs being transported in private vehicles without registration numbers in Uttar Pradesh.
9 people suspected of double voting in 2018 election, referred for prosecution

III. METHODOLOGY

3.1 HISTORY:
The first work on a cryptographically[8] secured chain of blocks was described in 1991 by Stuart Haber and W. Scott Stornetta. They wanted to implement a system where document timestamps could not be tampered with.

In 1992, Bayer, Haber and Stornetta incorporated Merkle trees to the design, which improved its efficiency by allowing several document certificates to be collected into one block.

The first blockchain was conceptualized by a person known as Satoshi Nakamoto in 2008. Nakamoto improved the design in an important way using a Hashcash-like method to add blocks to the chain without requiring them to be signed by a trusted party.

The design was implemented the following year by Nakamoto as a core component of the crypto currency bitcoin, where it serves as the public ledger for all transactions on the network.

In August 2014, the bitcoin blockchain file size, containing records of all transactions that have occurred on the network, reached 20 GB.

In January 2015, the size had grown to almost 30 GB, and from January 2016 to January 2017, the bitcoin Blockchain grew from 50 GB to 100 GB in size.
The words block and chain were used separately in Satoshi Nakamoto's original paper, but were eventually popularized as a single word, blockchain, by 2016.

IBM opened a blockchain innovation research center in Singapore in July 2016. A working group for the World Economic Forum met in November 2016 to discuss the development of governance models related to blockchain.

Fig-5.1: Blockchain

3.2 STRUCTURE:
A block chain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that any involved record cannot be altered.
This allows the participants to verify and audit transactions independently and relatively inexpensively.
A block chain database is managed autonomously using a peer-to-peer network and a distributed time stamping server.

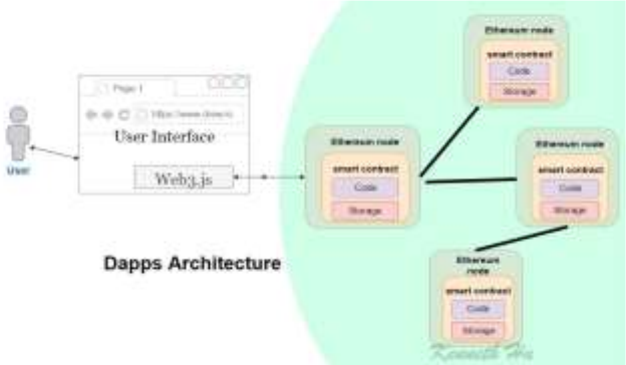


Fig-3.2 Daaps Structure

It confirms that each unit of value was transferred only once, solving the long-standing problem of double spending.
A block chain has been described as a value-exchange protocol. A block chain can maintain title rights because, when properly set up to detail the exchange agreement, it provides a record that compels offer and acceptance.

3.3TYPES OF BLOCK CHAIN:
Currently, there are three types of blockchain networks public blockchains, private blockchains and consortium blockchains.

Public blockchains
A public blockchain has absolutely no access restrictions. Anyone with an Internet connection can send transactions to it as well as become a validator.
Usually, such networks offer economic incentives for those who secure them and utilize some type of a Proof of Stake or Proof of Work algorithm.
Some of the largest, most known public blockchains are the bitcoin blockchain and the Ethereum blockchain.

Private block chains
A private blockchain is permissioned. One cannot join it unless invited by the network administrators. Participant and validator access is restricted.

This type of blockchains can be considered a middle-ground for companies that are interested in the blockchain technology.

They seek to incorporate blockchain into their accounting and record-keeping procedures without sacrificing autonomy and running the risk of exposing sensitive data to the public internet.

Consortium blockchains
A consortium blockchain is often said to be semi-decentralized[9]. It, is permissioned but instead of a single organization controlling it, a number of companies might each operate a node on such a network.

The administrators of a consortium chain restrict users' reading rights as they see fit and only allow a limited set of trusted nodes to execute a consensus protocol.

3.4 BENEFITS OF USING BLOCKCHAIN TECHNOLOGY:
Immutable Transaction Ledger and Audit Trails
Blockchain data is tamper-resistant, meaning that one can’t simply modify the ledger without anyone else knowing.

Blockchain data is cryptographically linked and secured so that making changes to the ledger is both difficult and easily detectable.

Indeed, participants must use digital signatures with private keys that track the transactions from specific participants.

While most blockchain transactions today are pseudo anonymous, some private blockchain entities require ID verification and two-factor authentication before allowing users to access their services.
This further reduces the dangers of malicious actors participating freely.

3.5 WHAT ARE DISTRIBUTED LEDGERS?

A distributed ledger is a database that is consensually shared and synchronized across multiple sites, institutions or geographies.

It allows transactions to have public "witnesses," thereby making a cyber attack more difficult.

The participant at each node of the network can access the recordings shared across that network and can own an identical copy of it.

Further, any changes or additions made to the ledger are reflected and copied to all participants in a matter of seconds or minutes.Underlying the distributed ledger technology is the blockchain, which is the technology that underlies bitcoin.

Distributed Ledgers Explained

A distributed ledger[10] can be described as a ledger of any transactions or contracts maintained in decentralized form across different locations and people, eliminating the need of a central authority to keep a check against manipulation. All the information on it is securely and accurately stored using cryptography and can be accessed using keys and cryptographic signatures.

Once the information is stored, it becomes an immutable database, which the rules of the network govern. While centralized ledgers are prone to cyber-attack, distributed ledgers are inherently harder to attack because all the distributed copies need to be attacked simultaneously for an attack to be successful. Further, these records are resistant to malicious changes by a single party.

Since ancient times, ledgers have been at the heart of economic transactions to record contracts, payments, buy-sell deals or movement of assets or property. The journey which began with recording on clay tablets or papyrus made a big leap with the invention of paper. Over the last couple of decades, computers have provided the process of record keeping and ledger maintenance great convenience and speed.

Today, with innovation, the information stored on computers is moving towards much higher forms which is cryptographically secured, fast and decentralized.

3.6 How Blockchain Technology Is Transforming the Legal Industry

You don't need to be doing initial coin offerings or issuing tokens to benefit from the blockchain," Judith Rinearson, a partner in K&L Gates' New York and London offices, told Bloomberg Law. Rinearson is leading an initiative at her firm that aims to eventually build an internal blockchain, which could be used in time-keeping, filing deeds, and handling merger and acquisition transactions, she said. Blockchain known as the technology underpinning bitcoin—allows for records of transactions to be kept on a digital ledger and shared by everyone in the network. There are multiple blockchains, and the Ethereum blockchain introduced a feature called "smart contract" that allows coded programs to act upon predefined triggers. Blockchain technology is now being used to build tools and infrastructure that help lawyers draft contracts, record commercial transactions, and verify legal documents. Two examples of such tools and infrastructure[11] are Open Law and Integra Ledger.

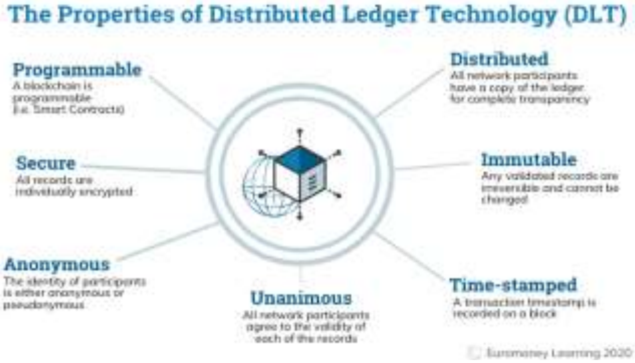

The Properties of Distributed Ledger Technology (DLT)
Programmable
A blockchain is programmable (i.e. Smart Contracts)
Distributed
All network participants have a copy of the ledger for complete transparency
Secure
All records are individually encrypted
Immutable
Any validated records are irreversible and cannot be changed
Anonymous
The identity of participants is either anonymous or pseudonymous
Unanimous
All network participants agree to the validity of each of the records
Time-stamped
A transaction timestamp is recorded on a block
© Euromoney Learning 2020

Fig-3.6- Properties of Distributed Ledger Technology

Open Law allows lawyers to automatically generate legal agreements and embed smart contracts that can be executed on the blockchain. Integra
Ledger provides a permissioned blockchain to increase the integrity of legal documents.

3.7SYSTEM DESIGN

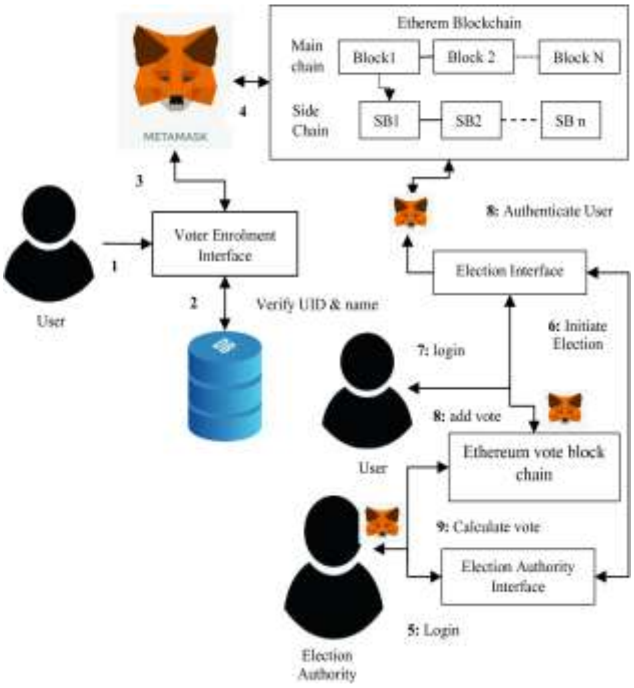
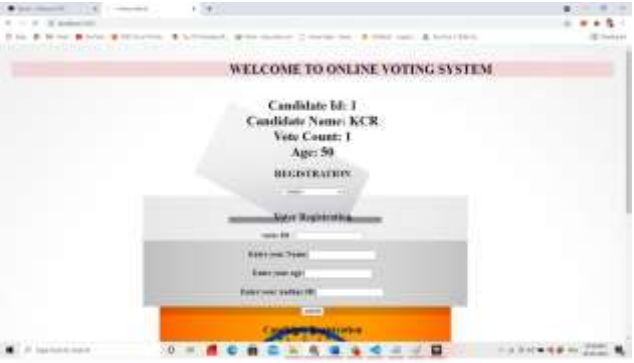


Fig-3.7- Architecture

IV. Results and Discussion

The implementation of the proposed system has been carried out within a controlled environment with a web-based application created to serve as the front-end application enabling the users to interact in a convenient manner. We have used Multichain as the blockchain platform to create a private blockchain for this application which is used for recording the voting transactions. This choice is influenced by the ease of use provided by this platform and therefore it was easily integrated into our proposed architecture.

The benefits of a successful secure and transparent online voting system are clear. Such a system would do away with the issues of postal ballots being delayed, waylaid, or lost en route.



WELCOME TO ONLINE VOTING SYSTEM

Candidate Id: 1
Candidate Name: KCR
Vote Count: 1
Age: 50

REGISTRATION

Voter Registration

voter ID

Enter your Name

Enter your age

Enter your aadhar ID

With the development of a scalable blockchain-based system, there need be no concerns about postal votes being deliberately delayed, or about non-verifiability of votes in existing electronic voting systems. At least some of the challenges facing e-voting – maintaining records securely, and ensuring auditability and transparency – can be solved. Better systems are certainly possible. So, what is holding back greater investment into more research for the design of secure online voting systems? Integrity of elections is the single most important activity for democratic governments.

V. Conclusion and Future Scope

We have learned from blockchain research that there may typically include potential weaknesses no matter how to enforce the security of a system. The potential security threats may occur in the various scenario since the blockchain technology has different system architecture from the centralized one.

The proposed approach has been implemented with Multichain and in- depth evaluation of approach highlights its effectiveness with respect to achieving fundamental requirements for an e-voting scheme. In continuation of this work, we are focused at improving the resistance of blockchain technology to 'double spending' problem which will translate as 'double voting' for e-voting systems.

REFERENCES

[1] Khan, K. M., Arshad, J., & Khan, M. M. Investigating performance constraints for blockchain based secure e-voting system. *Future Generation Computer Systems*. Pawade, D. **105, 13-26, 2020.**

[2] Sakhapara, A., Badgujar, A., Adepu, D., & Andrade, M. Secure online voting system using biometric and blockchain. In *Data Management, Analytics and Innovation*. Springer, Singapore. **pp. 93-110, 2020.**

[3] Krishnan, R., Thangavelu, A., Prabhavathy, P., Sudheer, D., Putrevu, D., & Misra, A. Web-based remote sensing image retrieval using multiscale and multidirectional analysis based on Contourlet and Haralick texture features. *International Journal of Intelligent Computing and Cybernetics*, **2021.**

[4] Elisa, N., Yang, L., Chao, F., & Cao, Y. A framework of blockchain-based secure and privacy-preserving E-government system. *Wireless Networks*, **1-11, 2018.**

[5] Ayed, A. B. A conceptual secure blockchain-based electronic voting system. *International Journal of Network Security & Its Applications*, **9(3), 01-09, 2017.**

[6] Daniel, M. Blockchain Technology: The Key to Secure Online Voting. *Regulation*, **2017.**

[7] Devulapalli, S., Potti, A., Krishnan, R., & Khan, M. S. Experimental evaluation of unsupervised image retrieval application using hybrid feature extraction by integrating deep learning and handcrafted techniques. *Materials Today: Proceedings*, **2021.**

[8] Daniel, M. Blockchain Technology: The Key to Secure Online Voting. *Regulation*, **2017.**

[9] Yu, B., Liu, J. K., Sakzad, A., Nepal, S., Steinfeld, R., Rimba, P., & Au, M. H. Platform-independent secure blockchain-based voting system. In *International Conference on Information Security*. Springer, Cham. **pp. 369-386, 2018, September**.

[10] Sudheer, D., & Krishnan, R. Multiscale Texture Analysis and Color Coherence Vector Based Fea-ture Descriptor for Multispectral Image Retrieval. *ASTES J.*, ***4*(6), 270-279, 2019.**

[11] Chaieb, M., Yousfi, S., Lafourcade, P., & Robbana, R. Verify-your-vote: A verifiable blockchain-based online voting protocol. In *European, Mediterranean, and Middle Eastern Conference on Information Systems*, **pp. 16-30, 2018, October**. Springer, Cham.

[12] Devulapalli, S., & Krishnan, R. Synthesized pansharpening using curvelet transform and adaptive neuro-fuzzy inference system. *Journal of Applied Remote Sensing*, **13(3), 034519, 2019.**

AUTHORS PROFILE

Mrs.C.GOUTHAMI Bachelor of Computer Science from JPNCE , MBNR in 2013 and Master of Computer Science from SDES in year 2017 and currently working as Assistant Professor in Department of Computerl Sciences, Department of Electronic and Communication, SDES of HYD, HYD since 2019. She main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Computational Intelligence based education. She has 3 years of teaching experience and 1 years of Research Experience.

Mrs.G.VIDYULATHA pursed Bachelor of Computer Science and engineering in BRECW in 2010, Master of Computer Science from SDES , HYD in year 2012. She currently working as Assistant Professor in Department of CSE, SDES, HYD since 2016. He has published more than 1 research papers in reputed international journals Her main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Computational Intelligence based education. She has 5 years of teaching experience and 1 years of Research Experience.