IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 2, November 2023

Secure Digital Voting System on Blockchain

Prof. Santosh Kumar Biradar[1], Diksha Mohod[2], Sampada Joshi[3], Rohini Role[4], Prasen Waikar[5]

Department of Data Science[1,2,3,4,5]

G. H. Raisoni College of Engineering and Management, Wagholi, Pune, Maharashtra, India

Abstract*: Every citizen's fundamental right, voting is a crucial part of democracy. Every nation benefits from blockchain-based elections sincethey allow for the conduct of elections online. It makes the election process safe, easy, and straightforward in contrast to the outdated (paper-based) and traditional (EVM) votingmethods. The main goal of this project is to design and build a decentralised, blockchain- based voting and analysis system that might beused to set up election systems in countries where traditional, in-person voting with readily manipulable assurances is the norm. The goals of this system's design are to providea safe voting process, save expenses, shorten wait times, eliminate inequalities brought on by different types of incorrect proxies, scale well, and operate independently of physicallocation. All in all, a reliable voting system willhelp the democratic system thrive. Voters may now cast their ballots from the convenience oftheir own homes thanks to our initiative, whichwill save them time and cut down on the number of invalid votes cast.*

Keywords: Blockchain, Ethereum, Decentralized, E-Voting, Phishing Website

I. INTRODUCTION

Without a shadow of a question, thegroundbreaking idea of the blockchain, which isthe underlying technology behind the popular cryptocurrency Bitcoin and its successors, isushering at the beginning of a new age for the Internet and online businesses. While most people's attention is on cryptocurrencies, many previously offline administrative tasks, finance procedures, and everyday activities are now being safely relocated to the Internet as online services. The Implementation of smart contracts, as seen on the Ethereum Space, makes it a potential medium for the global digitalisation of mundane services. Integrating smart contracts onto the blockchain and having them run as planned throughout each round of blockchain updates is a key function of thistechnology. On the other hand, electronic votingis another hot subject that's also crucial to the future of internet businesses. An attractive option for creating trustworthy, inexpensive, secure, transparent, and user-friendly electronic voting systems is the blockchain coupled with smart contracts. Due to its reliability, popularity,and availability of smart contract logic, Ethereum and its network are among the best options. It is important for an electronic voting system to be trustworthy in that it prevents voters from casting the same ballot more than once, is completely open and public, and keeps voters' personal information confidential. Here, we show how to use Ethereum wallets and the Solidity programminglanguage to build a working smart contract for example electronic voting application on theEthereum network. People who don't have an Ethereum wallet may still be able to cast a voteby using the Android platform.

Modern voting procedures like ballot box votingand electronic voting, which demand a lot of paperwork, labour, and time, are also susceptible to virus attacks, DDoS attacks, polling booth capture, and other security issues such vote tampering and manipulation. Consequently, people tend to lose faith in the current order of things. Voting data will be stored in the Ethereum wallet after an election has concluded. Every node in the EthereumSpace must agree on the results of a vote cast bya user on an Android device or via an Ethereumwallet. In this work, we present a new approach for a trust-free, distributed voting platform usingBlockchain technology to eliminate the need forcentralized authority.

In this age of industry 4.0, blockchain technology is becoming increasingly popular. Because of its high security and openness, it is widely used in a broad range of applications, including voting systems, supply chain management software, healthcare payment systems, commercial enterprise, the Internet of Things, and more. A distributed, unchangeable database, blockchain allows businesses to record transactions and keep track of assets. Theinnovation brought about by blockchaintechnology is that it provides a safe and secure method of recording data and building trust among those involved along with a neutral thirdparty. According to the findings, the method is workable and might

DOI: 10.48175/IJARSCT-13850

pave the way for the creation of optimal settings for such an adventure. Data in a blockchain database is stored in a series of blocks. As the chain cannotbe removed or changed without network consensus, the data is chronologically consistent. In light of this, blockchain technology enables you to build an immutable or unchangeable ledger for keeping track oforders, payments, accounts, and othertransactions. Mechanisms are included into the system to guard against illegal transaction inputsand guarantee consistency in the shared view ofthese transactions.

At this stage, technological use is crucial for assisting in meeting human requirements. Giventhat most people nowadays don't trust their governments and that elections are crucial in contemporary democracies, the growing use of technology has brought new difficulties to democracy. Elections are crucial in decidingwho will lead a country or organisation, or you might say that they are the event that determines the future of any nation. Elections, which are the core of a parliamentary system, enable every member of the community to express their thoughts by voting. Considering elections are so vital to our society, the process should be transparent and reliable in order to guarantee parties of its authenticity. The manner of votingin these circumstances has been an ever-shiftingfield. The goal of making the system visible, dependable, and easily accessible is driving this progress. Given its relevance, continual efforts have been undertaken to improve the functionality and endurance of the polling system. E-voting, often known as voting via the internet, plays an integral part in this process.

Because of the usage of internet technology, electronic voting systems have expanded enormously since they were initially implemented as punch card ballots in the 1960s(Gobel et al, 2015). Voting via the internet solutions have to adhere to specific benchmark criteria in order to get mainstream recognition. Among these factors are the confidentiality of the voter and the genuineness of a ballot.

Modern democracies rely heavily on elections, however there is cause for concern because large portions of the population worldwide lackfaith in their electoral system.

Even the most developed democracies, such as India and the United States, have faulty voting processes. Vote rigging, EVM hacking, electiontampering, and polling place capture are theprimary issues with the current voting system.

Challenges To Existing Voting System

Vote Rigging

Vote rigging, which is also known as election tampering voter fraud, or is the illegal affectingin an election, either to boost the vote percentage of a preferred politician, lower the vote % of an opposing party, or both.

While it is distinct from voter intimidation, it frequently coexists with it. Election fraud can take many different forms depending on thecountry.

EVM Hacking

There are two primary methods of hacking EVMs: wireless and wired. Several cybersecurity and election specialists have concluded that EVM hacking is a very difficult achievement. EVMs are not networked devices, so to hack one would require changing the actualmachine.

This means that anyone seeking to hack an EVMwould need physical access to the machinesitself, which would require them to work inconcert with organisations responsible for the manufacture of EVMs, the ECI, as well as businesses that produce the chips used in EVMs.

Election Manipulation

Elections that are fair, free, and frequently heldare the foundation of democracy. But if one of the contenders tinkers with the regulations or improperly levels the level field in their favor, elections cannot be free and fair.

Alarming instances of state and federal elected officials improperly interfering in their own elections have occurred in recent years. This misuse of authority hits at the very foundation of Indian democracy and jeopardizes the fairness of our election system.

Polling Place Capturing

Booth capturing, also known as booth looting, is a kind of election fraud in which paid criminals or party supporters "take" a polling location andcast votes for a certain candidate in place of eligible voters to assure their victory. It is a

DOI: 10.48175/IJARSCT-13850

method of suppressing the vote. In Indian elections, it is customary for representatives of each candidate to be present at the polling place. However, in many instances, these representatives face threats or physical harm and must leave the polling place. A portion or half of one of the Central Paramilitary Forces is sufficient, according to the general terminologyof the Indian Election Commission, to avertdisturbances.

Blockchain And Secure Voting

Blockchain is a cutting-edge technology with strong cryptographic fundamentals that enable applications to take advantage of these characteristics to provide effectivesecurity alternatives.A distributed ledger of block chain technology is analogous to a data structure in that it records and transmits all transactions executed from its inauguration. It isprimarily composed of a set of databases that maintain an extensive collection of continuouslyevolving and growing data records that provideprotection from criminalized manipulation, deceit, and tampering. Each person connectedto the network can transmit transaction records,validate transactions, and add new blocks usingthe blockchain technology.

As long as the pieces of a block are not amended, a cryptographic hash is generated foreach of the components, which may also bethought of as the signature of the block. If the block is changed in any a fashion, the cryptographic hash changes swiftly, indicating that the contents has changed, possibly as aresult of a criminal act. As a result of its robust encryption foundations, blockchain technology is becoming increasingly used to prevent illicit payments in a broad range of domains. Although Bitcoin continues to be the most notable blockchain application, academics are eager to investigate how blockchain technology may be used to support programs across various sectors by exploiting advantages like non- repudiation, reliability, and anonymity.Due to its intrinsic ability to retain anonymity, maintaina a decentralized and publicly distributed system, and play a significant part in electronic voting a log of all node-wide transactions. Due to this, blockchain technology is particularly effective at addressing the risk of using a voting token more than once as well as attempts to sway the outcome's transparency.

Requirements For Secure Voting System.

In spite of opposition from software engineers, Direct Recording Electronic (DRE) votingtechnologies were ultimately implemented and highly praised and recognized by the electorate

Voters' understanding of the voting process cangreatly improve how usable the system is.

Particularly DRE systems have had a lot ofsuccess in getting voters to adopt this technology. These procedures operate essentially in the same manner as a traditional election device does. In the case of DRE, a voterstarts his or her journey by attending the polls toobtain a token, which they then use at the ballotterminal to cast their ballot for their candidate.

After the candidate selection process is finished,the DRE system in the context of the final selection to the voters before they cast theirballot (in case they wish to alter their minds), and then the vote casting process is finished.

Due to the benefits of final authenticity,decentralized ledger technologies like blockchain have lately been employed to create e-voting systems Due to qualities such as anonymity as well as confidentiality, block chain technology is an especially attractive alternative to present electronically casting votes solutions.The general specifications for a typical electronic voting system have been laid out in (Rura et al, 2016). We list eachrequirement's brief description below:

Only Eligible Voters Are Permitted To CastBallots, And Each May Only Do So Once.

All qualified users must register usingdistinctive identification, such as official documents, to demonstrate their status. Additionally, the system uses finger printingtechniques to create a secure authentication process that guarantees that only authorized participants can utilize the system. Moreover, the method can avoid duplicate votes thanks to the usage of biometrics technology. Votersshould not have to be able to show their voting record to a third party in order to claim receipt independence. The suggested solution creates a cryptographic hash for each such occurrence(transaction) and lets voters cast their ballots however they see fit. To establish formal verification or ascertain whether a certain vote was counted, this is required. Nevertheless, possessing this hash makes it impossible for youto decipher the voters' voting patterns.

Convenience: Voting should be easy for voters,and everyone who is eligible should be able to participate.

DOI: 10.48175/IJARSCT-13850

Due to the system's user-friendly web-based UI, little user interaction is required throughout the voting process. As an example, fingerprinting isemployed as an authentication technique to do away with the need to remember usernames andpasswords. The user may interact with the process in a variety of ways since everything is connected.

II. TECHNOLOGY

The technology used here to crack the problem is Blockchain-Based Computing. Since the initiation of familiar and acquainted initiatives in cryptocurrencies. Bitcoin was the first digitalcurrency to employ Cryptocurrency transactions. Ethereum brought on smart contracts that highlight the benefit and power and elevated results while providing a Stable cryptocurrency solution to Cryptocurrency Transactions. According to Nick Szabo, smart contracts are "a collection of promises defined in digital form, including protocols within which the parties carry on these promises." These rumors about smart contracts date back tothe 1990s. In Ethereum, a contract is a section of code that the whole public may view and distribute to the network. The outcome for this type of code is successfully segregated and verified.

At the moment, we define a Blockchain-based computational system as a collection of technologies that include smart contracts, distributed evaluation, key cryptography, andthe blockchain data structure. These technologies are more fully explained in this section.

A peer-to-peer network repeats a series of blocks created by blockchain technology. A block includes the Merkle structured tree header block as well as multiple transactions. Cryptography, being a very sophisticated technological division uses both computer science and mathematics to derive the Data andimplement Security. It enables the secure transmission of encrypted and decrypted data over an insecure network. By making the voting process clear and accessible, avoiding fraud, strengthening data security, and certifying the outcomes of the vote, blockchain technology addressed flaws in the present electoral system.

A blockchain's ability to keep data securely and privately is made possible by encryption technology. Encryption includes transforming ordinary text or data into a ciphertext, which can only be decrypted with the necessary key. Encryption is commonly applied in blockchain in two ways:

Data encryption on the blockchain: To prevent unwanted access, all data on the blockchain is encrypted. This contains transaction data, walletaddresses, and other encrypted using public-keycryptography every single user owns their own private key and a public key. Data has been encrypted using the public key and recovered with the private key.

Communication between nodes is encrypted in order to protect the confidentiality of transactions and preserve the integrity of the blockchain. These messages are shielded from eavesdropping and manipulation through the use of encryption. For securely transmitting messages between the nodes, secure communication protocols such as Transport Layer Security (TLS) and Secure Sockets Layer(SSL) are frequently used. Ultimately, the security and privacy of data on the blockchain depend heavily on encryption technology. By encrypting data and communications, blockchain systems can provide a high level of security and safeguard against illegal access, tampering, or theft.

Technology can benefit from encryption in a number of ways: Sensitive data, such as private financial information, personal information, and confidential corporate information, can be protected using encryption technology. Data is made unreadable to unauthorized parties viaencryption and is only accessible with the right decryption key.

Users' privacy can be safeguarded via encryption technology. To ensure that only the sender and intended recipient may read messages, end-to-end encryption can be used inmessaging apps to block third-party access. Secure communication between devices and networks can be achieved using encryption technologies. Data can be transmitted safely and safeguarded from interception by encrypting communication routes. Users and devices can beverified using encryption technologies. Public- key cryptography, for instance, can be used to confirm user identities and guarantee that only authorized users have access to particular data or services.

A variety of laws and standards that call for theprotection of data can be complied with using encryption technology. For instance, theGeneral Data Protection Regulation (GDPR) mandates that businesses put in place suitable safeguards, such as encryption, to safeguard personal data. The security, privacy, and compliance of data and communication in technology can all be significantly improved by the use of encryption technology. The importance of encryption technology in preventing data breaches, identity theft, and other criminal actions will rise as cybersecurity threats continue to develop.

III. LITERATURE REVIEW

This legacy is Satoshi Nakamoto's completeunderstanding of blockchain and how it works. Indonesia held simultaneous presidential and parliamentary elections on April 17, 2019. This election had at least four major issues: logistics distribution, count of ballots that took a very crucial time, irregular regulation of vote counting, and vote recapitulation errors.Blockchain technology may solve those issues.

With regard to an efficient real-time implementation, they have used the concept in this presented paper, but for a number of different use cases, and we have utilised it as a starting point to construct a peer-to-peer transaction system in place of a decentralised voting system.

In the current time, there has been a phenomenal boost in the number of wireless technologies, smart gadgets, and sensors. IT hasbeen anticipated that trillions upon Billions of gadgets will be associated with each other in thenot-too-distant future. In order to support such avast number of devices, network solutions mustbe scalable, flexible, sustainable, and foreseeable.

The distribution of key functions over anumber of different entities, often known astrustees, is a typical method that is used to assurethe security of voting systems. Small Scale elections can be held in a centralised system, taking the role of trustees. Unlike other electionsituations, in which election officials serve as trustees, this one does not. Given that all candidates have an equal amount of support, thisis the most likely outcome of an election.

The usage of online voting is expanding at arapid rate in Canada, with most of the activity centred on union elections, leadership contests for political parties, and local elections. Thefederal structure of the state of Canada can, at times, make the use of the internet to vote easier,while at other times it can make its usage more difficult.

While taking a one-time course on blockchain technology, students at the University of Seattle created multiple voting systems. The original (re-use) system forkedEthereum for the sake of secrecy and security. In the second method, called "re-invent," two blockchains were developed: one for validatingvoters, and another for protecting their ballots.

Here, the election mechanism is delineated by a set of smart contracts that has to be deployed on the blockchain and managed by relevant authorities. Every voting precinct has its own blockchain-based election smartcontract. E-Voting with Blockchain: A Decentralized, Private, and Secure System for Voting was written by Freya Sheer Hardwick, Konstantinos Marcantonio, Raja Naeem Akram, and Apostolos Gioulis. The foundation for electronic voting in this system is commercial protocols like Bit Congress, Follow My Vote, and TIVI. The paper "Securing e-voting based on blockchain in P2P network," by Haibo Yi.

Academic papers in Lieu of e-voting systemhave increased over the past two years, despite a decline in the number of nations that have implemented it. There is currently no well- developed storyline in the literature explaining the development of study into the exasperation of electronic voting. This essay's goal is to lookat how academic research has changed over thepast 15 years in response to the growing usage of electronic voting. In this article, 78 papers from 2005 to 2020 are examined using a semi- systematic methodology.

Electronic voting, or "E-Voting," is a more up-to-date alternative to the use of paper ballotsin elections. The suggested system's architecturemust enable dependability and security in orderto facilitate the widespread use of electronic voting. We propose leveraging the Hyperledger Sawtooth blockchain platform to create a trustworthy, open, and distributed online votingsystem. Votes are cast and recorded in an immutable blockchain state, and access to the system is restricted to election polling sites.

Elections can be held using e-voting technology, sometimes referred to as electronic voting, instead of paper ballots. There are issueswith the security and dependability of the system that must be resolved before e-voting can be utilised widely. In 2008, Satoshi Nakamoto announced the Blockchain technology underlying the cryptographic currency Bitcoin. This technology enables the construction and development of a safe, transparent, and decentralized system in which no centralized authority has access to orinfluence over the voting process.

IV. PROPOSED SYSTEM

One area where blockchain has a significantinfluence is electronic voting. E-voting as astandalone system is not a viable solution due tothe high degree of obstacles. There will be serious consequences if an electronic voting system is hacked. Because a blockchain networkis fully centralized, fraud is theoretically impossible until it is properly deployed. Nothing logical about blockchain technology disallows its use with other cryptocurrencies. The idea of leveraging blockchain technology to build an unbreakable e-voting network is gaining popularity. Users would be unable to tell the difference between a voting system built onblockchain and a traditional electronic voting system while casting their ballots. By automating the voting process and assuring the accuracy of the results, smart contracts can be utilized to construct a safe and open voting system.

The election procedures and prerequisites are encoded into the contract in a voting system based on smart contracts. This can include specifics like voter eligibility, voting deadlines, and the available candidates or options. Thenecessary quorum for the election to be deemedvalid can also be stated in the smart contract. Voting is secure and anonymous after the contract is implemented on the blockchain, allowing for participation from all eligible voters. One vote per voter, for example, can be enforced by the smart contract, eliminating anychance of voter fraud or manipulation. The election results can be independently verified byany party with an interest if the voting process is transparent and auditable.

The smart contract automatically counts the votes and selects the winner after the voting session has concluded. The blockchain is used to store the election results, making them transparent and unchangeable.

In general, a voting system based on smart contracts can offer a safe and open way to conduct elections, free from the risk of fraud or manipulation. Elections may be held more affordably and quickly by automating the voting process, which also makes it more convenient for all parties involved.

Democracy on the platform's blockchain will include a completely accessible to everyone, anonymized piece of personal informationstored throughout an all-encompassing blockchain network instead of through a single server. Use our online voting method powered by the Ethereum Blockchain to ensure that yourvote is counted fast and correctly. Any computerwith an internet connection can be used by voters to cast their ballots. Data is safe from harm because to the system's secure blockchaindesign and several levels of protection. By leveraging blockchain technology, we can havea more trustworthy voting process that is also more secure, transparent, and unchangeable. In order to cast a ballot, voters must input their personal information. Following encryption, thedata is recorded as a financial transaction. The transaction is subsequently copied to every nodein the network, which then verifies its accuracy. With consensus, the transaction is added to the chain and recorded in a block

A block that has been added to the chain cannotlater be changed or withdrawn. The outcomes are now visible, and users may go back through their previous transactions if they so want. We need to create a voting system that combines security, convenience, and confidence since existing voting methods cannot keep up with the security needs of the present age. As a result, Blockchain technology is being implemented into voting systems to boost voting security, encourage voting independence from time and location, and reduce the time and expense associated with the voting process. Also, The scalability of the proposed system is due in largepart to the web application that is built using theReact framework. Our project's loading timeand overall performance have both been improved because to our use of React JS.

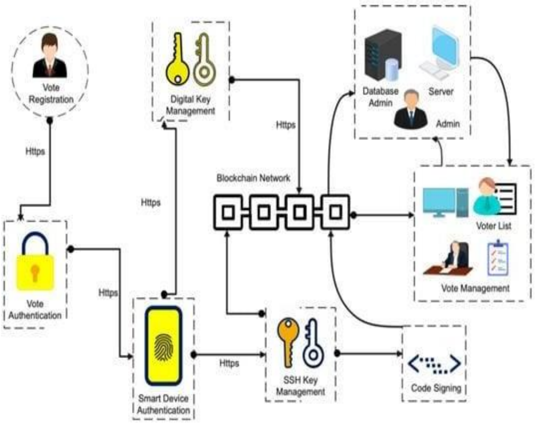


Fig 1.1 SYSTEM FLOW DIAGRAM

V. ARCHITECTURE DIAGRAM

The project's blueprints are laid out in detail. inFig 1.2. The user is required to log in using theircredentials, they can register new voters after verifying their details. If the verification is unsuccessful then the application is rejected.Some of the functions are to cast votes, count the votes, add the candidates, and register and verify the voters. All these are performed by using the Ethereum server. The construction of a blockchain system, although necessary, is notenough. It has to be decentralized so that if one server goes down or a problem arises on one node, the rest of the nodes can keep running without interruption.

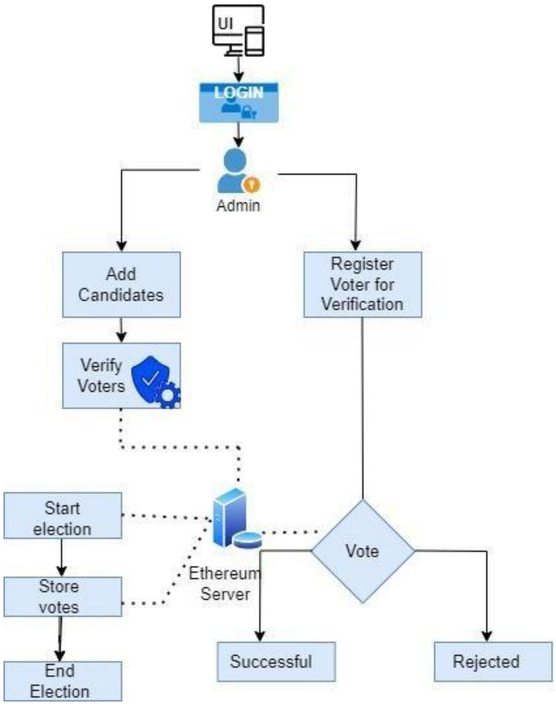


Fig 1.2 ARCHITECTURE DIAGRAM

VI. DESCRIPTION OF THE PROPOSED MODEL/SYSTEM

LOGIN

With wallet-based authentication in Web3 apps,the requirement for a username and password iseliminated. In contrast to the public key, which is used to specifically identify the account holder, the private key is utilised forauthentication. Our voting web app makes use of the meta mask wallet, a plug-in for many webbrowsers. In order to access the app, the user needs just link it to a payment account stored inthe user's digital wallet. The suggested system isdesigned such that each voter needs only one login. The key features of this system are its privacy protections, its one-vote-per-mobile-phone-number voting policy, and its commitment to data accuracy and openness.

INITIATING A NEW BALLOT

A new ballot may be initiated by any user by providing ballot details and authorizing the transaction using the wallet. With the blockchain network's approval, the transaction is added to the permanent record. The voter must supply a list of legitimate addresses whilecasting their ballot (the public addresses of useraccounts).

VOTING PROCESS

Users who are of voting age can do the same thing using a meta mask to link their accounts. After a search for a matching voter, a list of candidates that are up for election will be displayed, along with the opportunity to vote against each of them. If, however, there is no successful match, access will be terminated immediately. When a user approves a transaction in their wallet, their vote is added tothe distributed ledger at the same time the transaction is broadcast to the network. To this aim, each valid vote counts as a separate transaction on the voting app's blockchain.

DOI: 10.48175/IJARSCT-13850

VII. METHODOLOGY

By initially developing a distributed ledger technology that offers an immutable and transparent record of each vote, a blockchain- based secured voting system can be constructed. Authorized parties, such as voters and election officials, may have access to this ledger and utilize cryptographic keys to securely sign and validate transactions. The system can also include consensus procedures, such as proof-of-work or proof-of-stake, to ensure the integrity ofthe voting process and avoid data tampering. Smart contracts can also be used by the system to automate vote counting and enforce laws andregulations. End-to-end verifiability, which the system can be built to give, enables voters to check that their votes were accurately recorded and counted without jeopardizing their anonymity. A blockchain-based protected voting system can offer a highly secure andtransparent platform for holding reliableelections by leveraging these methods.

Two well-known blockchain platforms that facilitate the execution of smart contracts and decentralized applications are Ethereum and Algorand. Building blockchain-based voting systems can take advantage of the distinctive features and capabilities that each of these platforms has to offer.

Algorand has been developed to address some of the scalability problems that other blockchainplatforms, like Ethereum, have had in terms of performance. The pure proof-of-stake consensus technique used by Algorand enables quick and safe transaction processing with less energy use. Moreover, it offers atomic swaps, which permit asset exchange and cross-chain interoperability between various blockchain networks. On the other side, Ethereum has a bigger development community and a more mature ecosystem of decentralized apps. It employs a proof-of-work consensus technique, which has drawn flak for being inefficient and having scalability issues. But, as part of the Ethereum 2.0 update, which should enhance its performance and scalability, Ethereum is in the process of switching to a proof-of-stake consensus method.

Both Ethereum and Algorand offer a number ofbenefits for developing a blockchain-based voting system. Each vote is recorded as a transaction on the blockchain, giving them the ability to provide a tamper-proof and transparent platform for conducting voting. The rules and logic of the voting process can be defined usingsmart contracts, ensuring that the results are accurate and fair. Additionally, by enabling remote and secure voting and lowering the possibility of fraud and manipulation,blockchain-based voting systems can boost voter engagement. In conclusion, both

Ethereum and Algorand can be utilized to create a high-performance voting system based on a blockchain, with each platform having certain benefits and capacities. Both the unique needs and goals of the voting system and the technological know-how and resources available for development and deployment will ultimately determine which of the two platformsis best.

Libraries Used

The right blockchain framework to run our project is one of the most basic and important things to think about.

Libraries Used for Smart ContractsHardhat

Hardhat is a specific environment for development where Ethereum software can be built. It is made up of different parts that work together to make a full development environment for editing, compiling, debugging, and deploying smart contracts and dApps. Hardhat Runner is the main part of Hardhat that we interact with. It is a flexible and extensible task runner that helps us manage and automate the repetitive tasks that come with building smart contracts and decentralized applications (dApps).

The main ideas behind Hardhat Runner are tasks and plugins. When we use the command line to run Hardhat, we are running a task. For example, the built-in compile task is run when we type npx hardhat compile. Tasks can call other tasks, which makes it possible to set up complex workflows. Existing tasks can be changed by users or plugins, which makes thoseworkflows flexible and easy to add to.

Hardhat is used in our project by setting it up locally. So, our environment will be easy to copy, and we won't have to deal with version conflicts in the future.

To install it, let’s go to an empty folder, run npminit, and follow the instructions. We could haveused a different package manager, like yarn, butwe thought it is better to use npm 7 or later because it makes it easier to install Hardhatplugins.

DOI: 10.48175/IJARSCT-13850

VIII. COMPARISON OF PROPOSED ANDEXISTING SYSTEM

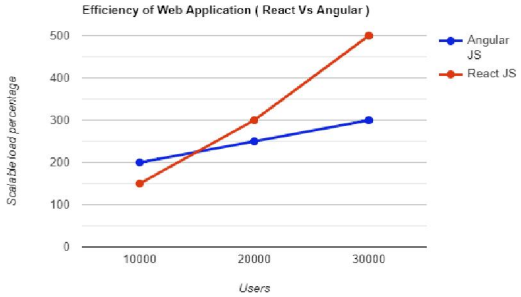
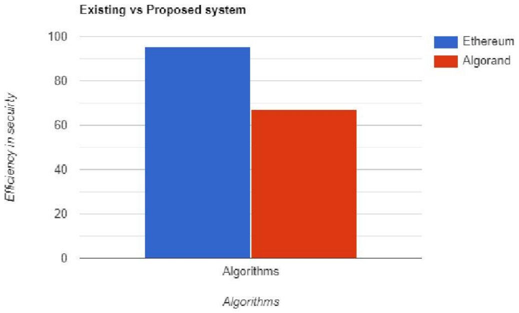


Fig 1.3 COMPARISON OF REACT ANDANGULAR JS

In the above figure, it can be understood that React Js is better in frontend because of itsdynamic reusable components and itscompatibility of creating dynamic web applications easier



.

Fig 1.4 COMPARISON OF ETHEREUM AND ALGORAND

The above figure shows the efficiency of a blockchain application when an Ethereum algorithm is used. The main advantage of using Ethereum is it ensures that the decentralisedapplications and smart contracts built on its blockchain function as intended, without thepossibility of fraud, interruption, or external meddling.

IX. RESULTS

Users can see the results of the vote once the voting period has ended. As soon as a vote is cast, it is stored in the blockchain as an introductory block and in the database's backend data tables. The system guarantees simply the "one person, one vote" (democracy) feature of electronic voting systems. It was determinedafter testing that the transaction hash representing the vote transfer was produced at the time the asset was sent to the address Therefore, the E-voting system should beimplemented initially in limited pilot areas before venturing into large-scale capacity. Boththe internet and voting machines continue to have severe security problems. Significantsecurity improvements will be needed for onlinevoting to be reliable and safe. Theseshortcomings prohibited the blockchain system from fully addressing all of the issues with the voting method, despite it seeming to be theperfect answer. This study showed that there arestill many technical issues with blockchain systems as well as challenges that needed to be solved. Recognizing that blockchain technologyis still in its infancy as an electronic voting alternative is crucial.

X. CONCLUSION

The implementation accustomed blockchain as a network-based E-voting system. This system will habituate blockchain as an integrated system as well as a database to accumulate and hoard voters' data or accreditation which is going to harness for their authentication. The system will be using candidates' or voters' details for the voting process. Smart contracts will be accounted as responsible for managing voting procedures and results. Our system boosts the efficacy of the authentication and of the conferring of a candidate's vote. Blockchaintechnology encrypts the vote, preventing every vote from being tampered with. A voter can onlychoose a candidate once, thanks to this rule. Thetechnology obtains election results rapidly, cutting down on labour expenses and counting mistakes.

DOI: 10.48175/IJARSCT-13850

REFERENCES

[1] The first decentralised digital currency, "A Peer-to-Peer Electronic Currency System," was introduced by Nakamoto Satoshi on March 20, 2014. He also invented bitcoin and the firstblockchain.

[2] Andrew Lippman, Azaria, Asaph, Ariel Ekblaw, and Thiago Vieira. Utilizing Blockchain for Medical Data Access and Permission Management is described in "MedRec." pp. 25–30 in Open and Big Data (OBD), International Conference on. IEEE, 2016.

[3] Computer Networks: The InternationalJournal of Computer and Telecommunications Networking, December 2017, Yaqoob, E. Ahmed, I. A. T. Hashem, A. I. A. Ahmed, A. Gani, and M. Imran.

[4] "A Peer-to-Peer Electronic Currency System," initially published on March 20, 2014, by Nakamoto Satoshi, inventor of bitcoin, first blockchain implementer, and first decentraliseddigital currency.

[5] Nicole J. Goodman and Jon H. Pammett, "Online Voting in a Municipal Election in Canada," Studies in Public Choice 31, edited byBernard Grofman, Alex Trechsel, and Mark Franklin, Springer Verlag, 2014.

[6] conference organised by Rafer Cooley, Shaya Wolf, and Mike Borowczak: 2018 IEEE International Smart Cities Conference (ISC2)

[7] Blockchain applications and future prospects in the financial sector, by Guo, Ye, and Chen Liang. (2017) Financial Innovation 2, no. 1: 24.

[8] E-voting adoption in various nations: A literature study, by Ikhsan Darmawan, first published on October 12, 2021

[9] Using Hyperledger Sawtooth, R.S. Yashank's E-Voting System, Communication & Materials (ICACCM), 2020 International Conference on

[10] 2020 Second International Conference on Innovative Research in Computing Applications, "E-Voting Systems UsingBlockchain: An Exploratory Literature Review"(ICIRCA)

[11] The author of "Electronic Voting Machines" is Nanula Shejvali. No. 1 from the Institute for Public Policy Research (IPPR) (2013).

[12] The effects of voting systems on voter participation: Ohio's punch card voting systems (machines, election administration, overvoting, equipment, ballot form) by Jeannete Lyn Fraser. dissertation for a doctorate. University of Ohio,2018.

[13] "E-Voting system in a smart phone utilisinga mobile app," Navin The 2020 sixth edition of the international conference on advanced computing and communication systems (ICACCS)

[14] Klaponin, Yurii 2020 IEEE International Conference on Issues of Information Communications: The Novel Idea of Assuranceof Confidence in the E-Voting System. Technology and Science (PIC S&T)

DOI: 10.48175/IJARSCT-13850