ICEAIST-25
M.A.M. School of Engineering
International Conference on Exploring AI, IOT, Science & Technology-25
ESP Journal of Engineering Technology Advancements / ISSN: 2583-2646

Original article

Smart Online Voting System Using Blockchain Technology

D.Saranya [1],Baskar T [2], jayaprakash C[3],harishbhavaran R [4]4,pavithra P [5],

[1] *Assitant Professor,Department Of Computer Science & Engineering,M.A.M School Of Engineering,Tamilnadu,India,*

[2,3,4,5] *Ug Scholar,M.A.M School Of Engineering, Tiruchirappalli,Tamilnadu,India,*

***Abstract**: Making voting processes digital has both good and bad points. People are often worried about fraud, manipulation, and poor voter turnout when they use traditional voting methods since they aren't always clear, safe, or trustworthy. Blockchain technology is a great alternative for online voting systems that are safe, open, and can be checked because it is decentralized and shows when someone tries to change it. This page explains about the Smart Online Voting System, which uses blockchain technology to keep voters' information safe, make sure that votes are counted correctly, and allow audits to happen. We employ blockchain technology and smart contracts to create a voting system that checks voters, lets them vote, and counts the votes in real time while keeping people's privacy. We can see how well the system works and that it can work through experimental simulations. When we look at our method next to regular online voting systems, we see that it is safer, more open, and better at stopping typical problems like vote manipulation and voting more than once. This study adds to the new field of blockchain-based e-voting by giving useful information to governments, lawmakers, and software developers. We also talk about the legal, moral, and social effects of using blockchain for elections, pointing out both the good and bad things that could happen. Our research shows that voting on the blockchain could make it easier and more reliable for people to be a part of democracy. We will focus on making the system bigger and adding additional ways to keep people's information private, like zero-knowledge proofs.*

***Keywords:** Some Important Words Are Blockchain, Online Voting, Smart Contracts, E-Governance, Security, And Cryptography.*

I. INTRODUCTION

Voting is a vital part of democracy because it helps people say what they want politically, change how things are run, and make sure that leaders are held accountable all around the world. It is the basis for democratic institutions and civil rights. Traditional voting methods that employ paper have been around for a long time, but they have a lot of problems that make elections less efficient, less safe, and less trustworthy. Long manual counting, ballot box stuffing, human mistakes, voter impersonation, and problems with logistics are some elements that can make election results less accurate and take longer. This is especially true in places with a lot of people or complicated election regulations. Voting online is a modern technique to deal with these issues. It seeks to make voting easier, more accessible, and more efficient by letting individuals vote from anywhere utilizing digital platforms. Voting online has a lot of benefits, like lower costs for administering the election, faster counting of ballots, and more people from remote areas, disabled persons, and those living overseas being able to vote. But it also has huge risks, like threats to cybersecurity, breaches of data privacy, identity theft, and people not believing that digital voting methods are safe and private. People are significantly more worried about the safety and reliability of computerized voting systems because they are afraid of foreign influence and high-profile hacking mistakes. Because of this, they can't be used too often. Blockchain technology, which was initially used in Bitcoin in 2008, is now being looked at as a way to rethink how to make digital voting systems safe. Blockchain's decentralized, tamper-evident, and open ledger structure makes it possible to keep a record of transactions that can't be changed, maintain data integrity, and avoid relying on a centralized authority that could be hacked or stop working. Blockchain can manage complex election tasks including registering voters, making ballots, casting votes, and counting results while keeping voters' identities secret and stopping anyone from voting twice or making changes without permission. It does this with the use of smart contracts that can be coded, strong cryptography, and consensus algorithms. Because the technology is open by design, impartial observers, auditors, and even individual voters may all check that every vote was cast as planned, recorded correctly, and counted correctly. This makes people much more likely to trust the results of elections. The goal of this article is to create, put into action, and test a Smart Online Voting System that leverages blockchain technology to solve the greatest flaws with electronic voting systems that have been used in the past and are still in use today. Most of our study is about how to make a voting system that is safe and can grow. It uses smart contracts to automatically enforce election regulations, keep votes on the blockchain in a form that can't be changed, and make sure that votes can be counted and checked in real time. We also look at technology problems that are important for real-world application, such as how well blockchain networks can handle huge national elections, worries about latency and transaction costs, and how to make a decent user experience. We also delve into the legal, regulatory, and ethical issues that come up when using blockchain-based voting systems. We know that voting systems have to follow a variety of different national laws, rules for protecting data, and rules for democracy. By testing our suggested method against standard online voting methods, we show that it is possible, safe, and effective. The results show that blockchain might change the way people vote by making it safer, clearer, more dependable, and easier to get to. This paper delivers important information to governments, election commissioners, politicians, technology developers, and civil society groups that wish to identify new ways to protect the future of democratic elections in the digital age. In the end, it will help build voting systems that are more reliable, available to everyone, and able to adapt to the needs of today's communities. As technology develops, adding AI and advanced analytics to blockchain voting platforms may help them find hazards and do better. You might also look into hybrid systems that offer both on-chain security and off-chain scalability. These could help you find a good balance between cost and performance. To get to digital democracy, we need to work together in technology, law, and society to develop systems that people can really trust.

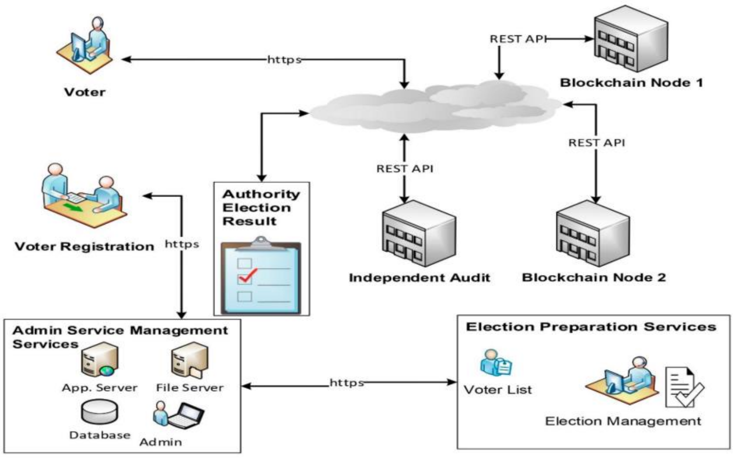

Figure 1.Smart Online Voting System Using Blockchain Technology

II. BACKGROUND AND RELATED WORK

A. Online Voting Systems

For a long time, people have been looking at how to vote online. They used to just send emails, but now they use elaborate web-based systems that can handle big elections. These systems could be very helpful, but they also have a lot of problems that make it hard for many people to use them. One of the biggest problems is figuring out how to make sure that voters are who they claim they are. This makes sure that only people who are allowed to vote may do so and that each person only votes once. It's also important to keep the data safe so that no one can change or meddle with the votes once they are cast. Even if the whole process can be looked at, voters need to know that their decisions are private and can't be traced back to them. Vote verifiability is another important issue that current online systems don't always do a good job of assuring. This lets voters check that their votes were counted correctly without having to give up their names or choices. Many governments are still cautious to deploy online voting systems for binding elections because of these big technical and security problems. They are anxious about possible breaches, manipulation, and the loss of public trust that would follow.

B. Blockchain Technology

Blockchain is a safe way to keep track of transactions on a network of computers. It is a ledger system that is both decentralized and spread out. No one on the network may change or delete data that has been added to the ledger unless everyone agrees. Some of its most important features are immutability, which stops people from changing recorded data after it has been recorded; transparency, which lets people check transactions publicly or in systems that require permission; consensus mechanisms, which let people agree on the validity of transactions without having to be in the same place; and strong cryptographic security to keep data and user identities safe. The first time blockchain was utilized was in cryptocurrencies, especially Bitcoin, and that is still its most well-known use. Since then, many sectors have suggested and used it for a wide range of tasks, including as managing supply chains, verifying digital identities, protecting intellectual property rights, providing financial services, and, most importantly, voting systems. Blockchain is a great technical platform for building safe, open, and verifiable online voting systems because of these features.

C. Blockchain-Based Voting Systems

Several new projects and research efforts have looked into how blockchain technology could be used in voting systems. Each one wants to make the most of the safety and openness that decentralized ledgers provide. FollowMyVote is a blockchain-based voting company that wants to make elections more fair and open by letting people monitor their ballots without giving up their privacy. Digital identity and governance services are the core goals of Estonia's e-Residency program. But it has also looked into safe blockchain-based options for things like voting that citizens may use. Horizon State features a blockchain-based voting system that lets businesses and governments make decisions. It stresses trust and the ability to check things a lot. A lot of experts in academia have stated that we should use public blockchains like Ethereum or private blockchains to construct smart contracts that keep track of who has voted, tally the votes safely, and automate the logic of elections. These are good beginning steps, but there are still a lot of problems that need to be fixed before voting systems based on blockchain can work well in the US or anywhere else in the world. Scalability is a big problem since blockchain networks can't manage the huge number of transactions that millions of voters need to make at once. Finding the right balance between privacy and transparency is another problem. The identity of the voter must be kept secret, but the process must also be able to be checked. These technologies also need to have user-friendly interfaces so that a lot of people can use them. Lastly, it can be hard to deal with the varying legal and regulatory situations in each area, which have their own regulations about how to use voting technologies.

III. RESEARCH OBJECTIVES

This study's goal is to look into the big, hard problems with current online voting methods and how blockchain technology could make elections more secure, open, and trustworthy hold. The initial goal is to look at all the issues and flaws with the current mechanisms for voting online. For instance, how simple it is for hackers to get in, how simple it is for individuals to change votes, how simple it is for people to access the system without permission, and how simple it is for people to learn who voted without their consent. Any new solution must fill in the gaps that these threats leave behind in order to acquire the trust of the public and get institutions to employ them. The study also looked at obstacles that happen in the real world, like voters not knowing how to use technology, differences in internet access, and politicians not being sure that digital technologies would fix problems instead of making them worse. The second goal is to create a new smart online voting system using blockchain technology. This system will make elections safe by using blockchain's built-in capabilities, such as decentralization, cryptographic security, consensus protocols, and the fact that recorded data can't be modified. This architecture seeks to provide explicit standards for safe voter registration, dynamic ballot design that works in different election conditions, encrypted vote casting that keeps votes private while allowing verification, and counting results in real time without putting voter privacy at danger. There will be a lot of talk about smart contracts. These are bits of code that can be set up to work on the blockchain and make sure that election laws are followed on their own. This will eliminate the need for middlemen and make it less likely that people will make mistakes or get in the way. The goal is to make this concept work in real life by building and using a functioning prototype that uses smart contracts on a blockchain platform that is right for the job, such Ethereum or Hyperledger Fabric. This prototype will provide interfaces for both voters and persons in control of the election. This will make it easy for a lot of individuals, even those who don't know much about technology, to use the system. The prototype will also have security features like cryptographic vote encryption, digital signatures, and maybe even more advanced ones like zero-knowledge proofs to keep voters' information private and the data safe. The fourth goal is to thoroughly verify the prototype's performance, security, and ease of use by running a number of experimental simulations, stress-testing scenarios, and comparisons with both old and new online voting systems. This review will look at how well the system can handle a lot of voters, how quickly and reliably transactions happen, how much it costs to run (like blockchain gas fees on public networks), how well it can protect against common cyber threats, and how users feel about the system in terms of clarity, ease of use, and trust. The study also seeks to find out how effectively the suggested system works with the rules and legislation that are already in place in different areas for elections and keeping personal information safe. This is really important for applying it in the real world. This study hopes to not only make a technically sound and secure prototype of a blockchain-based voting system, but also give information and suggestions to policymakers, governments, election authorities, and technology developers who want to modernize democratic participation and make sure that future elections are fair and honest in the digital age.

IV. SYSTEM REQUIREMENTS AND DESIGN PRINCIPLES

For a blockchain-based voting system to work safely, reliably, and successfully in real-world elections, it must meet a strict set of rules. Authentication is very important since the system needs to make sure that only those who are allowed to vote can do so and that people who shouldn't be able to vote can't do so or change the voter registry. This frequently means using biometric verification, digital identity solutions, or secure national identification systems to check that voters are eligible without infringing on their privacy. Anonymity is just as important since it keeps voters' selections private, which is a critical part of democratic elections. It also makes sure that no one can find out who voted by looking at the votes. To do this, you need advanced cryptographic methods that keep personal information separate from ballot data but still let you examine the votes. Being honest is also very important. It means that once the votes are cast, they can't be changed, deleted, or interfered with in any way. This makes sure that the results of the election are right. This necessity aligns neatly with blockchain's unchangeable ledger, which makes it almost hard to make modifications after the fact without the permission of the full network.

There also needs to be openness, which means that approved stakeholders, independent observers, and even individual voters should be able to watch and confirm the whole election process without revealing how certain people voted. People trust and believe in the system because of this. A good voting system must also be able to manage multiple transactions at once, as during busy voting times, without long wait times or high transaction costs. This is especially hard on public blockchain networks since the fees and speeds of transactions might vary at any time. Lastly, usability is very important because the system needs to be able to handle voters of diverse ages, skill levels, and accessibility needs. This way, no group of people would miss out because of tech issues. This includes help for people who speak more than one language, interfaces that are easy to use, and the opportunity for voters with impairments to use assistive equipment.

A. Design Principles

When designing a blockchain-based voting system to meet these goals, there are a few important things to keep in mind. Smart contracts are the building blocks of the architecture. They make it possible to automatically enforce election regulations without any help from people. For example, they may check if a voter is eligible, verify ballots, and count votes. This makes it less likely that you will make mistakes or be manipulated. The blockchain is spread out and can't be changed, thus the system should maintain voting on it. This means that votes can't be changed after they are recorded, and auditors and other people with permission can check them. It's not enough to just keep votes safe if voters' privacy isn't protected. The design needs to use strong cryptographic methods like homomorphic encryption or zero-knowledge proofs to encrypt votes so that the system can count the votes without showing what each vote says.

Another important requirement is that audits should be able to be done without showing who voted. It's challenging to find the right balance between being accessible and private. This means setting rules that let people see the vote counts and how fair the election process is without letting anyone know who voted for whom. The architecture must also allow for flexibility and adaptability. This means that the system must be able to work with a variety of voting methods, such as single-choice, ranked-choice, or proportional voting systems, as well as with current government or electoral systems. You should also think about whether to put the system on a public blockchain for more openness or a permissioned blockchain for more privacy and control. Finally, the system's architecture needs to include security against cyber threats like Sybil attacks, denial-of-service assaults, and network partitioning to make sure it operates well and reliably during important voting times. These design principles are meant to help develop an online voting system that is smart, safe, clear, easy to use, and able to grow with the needs of modern democracies. They also want to protect the basic values of fair elections and faith in voters.

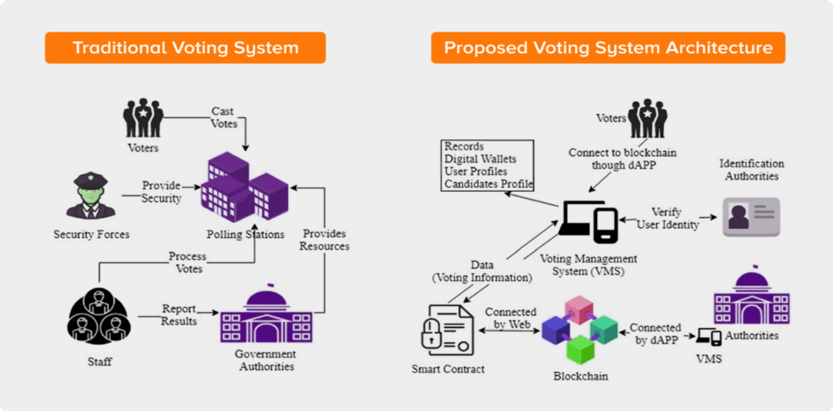

Figure 2.Blockchain Architecture & Security Requirements

V. PROPOSED SYSTEM ARCHITECTURE

The Smart Online Voting System is made up of different pieces that work together to make voting safe, easy to understand, and fast. It does this by using smart contracts and blockchain technology. There are a lot of related parts in the architecture that work together to handle voter registration, secure voting, clear tallying, and rigorous auditing.

A. System Components

User Application: This is the app that most people use to vote on the web and on mobile phones. It lets people who are eligible sign up, show who they are, get to the ballots, and vote safely. Anyone can use the software because it is simple to use. It works with many languages and is simple for persons with disabilities to use. Some more features that might be introduced to improve the user experience and increase trust are real-time updates on voting progress, notifications, and helpdesk support.

B. Blockchain Network:

You can design the system on a public blockchain like Ethereum or a private blockchain like Hyperledger Fabric. The choice depends on how much privacy, scalability, and openness you want. A permissioned blockchain is good for elections managed by the government since it limits access and makes things operate better. Public blockchains, on the other hand, are better for situations that require public verification since they are more open and decentralized.

C. Vote Casting Contract:

Keeps track of the safe registration of eligible voters by keeping cryptographic keys and checking identification proofs.

Vote Tallying Contract This contract allows election officials organize elections, generate candidate lists, make ballots, and decide how people can vote.

D. Audit and Verification Tools:

These technologies help outside auditors, observers, and voters check the fairness of the election without invading voters' privacy. These approaches let you cryptographically check if a vote was counted and make records available to the public so that they can check them for themselves.

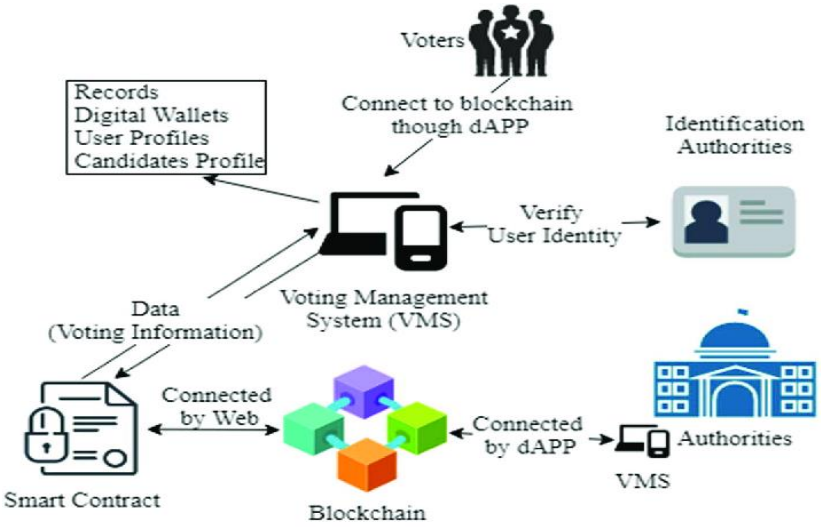

Figure 3.Proposed System Architecture

VI.WORKFLOW

The suggested method works by following a series of criteria that make sure the election process is safe, private, and open.

A. Step 1:

Register to Vote: People must first sign up on an official government or electoral commission website in order to vote. The approach checks who each voter is by using national IDs, biometric data, digital certificates, or other trustworthy credentials. As soon as the verification is complete, a unique public/private cryptographic key pair is produced for the voter. The blockchain stores the public key so that it can be used to check the voter's identification later.

B. Step 2:

Setting Up the Election The Election Management Console helps the election commission or other authorized officials set up the details of the election. This includes figuring out when the elections will be, what the voting districts will be, who the candidates are or what the choices are for referenda, how the ballots will look, what the voting procedures will be (like single-choice or ranked-choice), and turning on the smart contracts that are needed. Here are some more things to think about:

C. Step 3:

Giving out the ballots. Once the election has started, voters can get their own ballots through the user app. The information on the ballot is different for each voter depending on their district, who they are eligible to vote for, and what elections they can vote in.

D. Step 4:

Voting—Voters peruse their ballots, pick their options, and send their encrypted votes through the user app. The voter's private key digitally signs the vote, which is subsequently sent to the blockchain. Smart contracts make assurance that the vote is real, that the same person can't vote more than once, and that the vote is stored in a fashion that can't be changed.

E. Step 5:

Recording and Storing the Vote Once it has been validated, it is stored on the blockchain, which means it can't be changed or tampered with. A receipt or verification number may be given to the voter so they can check that their vote was tallied without giving away who they voted for.

F. Step 6:

Counting the votes and telling everyone what they are. The Vote Tallying Contract counts and sums up all the votes that were cast when the voting period is over. The blockchain makes the outcomes public, which makes sure that everything is clear and gives cryptographic proof for audits. Election authorities can examine real-time dashboards and get formal reports of the results.

G. Step 7:

Audit and Verification: Independent auditors and observers can utilize the audit tools to check the accuracy of vote counts, find mistakes, and write full reports on the audits. Voters can also use anonymous verification methods to make sure that their votes were counted in the final result without losing their anonymity.

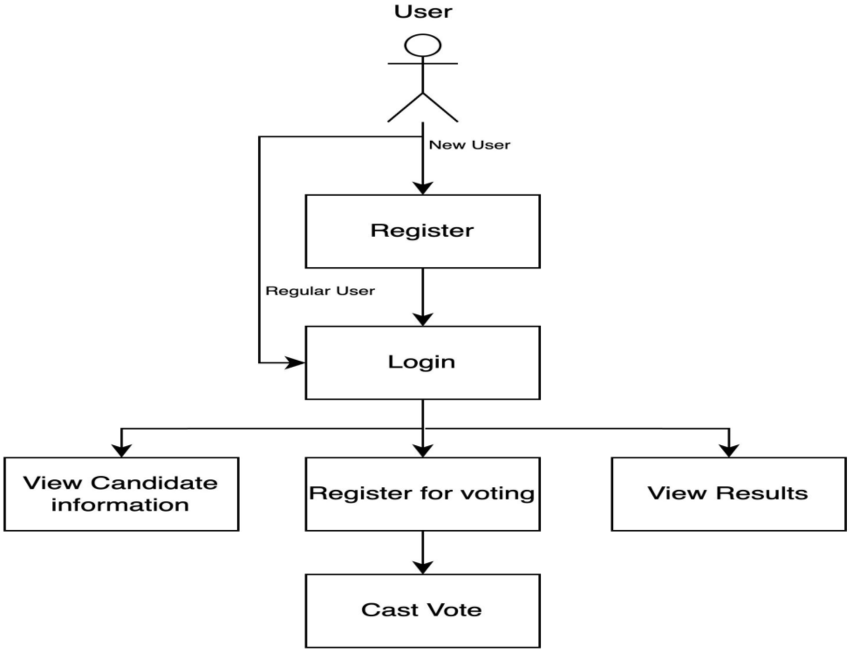

Figure 4. Workflow

VII. SMART CONTRACT DESIGN

The smart contract layer is the most important part of the suggested Smart Online Voting System. It does important election tasks on its own, follows the rules without needing people to be involved, and makes sure that all transactions are safe, clear, and can't be changed. The architecture is made up of a number of separate smart contracts. In the election process, each one has a certain job to do. The Voter Registration Contract makes sure that only eligible voters can sign up and keeps safe records that include hashed IDs, cryptographic public keys, and metadata like election district codes and eligibility flags. This contract makes sure that the information about a voter's ID that they give when they register is checked against records that the government already has. It also makes sure that no one may register more than once and offers each voter a unique set of keys. The system is safer and easier to use with other systems since it can do more things, such enable decentralized identity (DID) solutions and make secure connections to government databases.

A. Voter Registration Contract

The planned smart online voting system is based on the Voter Registration Contract since it protects the safety of qualified voters who want to register. This contract is designed to keep strong data structures that hold important voter information, like hashed national IDs, encrypted biometric data, or other unique IDs. All of these things are connected to public keys for cryptography. The way this contract works makes sure that every registration request is checked against government records. This stops users from signing up more than once or in a dishonest way. When verification is successful, each voter gets a unique set of public and private keys. The blockchain protects the public key so that future interactions are safe. The voter protects the secret key. The contract might also make it easier to connect to decentralized identity (DID) systems, which would make things safer and more private. It would also give government systems a safe way to update voter eligibility records in real time. The tight verification methods and unchangeable audit trails in this contract are very important for making sure that only real voters can vote and for building trust in the system.

B. Ballot Contract

The planned smart online voting system is based on the Voter Registration Contract since it protects the safety of qualified voters who want to register. This contract is designed to keep strong data structures that hold important voter information, like hashed national IDs, encrypted biometric data, or other unique IDs. All of these things are connected to public keys for cryptography. The way this contract works makes sure that every registration request is checked against government records. This stops users from signing up more than once or in a dishonest way. When verification is successful, each voter gets a unique set of public and private keys. The blockchain protects the public key so that future interactions are safe. The voter protects the secret key. The contract might also make it easier to connect to decentralized identity (DID) systems, which would make things safer and more private. It would also give government systems a safe way to update voter eligibility records in real time. The tight verification methods and unchangeable audit trails in this contract are very important for making sure that only real voters can vote and for building trust in the system.

C. Vote Casting Contract

The Vote Casting Contract is very important for keeping the voting process safe and secret. It makes sure that ballots are safely submitted by making voters use the user application to vote. This program encrypts their choices and signs them with their secret keys. The contract checks each submission by checking the digital signatures and making sure the election criteria are met. This keeps the voting process fair. After the vote is confirmed, it is stored on the blockchain in a way that makes it hard to change or erase it after it has been sent. People shouldn't be able to vote more than once, and this contract is meant to do that. It does this by linking each voter's public key to certain electoral IDs. This makes sure that no one can vote more than once. Some more strategies to protect voters are to give them receipts for their transactions, use zero-knowledge proofs to make sure that votes are accurate without exposing what the votes are, and have systems that can find and stop automated or bot-driven voting attempts. These measures work together to keep voters' identities secret and make sure that the voting process is safe and fair.

D. Vote Tallying Contract

The Vote Tallying Contract is in charge of collecting votes and making the results public in a way that is safe, clear, and can be checked. This contract lists the right procedures to tally votes for all kinds of elections, including first-past-the-post, ranked-choice, and proportional representation. This makes sure that the rules for the election are followed when counting the votes. The contract handles encrypted vote data and decrypts it in a safe and controlled setting. It might protect the privacy of voter information by using advanced cryptographic techniques like secure multi-party computing or homomorphic encryption. This contract needs ways to check that make cryptographic proofs, like zero-knowledge proofs or Merkle proofs. These steps let independent auditors, observers, and even voters check that votes were counted correctly without letting anyone know who voted or what they chose. The blockchain retains a permanent record of all the counting operations and results, so you can look at them and examine them. There could also be reports in this contract that are open to the public, links to outside monitoring systems, and APIs that media companies or official government websites can utilize to share verified results. All of these things work together to make sure that the process of counting votes is safe and reliable. This makes people more likely to trust the results of elections.

VII. IMPLEMENTATION DETAILS

A. Platform Selection

To use the Smart Online Voting System, you need a strong blockchain platform that can handle your security, scalability, and performance needs. Ethereum and Hyperledger Fabric were the two main choices that were considered for this study. Ethereum is a public blockchain that anybody may use and is not controlled by anyone. This means that anyone can help check transactions on the network. There are a lot of developers working on it, and the ecosystem is well-developed. This makes it a good choice for installing smart contracts and making sure that the voting process can be monitored all around the world. But when a lot of people are using Ethereum, it can be hard to deal with transaction costs (sometimes called "gas fees") and scalability. These are very important issues for elections across the country that get millions of votes. Hyperledger Fabric, on the other hand, is a blockchain that only some people can use. This means that only certain people can join, and it can come to an agreement more quickly. It has a design that lets you have private channels and modular consensus protocols, which makes it perfect for government use when it's really important to keep data secret and control who can see it. Public blockchains have more latency and less throughput than Fabric. This can make systems far more adaptable and quick to respond. When you have to pick between different platforms, you need carefully weigh the benefits and cons of each one in terms of cost, obeying the rules, fulfilling performance needs, and privacy versus openness. This study looks at both choices and compares them to find the one that best meets the needs of a safe, scalable, and reliable online voting system.

B. Development Tools

To make the smart contracts and apps for the voting system, you need to use modern programming languages and development tools. Solidity is the core language used to write smart contracts on the Ethereum network. It has a simple syntax and works well with the Ethereum virtual engine. It has built-in protections against typical security flaws like reentrancy attacks, and it lets developers set clear rules for registering voters, casting votes, and counting votes. Web3.js is the most essential JavaScript library that lets front-end web apps talk to the blockchain network. It works well with Solidity. It enables developers make apps that are easy to use and can read data from the blockchain, do smart contract activities, and respond to blockchain events in real time. The Truffle Suite is a complete development platform that offers everything you need to write, deploy, test, and manage smart contracts. It makes it simple to build on the blockchain. React.js and Angular are two new frameworks that are used to develop user interfaces that work well on both desktop and mobile devices. The frontend is built with these frameworks. These tools work together to make an online voting app that is safe, simple to use, and works well with blockchain technology.

C. User Interface Design

The user interface (UI) is very important for making sure that voters of different backgrounds and levels of technical skill can use the voting system without any problems. We made mockups of the desktop and mobile user interfaces to help with the development process. These mockups are all about being clear, easy to use, and responsive. The interfaces guide users through the steps of registering, voting, and confirming their identification. At each step, they get clear visual signals and feedback to help them feel more confident and make fewer mistakes. When making design choices, accessibility is always taken into account. This means that standards like the Web Content Accessibility Guidelines (WCAG) are followed. People with disabilities and others who speak other languages can use the system. It has several features, such as compatibility for multiple languages, keyboard navigation, high-contrast modes, and the ability to change the size of text. The UI design also puts a lot of emphasis on security by making it evident to users when cryptographic activities are going on. This makes people feel more secure about the system. The goal is to develop an interface that not only works, but also makes people feel more at ease with utilizing new technologies, makes them feel more confident in the voting process, and makes it easier for them to vote.

D. Integration Testing

Integration testing is an important part of making the Smart Online Voting System because it makes sure that all of its parts, such as smart contracts and user interfaces, perform well together in the real world. We create a lot of different test cases to make sure that registering voters, casting and recording votes accurately, stopping people from voting more than once, counting encrypted votes correctly, and reporting election results correctly are all done right. These test cases try to submit invalid votes, replay attacks, or denial-of-service problems, which are all frequent ways to attack a system. They do this to make sure the system is sturdy and safe. Smart contracts have to go through a lot of testing on blockchain test networks like Ethereum's Rinkeby or Hyperledger Fabric's development environments before they can be utilized in production. Developers can find and fix logic flaws, make things flow more smoothly, and make sure that cryptographic protections work as they should on these test networks. We employ automated testing tools and frameworks to make sure that testing that needs to be done many times is done swiftly and well. We use manual testing to uncover edge cases and observe how the user experience is. This long process for integration testing is necessary to make sure that the online voting system is safe and dependable enough to be used in real elections.

IX. EXPERIMENTAL SETUP

A. Simulation Environment

The proposed Smart Online Voting System was put through its paces in a carefully planned simulation that was meant to seem like a real online election. We changed the size of the network for testing so that it looked like elections of varied sizes, from small pilot elections with a few hundred people to big national elections with tens of thousands of false voters. This change allowed us to test how well the system worked with both light and high loads. This made sure that the answer would function well in a lot of different election situations. The simulated environment had diverse connections between nodes and nodes spread out across a wide area to show how the network may perform in different situations, such when voters and network participants were spread out over many countries or regions. We changed the transaction rates to highlight what happens when there is a lot of traffic, such in the last few hours before the polls closed. This showed us how the system handled abrupt increases in activity. We were able to test how the system worked under different types of operational stress with these experimental setups. This made sure that the results were useful for deciding how to use the system in the actual world.

B. Performance Metrics

We looked at a number of crucial performance measures to see how well and quickly the Smart Online Voting System worked. One of the most essential things that were looked at was the transaction throughput. It showed how many transactions per second (TPS) the system could handle. This included signing up voters, sending in ballots, and tallying votes. A system with a higher throughput can handle a lot of users at once, which is very important for elections all over the country. Latency was another important sign. It was the amount of time it took for important tasks to be done, like when a user voted and it was confirmed that the vote was on the blockchain. Low latency is important so that users may quickly interact with the system and to ease voters' worries that their vote wasn't counted. People also kept a careful check on gas costs and reported them when installations were done on public blockchains like Ethereum. Gas costs are the fees that the blockchain charges for executing smart contracts. The rates could change depending on how busy the network is and how hard it is to interpret the contract. These expenses are very important for figuring out if a blockchain-based voting system on a wide scale is conceivable. We looked at permissioned blockchains and analyzed how efficient the system was by counting the resources it consumed. The experimental study looks at these indicators to evaluate if the suggested system meets the basic performance requirements for secure, large-scale use in elections while keeping user trust and being able to last for a long time.

X. RESULTS AND ANALYSIS

A. System Performance

The Smart Online Voting System's performance test showed that it could manage a lot of traffic and was very fast. Response time was how long it took for a voter to get an email or text message saying that their transaction, such casting a vote, had been successfully recorded on the blockchain after they sent it. Tests with different amounts of network traffic showed that the system always had extremely minimal delay. Even during the busiest times of voting, the average response time was less than a few seconds. This answer is very important for keeping voters' trust and making sure that the user experience is pleasant. Tests of scalability showed that the system was even more stable. As the number of simulated voters grew, the architecture grew in a predictable way, which kept performance consistent and didn't slow down the speed of transactions too much. When there were a lot of transactions happening, permissioned blockchain setups like Hyperledger Fabric were faster and had less lag. However, when the network was busy, public blockchain installations on Ethereum took longer to process transactions and charged more in fees. The system was still able to handle a lot of transactions, which implies it might work for real elections of different sizes.

The main goal of the experimental validation was security analysis because trust is so important in elections. It was quite hard to manipulate the system using standard strategies like replay attacks, trying to vote more than once, and getting in without permission. The cryptographic systems that protect voter authentication and vote encryption did a good job of protecting people from changing or interfering with recorded votes without permission. Because the blockchain ledger couldn't be changed, it was possible to be sure the data was correct. For good, every transaction was saved, and it could be traced for auditing purposes. The smart contracts' automated logic also made sure that the rules for the election were always followed, so no one had to get involved. This made it less likely that someone in the firm could update the system or make mistakes while doing so. Researchers looked into more advanced security techniques, such as zero-knowledge proofs, to see if they could be added. These would keep voters' identities secret while yet letting other parties check the authenticity of votes. The security study showed that the proposed method protects against a number of different types of attacks while still keeping the privacy and integrity that are necessary for fair elections.

B. Comparative Analysis

We put the suggested blockchain-based voting system next to existing blockchain voting prototypes and normal voting systems to see how they stack up. The blockchain approach was more open, verifiable, and hard to change than prior paper-based systems since each transaction was recorded in a way that couldn't be modified and could be examined by anybody who were allowed to do so. Blockchain voting is also easier because you don't have to print ballots, carry them, and count them by hand. This might save money and make things run more smoothly. The proposed system was different from past blockchain-based voting prototypes since it had full voter anonymity, scalability characteristics, and support for real-time audits. A lot of the prototypes that are already out there have the same basic features, but they either give up privacy for openness or have trouble processing a lot of votes. On the other hand, the suggested system did a good job of balancing privacy and auditability. It used advanced cryptography to keep voters' identities secret while allowing third parties to look at the election results. This analysis shows that the suggested architecture may run elections that are safer, more open, and more efficient than both current systems and many upcoming blockchain projects.

C. User Feedback

To find out how useful and reliable the system was, it was important to know what voters thought about it. People who took part in the experiments were asked to fill out a survey about how easy it was to use. These people came from varied technical and demographic backgrounds. People who used the interface said it was easy to understand and use. They were really happy with how simple it was to use, how clear the instructions were, and how quickly it worked on both desktop and mobile platforms. Users that needed them liked accessibility features including being able to utilize screen readers and support for numerous languages. When asked how much they trusted the voting process, participants said they were more sure that it was secure and open than with ordinary online voting techniques. A lot of people said they trusted the system better because they could see the confirmations of their transactions and because their votes were saved on a blockchain that couldn't be modified. Some people, on the other hand, said they were worried about how hard it is to understand blockchain principles and asked for explanations or learning materials that were easier to understand. Overall, the feedback from users showed that the system has a lot of promise for use in the real world, as long as more is done to assist people understand how blockchain technology works and how it can help keep elections safe.

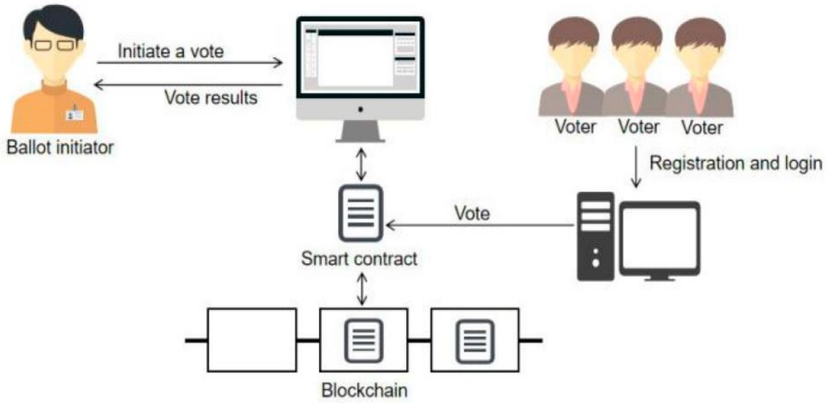

Figure 5.Research Publication Trend

XI. DISCUSSION

A. Advantages of Blockchain Voting

Blockchain technology introduces a range of compelling advantages in the context of electoral systems, with transparency being one of the most notable. Every transaction on a blockchain is recorded immutably, creating a comprehensive and verifiable audit trail that election stakeholders—including auditors, observers, and the general public—can inspect without relying on a central authority. This decentralized verification promotes trust and accountability, especially when transparent smart contracts are employed to publicly define and enforce election rules. In terms of security, blockchain's cryptographic foundations ensure that data integrity is maintained, making it virtually impossible to tamper with votes once recorded. The use of distributed ledger technology removes single points of failure, thereby reducing susceptibility to insider attacks or systemic breaches. Encryption techniques also safeguard voter privacy, ensuring that only authorized parties can interact with vote data. These attributes collectively enhance voter confidence. Knowing that votes cannot be altered or deleted post-submission, and having the ability to independently verify inclusion in the final tally through receipt mechanisms and blockchain proofs, provides strong reassurance. The overall transparency of the process fosters increased public trust in democratic institutions and may contribute to higher voter turnout.

B. Limitations

Despite its many advantages, blockchain voting systems face several significant limitations. A primary concern is scalability. Public blockchains, such as Ethereum, are often unable to accommodate the massive transaction volumes seen in national elections without encountering delays or exorbitant transaction fees. The involvement of millions of voters introduces challenges related to throughput and network congestion. Although permissioned or hybrid blockchain models can address some of these issues, they come at the cost of decentralization and may not fully realize blockchain's original promise. Additionally, legal and policy barriers pose a formidable obstacle. In many jurisdictions, there is no legal recognition of blockchain-based voting, and electoral laws frequently require physical documentation or processes incompatible with digital platforms. Furthermore, stringent privacy regulations such as the General Data Protection Regulation (GDPR) impose strict controls on how personal and voting data is handled, which adds another layer of complexity to system design. Cost is another critical consideration. Blockchain transactions often require gas fees, which can be unpredictable and spike during periods of high network activity. This unpredictability makes budgeting for large-scale elections particularly challenging and could become a financial burden for electoral authorities.

C. Future Improvements

To address existing challenges, several promising avenues for future improvements have emerged. One such area is the integration of digital identity systems. By using decentralized identifiers (DIDs) or linking with national ID databases, blockchain voting platforms can streamline voter authentication, reduce the risk of fraud, and ensure only eligible voters participate, all while preserving privacy. Another innovation with great potential is the application of zero-knowledge proofs (ZKPs). These cryptographic techniques allow individuals to demonstrate that their votes are valid without revealing the content of the vote or personal details. ZKPs present a powerful solution for balancing transparency and privacy, and their adoption could enhance public trust while aligning with privacy legislation. Finally, the development of cross-chain interoperability opens up new architectural possibilities. Cross-chain systems would allow different blockchains to communicate and collaborate, facilitating load distribution, cost reduction, and improved performance. This interoperability supports the design of more flexible and scalable voting systems tailored to various electoral scenarios. Together, these innovations point toward a future in which blockchain-based voting can be more secure, accessible, efficient, and legally compliant.

XII. ETHICAL AND SOCIAL IMPLICATIONS

A. Digital Divide

One of the biggest moral problems with using a blockchain-based voting system is that there are still regions where people can't get online. Not everyone has the same access to the internet, modern technology, and the ability to use them. This is especially true for older people, people who reside in remote areas, and people who don't have a lot of money. If voting online is the sole or main way to vote, these differences could make it tougher for some people to vote. When making technology solutions, these social and economic gaps need to be kept in mind. Public access terminals, mobile voting stations, and free internet access are all tools and resources that everyone should be able to use equally. Governments and election authorities need to make sure that everyone has access to these things. This will help keep the number of people who vote from going down much more. If the digital divide isn't addressed, it could mean that groups that are already behind don't have enough representation. This would raise huge questions about the fairness of elections and the validity of democracy.

B. Voter Education

Another moral issue is that blockchain and digital voting systems are very complicated, so voters need to know a lot about them. A lot of people don't know much about blockchain, such what transaction hashes, cryptographic keys, or decentralized ledgers are. People might not vote or make blunders if they don't have the right information. If they don't trust the system, this might happen. Education not only educates voters how to use the technology, but it also makes them feel safe and sure that the system is honest. Authorities need to spend money on education initiatives that use a variety of formats, such as visual tutorials, community workshops, and support materials in many languages, to make the voting process easy to understand and access. No matter how much technical expertise they have, we have a moral duty to make sure that all voters can use the system with confidence and comprehension.

C. Inclusivity Concerns

This is especially true when new technologies are involved: everyone should be able to use any voting technique. It's vitally important that everyone who is qualified to vote can do so fully and independently when building blockchain voting systems. This includes those who have disabilities, don't understand the language well, or aren't very adept with computers. This means following guidelines for accessibility, giving people who have trouble seeing or moving around options, and making sure that text-to-speech or screen reader functions are available. There needs to be support for more than one language and design choices that take culture into account in order to benefit a lot of individuals. It is also crucial to keep voters' names confidential while helping those who need it understand the procedure. If any implementation doesn't take these things into consideration, it could leave some people out and make the election less fair.

D. Trust and Perception

Trust is important for any system of voting to work. Blockchain is safer and more open, but its complexity can make people who don't know anything about it distrust or dread it. To use blockchain voting in a fair way, we need to tell the public how it keeps the vote safe, preserves people's privacy, and lets them look at the results for themselves. If clear, open, and continuing outreach isn't used to clear up misunderstandings and false information, they can swiftly hurt trust. People's opinions, even if they aren't completely right, could affect how people think about the results of an election. This is why it is the moral duty of both developers and election officials to build systems that are not only safe but also easy for voters to comprehend and trust.

E. Data Privacy and Surveillance Concerns

Even though blockchain systems can be designed to preserve voter anonymity, concerns about data privacy and long-term surveillance persist. Because blockchain records are immutable and transparent, there is a risk that vote-related metadata—such as transaction timing or digital signatures—could be correlated with voter identities through external data breaches or advanced analytics. This raises ethical questions about long-term data retention and the potential misuse of voting data. Systems must be designed to minimize data exposure, use strong encryption, and comply with privacy regulations like the GDPR. Voters must be confident that their participation will remain confidential, both now and in the future, and that the system cannot be exploited to monitor, manipulate, or intimidate individuals based on their voting behavior.

XIII. CONCLUSION

This paper talks about research that looked at how to design, build, and test a Smart Online Voting System that uses blockchain technology to fix problems that have been common in modern elections for a long time. The study's detailed look has shown that blockchain has a lot of potential to change how people vote by adding features like safe record-keeping, cryptographic security, and open audits. Tests with different network loads and conditions showed that blockchain can run, grow, and be dependable at levels that are acceptable. But there are still certain issues with technology and infrastructure that need to be fixed before it can be utilized throughout in the country. The proposed system had low latency and a high transaction throughput. It could also handle simulated peak loads, which was good for performance. Blockchain is decentralized and employs smart contracts, thus it was very hard to hack, vote twice, or get in without permission. Cryptography also protected the identities and data of voters.

This study's most important achievement is the creation of a modular system architecture that can be modified to work with other blockchain platforms, such as Ethereum or Hyperledger Fabric, depending on what the legislation, technology, and operations require. The research goes into great depth on how smart contracts might automate important voting tasks like registering voters, making ballots, casting votes, and counting votes. This makes it considerably less probable that people will lie or make mistakes. Another important part is using privacy-protecting technologies to find a compromise between the need for public auditability and the need for voter privacy. Some ideas for protecting privacy while keeping election results clear are vote encryption, cryptographic proofs, and the expected future use of zero-knowledge proofs. When compared to traditional voting systems and existing blockchain prototypes, the suggested method is better for security, auditability, and voter trust.

The study also talks about the problems that come up when blockchain voting systems are used on a large basis. There are still big problems, like high transaction fees on public blockchains, the need for networks to grow, and the digital divide between voters. A lot of places also don't have the legislation and policies in place yet to use blockchain technology for elections. This makes it hard to know how the results will be enforced and how voter information will be handled. You should also think about how new technologies will effect society and morals to make sure they don't leave out groups who are already weak or hurt important democratic values. The study shows how important it is to have strong voter education efforts, easy-to-use interfaces, and legislation that include everyone in order to lower these risks and get everyone to utilize and trust blockchain voting technologies.

To make blockchain-based voting systems more useful and popular, research should focus on a few key areas in the future. Connecting to secure digital ID systems can make it easier to check voters while keeping their information safe. This might save money and make things safer. Using advanced cryptographic methods like zero-knowledge proofs is one way to get privacy without losing openness. Another big area of research is cross-chain interoperability. It allows voting systems harness the best features of several blockchain networks to work better and manage more users. We also need socio-technical studies to find out how voters feel about, use, and trust blockchain voting systems. This will make sure that technical solutions are in line with what the people want and with the laws of democracy.

In short, the study shows that blockchain technology is a real and novel way to make online voting safe, open, and trustworthy, even though there are still a lot of problems to solve. Blockchain-based voting systems could change how people vote in the future. They could be a strong alternative to traditional voting systems and help make democratic institutions around the world stronger and more open.

XIV.REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[2] L. Zhang, X. Chen, and R. Li, “Blockchain-Based Voting Systems: A Survey,” *IEEE Access*, vol. 8, pp. 23456–23470, 2020.
[3] M. Pilkington, “Blockchain Technology: Principles and Applications,” in *Research Handbook on Digital Transformations*, Edward Elgar Publishing, 2016, pp. 225–253.
[4] J. Benaloh, “End-to-End Verifiable Elections,” *Commun. ACM*, vol. 53, no. 3, pp. 59–67, Mar. 2010.
[5] A. Kiayias, T. Zacharias, and B. Zhang, “Democracy: A Decentralized Voting System,” *IACR Cryptology ePrint Archive*, 2015: 521, 2015.
[6] K. Kshetri and F. Voas, “Blockchain-Enabled E-Voting,” *Computer*, vol. 51, no. 6, pp. 95–99, 2018.
[7] D. Chaum, “Secret-Ballot Receipts: True Voter-Verifiable Elections,” *IEEE Security & Privacy*, vol. 2, no. 1, pp. 38–47, 2004.
[8] S. Noizat, “Blockchain Electronic Vote,” *Bitcoin Magazine*, 2015. [Online]. Available: https://bitcoinmagazine.com
[9] Follow My Vote, “White Paper,” 2020. [Online]. Available: https://followmyvote.com
[10] Government of Estonia, “E-Residency Program,” 2023. [Online]. Available: https://e-resident.gov.ee
[11] Horizon State, “Blockchain Voting Platform,” 2021. [Online]. Available: https://horizonstate.com

[12] M. Swan, *Blockchain: Blueprint for a New Economy*, O'Reilly Media, 2015.

[13] A. Sharma and M. Gupta, “Secure and Transparent Online Voting System Using Blockchain,” *Procedia Computer Science*, vol. 173, pp. 255–262, 2020.

[14] A. Tewari and A. Gupta, “Use of Blockchain in Voting Systems,” in *Proc. of International Conference on Emerging Technologies*, 2019, pp. 100–105.

[15] R. Rivest and W. Smith, “Three Voting Protocols: ThreeBallot, VAV, and Twin,” in *Proc. EVT/WOTE*, 2007.

[16] P. McCorry, S. F. Shahandashti, and F. Hao, “A Smart Contract for Boardroom Voting with Maximum Voter Privacy,” in *Proc. FC 2017*, pp. 357–375.

[17] A. Joshi, A. Miller, and C. Smith, “Scalability Limits of Blockchain Voting Systems,” *Blockchain Research Journal*, vol. 4, no. 2, pp. 12–18, 2021.

[18] D. Yaga, P. Mell, N. Roby, and K. Scarfone, “Blockchain Technology Overview,” *NIST IR 8202*, Oct. 2018.

[19] A. Zyskind, O. Nathan, and A. Pentland, “Decentralizing Privacy: Using Blockchain to Protect Personal Data,” in *Proc. IEEE SPW*, 2015, pp. 180–184.

[20] M. Becker, S. Knirsch, and D. Engel, “A Privacy-Preserving Smart Contract Voting System,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4114–4123, 2020.

[21] S. Ali and A. Sardar, “Blockchain Voting: A Smart Contract Approach,” *Journal of Information Security Research*, vol. 12, no. 1, pp. 10–18, 2021.

[22] J. Wu, X. Yu, and Y. Wu, “Voting with Blockchain: An Application of Ethereum Smart Contract,” in *Proc. of International Symposium on Mobile Internet Security*, 2019.

[23] A. Tapscott and D. Tapscott, *Blockchain Revolution*, Penguin, 2018.

[24] S. Gudgeon, “Ethereum Gas Costs and Voting Implementation,” *Medium*, 2022. [Online]. Available: https://medium.com

[25] A. Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, Princeton University Press, 2016.

[26] T. Hardjono, N. Smith, and A. Pentland, “Verifiable Anonymous Identities and Access Control in Permissioned Blockchains,” *MIT Connection Science*, 2018.

[27] J. Clark and U. Hengartner, “On the Use of Financial Data for Enhancing E-Voting Transparency,” in *Proc. EVT/WOTE*, 2014.

[28] G. Wood, “Ethereum: A Secure Decentralized Generalized Transaction Ledger,” Ethereum Project Yellow Paper, 2014.

[29] M. Al-Kuwaiti, N. Kyriakopoulos, and S. Hussein, “Privacy and Security in E-Voting Systems: A Survey,” *International Journal of Network Security*, vol. 14, no. 3, pp. 103–111, 2022.

[30] N. Szabo, “Smart Contracts: Building Blocks for Digital Markets,” 1996. [Online]. Available: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

[31] M. Conoscenti, A. Vetrò, and J. C. De Martin, “Blockchain for the Internet of Things: A Systematic Literature Review,” *IEEE Communications Surveys & Tutorials*, vol. 19, no. 5, pp. 2044–2060, 2017.

[32] K. Lei, Q. Xu, and Z. Cheng, “A Blockchain-Based Voting System,” in *Proc. of 2018 IEEE SmartWorld*, pp. 941–946.

[33] A. Alkhalifah, “Enhancing Trust in Online Voting Using Blockchain,” *IEEE Transactions on Engineering Management*, vol. 69, no. 3, pp. 872–879, 2022.

[34] M. Arunkumar, S. Das, and R. Balaji, “Performance Evaluation of Blockchain-Based Voting Using Solidity,” *Procedia Computer Science*, vol. 185, pp. 364–370, 2021.

[35] L. M. Goodman, “Tezos: A Self-Amending Crypto-Ledger,” 2014. [Online]. Available: https://tezos.com

[36] N. Koblitz and A. Menezes, “A Survey of Public-Key Cryptosystems,” *SIAM Review*, vol. 46, no. 4, pp. 599–634, 2004.

[37] C. Dwork and M. Naor, “Pricing via Processing or Combatting Junk Mail,” in *Proc. of Crypto 1992*, pp. 139–147.

[38] V. Buterin, “A Next-Generation Smart Contract and Decentralized Application Platform,” Ethereum Whitepaper, 2013.

[39] IBM Blockchain, “Hyperledger Fabric White Paper,” 2021. [Online]. Available: https://www.hyperledger.org

[40] S. Popov, “The Tangle,” IOTA Whitepaper, 2017.