Banavath Prashanth, 2023, 11:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

An E-Voting System Based on Blockchain Technology

Banavath Prashanth, Medipally Shravya, Asst. Prof. S.Bhavana
Department of Internet of Things,
Sreenidhi Institute of Science and Technology,
Yamnampet, Hyderabad, Telangana

Abstract-Internet voting is becoming more popular because it can save money and make it easier for people to vote. Instead of using paper ballots or going to a polling station, people can vote online from anywhere with an internet connection. However, some people are worried about the risks of online voting. If there is a problem, it could affect a lot of votes. To make online voting safe and reliable, blockchain technology is being used. This technology helps protect votes and make sure they are counted correctly. This article explains how blockchain can be used for online voting and what challenges still need to be solved. Overall, using blockchain for voting could help solve some of the problems we have with elections, but there are still some issues that need to be addressed.

Keywords- electronic voting, privacy,voting, blockchain-based electronic voting,security, blockchain technology, trust.

I. INTRODUCTION

Being honest is very important in countries where people vote for their leaders. It helps people trust and believe in the leaders they choose. Technology can also help make voting easier and more trustworthy. Elections are a way for people to make decisions together, and they are very important. The democratic system is how people choose who will represent them in government and other places of power. People need to have confidence in the election process for it to work well [1, 2].

Different groups of people make rules and decisions for different things, from schools to countries. Voting is the main way for people to show what they want and who they want to represent them [3].

Voting is an important way for people to choose their leaders and have a say in how their country is run. In the past, people would fill out paper ballots to vote, which helped them feel confident in the results. However, some countries don't have fair and equal voting systems [4, 5].Recently; people have started using electronic voting machines to make voting easier and more efficient.

But, there are concerns that these machines could be manipulated and not keep people's votes private. It's important to find a way to make sure voting is fair and transparent, so everyone's voice can be heard.

On the other hand, electronic voting protocols have a person in charge who oversees the whole voting process [6]. This can lead to mistakes because the person in charge may be dishonest. Using a decentralized network, like blockchain technology, can help avoid this problem. Blockchain technology allows for online or electronic voting without relying on one person to control everything. It has features like decentralization and security, making it a good alternative to traditional electronic voting systems [7].

A blockchain is like a chain of blocks that contains information about previous blocks. It was designed to be resistant to changes. Researchers are exploring how blockchain can be used for voting, as it offers benefits like transparency and security. The rest of the paper explains how blockchain technology works, how it can be used for electronic voting, the problems and solutions of developing online voting systems, the security requirements for electronic

voting, and the available blockchain-based electronic voting systems. The paper also discusses the latest research and future trends in this field. In conclusion, blockchain technology has the potential to improve electronic voting systems.

II. BACKGROUND

The blockchain is often associated with digital money and smart contracts, which are like digital promises that are kept using the blockchain. Bitcoin was the first example of this and Ethereum added smart contracts [8]. A smart contract is a computer program that is shared with everyone on the network and is checked by everyone to make sure it is correct. The blockchain is made up of different technologies that work together to keep information safe and secure [9]. It uses math and computer science to protect the information while it is being sent across the internet.

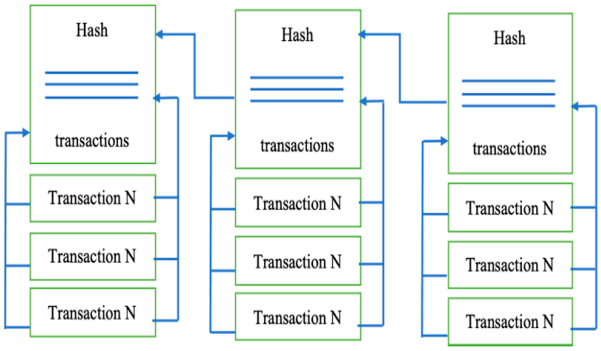

Fig 1.The blockchain structure.

The blockchain is like a special way of organizing information as shown in Figure 1. The information is split into blocks, and each block has a special code that connects it to the block before It [10]. This helps make sure that nobody can change the information without everyone noticing. The first block is extra special and has some important information about how everything works. The blockchain is made to be used by many people, all working together without one big boss. They use a special way of agreeing on things that helps make sure everything is fair and nobody can cheat.

Private Blockchain networks [11][12], have different ways to solve these problems based on how the network is set up. Smart contracts brought new life to blockchain solutions and helped improve many areas. A smart contract is like a rule written in code that everyone agrees to follow. It can't be changed once it's written, and everyone in the network checks to make sure it's followed correctly. The cool thing is that anyone who can use a blockchain can check that the smart contract worked. But like any technology, blockchain has some problems. It's hard to make it work faster when more people use it because every person has to do all the work. This also makes it easier for bad people to attack the network and make it stop working. If someone puts a never-ending rule in a smart contract, it can break the whole network.

Sending too many transactions can also make the system stop working. In crypto currency solutions, transactions cost money, and if they use too many resources, they can be too expensive or even get ignored.

1. Fundamental Elements of Blockchain Architecture:

These are the real architecture parts of Blockchain as displayed in Figure 2.

- Hub: Clients or PCs in blockchain format (each gadget has an alternate duplicate of a complete record from the blockchain).
- Exchange: It is the blockchain framework's littlest structure block (records and subtleties), which blockchain utilizes.
- Block: A block is an assortment of information structures used to deal with exchanges over the network conveyed to all hubs.
- Chain: A progression of blocks in a specific request.
- Excavators: Journalist hubs to approve the exchange and add that block into the blockchain framework.
- Agreement: An assortment of orders and associations to do blockchain processes.

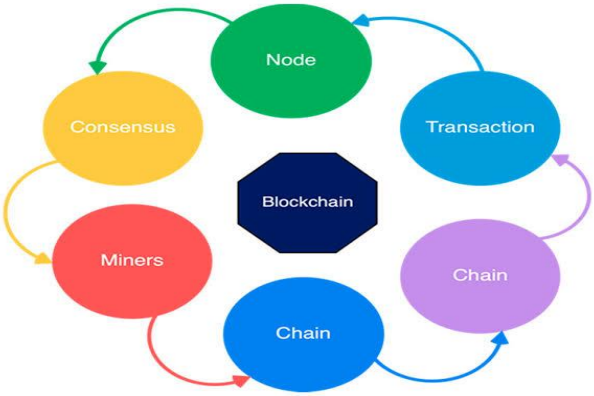

Fig 2.Fundamental elements of the Blockchain architecture.

2. Basic Attributes of Blockchain Architecture:

Blockchain design has many advantages for all areas that consolidate blockchain. The following are various installed qualities as depicted in Figure 3:

- Cryptography: Blockchain exchanges are verified and precise on account of calculations and cryptographic proof between the gatherings in question.
- Unchanging nature: Any blockchain archives can't be changed or erased.
- Provenance: It alludes to the way that each exchange can be followed in the blockchain record.
- Decentralization: The whole circulated information base might be open by all individuals of the blockchain network. An agreement calculation permits control of the framework, as displayed in the center cycle.
- Namelessness: A blockchain network member has produced a location as opposed to a client ID. It keeps up with namelessness, particularly in a blockchain public framework.
- Straightforwardness: It implies being not able to control the blockchain network. It does indeed not occur as it takes massive computational assets to delete the blockchain network.

Fig 3.Basic attributes of Blockchain architecture.

III. HOW BLOCKCHAIN CAN CHANGE THE ELECTRONIC DEMOCRATIC FRAMEWORK

Blockchain technology improved the way we vote in elections. It made the process clearer and easier for everyone to understand, and it stopped people from voting illegally. It also made sure that our personal information was safe, and it checked to make sure the results of the election were accurate. Even though electronic voting can be risky because someone could change the votes if they hacked into the system, blockchain technology can help make it safer.

As shown in Figure 4, in traditional voting systems, one person or group has control over the votes, and they could easily change them. But with blockchain, the votes are stored in many different places, so it's much harder for someone to cheat. This means that we can trust the results of the election and make sure that every vote is counted correctly.

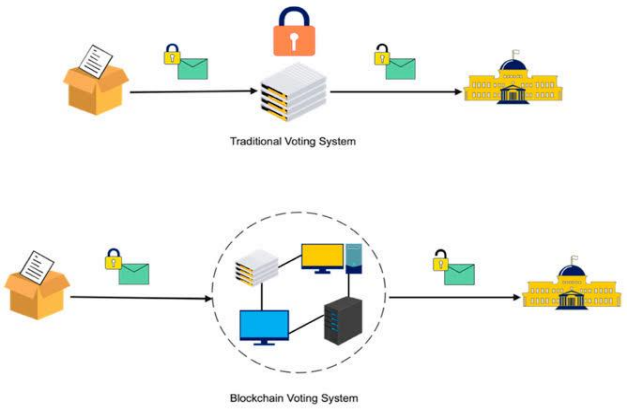

Fig 4.Voting methods: traditional vs. blockchain.

The blockchain is a special kind of computer system that keeps track of things in a way that can't be changed or cheated. Using this system for electronic voting can make it harder for people to cheat and make voting more fair. But it only works if no one controls it completely, not even the government. We need to make sure people believe the voting is fair for it to work well. Some people are testing this idea to see if it can make voting easier and if more people want to participate.

IV. ISSUES AND ARRANGEMENTS OF CREATING INTERNET CASTING BALLOT FRAMEWORKS

When we vote, we can do it on paper, on a computer, or on the Internet. But there are rules and things we need to do to make sure everything is fair and works correctly.

- Qualification: Just authentic citizens ought to have the option to participate incasting a ballot.

Tab.1: Unreusability: Every citizen can cast a ballot just a single time.

Tab.2: Protection: Nobody aside from the citizen can acquire data about the elector's decision.

Tab.3: Decency: Nobody can acquire transitional democratic outcomes.

Tab.4: Sufficiency: Invalid voting forms ought to be distinguished and not considered during counting.

Tab.5: Fulfillment: All substantial polling forms ought to be counted accurately.

The following is a concise outline of the answers for fulfilling these properties on the web-casting ballot frameworks.

1. Qualification:
To solve the problem of who can participate in online voting, people need to prove that they are using a special ID system. The names of all the people who are allowed to vote will be put on a list. But there are two problems. First, we need to make sure that no one adds fake names to the list [13]. And second, the ID system needs to be safe so that no one can steal someone else's account. Making this kind of ID system is a hard job. But since we need a similar system for other things too, it's better to use one that already exists instead of making a new one.

2. Unreusability:
At first, it may seem easy to make sure people can't vote more than once - just put a mark next to their name when they vote. But we also have to think about keeping their vote private. This makes it a bit harder. Sometimes, we might even need to let someone vote again, which makes it even more complicated [14].

3. Security:
Online voting privacy means that only the voter knows how they voted. This is done through techniques like blind signatures, homomorphic encryption, and mixed networks. Blind signatures involve signing a message without knowing what it is, and then unblinding it later. Homomorphic encryption allows math operations to be done on encrypted data without decryption. These techniques ensure that only eligible voters participate and that their votes remain secret [15].

Mix networks are a way to keep things secret when people vote or make choices. It works by sending the choices through a series of servers that mix them up and either decrypt or re-encrypt them. In one type of mix-network, each server has a special key, and the choices are encrypted like layers of an onion. Each server takes off one layer of encryption. In another type, each server just re-encrypts the choices. There are many different mix-network ideas, but the important thing is that if at least one server does its job honestly, the choices stay private. This is different from other ways of keeping things private where we have to worry about how many bad people there might be. Mix networks can also be used to make other things secret too.

4. Reasonableness:
Reasonableness as far as nobody getting moderate outcomes is accomplished clearly: Electors scramble their decisions before sending, and those decisions are decoded at the end of the democratic cycle. The basic thing to recall here is that assuming somebody claims an unscrambling key with admittance to encoded choices, they can get transitional outcomes. This issue is addressed by appropriating the key among a few key holders [16].

A framework where every one of the key holders is expected for unscrambling is temperamental — if one of the key holders doesn't take part, decoding can't be performed. Along these lines, limit plans are utilized by which a particular number of key holders are expected to perform decoding. There are two fundamental methodologies for circulating the key: secret sharing, where a trusted seller separates the produced key into parts and disseminates them among key holders (e.g.,Shamir's Mystery Sharing convention); and disseminated key age, where no confided in the vendor is required, and all gatherings add to the computation of the key (for instance, Pedersen's Appropriated Key Age convention).

5. Adequacy and Fulfillment:
This is about how voting systems work and the challenges they face. Completeness and soundness properties are important for a voting system to be reliable, but it can be difficult to achieve them. When using homomorphic encryption, it becomes harder to tell if a ballot is valid or not. To solve this problem, we use a method called zero-knowledge proof [17], which allows us to prove something without revealing the actual information. Verifiability is also crucial for a voting system to be trusted. It involves ensuring that everyone can confirm the system works correctly, both at a personal level for individual voters and at a universal level for the entire system.
This requires publishing the inputs and outputs of the voting process and providing proof of correct execution. However, online voting introduces new challenges like coercion and vote-buying, where people try to force or pay others to vote a certain way. To address this, online voting systems need to

be resistant to coercion and take measures to lower the risk of interference.

Some voting systems have a special feature called receipt-freeness, which means that a voter can't prove how they voted. This is done by hiding certain information from the voter, but it also means they can't prove if their vote was recorded incorrectly. Many different technologies have been used to make online voting secure, but some trade-offs have to be considered. Unfortunately, there is no perfect solution yet, so there is no completely reliable online voting system.

V. SECURITY PREREQUISITES FOR CASTING A BALLOT FRAMEWORK

Reasonable electronic democratic frameworks ought to meet the accompanying electronic democratic prerequisites. Figure 5 shows the fundamental security prerequisites for electronic democratic frameworks.

1. Obscurity:
All through the surveying system, the democratic turnout should be gotten from outer understanding. Any relationship between's enrolled votes and citizen personalities inside the appointive construction will be obscure [18][19].

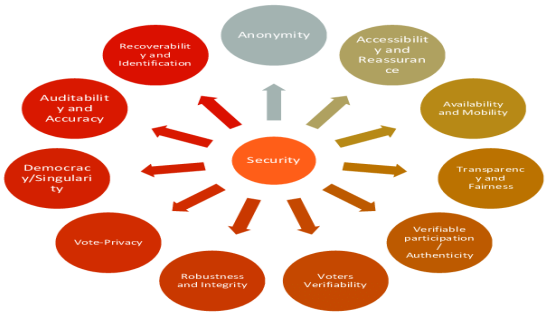

Fig 5.Security Prerequisites for Casting a Ballot Framework.

2. Auditability and Precision:
Exactness, additionally considered rightness, requests that the proclaimed outcomes compare unequivocally to the political decision results. It implies that no one can change the democracy of different residents, that the last count incorporates all genuine votes [20], and that there is no conclusive count of invalid polling forms.

3. A majority rules government/Peculiarity:
A "popularity-based" framework is characterized if by some stroke of good luck qualified electors can cast a ballot, and just a solitary vote can be projected for each enlisted elector [21]. Another capability is that no other person ought to have the option to copy the vote.

4. Vote Protection:
After the vote is projected, nobody ought to be in a situation to join the personality of a citizen with their vote. PC mystery is a delicate sort of secrecy, and that implies that the casting of a ballot relationship stays concealed for a drawn-out period as long as the ongoing rate keeps on changing with PC power and new methods [22][23].

5. Power and Respectability:
This condition implies that a sensibly enormous gathering of voters or delegates can't upset the political decision. It guarantees that enrolled electors will avoid issues or then again urge others to project their real decisions in favor of themselves. In the debasement of residents also, authorities are precluded from denying a political race result by contending that some other part has not played out their piece accurately [24].

6. Absence of Proof:
While mysterious security guarantees discretionary extortion protects, no strategy can be guaranteed that votes are put under payoff or political decision fixing in any capacity. This inquiry has its root from the very beginning [25].

7. Straightforwardness and Decency:
It intends that before the count is delivered, nobody can figure out the subtleties. It evades acts, for example, controlling late citizens' choices by giving an expectation or offering a huge however of-line advantage to specific people or gatherings to be quick to know [26].

8. Accessibility and Portability:
During the democratic period, casting a ballot framework ought to continuously be accessible. Casting ballot frameworks shouldn't restrict the spot of the vote.

9. Evident Cooperation/Realness:
The model additionally alluded to as allure [27] makes it conceivable to survey whether or not a

solitary citizen took part in the political decision [28]. This condition should be satisfied where a vote by electors becomes mandatory under the constitution (similar to the case in certain nations like Australia, Germany, and Greece) or in a social setting, where abstention is considered to be a discourteous motion, (for example, the little and medium-sized decisions for a designated corporate board).

10. Openness and Consolation:

To guarantee that every individual who needs to cast a ballot has the chance to benefit from the right surveying station and that the surveying station should be open and available for the elector. As it were qualified electors ought to be permitted to cast a ballot, and all voting forms should be precisely counted to ensure that races are certified [29].

11. Recoverability and ID:

Casting a ballot framework can follow and reestablish casting ballot data to forestall blunders, delays, and assaults.

12. Citizens Unquestionable status:

Evidence implies that cycles exist for political race evaluation to guarantee that it is finished accurately. Three separate sections are feasible for this reason:

- Uniform check or public confirmation [30] that infers that anyone like electors, legislatures, and outside evaluators can test the political decision after the statement of the count;
- Straightforward obviousness against a survey [31], which is a more vulnerable essential for every citizen to confirm whether their vote has been considered appropriately.

VI. ELECTRONIC DECIDING ON BLOCKCHAIN

Electronic voting is a way of voting where machines are used to record and count the votes. These machines can be found in different forms, like kiosks, laptops, and mobile devices. The machines need to be able to do different things, like registering voters, checking their identity, and counting the votes. However, electronic voting can be risky because if someone hacks the system, it could cause big problems. That's why people are looking into using blockchain technology for voting because it can make the system more secure and prevent fraud. Using blockchain technology as displayed in Figure 6, we could make electronic voting safer, without making much of a difference in how people vote.

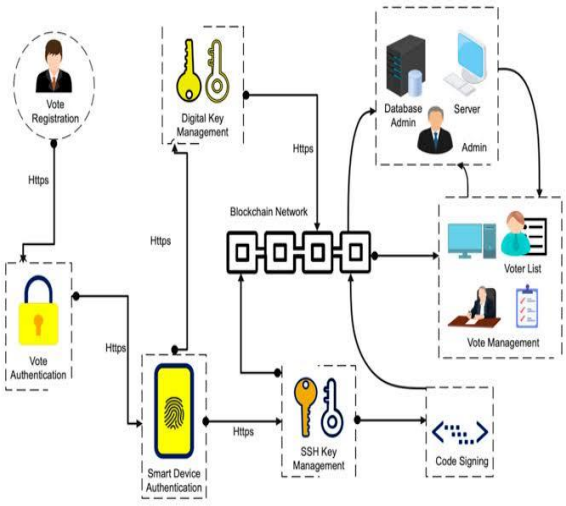

Fig 6.Electronic Deciding on Blockchain.

Blockchain voting is a way of voting where all the votes are kept safe and secure on many different computers instead of just one. Each vote is checked and recorded by many different computers to make sure it is valid. The government can see how people voted, but they can't see who voted for whom. This type of voting is fair and open to everyone. It is different from regular electronic voting because it uses a special technology called blockchain.

VII. CURRENT BLOCKCHAIN-BASED ELECTRONIC DEMOCRATIC FRAMEWORKS

There are some businesses and groups that have started working on ways to make voting more fair and transparent using a technology called blockchain. However, the current systems they have created have a problem with being able to handle a large number of votes all at once. They can work okay for small elections, but not for big ones like national elections. This is because the technology they use has limitations. Blockchain technology is also slow compared to other systems that handle a lot of transactions, like Visa. Many companies have tried using blockchain, but they have found that it is not fast enough for their needs. In the past, there have been examples of blockchain systems being slow and causing problems like the Bitcoin network having delays and the Ethereum network getting clogged up by a popular app. So, even though blockchain is a promising technology, there are still

some challenges to overcome before it can be widely used for voting.

1. Follow My Vote:
An organization has a protected web-based casting a ballot stage jogged on the blockchain with surveying box review capacity to see ongoing popularity-based advancement [32]. This stage empowers the citizens to protect their votes from a distance and securely and vote in favor of their optimal up-and-comer. It can then utilize their ID to open the voting booth in a real sense and find their polling form furthermore, make sure that both that it is right and that the political race results have been demonstrated to be exact numerically.

2.Voatz:
This organization laid out a cell phone and put together a democratic framework with respect to blockchain to cast a ballot from a distance and secretly and confirm that the vote was counted accurately [33]. Citizens affirm their candidates and themselves on the application and confirm by a picture what's more, their distinguishing proof incorporates biometric affirmation that either a particular mark like fingerprints or retinal outputs.

3.Polyas:
It was established in Finland in 1996. The organization utilizes blockchain innovation to furnish general society and confidential areas with an electronic democratic framework [34]. Polyas has been certifying as secure sufficient by the German Government Office for Data Security for electronic democratic applications in 2016. Numerous critical organizations all through Germany use Polyas to perform electronic democratic frameworks. Polyas currently has clients all through the US and Europe.

4.Luxoft:
The first tweaked blockchain electronic democratic framework utilized by a huge industry was created by the worldwide I.T. specialist organization LuxoftHarding, Inc., in association with the City of Zug and Lucerne College of Applied Studies of Switzerland [35]. To drive government reception of blockchain-based administrations, Luxoft declares its obligation to open source at this stage and lays out an Administration Partnership Blockchain to advance blockchain use in open foundations.

5. Polys:
Polys is a blockchain-based internet casting a ballot stage and upheld with straightforward crypto calculations. Kaspersky Lab powers them. Polys uphold the association of surveys by understudy chambers, associations, and affiliations and assists them with spreading appointive data to the understudies [36]. Online races with Polys lead to efficiency locally, further, develop contact with bunch pioneers, and draw in new allies [37]. Polys mean to lessen time and cash for nearby specialists, state legislatures, and different associations by making a difference for them to zero in on gathering and getting ready propositions.

6. Agora:
A gathering has presented a blockchain computerized casting a ballot stage. It was laid out in 2015 and to some degree executed in the official political decision in Sierra Leone in Walk 2018. Agora's engineering is based on a few mechanical developments: a custom blockchain, novel participatory security, and a genuine agreement component [38]. The vote is the local token in Public Square's environment. It energizes residents and picked bodies, filling in as essayists of decisions overall to focus on a safe and straightforward discretionary process. The vote is the Agora biological system's widespread token.

VIII. RELATED LITERATURE SURVEY

A few articles have been distributed in the new time that featured the security and security issues of blockchain-based electronic democratic frameworks. Mirrors the examination of chosen electronic democratic plans in view of blockchain[44][45].

The open vote organization (OVN) was introduced by [50], which is the principal arrangement of a straightforward and self-counting web casting a ballot convention with complete client security by utilizing Ethereum. In OVN, the democratic size was restricted to 50-60 balloters by the system. The OVN can't prevent deceitful diggers from undermining the framework. A deceitful citizen may likewise dodge the democratic interaction by sending an invalid vote. The convention does nothing to ensure the protection from brutality, and the electing executive needs to trust [51][52].

Besides, since strength doesn't uphold elliptic bend cryptography, they utilized an outer library to do the calculation [53]. After the library was added, the democratic agreement turned out to be too huge to be put away on the blockchain. Since it has happened over the course of the Bitcoin organization, OVN is vulnerable to a forswearing of-administration assault [54]. Table 3 shows the fundamental correlation of chosen electronic democratic plans in view of blockchain.

Lai et al. [55] recommended a decentralized mysterious straightforward electronic democratic framework (DATE) requiring an insignificant level of certainty between members. They think that for huge scope electronic races, the ongoing DATE casting a ballot technique is fitting. Sadly, their proposed framework isn't sufficiently able to get from DoS assaults since there was no outsider expert on the plan answerable for examining the vote after the political decision process. This framework is reasonable just for little scopes in view of the restriction of the stage [7].

IX. DISCUSSION AND FUTURE WORK

Many issues with electronic democratic can be settled utilizing blockchain innovation, which makes electronic democratic more financially savvy, lovely, and protected than some other organizations. Over the long run, research has featured explicit issues, like the requirement for additional work on blockchain-based electronic democratic and that blockchain-based electronic democratic plans have huge specialized difficulties [56].

1. Adaptability and Handling Overheads:
For a few clients, blockchain functions admirably. In any case, when the organization is used for huge scope decisions, the quantity of clients increments, bringing about a greater expense furthermore, time utilization for consuming the exchange. Versatility issues are exacerbated by the developing number of hubs in the blockchain network. In the political race circumstance, the framework's versatility is now a critical issue [39]. Electronic democratic coordination will further affect the framework's versatility given blockchain [40, 41].

Table 3 clarifies various measurements or properties intrinsic to all blockchain systems and presents a similar investigation of some blockchain-based stages like Bitcoin, Ethereum, Hyperledger Texture, Litecoin, Wave, Dogecoin, Peercoin, and so on. One method for improving blockchain scaling would be to parallelize them, which is called sharding. In an ordinary blockchain network, exchanges and blocks are confirmed by every one of the taking-an-interest hubs. To empower high simultaneousness in information, the information ought to be evenly apportioned into parts, each known as a shard.

2. Client Personality:
As a username, blockchain uses pen names. This methodology doesn't give complete security and mystery. Since the exchanges are public, the client's character may be found by looking at and investigating them. The blockchain's usefulness isn't well fit for public races [42][47][48][49].

3. Value-based Security:
In blockchain innovation, value-based obscurity and security are hard to achieve [43]. Be that as it may, conditional mystery and secrecy are expected in a political race framework because of the presence of the exchanges in question. For this reason, an outsider authority is required however not incorporated, this outsider authority ought to check and adjust on protection.

4. Energy Productivity:
Blockchain integrates energy-serious cycles like conventions, agreement, peer-to-peer correspondence, and awry encryption. Fitting energy-proficient agreement techniques is a requirement for blockchain-based electronic democracy. Specialists proposed adjustments to currently distributed conventions to make them more energy-productive [44][45].

5. Immatureness:
Blockchain is a progressive innovation that represents a total shift to a decentralized organization. It can reform organizations concerning systems, construction, cycles, and culture. The ongoing execution of blockchain isn't without imperfections. The innovation is as of now futile, and minimal public or expert is figuring out about it, making it difficult to assess its future potential. All current specialized issues in blockchain reception are typically brought about by the innovation's youthfulness [46][57[58].

6. Agreeableness:

While blockchain succeeds at conveying exactness and security, individuals' certainty and trust are basic parts of powerful blockchain electronic democracy [47]. The complexity of blockchain may make it hard for individuals to acknowledge blockchain-based electronic democratic, furthermore, it tends to be a critical hindrance to eventually embracing blockchain-based electronic democratic in overall population acknowledgment [48][57]. A major promoting effort is required for this reason to give attention to individuals about the advantages of blockchain casting ballot frameworks, so it will be simple for them to acknowledge this innovation.

7. Political Pioneers' Obstruction

Focal specialists, for example, political race specialists and government offices, will be moved away from electronic democratic in light of blockchain. Therefore, political pioneers who have benefitted from the current political decision process are probably going to go against the innovation since blockchain will engage social obstruction through decentralized independent associations [49].

X. CONCLUSION

This paper is about studying how electronic voting can be improved using a special technology called the blockchain. The article talks about how blockchain works and how it can be used in voting. It also points out some problems with current electronic voting systems and suggests ways to fix them using blockchain. Some experts think that blockchain could be a good way to make voting fair and transparent.

However, there are still some issues and risks that need to be figured out before we can use blockchain for voting everywhere. So, it's important to test it in a small area first and make sure it's safe and reliable. In conclusion, blockchain is a new and promising technology for voting, but it still needs more research and development before it can be widely used.

REFERENCES

[1] Blockchain and Democracy. Soc. Econ. 2019, 41, 353-369. Racsko, P.

[2] Yaga, D., Mell, P., Roby, N., and Scarfone. Overview of blockchain technology, arXiv 2019:1906.11078.

[3] Trustworthy Electronic Voting Using Modified Blockchain Technology. Shahzad, B.; Crowcroft, J. 2019, IEEE Access 7, 24477–24488.

[4] The Economist, 2017 EIU Democracy Index. It's possible to access it online at https://infographics.economist.com/2018/DemocracyIndex/.(Retrieved on January 18, 2020).

[5] Houghton, C.; Cullen, R. An analysis of the New Zealand government's websites about democracy online. 2000, 17, 243-267, Gov. Inf. Q.

[6] Wang B., Sun J., He Y., Pang D., and Lu N. Blockchain-based general election on a large scale. 2018; Procedia Computer Science; 129: 234–237.

[7] S. Gao; D. Zheng; R. Guo; C. Jing; and C. Hu. A blockchain-based anti-quantum electronic voting protocol with an audit function. 2019 IEEE Access 7, 115304–115316.

[8] Szabo, N. Securing and formalizing connections over open networks. 1997, January 1st, 2, 9.

[9] Zhao, Y., Da Xu, L., Tan, J., Tan, W., Zhu, H., Guo, K. Using blockchain technology and smart contracts, a unique service level agreement paradigm for industrial cloud manufacturing 4.0.

[10] Al-Shayeji, M., Mohd, B.J., and Jaffal, R. A review and assessment of compact hashing algorithms for Internet of Things (IoT) devices.2021 Clust. Comput.

[11] Mattos, D.; Albuquerque, C.; Carrano, R.C.; Medeiros, D.S.V.; Oliveira, M.T.; Carrara, G.R. employing a realistic workload to assess the performance of private blockchain platforms. 19–21 February 2019; Paris, France: Proceedings of the 22nd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN).

[12] Mansor, Z., Shukur, Z., and Hussain, H.A. A thorough analysis and future directions for research on blockchainIoT access control. Global Journal of Advanced Computer Science Applications, 2021, 12, 239–244.

[13] Oliver, J.E. The impact of party activity and eligibility constraints on absentee voting and overall turnout. Am. J. Political Science 40:498–513 (1996).

[14] Voting eligibility: Strasbourg's timidity. Ziegler, R. Human Rights in the UK and Europe: A Tense Relationship; Bloomsbury Publishing: London, UK, 2015; pp. 165–191.

[15] Wang W., Xu H., Alazab M., Gadekallu TR, Han Z., and Su C. Reliable and effective certificateless signature for IoT devices based on blockchain. 2021 IEEE Trans. Industrial Inform.

[16] Okamoto, T., Ohta, K., and Fujioka, A. A workable system for secret voting in large-scale elections. In the documentation of the Queensland, Australia, 13–16 December 1992, International Workshop on the Theory and Application of Cryptographic Techniques.

[17] Definitions and characteristics of zero-knowledge proof systems. Goldreich, O.; Oren, Y. 1994, J. Cryptol., 7, 1-32.

[18] The authors are S.K. Aggarwal, S.K. Kothuri, S.B. Bisht, S.Gupta, K. Garg, and P. Saraswat. A comparison of the electronic voting system based on blockchain. It was presented at the 2019 Fourth International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), which took place in Ghaziabad, India, on April 18 and 19.

[19] Wang, S., Jiang, C., Zhou, Y., and Liu, Y. a blockchain-based FOO voting system that is improved. Int. J. Inf. Secur. 2020, 19, 303–310.

[20] Sadia, K.; Islam, A.; Masuduzzaman, M.; Paul, R.K. Secure electronic voting on the blockchain assisted by smart contracts. Pages 161–176 are included in IC-BCT 2019; Springer: Berlin/Heidelberg, Germany, 2020.

[21] Adeshina, S.A. and Ojo, A. released the proceedings of the 15th International Conference on Electronics, Computer, and Computation (ICECCO), which took place from December 10 to December 12 in Abuja, Nigeria and focused on maintaining vote integrity with blockchain.

[22] V. Augoye and A. Tomlinson. Analyses of Electronic Voting Systems in Real Environments. Online: (accessed on July 28, 2020) https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1013&context=ukais2018.

[23] N. Singh and M. Vardhan are 23. Block size multi-objective optimization for blockchain applications depends on CPU power and network bandwidth. In the 2019 Ranchi, India, 11–12 May Proceedings of the Fourth International Conference on Microelectronics, Computing, and Communication Systems.

[24] Wei, P., Wang, D, Zhao, Y, Tyagi, S.K.S., and Kumar, N. 24. cloud data integrity protection system based on blockchain technology. 2020, 102, 902–911. Future Generation Computer Systems.

[25] Feng, Q., He, D., Zeadally, S., Khan, M.K., and Kumar, N. A study on the blockchain system's protection of privacy. J. Network Computing Applications 2019, 126, 45–58.

[26] Poniszewska-Maranda, A., Pawlak, M., and Guziur, J. Blockchain technology applied to the electronic voting process to create an auditable voting system. 2020, 16(1), Int. J. Web Grid Serv.

[27] Secure Electronic Voting Using a Hybrid Cryptosystem and Steganography by Okediran, O.O., Sijuade, A.A., and Wahab, W.B. J. Advanced Mathematical Computer Science 2019, 34, 1–26.

[28] Jafar, U.; Aziz, M. J. A. State-of-the-art analysis and future research plans for blockchain-based electronic voting. In the abstracts of the Penang, Malaysia, 8–9 December 2020, International Conference on Advances in Cyber Security.

[29] Broncovote: Secure Voting System Using Ethereum'sBlockchain. Dagher, G.G., Marella, P.B., Milojkovic, M., Mohler, J. 2018 January 22–24, Funchal, Madeira, Portugal: Proceedings of the Fourth International Conference on Information Systems Security and Privacy.

[30] Rao, A.A., Tentu, A.N., Yerukala, and Sree, T.U. Identity-based signatures are used in a secret-sharing scheme. The 2019 IEEE International Conference on Electrical, Computer, and Communication Technologies (ICECCT), held in Tamil Nadu, India, from February 20 to 22, was published in the conference proceedings.

[31] Utilising re-voting in the Helios election system. Meyer, M.; Smyth, B. 143, 14–19, Inf. Process. Lett., 2019.

[32] Vote, F.M. 32. Follow My Vote: The Future's Secure Mobile Voting Platform. 2020. You can access it online at https://followmyvote.com/. (Viewed on July 26, 2021).

[33] .Voatz, 2020. Voatz—Voting Redefined®®. accessible on the web at https://voatz.com (viewed on July 28, 2020).

[34] Polyas. Polyas. accessible on the internet at https://www.polyas.com (viewed on July 28, 2020).

[35] Luxoft is number 35. Online at https://www.luxoft.com (accessed on July 28, 2020).

[36] Sayyad, S.F., Pawar, M., Patil, A., Pathare, V., and Poduval, P. Sayyad, S., Pawar, M., Patil, A., Pathare, V., and Poduval, P. A survey of the

blockchain voting features. Int. J. 2019, 5, 12–14.

[37] Polys, 2020. Polys—Online Voting System. Easily accessible online at https://polys.me (accessed on July 28, 2020).

[38] Agora, 2020, number Visit https://www.agora.vote to access it online. (Viewed on July 28, 2020).

[39] J.-G. Song, S.-J. Moon, and J.-W. Jang. Sensors 2021, 21 and 3958: A Scalable Implementation of Anonymous Voting over EthereumBlockchain.

[40] Pawelak, M., Poniszewska-Maranda, A., and Kryvinska, N. For the blockchain electronic voting system, towards intelligent agents. Procedia Computer Science 141 (2018) 239–246.

[41] Zakaria, M.S.; Ghani, A.T.A. A case study of a method for methodically designing scalable microservice-based applications. Int. J. Adv. Computer Science and Applications 2018, 9, 125–135.

[42] Javed, I., Alharbi, F., Bellaj, B., Margaria, T., Crespi, N., and Qureshi, K. Health-ID: A Decentralised Identity Management for Remote Healthcare Based on Blockchain. 9, 712 in healthcare in 2021.

[43] Bernabe, J.B., Skarmeta, A., Canovas, J.L., Hernandez-Ramos, J.L. Blockchain privacy-preserving solutions: A review and problems. 2019 IEEE Access 7, 164908–164940.

[44] Validators Performance Efficiency Consensus (VPEC): A Public Blockchain. Test Eng. Manag. 2020, 83, 17530-17539. Jalal, I., Shukur, Z., and Bakar, K.A.B.A.

[45] Saheb, T., and Mamaghani, F.H. investigating the organizational values and hurdles to blockchain adoption in the banking sector. 2021, 32, 100417 J. High Technol. Manag. Res.

[46] Survey of security oversight on blockchain from a technological standpoint by Wang, Y., Gou, G., Liu, C., Cui, M., Li, Z., and Xiong, G. 2021, 60, 102859 J. Inf. Secur. Appl.

[47] Wang Y, Gou G, Liu C, Cui M, Li Z, and Xiong G. An examination of blockchain security oversight from a technological angle. 2021, 60, 102859 J. Inf. Secur. Appl.

[48] Blockchain-enabled e-voting. Kshetri, N.; Voas, J. IEEE Software, 35, 95–99 (2018).

[49] Krishnan, A. The Blockchain Enables Terrorism and Social Resistance through Decentralised Autonomous Organisations. 2020, 13, 41–58, J. Strateg. Secur.

[50] McCorry, P., S. F. Shahandashti, and F. a smart contract with the highest level of voter privacy for boardroom voting. In the papers from the Sliema, Malta, 3–7 April 2017 International Conference on Financial Cryptography and Data Security.

[51] Xiong, H., Zhang, S., and Wang, L. Chaintegrity: A strong, globally verifiable, large-scale electronic voting system powered by blockchain. Journal of Information Security, 2019, 19, 323–341. [CrossRef]

[52] DABSTERS: Distributed Authorities Using Blind Signature to Effect Robust Security in E-Voting. Chaieb, M.; Koscina, M.; Yousfi, S.; Lafourcade, P.; Robbana, R. 78. Accessed on July 28, 2020 at https://hal.archives-ouvertes.fr/hal-02145809/document.

[53] Woda, M., and Huzaini, Z. A proposal for a blockchain-based electronic voting system that secures the block using elliptical curves.

[54] In the conference's proceedings, published in Wroclaw, Poland, from June 28 to July 2, 2021.

[55] Hjalmarsson, F., Hreiarsson, G.K., Hamdaqa, M., and Hjlmtsson, G. e-voting system based on a blockchain. In the papers from the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), which took place in San Francisco, California, USA, from 2–7 July 2018?

[56] Lai, W.J., Hsieh, Y.C, Hsueh, C.W., and Wu, J.L. An electronic voting system that is decentralised, anonymous, and transparent. In the papers presented at the 2018 Shenzhen, China, 15–17 August 1st IEEE International Conference on Hot Information-Centric Networking (HotICN).

[57] T. VenkatNarayanaRao, S. ManasaArtificial Neural Networks for Soil Quality and Crop Yield Prediction using Machine Learning, International Journal on Future Revolution in Computer Science & Communication Engineering, Vol.: 5, Issue 1, Jan. 2019.

[58] T. VenkatNarayanaRao AkhilaGaddamMuralidhar Kurni K. Saritha, "" Reliance on Artificial Intelligence, Machine Learning and Deep Learning in the Era of Industry 4.0", wiley publisher,17 June 2021.