Proceedings of the International Conference on Sustainable Computing and Smart Systems (ICSCSS 2023)
DVD Part Number: CFP23DJ3-DVD; ISBN: 979-8-3503-3359-6

Decentralised Ballot System

Shaik Khaleelullah
Assistant Professor
Department of Information Technology
Vignan Institute of Technology and Science
Hyderabad, India
khaleel1245@gmail.com

Dosapati Sai Hemanth
UG Scholar
Department of Information Technology
Vignan Institute of Technology and Science
Hyderabad, India
dosapatisaihemanth@gmail.com

Endroju Kavitha
UG Scholar
Department of Information Technology
Vignan Institute of Technology and Science
Hyderabad, India
endrojukavitha03@gmail.com

Bommaraju Viswadutt
UG Scholar
Department of Information Technology
Vignan Institute of Technology and Science
Hyderabad, India
duttu2422@gmail.com

Battini Sri Vamshi Teja
UG Scholar
Department of Information Technology
Vignan Institute of Technology and Science
Hyderabad, India
srivamshi.battini@gmail.com

***Abstract*—Online voting is getting increasingly popular in modern society. It has the potential to cut administrative costs while increasing participation rates. Citizens can vote online from any place with an Internet connection, eliminating the need to print ballots or build up polling locations. Despite these benefits, remote voting systems have to be approached with extreme caution since it represents new hazards. A single weakness might make it trivial to manipulate votes on a large scale. Electronic voting systems used in elections must be trustworthy, precise, secure, and practical. However, problems with electronic voting machines may prevent their broad use. To overcome these concerns, block chain technology was developed, which provides decentralised nodes for vote processing and is utilised to build electronic voting systems. Because it provides shared, not repudiating, and security protection features, this technology is an excellent alternative to standard electronic voting systems. The following article provides an overview of electronic voting systems that use block chain technology. The primary purpose of this analysis was to assess the current state of blockchain-based voting studies and balloting systems as a whole as well as any associated issues, in order to forecast future advances. This study offers a conceptual overview of the anticipated block chain-based electronic voting application, as well as an introduction to the blockchain's core structure and properties in connection to electronic voting. This investigation indicated that blockchain technology may be able to solve some of the problems now plaguing voting methods. However, the most often raised concerns about blockchain applications are transactions timelines and privacy protection. A based on blockchain technology electronic voting system must be scalable in terms of transaction speed as well as distance voting security. Because of these problems, it was decided that current structures needed to be modified in order to be used in voting systems.**

***Index Terms*—Voting, Electronic, Systems, Blockchain-based, Blockchain, Online, Problems, Speed, Technology**

I. Introduction

Blockchain technology has recently attracted a lot of attention from a variety of industries, including banking, healthcare, and logistics. The voting system, however, is one area where blockchain technology has the potential to transform. Blockchain technology can offer a safe and trustworthy platform for voting, maintaining the integrity of the election process thanks to its decentralised and transparent nature. An intriguing possibility in this situation is a blockchain-based voting system for students, which would provide a fresh method for holding elections and polls in colleges. Student elections and polls have historically been held utilizing paper ballots. Online voting methods may be subject to hacking or other security flaws, whilst paper ballots might be easily misplaced or altered. To assure the accuracy and impartiality of the findings, these conventional methods may also be time-consuming and expensive to manage. Several of these issues may be resolved by using a blockchain-based voting system, which offers a safe, open, and affordable method of holding student elections and polls. The decentralized structure of the blockchain may be utilized to do away with the requirement for a central authority or third-party mediator, preserving the integrity of the voting process.

A. *Leveraging Blockchain as the platform*

- Blockchain technology first garnered appeal as a tool to decentralize the system and eliminate intermediaries. A blockchain is a shared, distributed ledger that records transactions and is maintained by different nodes in the network who do not trust each other. Blockchain is a distributed transaction processing system with Byzantine fault tolerance and entrusted nodes.
- Organizations find it helpful to connect different systems without building a centralized solution and to build trust between parties who do not trust each other or bring in a trusted third party. This blockchain property offers a secure, transparent, and immutable way to vote.

With the use of distributed ledger technology like blockchain, records may be kept securely and openly. Stuart Haber and W. Scott Storyette initially offered the notion of employing cryptography methods to construct a tamper-proof ledger in 1991. This was the beginning of the idea of a

distributed ledger system. Blockchain technology, however, wasn't utilised in real-world applications until the 2009 creation of Bitcoin. The creator of Bitcoin, who went under the alias Satoshi Nakamoto, remains unidentified. Based on a decentralized network of nodes that keep a public ledger of all transactions, Bitcoin is a form of the online payment system. Cryptographic security measures have been taken to protect this ledger. Due to Bitcoin's popularity, additional blockchain-based cryptocurrencies including Litecoin, Ethereum, and Ripple were created. Blockchain technology is used by these cryptocurrencies to facilitate safe and open transactions without the involvement of middlemen like banks.

A blockchain-based ballot system's transparency is one of its main advantages. A visible and auditable record of all votes cast is provided by the fact that every transaction on the blockchain is tracked and preserved in an impenetrable, secure ledger. With no chance of manipulation or tampering, this guarantees that the election results are exact. Furthermore, the implementation of smart contracts in a voting system built on a blockchain can contribute to ensuring the integrity of the election process. The rules and regulations of the voting system are enforced through smart contracts, which are self-executing contracts. It can aid in ensuring that only legitimate voters are allowed to cast ballots, that each voter is only allowed to cast one vote, and the election results are correctly tabulated.

Security is another advantage of a blockchain-based ballot system. The security and integrity of the system can be helped by the blockchain's usage of encryption and consensus techniques. A network of nodes verifies and validates transactions on the blockchain, guaranteeing that the election results are accurate and unchangeable. Furthermore, compared to conventional voting systems, the blockchain is more secure and less susceptible to hacking due to its decentralized structure. A blockchain-based ballot system can be economical in addition to offering a safe and open voting platform. To assure the accuracy and impartiality of the outcomes, traditional voting methods can be expensive to manage and call for substantial resources. On the other hand, a blockchain-based ballot system can do away with many of the expenses related to conventional voting systems. Overall, a student voting system powered by blockchain presents an intriguing possibility for colleges and schools. A safe, transparent, and affordable platform for holding student elections may be provided by utilizing the advantages of blockchain technology. Nevertheless, the creation of such a system takes careful research and preparation, which also includes choosing the best blockchain platform, creating smart contracts, and putting the system through testing before it is made public. Also, it's crucial to make sure that all students can access the system and that the right instruction and assistance are given so it is aware of how to utilize it.

As a result, the usage of blockchain technology presents a promising future for student elections and surveys. The integrity of the election process may be ensured by using a blockchain-based voting system, which can offer a safe, open, and affordable platform for conducting these activities. To make sure that the system fits the goals of the business and offers a user-friendly experience for all students, it is crucial to give serious consideration to its creation and implementation.

II. LITERATURE SURVEY

The project focuses on an Online Voting system For this, some references have been taken from few previously published papers and works of various individuals in this field.

In 2021, Rathee, Waqar and Kashif Bashir in their paper "On the Design and Implementation of a Blockchain-Enabled E-Voting Application Within IoT-Oriented Smart Cities"[1] the blockchain can be utilized in an environment with advanced technology. The system mistakenly believed that all were associated. Various factors can be trusted. The system's security flaws, however, pose a significant threat because it is possible for hackers to manipulate the voting results.

In 2018, M. Pawlak and Aneta in their paper "The Intelligent Agents for the Blockchain e-voting system"[2] do not need any operating entitiesFurthermore, it required a large amount of computer power and failed to secure voter identities. Although the software could gather user votes, the complex processing caused lag to become a problem when the user's vote rate increased. The identities of the voters were made public. The system couldn't manage the volume.As a result, large-scale implementation was not successful.

In 2008, D. Chaum in his paper "Scantegrity: End-to-End Voter-Verifiable Optical-Scan Voting"[3] states that voters now have the ability to ensure that their votes are included in the vote count by utilizing end-to-end verification. Each voter had the ability to check if their vote had been counted and accurately recorded. A special code was provided to each voter, which it could use to enter the system and confirm their vote. However, the verification of votes has been significantly simplified in this suggested voting system. Voters can confirm their ballots by analyzing their logged-in email addresses. When votes can be verified after they are casted, voter trust strengthens.

P. McCorry in his paper "A Smart Contract for Boardroom Voting with Maximum Voter Privacy"[4] discussed voting procedures without mentioning polling stations. He claimed that, if done correctly, balloting online via blockchain technology may have beneficial effects. The technological flaws in computerized voting systems were discussed. The system's robustness was uncontrollable. Using end-to-end verification reduces the error caused by users being doubled. Low-latency voting systems that did not protect voters' privacy were used. In order to decrease system delay, the proposed blockchain voting system makes use of intelligent agreements and an extending compromise algorithm.

In 2020, Akhil Shah, Nishita, Shruti and Madhuri Chavan in their paper "Blockchain Enabled Online-Voting System"[5] proposed that as an Android application, the recommended solution is more accessible and has higher levels of protection thanks to authentication, authorization, and verification. The voter or user in this system must first register by filling out a registration form found within the Android application, and once that form is accepted, a record is produced in the central database. The user can log into the application and participate in the polling process after registering. When a user has valid credentials, it can log in to the system and validate them by inputting a one-time password that is only good for so long. The dashboard has all the data that is retrieved from the corresponding account once the user has logged in.

In 2022, Yash Sangolkar, Nikita Marode, Vikas Meshram, Pranav Sarve, Akhilesh Shambharkar and Sujit Meshram in their paper "Online Voting System Using Blockchain suggested design"[6] provided a concept that an Android app with improved security features that include authentication and authorization. This project uses blockchain technology, 128-bit AES encryption, and SHA-256 to create security. The vote is cast as a transaction, and a blockchain is developed to keep track of vote totals. Atomicity and integrity are preserved in this way.

III. Architecture and Methodology

A. *Blockchain*

An open, distributed, and decentralized ledger is a blockchain. Public, private, and consortium blockchains are the three subcategories of blockchain technology that may be categorized according to network architecture. Data performance, analysis, and accessibility by network users all play a role in blockchain network building.

Each organization's development depends on the employment of the three forms of blockchain, which all play a significant role. As the blockchain is more dependable and secure, the company transfers data from its databases to it.

Public Blockchain: An open blockchain functions without limitations. The network may be accessed and the transaction can be initiated as long as you have an internet connection.

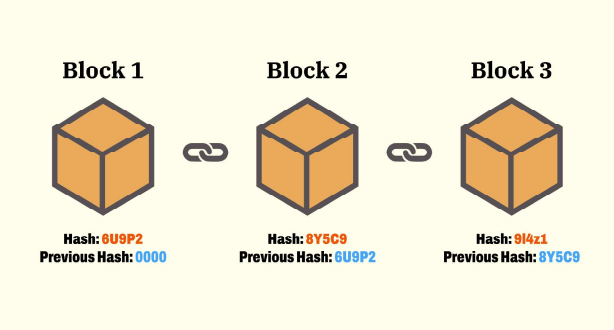

Fig. 1. Blockchain Architecrure

Private Blockchain: Blockchain that has been authorized is referred to as a private blockchain. Private blockchains function via access controls that impose restrictions on who may join a network.

Consortium blockchain: A consortium blockchain combines both public and private blockchains. As with the public blockchain, anyone can join the consortium blockchain without obtaining permission, however when individuals join the network, control of the network does not go to a single owner.

Some examples of a public blockchain are Ethereum and Bitcoin. The sophisticated mathematical operations serve as proof for this. This study makes advantage of open blockchain (Ethereum). A block is the foundation of a blockchain, which is fundamentally made up of a chain of blocks. A block has a header and a body, and the body of the block is where the network transactions are recorded. The block information, including the previous hash, block timestamp, and transactions, is contained in the block header. Each block also contains data on the party taking part in the transaction. The block size varies and is said to range between 1 and 8 MB.

A number of strategies may be employed to increase the functionality of a decentralised ballot system. Here are some ideas for increasing system efficiency:

Scalability: To overcome the scalability issue, employ techniques like as sharding or sidechains. The blockchain network may be sharded into smaller pieces in order to complete transactions in parallel. Sidechains reduce a portion of the processing burden on the primary blockchain by offering secondary chains that can execute certain tasks. These techniques can increase a system's performance and capacity.

Network Infrastructure: Enhancing the network infrastructure that drives the blockchain voting system. To ensure that the network's nodes are well-connected, a high-speed, reliable internet link should be employed. Use load balancing mechanisms to distribute the handling of transactions over several nodes, minimising bottlenecks and improving performance.

Data Management: Improve your data management strategies to reduce storage and retrieval times. Implement effective information architectures and indexing approaches to enable quick access to relevant information. Consider employing off-chain storage solutions for non-critical data to reduce the burden on the blockchain.

Transaction Batching: Reduce block production and validation costs by merging many activities into a single block or batch. This method has the potential to significantly boost the system's overall capacity as well as transaction processing speed.

Regular Updates and Optimization: Maintain up with the latest blockchain innovations and apply them into application to improve efficiency. Collaborate in the Body and include platform-specific optimising tactics using best practises provided by blockchain expertise.

Off-Chain Processing: Consider off-chaining any computa-

tionally difficult or non-essential tasks. By using trusted third-party services, you may reduce the processing burden on the shared ledger network while increasing overall performance.

Continuous Monitoring and Optimization: The voting mechanism's effectiveness should be evaluated in real time on a regular basis. Measure and evaluate performance to discover opportunities for improvement. Gradually increase the system's performance based on what you've come to learn through monitoring.

The block header specifically identifies the block that has to be inserted. Blockchain combines three of currently prominent technologies: A one another system with a common ledger that utilises a computational technology that enables network-related transactions and information to be stored. In cryptography, the two keys are the public and private keys. These keys aid in the efficient interaction of two parties. Both of these credentials are specific to each individual who relies on them to establish a link to a protected digital identity. This secure identification is a critical aspect of Blockchain technology. In the cryptography sector, this identification is referred to simply a "digital signature" and is used to authorise and manage transactions.One of the distinguishing features of blockchain technology is the method in which it confirms and authorises transactions. If each of the parties were to conduct an interaction with both of their private and public keys, the first portion would connect the transaction data to the other party's public key. This complete information is put into a block. The data block contains a date and time stamp, an electronic signature, and other critical information. It should be noted that the block of transactions does not contain any information on the identities of the transaction's parties. The block is then distributed around the network for distribution, and when the proper user uses his personal data to compare it to the earlier interfere with, the transaction is completed successfully.In Blockchain technology, adding transactions data to the existing online/public database is referred to as "mining." Although the term is associated with Bitcoin, it may also refer to other Blockchain technologies. Mining guarantees the integrity of the entire Blockchain by establishing a difficult-to-forge block transaction hash.

There are a few crucial variables to consider and practises to follow in order to maintain reliability in a decentralised ballot system. Here are some crucial steps to take:

Decentralisation: Ascertain the fact that the decentralised ballot system is distributed, which means that many nodes participate in the confirmation and validation process. As an outcome, the system is more dependable overall and helps to eliminate just one cause of failure.

Security: Strong security measures should be used to ensure the correctness of the voting process. These cryptography approaches involve authentication, encryption, and secure key management. Regularly scan your machine for vulnerabilities, then apply the necessary updates and patches.

Transparency: Since every transaction have been recorded on an open ledger, the blockchain by definition encourages transparency. Ensure that the voting method is clear and available to all participants, allowing them to verify their votes and ensuring that no unauthorised alterations have been made.

Immutable Records: Use the blockchain's immutability to prevent tampering with voting records. After a vote is recorded on the blockchain, it should be difficult to edit or erase it. As a result, the votes' legitimacy and reliability are ensured.

Consensus Mechanism: Consider a system for consensus that is suitable for casting votes, such as Proof of Stake (commonly known as PoS), which enables speedy and trustworthy methods of transaction verification. These strategies help to defend against attacks by ensuring that a significant majority of participants believe the votes are genuine.

Redundancy and Backup: Maintain numerous replicas of the blockchain to ensure fault tolerance. To protect against corruption or loss, maintain a lot of backup of the decentralised ledger's data. Because of this redundant operation, the system will always work even if some nodes fail.

Remember that building trust and reliability in a distributed voting system is an ongoing process that necessitates an all-encompassing security and transparency approach. It's critical to stay up to date on the latest blockchain developments and adapt your system as needed.

B. Ethereum

Decentralized applications may be created and deployed on top of the Ethereum network thanks to its open-source, decentralized architecture. In order to offer a platform that was more adaptable and programmable than Bitcoin, Vitalik Buterin developed it in 2014. The usage of smart contracts, self-executing contracts that can be designed to automatically carry out certain activities when certain criteria are satisfied, is one of Ethereum's core characteristics. This makes a variety of decentralized applications conceivable, including those for non-fungible tokens (NFTs), decentralized finance (DeFi), and more. As a payment method for network transactions and computational services, Ethereum also has its own money called Ether (ETH).

C. Smart Contract

An output with a defined size, known as a hash, is produced by the process of hashing input data of arbitrary length. In addition to storing passwords, it is frequently used to verify.

An output with a fixed size of 512 bits is produced by the cryptographic hash algorithm SHA-512. The National Security Agency (NSA) created this SHA-2 family hash algorithm to be resistant against future assaults. The output of SHA-512 is a fixed-size message that is specific to the input and may be generated from an input message of any length. Digital signatures, password storage, and data integrity checks are among popular uses. Since it is so powerful against collisions and pre-image attacks, SHA-512 is regarded as being quite secure. All things considered, SHA-512 is a popular cryptographic hash algorithm that is trusted and secure for usage in many security applications.

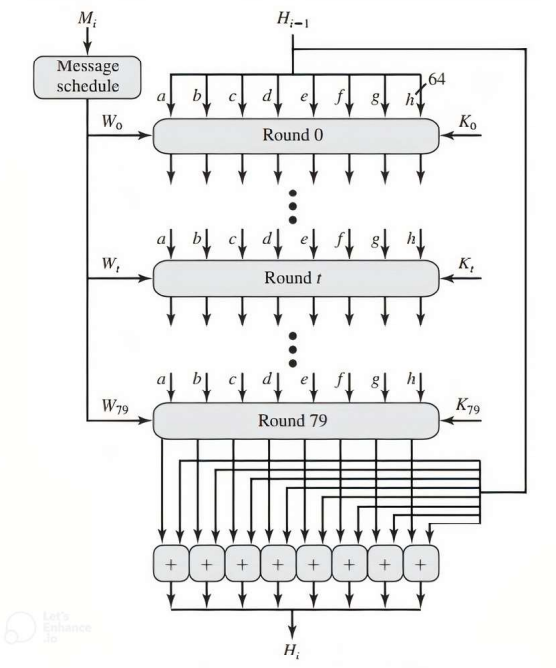

Fig. 2. SHA-512

D. *Hashing Function SHA 512*

The SHA-512 algorithm is a cryptographic hashing function that accepts any length input and returns a 512-bit fixed-size output. It is regarded as a secure hashing technique and is frequently utilized in applications other than blockchain, such as password storage and digital signatures. To secure the security and integrity of the blockchain, SHA-512 is frequently employed in conjunction with other cryptographic techniques such as public key encryption and digital signatures. The method can build a decentralized, tamper-proof ledger that can be trusted by all network participants by employing SHA-512 to create unique, unalterable fingerprints of each block in the blockchain.

E. *Architecture*

A blockchain and SHA-512-based online voting system architecture includes numerous critical components. The user interface is the platform through which voters access the system, but the blockchain is a decentralized database that secures all transaction records. Smart contracts automate a variety of operations, including voter registration and voting. The SHA-512 hashing algorithm creates a unique digital fingerprint for each vote that is kept on the blockchain, safeguarding the integrity of the vote.

The consensus procedure ensures that each vote is checked and counted correctly and that the election results are correctly recorded. The combination of blockchain with SHA-512 enables secure and transparent online voting. The usage of blockchain ensures that all transactions are securely recorded and stored, giving transparency and removing the possibility of

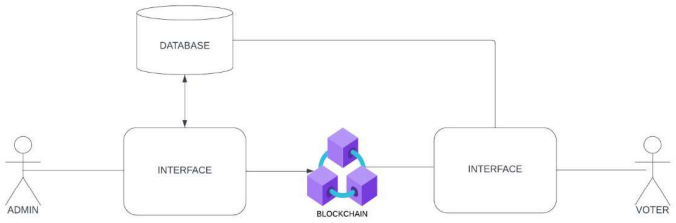

Fig. 3. System Architecture

fraud or manipulation. The SHA-512 hashing algorithm generates a unique digital fingerprint for each vote that is nearly impossible to recreate, adding an extra layer of protection. The consensus mechanism ensures that all transactions are accurately validated and that the election results are correct.

IV. Implementation

The blockchain-powered technology is kept up to date in order to execute the voting process. The transaction hash is preserved on the chain along with all of the voting results, which will be displayed on the voter's dashboard. Once a voter first signs up, the system runs checks to determine if they have a university Ids and whether the vote have previously casted.

A. *dApp configuration*

This section describes the components of the Vote Management System. It provides a user interface and front-end security for secure voter interaction with the system. The VMS front end now has a dAPP interface. A dAPP is a decentralized application built on the blockchain. It is based on a blockchain network that is peer-to-peer. Because the user enters his or her login information on this user interface the authentication process needs to be tamper-proof and simple. The technology guarantees that everyone who votes has equal access to the ballot box as well as that their participation can be traced once finishing the casting. The voter enters his or her login information into the system. The platform registers a user by using the user's ID and linking it with the database. In order to log in, the platform provides a one-time password (OTP) to the voter registered email address, which it must be input. Whenever the candidates log into the VMS, an OTP is generated. The dAPP technology is used to ensure VMS stability because of its effectiveness of distributed processing at all nodes. If one of the nodes in the system fails during the voting procedure, the remaining nodes are unaffected.

The other nodes aid the vulnerable node by restoring it. Decentralised apps (dApps) are distributed, decentralised publicly accessible software programs that run over a decentralised peer-to-peer network. Consider the Twitter app on your phone. You may publish whatever you want on Twitter, but it is ultimately owned by a single firm that can remove the tweets if they break community rules or for any other reason. However, if a dApp like Twitter existed, it would be decentralised and not owned by a single individual. Nobody, including its

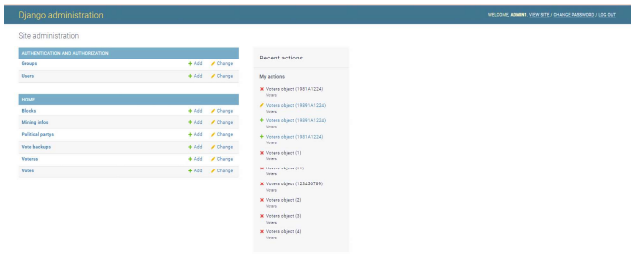

Fig. 4. DAPP configuration

designers, would have been able to erase anything you placed there.

B. *Registration to vote*

Users' uniqueness can be determined by using their digital college ID. Once submitted, voter information is verified with the help of identifying authorities. This makes it impossible for another voter to use a voter's identity. Authorities use credentials to determine whether a person is eligible to vote in a specific ballot and if their university ID has already been hashed. When a person votes, an exchange hash is issued to their ID. Because the blockchain changes and saves a voter's vote, the user is not allowed to vote again until a fresh VC is granted.

C. *Deployment of clusters*

The chain deployment is covered in more detail in this section. Following the voter's submission of their ballot to the system, the balloting process is extracted and put into the blockchain. The voter receives notifications about each successful blockchain transaction at the provided phone number. Using the transaction's hash value, the voter may verify his choice. Because the issue of unfinished process transactions is eliminated by this method of changing the current state of vote operations on the chain, the chain only processes successful transactions in order to compute the voting result because only those votes are tallied. A 10-minute lag has been chosen in order to reduce the volume of transactions on the blockchain. Election officials can review the voter's outcomes on the VMS dashboard after casting their ballots.Data about registered voters, qualifying applicants, and election outcomes are displayed on the dashboard. A country's low literacy rate may be a weakness in the structure, but it may be remedied by giving media education a chance to make the interface as easy as feasible. Voters with native language backgrounds may readily use the multilingual interface of the technology.

V. Conclusion

In this paper, the major goal of the project was to create a safe online voting system that would be used. The project's goal was to transition from paper-based voting to electronic voting, which would let citizens to vote remotely from any location via the internet.

VI. Acknowledgement

We would like to convey our heartfelt appreciation to the Information Technology Department at Vignan Institute of Technology and Science in Hyderabad for giving us with all of the resources, support, and direction we required to complete this research.

References

[1] Geetanjali Rathee, Razi Iqbal Omer Waqar, and Ali Kashif Bashir,“ On the Design and Implementation of aBlockchain Enabled E-Voting Application Within IoT Oriented Smart Cities,” Tomsk Polytechnic University March 4, 2021.
[2] Michał Pawlaka , Aneta Poniszewska-Maranda ´ a Natalia Kryvinskab, “The Intelligent Agents for the Blockchain e-voting system,” EUSPN 2018
[3] David Chaum “Scantegrity: End-to-End Voter Verifiable Optical- Scan Voting” June 2008
[4] Patrick McCorry, Siamak F. Shahandashti and Feng Hao “A Smart Contract for Boardroom Voting with Maximum Voter Privacy,” School of Computing Science, Newcastle University UK
[5] Akhil Shah, Nishita Sodhia, Shruti Saha, Soumi Banerje, Madhuri Chavan “Blockchain Enabled OnlineVoting System,” ITM Web of Conferences 32, 03018 (2020).
[6] Yash Sangolkar, Nikita Marode, Vikas Meshram, Pranav Sarve, Akhilesh Shambharkar, Sujit Meshram, “Online Voting System Using Blockchain suggested design” Computer Science Engineering, Dr. Babasaheb Ambedkar College of Engineering Research , India, :05/May-2022
[7] Nakamoto, Satoshi. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System.
[8] Stamatellis, Charalampos, Papadopoulos, Pavlos, Pitropakis, Nikolaos,Katsikas, Sokratis, and William J. Buchanan. ”A Privacy-Preserving Healthcare Framework Using Hyperledger Fabric.” Sensors 20, no. 22(2020): 6587. https://doi.org/10.3390/s20226587.
[9] M. Castro and B. Liskov. Practical byzantine fault tolerance. In Proceedings of the Third Symposium on Operating Systems Design and Implementation, OSDI ’99, pages 173–186, Berkeley, CA, USA, 1999. USENIX Association
[10] Parth Thakkar, Senthil Nathan, and Balaji Vishwanathan. (2018). Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain-Platform.
[11] Why new off-chain storage is needed for blockchains. https://www.ibm.com/downloads/cas/RXOVXAPM
[12] H. Mukne, P. Pai, S. Raut and D. Ambawade, ”Land Record Management using Hyperledger Fabric and IPFS,” 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur,India, 2019, pp. 1-8, doi: 10.1109/ICCCNT45670.2019.894447
[13] Yogesh Sharma, Dhruv Kapoor,Divyaansh,Divyam Sinha“Online Voting System using Blockchain”December-2021
[14] http://codewalkers.com/tutorialpdfs/tutorial79.pdf
[15] Shaik Khaleelullah, Dr. Prabhakar Marry “A Framework for Design and Development of Message sharing using Open Source Software Dept of CSE, Vignan Institute of Technology and Science, Hyderabad, India