BLOCKVOTE-BLOCKCHAIN BASED ELECTION

[1] S. VARSHA REDDY, [2] A. VENU, [3] P. VEERANNA

[1,2,] *Assistant Professor, Department of IT, Sri Indu College of Engineering and Technology, Hyderabad, Telangana-501510*

[3]*Assistant Professor, Department of Computer Science and Engineering, Sri Indu College of Engineering and Technology, Hyderabad, Telangana-501510*

ABSTRACT

Voting is the fundamental right for every nation. An Electronic Voting (E-Voting) system is a voting system in which the election process is notated, saved, stored, and processed digitally, which makes the voting management task better than the traditional paper-based method. Block chain is offering new opportunities to develop new types of digital services. While research on the topic is still emerging, it has mostly focused on the technical and legal issues instead of taking advantage of this novel concept and creating advanced digital services. Block chain-enabled e-voting (BEV) could reduce voter fraud and increase voter access. Eligible voters cast a ballot anonymously using a computer or smartphone. BEV uses an encrypted key and tamper-proof personal IDs. Electronic credibility services have become an integral part of the information space. With the reliable implementation of basic services as an electronic signature and electronic authentication, it is possible to build more complex systems that rely on them, particularly the electronic voting system. In this paper, the concept of developing an electronic voting system using block chain technology is implemented. The two-level architecture provides a secure voting process without redundancy of existing (not based on block chain) systems. The block chain-based voting project has two modules to make the whole paper integrated and work along. One will be the Election Commission who will be responsible for creating elections, adding registered parties and candidates.

INTRODUCTION

Modern democracies are built upon traditional ballot or electronic voting (e- voting). In these recent years, devices which is known as EVMs are hugely criticized due to irregular reports of the election results. There have been many questions regarding the design and internal architecture of these devices and how it might be susceptible to attacks. This paper has analyzed different techniques of tampering the EVMs. Online-voting is pushed as a potential solution to attract the young citizens and the non- resident of the country [1]. For a robust online election scheme, a number of functional and security requirements are to be met such as transparency, accuracy, auditability, data privacy, etc. We have worked the following ideas by having the two different set of modules: election commission and the voter(s). Election Commission creates elections and ads registered candidates along with the parties for contesting the election. Using an election's REST API hosted on Ethereum's Block chain, the details are shown at the front-end of the voter for casting the vote [2]. Then, while polling the vote is stored on our block chain framework of which the Election Commission fetches the vote count. The limitation which we have faced due to not

using the traditional way of smart contracts is that the block chain framework which we have coded cannot run on the main net as it needs to be hosted and a separate web3 provider have to be used for interacting with it and not having a public API of voter ID creates a drawback of not having authentication of a voter. The most important factor of this application is to integrate the block chain framework with both the modules for seamless voting. BlockVote is a blockchain-based platform that aims to provide a secure and transparent method for voting and decision-making. The purpose of the BlockVote blockchain is to enable organizations, communities, and governments to conduct efficient and tamper-proof voting processes [3].

With the help of smart contracts, BlockVote allows the creation of voting rules and processes that are transparent and auditable. It ensures that the voting process is secure and reliable, with every vote being recorded on the blockchain, which can be easily audited by anyone. BlockVote's decentralized architecture also ensures that there is no central authority controlling the voting process, which reduces the potential for fraud and manipulation. The purpose of this work is to make the functional and non-functional requirements of the Online Election System using Blockchain Technology easy to comprehend [4]. It also serves the purpose of making the functionality clear to end users.

LITERATURE SURVEY

Existing Problem

In India, before 2004 there was a paper-based voting system. This is called as ballot Paper system. Voters had to go to polling booth and cast their vote by marking on seal in front of the symbol of a candidate for which they wanted to cast their votes on ballot paper. Results were announced by counting the votes.

The maximum vote gainer was declared as winner. India has population more than 120 crores the ballot paper voting is not much reliable, time consuming and very difficult to count the vote and there are also problems like replacement of ballot paper boxes with duplicate, damage of ballot paper, marking stamp seal for more than one candidate hence there is a strong need to overcome these problems. In order to overcome these problems Electronic Voting Machines Were introduced [5].

1. Control Unit: It stores and assembles votes, used by poll workers.
2. Ballot Unit: It is placed in the election booth and is used the voters.

The control unit has a battery pack inside, which motorizes the system. The ballot unit has 16 candidate button and the unused buttons are covered with a plastic masking tab inside the unit. Main Problem lies in authentication, the person who is voting may not be the legitimate person. Other problems like capturing of booth by political parties, casting of votes by underage people and fraud voting may occur. A person is provided with the voter id card as a proof of identity, issued by Indian government. Lot of problems are seen in voter id cards like name misprinting, missing of name, no clear photo on photo id card, etc [6].

Literature Review

Survey 1:

Title: Challenges in multi-layer data security for video steganography revisited.

Author: S Kamil Year: 2019

The steganography is prone to number of attacks such as geomatical, salt and pepper gaussian, median filtering, attacks. To overcome these problems, the cryptography and error correction codes are comes in the pictures and hybrid with steganography algorithms. The cryptography algorithms add one layer of security on steganography algorithms and error correction codes improves the robustness of steganography algorithms [7].

Advantages

- It is rather obvious that most software development life cycles will include some form of versioning, indicating the release stage of the software at any particular stage.
- The iterative model makes this even easier by ensuring that newer iterations are incrementally improved versions of previous iterations [8].

Survey 2:

Title: A survey on applications and security privacy challenges

Author: Mohanta B.K. Year: 2020

Blockchain Technology has received a lot of attention from both industry and academia due to its decentralized, persistency, anonymity and auditability properties. In this survey, use of Blockchain technology in wide applications area and its implementation challenges have been done. A rigorous search for journal/research article related to Blockchain technology have been reviewed. We have considered five databases to conduct this survey namely Science direct, IEEE Xplore, Web of Science, ACM Digital Library and Inderscience are being used. After initial phase elimination 135 research articles are considered in final databases for the survey. Main focus of the survey is to provide a comprehensive analysis on wide applications of Blockchain technology for the academic research community. In this paper challenges in implementing of Blockchian and its associated security and privacy issues have been discussed. For the first time a survey of this type have been done where Blockchain with application and its associated security and privacy issue have been reviewed [9].

Advantages

- While it may seem like each stage of the iterative process isn't all that different from the stages of a more traditional model like the waterfall method.
- Each subsequent iteration will be faster and faster, lending itself to that agile moniker so very well.

Survey 3: Title: Comprehensive Survey and Research Directions on Block chain Iot Access Control

Author: Hussain H.A Year: 2021

The Internet of Things (IoT) is a widely used technology in the last decade in different applications. The Internet of things is wirelessly or wired to communicate, store, compute and track various real-time scenarios. This survey mainly discussed the core problems of Internet of things security and access control to unauthorized users and security requirements for IoT. The Internet of things is a heterogeneous device and has low memory, less processing power because of the small sizes. Nowadays, IoT systems are not sure and powerless to protect themselves against cyber-attacks. It is mainly due to inadequate space in IoT gadgets, immature standards, and the lack of protected hardware and software design, development, and deployment. To meet IoT requirements, the authors discussed the limitations of traditional access control [10]. Then the authors examined the potential to spread access control by implementing the safe architecture accommodated by the Blockchain. The authors also addressed

how to use the Blockchain to work with and resolve some of the standards relevant to IoT security issues. In the end, an analysis of this survey shows future, open-ended problems, and challenges. It offers how the Blockchain potentially ensures reliable, scalable, and more efficient security solutions for IoT and further research work [11].

Advantages

Users' can vote from anywhere in the world until he possess a citizenship of the country.

- The voting is stored in the Blockchain which makes it tamper proof.
- As there's no standing in queue for casting vote it will save a lot of time and reduce the workload.

Survey 4: Title: An Enquiry into the Vision of Blockchain-Powered E-Voting Start-Ups.

Author: Imperial. M Year: 2021

This research sets out to analyze the message promoted by start-up enterprises that apply blockchain technologies for the purpose of e-voting [blockchain-powered e-voting (BPE)], and their perceived effects of this technological solution on democratic outcomes. Employing Norman Fairclough's critical discourse analysis (CDA), I examined the written output of seven BPE start-ups (Agora, DemocracyEarth, Follow My Vote, Polys, Voatz, Votem, and VoteWatcher), as displayed in their websites [12]. The close attention of CDA to power relations brought out relevant topics of discussion for analysis. Notably, these included: voting as an expression of democracy; technological determinism; individual versus communitarian understandings of democracy; the prominence of neoliberalism and the economic sphere; and technological literacy. Findings from the literature suggest that the assumptions of BPE start-ups about a blockchain-powered democracy diverge from widely accepted understandings of democracy. BPE start-ups envision a democracy determined by positions and institutions of power, by the technologically able, and by economic interests [13]. This research argues that this conception of democracy disempowers voters from any form of decision-making regarding how democracy is run beyond their expression in the form of a vote decided by these established powers. The widespread addresses to existing elites to enable BPE, as well as what is left unsaid about community, collective rights and the not so technologically literate population, imply that BPE developers display concern for one particular expression among the many diverse and heterogeneous understandings of democracy, while disregarding outstanding privacy, security and accountability concerns associated to implementations of the technology for BPE. This work is a contribution to much needed research on technology and democracy's deepening intersections, at a time of rapid technological innovation and turbulent democratic scepticism [14].

Advantages

- Blockchain-based e-voting (BPE) as the research analyzed the message promoted by BPE start-ups and their perceived effects on democratic outcomes.
- BPE could include increased transparency and immutability of voting records, reduced instances of voter fraud and tampering [15].

Disadvantage

- BPE solutions may not be accessible to all citizens, especially those who are not technologically literate or do not have access to the necessary devices.
- BPE solutions are dependent on technology, which can be prone to technical issues or malfunctions.

Survey 5: Title: Security Analysis and Improvement of a Redactable Consortium Blockchain for Industrial Internet-of-Things.

Author: Gao W,Chen L Year: 2021

A redactable consortium blockchain (RCB) can build a trust layer for industrial internet of things (IIoT) so as to enable IIoT to resist certain powerful attacks resulting in improper block content. The redactability is particularly important for blockchains applied in IIoT with valuable or sensitive activities such as financial IoT or energy-trading IoT. Huang et al. proposed a threshold chameleon hash (TCH) scheme and then constructed an accountable-and-sanitizable chameleon signature scheme based on TCH. These two primitives are further used as fundamental modules to build an RCB. Specifically, we find out that if a transaction in a given block is legally redacted by all authorized sensors who collectively hold the private redacting key, anyone (without any private information) can further redact this redacted transaction and delete any transaction within this redacted block and, meanwhile, any sensor user with a private signing (not redacting) key can insert a forged transaction into this redacted block. We further address this threat by replacing the TCH module in Huang et al.'s RCB with our designed TCH [16].

Advantage

- RCBs can enable IIoT devices to operate the blockchain in a controllable way.
- TCH scheme and accountable-and-sanitizable chameleon signature scheme based on TCH can be used as fundamental modules to build an RCB.

Disadvantage

- The RCB proposed by Huang et al. suffers from a security problem that weakens the crucial redactability.
- The security issue can undermine the reliability and security of the RCB, which is intended to provide a trustworthy platform for IIoT.
-

PROPOSED SYSTEM

Several studies have been done on using computer technologies to improve elections. These studies tell about the risks of adopting electronic voting system, because of the software challenges, insider threats, network vulnerabilities, and the challenges of auditing.We've proposed to design the existing online voting system which is integrated with the Blockchain technology. The proposed system has the following advantages as compared to the existing system:

- Users' can vote from anywhere in the world until he possess a citizenship of the country.
- The voting is stored in the Blockchain which makes it tamper proof.
- As there's no standing in queue for casting vote it will save a lot of time and reduce the workload.

Cost-Effective: BlockVote can reduce the cost of conducting elections by eliminating the need for physical polling stations and manual vote counting. Transparent and Auditable: BlockVote's use of smart contracts ensures that voting rules and processes are transparent and auditable, enabling anyone to verify the integrity of the voting process. Decentralized Architecture: BlockVote's decentralized architecture ensures that no central authority controls the voting process, reducing the potential for fraud and manipulation [17].

System Architecture

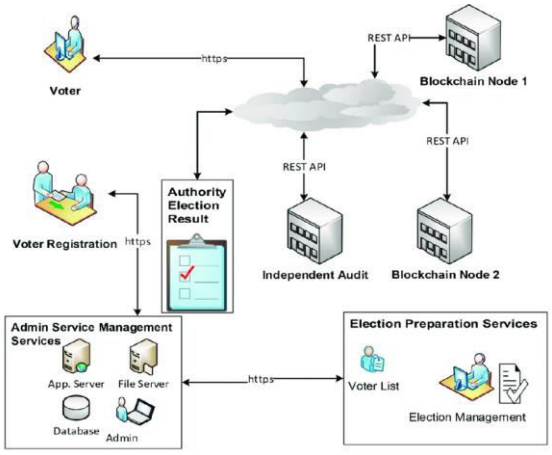

Fig1 System Architecture

IMPLEMENTATION

Modules Description:

Customer Involvement

Agile Iterative development encourages user contribution. After each iterative cycle, customer feedback is obtained, and the product is then subjected to necessary changes based on that feedback. This aspect brings adaptability into the project's framework.

The work has been divided into many modules in which for every functionality we have designated modules. Any software comprises of many systems which contains several sub-systems and those sub-systems further contains their sub-systems. So, designing a complete system in one go comprising of each and every required functionality is a hectic work and the process can have many errors because of its vast size [18].

Effective modular design can be achieved if the partitioned modules are separately solvable, modifiable as well as compliable. Following are the project modules:

(i) Election Commission: In this module, an entity named Election Commission will be responsible to setup the smart contract and register candidates, parties and start off an election.

- Creating the Election: The Election Commission Module creates the election by setting up the necessary parameters, such as the date and time of the election, the number of candidates contesting, and the number of Assembly Constituencies.
- Adding Registered Parties and Candidates: The Election Commission Module adds registered parties and candidates who are contesting for the election. The parties and candidates will be verified and registered to ensure that only legitimate parties and candidates are contesting.
- Setting up Smart Contracts: The Election Commission Module sets up smart contracts that will govern the voting process. The smart contracts will ensure that the voting process is transparent, tamper-proof, and secure.

- Storing Election Data on the Blockchain: The Election Commission Module stores all data related to the election process on the blockchain ledger to ensure that it is tamper-proof and transparent.

Algorithm Implementation:

1. The Election Commission Module verifies and registers parties and candidates who will be contesting for the election.

2. The Election Commission Module sets up smart contracts that will govern the voting process.

3. The Election Commission Module creates the election by setting up the necessary parameters such as the date and time of the election, the number of candidates contesting, and the number of Assembly Constituencies.

4. The Election Commission Module stores all data related to the election process on the blockchain ledger.

5. Voter Module:

The Voter Module is responsible for allowing voters to cast their vote securely and anonymously. It includes the following components:

- Registering and Verifying Voters: The Voter Module registers and verifies voters using encrypted keys and tamper-proof personal IDs.
- Allowing Voters to Cast Their Vote: The Voter Module provides voters with access to the voting system. Voters can cast their vote securely and anonymously using the Voter Module.
- Storing Vote Data on the Blockchain: The Voter Module stores all vote data on the blockchain ledger to ensure that it is tamper-proof and transparent.

(ii) Voter Module: In this module, voters who have been provided with the personal ETH wallet will import onto the voting portal using the Metamask extension and cast their vote.

Algorithm Implementation:

1. Voters are verified and registered using encrypted keys and tamper-proof personal IDs.
2. Voters are provided access to the Voter Module to cast their vote.
3. The Voter Module stores all vote data on the blockchain ledger.

Implementations

Client:

Client is any user or program that wants to perform an operation over the system. Clients interact with the system through a presentation layer.

Presentation Layer:

This layer is responsible for the presentation of data at the client side, i.e., it provides an interface for the end-user into the application to cast the votes.

Resource manager:

The resource manager deals with the organization (storage, indexing and retrieval) of the data necessary to support the application logic. This resource manager here is the Local Blockchain server maintained by Ganache.

Application logic:

The application logic figures out what the system actually does. It takes care implementing the business rules and establishing the business processes.

RESULTS

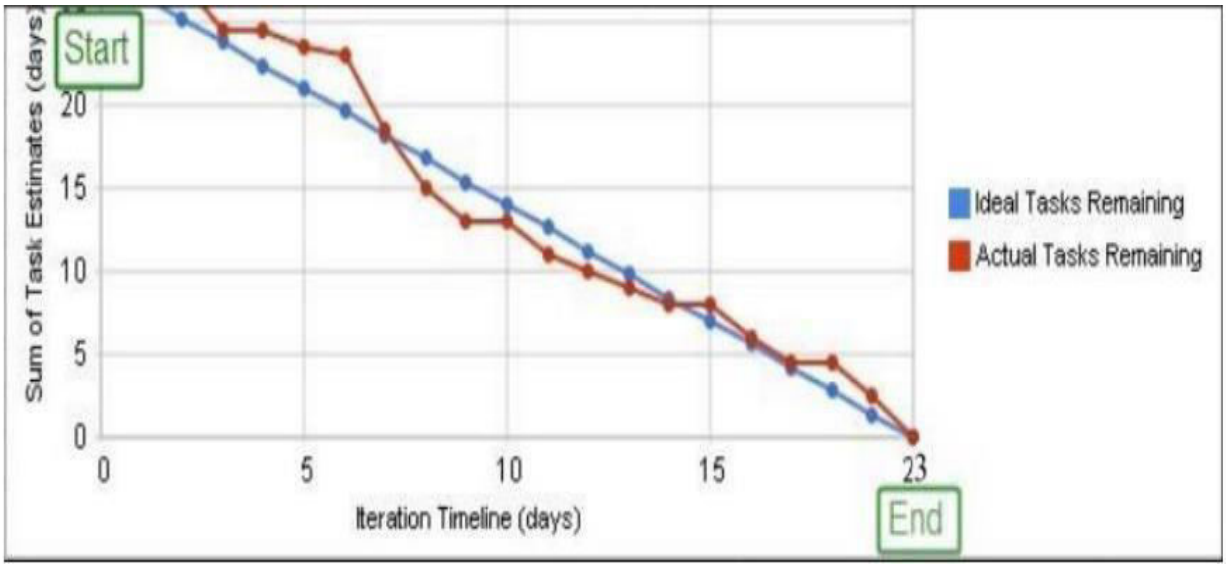

Fig 2.Reports from JIRA

The system is expected to allow voters to cast their votes securely and anonymously, with each vote recorded on the blockchain ledger. The ledger will be distributed across a network of nodes, making it virtually impossible for any individual or organization to tamper with the voting results.

The result of the election will be determined by the votes recorded on the blockchain ledger, which will be counted using a consensus mechanism. This will ensure that the result is accurate and trustworthy, with a high degree of confidence that it has not been manipulated.

Performance Metrics

Transaction Throughput:

Transaction throughput measures the number of transactions that can be processed by the system in a given period. This metric is critical for a blockchain-based voting system, as it must be able to handle a large volume of transactions within a short period to ensure that the voting process is completed in a timely manner.

Latency:

Latency measures the time it takes for a transaction to be processed by the system. This metric is important for a voting system, as delays in processing transactions can lead to frustration among voters and could potentially impact the election results.

Availability:

Availability measures the amount of time the system is available for use. This metric is critical for a voting system, as it must be available 24/7 to allow voters to cast their votes at any time.

CONCLUSION AND FUTURE WORK

Democracies depend on trusted elections and citizens should trust the election system for a strong democracy. However traditional paper-based elections do not provide trustworthiness. The idea of adapting digital voting systems to make the public electoral process cheaper, faster and easier, is a compelling one in modern society. Making the electoral process cheap and quick, normalizes it in the eyes of the voters, removes a certain power barrier between the voter and the elected official and puts a certain amount of pressure on the elected official. It also opens the door for a more direct form of democracy, allowing voters to express their will on individual bills and propositions.

This work has been developed to a blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient election while guaranteeing voters privacy. It outlines the systems architecture, the design, and a security analysis of the system. In the next build of this application, it has been proposed to create separate client designs for various roles such as one for election commission and one for candidates registered to a certain party with the existing voting client design. Also, the current versions lack authentication as we don't have access to current Aadhar's or Voter SDK to integrate in our application. Also, it is planned that in the next build notification prompt will be given on the day of voting to all the voters to cast their vote so that the voter turnout is maximum for that election.

REFERENCES

[1]. Gao, W.; Chen, L.; Rong, C.; Liang, K.; Zheng, X.; Yu, J. (2021) 'Security Analysis and Improvement of a Redactable Consortium Blockchain for Industrial Internet-of-Things'. Comput. J.

[2]. Hussain, H.A.; Mansor, Z.; Shukur, Z (2021). 'Comprehensive Survey And Research Directions On Blockchain Iot Access Control'. Int. J.Adv. Comput. Sci. Applications.

[3]. Imperial, M. (2021) 'The Democracy to Come? An Enquiry into the Vision of Blockchain-Powered E-Voting Start-Ups. Front.' Blockchain,

[4]. Jaffal, R.; Mohd, B.J.; Al-Shayeji, M. (2021). 'An analysis and evaluation of lightweight hash functions for blockchain-based IoT devices'. Clust. Comput.

[5]. Kamil, S.; Ayob, M.; Sheikhabdullah, S.N.H.; Ahmad, Z. (2021). 'Challenges in multi-layer data security for video steganography revisited'. Asia-Pacific J. Inf. Technol. Multimed

[6]. Mohanta, B.K.; Jena, D.; Panda, S.S.; Sobhanayak, S(2019). 'Blockchain technology: A survey on applications and security privacy challenges'. Internet Things

[7]. Poniszewska-Marańda, A.; Pawlak, M.; Guziur, J.(2020)' Auditable blockchain voting system-the blockchain technology toward the electronic voting process'. Int. J. Web Grid Serv.

[8]. Prashar, D.; Jha, N.; Jha, S.; Joshi, G.; Seo, C. (2020). 'Integrating IOT and blockchain for ensuring road safety:' An unconventional approach. Sensor .

[9] K. Bhargavi. An Effective Study on Data Science Approach to Cybercrime Underground Economy Data. Journal of Engineering, Computing and Architecture.2020;p.148.

[10] [21] M. Kiran Kumar , S. Jessica Saritha. AN EFFICIENT APPROACH TO QUERY REFORMULATION IN WEB SEARCH, International Journal of Research in Engineering and Technology. 2015;p.172

[11] K BALAKRISHNA,M NAGA SESHUDU,A SANDEEP. Providing Privacy for Numeric Range SQL Queries Using Two-Cloud Architecture. International Journal of Scientific Research and Review. 2018;p.39

[12] K BALA KRISHNA, M NAGASESHUDU. An Effective Way of Processing Big Data by Using Hierarchically Distributed Data Matrix. International Journal of Research.2019;p.1628

[13] P.Padma, Vadapalli Gopi,. Detection of Cyber anomaly Using Fuzzy Neural networks. Journal of Engineering Sciences.2020;p.48.

[14] Kiran Kumar, M., Kranthi Kumar, S., Kalpana, E., Srikanth, D., & Saikumar, K. (2022). A Novel Implementation of Linux Based Android Platform for Client and Server. In A Fusion of Artificial Intelligence and Internet of Things for Emerging Cyber Systems (pp. 151-170). Springer, Cham.

[15] Kumar, M. Kiran, and Pankaj Kawad Kar. "A Study on Privacy Preserving in Big Data Mining Using Fuzzy Logic Approach." *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* 11.3 (2020): 2108-2116.

[16] M. Kiran Kumar and Dr. Pankaj Kawad Kar. “Implementation of Novel Association Rule Hiding Algorithm Using FLA with Privacy Preserving in Big Data Mining”. Design Engineering (2023): 15852-15862

[17] K. APARNA, G. MURALI. ANNOTATING SEARCH RESULTS FROM WEB DATABASE USING IN-TEXT PREFIX/SUFFIX ANNOTATOR, International Journal of Research in Engineering and Technology. 2015;p.16.

[18] Rawat, D.B.; Chaudhary, V.; Doku, R. (2021) ‘Blockchain technology:Emerging applications and use cases for secure and trustworthy smart systems’. J. Cybersecur. Priv.