Advances in Consumer Research
https://acr-journal.com/

Volume-3 | Issue-4 |April 2026

Original Researcher Article

Securing Online Voting For Democracy In Pandemic Times Using Blockchain Technology

Heena [1], Anil Pandit [2]
[1]Research Scholar, GNA University, Punjab, India
Email ID : guptaheena666@gmail.com
[2]Associate Professor, GNA University, Punjab, India
Email ID : Anil.pandit@gnauniversity.edu.in

ABSTRACT
Given the current COVID-19 outbreak, it is very important to have a strong democratic process that includes safe ways to vote online. It is not simple to maintain conventional voting methods safe, open, and unchanged in the face of huge changes throughout the world. This paper examines the creation and implementation of a blockchain-based online voting system that addresses these challenges. Blockchain's decentralization, transparency, and immutability might make online voting systems more accurate, reliable, and safe. Using blockchain technology, a distributed ledger, the suggested system protects voter identity, vote integrity, anonymity, and fraud prevention. The study evaluates the system on key parameters like security, accuracy, scalability, and efficiency in accordance with more traditional and established online voting options. By means of extensive simulations and comparative research, the study reveals that blockchain has the capacity to lower hazards pertaining to hackers, tampering, and unauthorised access. Should a pandemic or other disaster make physical voting impossible, the findings suggest that online voting using blockchain technology may improve democratic resilience and trust. By detailing actions to be taken to establish an online voting system that is secure, efficient, and trustworthy, this paper contributes to the continuous debate on technology developments in democratic processes.
Keywords: Online Voting, blockchain, Pandemic times, security, Encryption.

INTRODUCTION:

Online voting grew in popularity throughout the epidemic as a way to reduce the public health concerns related with in-person voting. In order to guarantee secure democratic voting during the epidemic, authorities in charge of elections and administrative review remote voting possibilities. Online voting has presented fresh cybersecurity issues, addressed the digital gap, and preserved public confidence in the democratic process that need for attention. Though online voting is convenient and flexible, it is imperative to closely review security, accessibility, and legal frameworks if we are to maintain democratic integrity and inclusion during pandemics and regular elections. Depending on how governments manage the epidemic, voting online might or not be significant in future elections. At the end of December 2019, Wuhan, China announced the first instance of SARS-CoV-2. Global growth of the COVID-19 epidemic brought about its causes. As things are, avoiding contact with people, hiding one's face with a mask, and keeping inside are necessary. National governments use the following steps to stop new coronaviruses from proliferating: Rising confirmed cases in March 2020 suggested Italy to be the first European country affected by the COVID-19 epidemic. Italy's first actions were a stop to numerous commercial activities, closing of educational institutions, travel restrictions, and social isolation. The epidemic had an effect on worldwide voter behaviour. The cornerstone of many democratic systems, voting in person at polling sites was never previously viewed as hampered by any unseen challenges. Measures like social distance, hygienic standards, and voting limits were taken to stop the virus from spreading. Both voters and poll workers have had to put up with long wait periods in line of work. In response to these issues, more and more countries let their citizens cast absentee or mail-based votes. Conversely, this change has brought to light problems with postal system pressure, fraud, and delayed vote delivery. Several governments are debating whether internet voting as a safe substitute for in-person voting is feasible. These policies underlined the importance of strong voting mechanisms in addition to guaranteeing the health of the people. Effective and safe enjoyment of democratic liberties depends on this. Often known as e-voting, internet voting is a fresh approach to cast a ballot in an election using electronic methods to guarantee the security of the vote itself as well as the count. Unlike traditional paper-based voting methods, Internet voting systems employ a range of technological devices and software to streamline the voting process and maybe make it accessible to a greater spectrum of voters.

Using a genuine and secure mobile app or website will let one vote online. Thanks to mobile voting software, voters now have a quick and easy way to cast their ballots using their tablets or cellphones. Certain modern online voting systems use biometric identification to ensure that only eligible voters may cast their votes. Blockchain

technology is occasionally utilised in online voting in order to increase security and openness. Among the easily available voting tools available to online-based voting systems to assist voters with disabilities are customisable text sizes, audio cues, and screen readers. Complete online voting systems may include real-time verification processes for voters' peace of mind. Certain techniques let voters, including those living abroad, who are unable to physically visit a polling station cast their votes from anywhere. Regarding online voting, E2E for Internet voting is mostly concerned with ensuring systems are uncompromising and safe. Guaranturing the integrity of votes cast via the Internet helps one to keep trust in the voting process and protect individuals's democratic rights. Although internet voting has great promise, there are many aspects to consider and deal with. Security Concerns are ensuring the security and integrity of E-Voting systems is paramount. Safeguarding voter privacy is crucial.

1.1 Internet Voting During Pandemic

For a few years now, people have been talking about and trying out Internet Voting, which is also called e-voting or online voting. During the COVID-19 pandemic, internet voting became more popular, largely as a way to avoid the health hazards that come with voting in person. Some countries and regions looked at remote voting technologies to lower the risk of virus spread instead of having people vote in person at polling places. Implementing Internet voting methods on a large scale might be hard and full of problems. Some individuals may not be able to vote online because they don't have a computer or another way to go online. Checking the identification and legitimacy of voters is an important part of any voting system. Hacking may happen to online voting systems, which makes elections less credible. To make it easier for people with disabilities to vote, online voting systems must be built to be accessible. Several experts say that you should have paper ballots or a paper trail on hand in case of disagreements or recounts. It is very important to maintain the public's trust in the honesty of the voting process. Online voting procedures and restrictions are different in each jurisdiction. A few places opted to run pilot programs to see how well online voting worked, how safe it was, and how people felt about it before making it available to everyone.

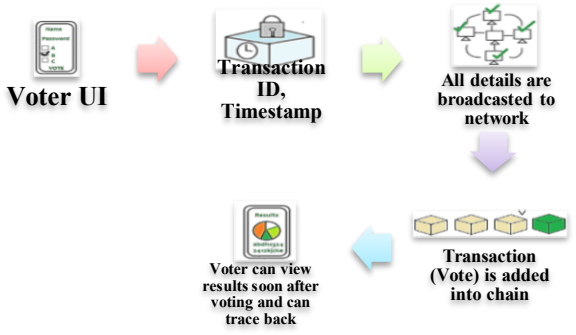

Fig 1. E-voting using blockchain during a pandemic situation

Some nations have had success with online voting, while others have had a lot of problems and arguments. When deciding whether or not to use Internet Voting during a pandemic or any other time, all relevant variables and hazards should be taken into account. For an electronic voting system to work well, the public has to be involved, the system needs to be open, and it needs to be tested and evaluated a lot. The epidemic has had a huge impact on almost every part of human existence. There are a lot of problems with democracy, including how elections are run. Health issues, lockdowns, and social isolation have made regular in-person voting less safe and useful. Because of this, some nations have looked into the idea of setting up full online voting systems to make sure that democratic procedures stay in place even during the epidemic. E-voting or online voting is a group of ways and technologies that let people vote digitally using a desktop computer, laptop, smartphone, or other digital device. Even though internet voting systems have been around for a while, the COVID-19 epidemic has made them much faster to build and put into use. This has made things harder and easier for democracy.

1.2 Different Types of Pandemic Situations

There is a pandemic or another hazardous or unpleasant condition, electronic voting might be a good way to vote instead of going to the polls in person. Electronic voting, which lets individuals vote from a distance via the internet or other technical means, might help stop the spread of infectious diseases during pandemics like the COVID-19 outbreak. Electronic voting devices might be useful in places that commonly have bad weather, such hurricanes, earthquakes, or wildfires. Electronic voting might let people vote more easily in places where traveling to the polls is hard because of safety issues, curfews, or civil unrest. If you can't go to your polling site in person because of an emergency or anything else that makes it hard to travel, you may be eligible to vote online. People who are told to stay at home or quarantine because of health problems or a pandemic may find it hard to vote in person.

1.3 Securing Internet Voting System Data

The security of data saved in an online voting system is very important for making sure that elections are fair. To keep the electronic voting system safe, here are some important steps:

- Encryption: Use strong encryption methods to keep data safe as it is sent and stored.
- Data Integrity: Use checksums and hash techniques to make sure the data is correct.
- Audit Trails: Keep a record of everything that happens on the system, including who did what and when.
- Network Security: Keep the networks that link electronic voting systems safe by protecting their infrastructure.
- Regular Updates and Patch Management: Firewalls, IDS, and IPS are some examples of cyber defenses.
- Voter Privacy: As part of the physical security measures, make sure that the servers and databases that hold the electronic voting system are secure.

- Redundancy and Backups: Use encryption and anonymization to keep voters' identities separate from their votes. This will help protect their privacy.
- Third-Party Verification: Hire a group of security experts to do security audits and penetration testing to find weaknesses in the system.
- Transparency: Make sure that the public and election monitors know precisely what the security measures are.
- Legal Framework: Make regulations and punishments for bad behavior and data breaches in electronic voting systems.

To keep the data in an online voting system secure, you constantly need to be on the lookout for emerging dangers and be ready to respond. Election managers may assist keep voter data in e-voting systems private and safe by following these best practices, keeping a careful eye on the system, and making security measures stronger. One way to show how encryption makes blockchain security better is to make a comparison table that just looks at encryption methods within the context of blockchain technology:

Table 1 Comparison of Encryption Techniques Considering Blockchain

Aspect	Encryption Techniques	Blockchain with Encryption
Purpose	Protect data confidentiality and integrity	Secure data within a blockchain, enhancing trust and privacy
Primary Use Cases	Data security, privacy	Cryptocurrency, data privacy, smart contracts
Data Protection	Secures data at rest and in transit	Enhances data security on the blockchain
Key Management	Utilizes keys for encryption and decryption	Adds an extra layer of security using cryptographic keys
Anonymity	Can protect user identities	Preserves user privacy by pseudonymizing transactions
Data Transparency	Ensures data is only accessible to authorized parties	Enhances blockchain transparency while securing data
Immutability	Does not inherently provide immutability	Reinforces blockchain's immutable ledger
Consensus Mechanism	Not related to consensus mechanisms	Complements blockchain consensus for secure data
Scalability	Encryption doesn't address scalability	Can affect blockchain scalability if encryption isn't optimized
Trust	Trust in encryption is based on cryptography and key management	Trust in blockchain comes from decentralization and consensus, with encryption as a security layer
Security Audits	Encryption techniques are audited for security	Blockchain networks undergo security audits, with encryption as a component
Governance	Encryption governance is typically centralized	Blockchain governance can be decentralized or centralized, depending on the network
Examples	AES, RSA, ECC, SSL/TLS	Bitcoin, Ethereum, Hyperledger Fabric with encryption
Aspect	Encryption Techniques	Blockchain with Encryption
Purpose	Protect data confidentiality and integrity	Secure data within a blockchain, enhancing trust and privacy

1.4 Different types of Encryptions with blockchain

Blockchain technology depends on various encryption techniques to ensure the security and integrity of data and transactions. Here are encryption techniques used in blockchain security:

- Hash Functions: Cryptographic hash functions like SHA-256 are used to create fixed-size, unique hash values for data stored in blocks.
- Public Key Cryptography: Public key cryptography, including RSA, ECC, and EdDSA, is employed for creating digital signatures and encrypting data.
- Digital Signatures: Digital signatures are generated using a private key and can be verified using the corresponding public key.
- Merkle Trees: Merkle trees (hash trees) are data structures that help efficiently prove the integrity of a subset of data within a larger dataset.
- Symmetric Encryption: Symmetric encryption algorithms like AES are used to encrypt sensitive data within a blockchain.
- Zero-Knowledge Proofs: Zero-knowledge proofs, such as zk-SNARKs, allow users to prove possession of certain information without revealing the information itself.
- Multisignature Wallets: Multisignature wallets require multiple private keys to authorize transactions.
- Consensus Algorithms: Consensus algorithms like PoW and PoS utilize cryptographic

techniques to secure the network and validate transactions.

- Secure Hash Algorithms: They are used for hashing data in way that is resistant to collisions and tampering.
- Quantum Resistance: As quantum computing advances, there is a growing need for encryption techniques that are resistant to quantum attacks.

[2] Role of Blockchain in Internet Voting to Security

All sorts of labour may be easily created thanks to this invention, all without the intervention of central management. It happens without a middleman or employee being involved. Because it generates decentralised, immutable, and transparent transactions, blockchain technology may dramatically alter several industries. In contrast to conventional databases, which organise data into rows and columns, Blockchain writes each block individually. When making a new block in the file, each new file is considered. The data in a block is connected in a chronological sequence when we fill it with data. Blockchain has various potential uses, but financial data have shown to be its most useful use so far. All users share ownership of Bitcoin's Blockchain, thus no one individual or organisation controls its usage. The purpose of this is to store all of the associated Bitcoin transactions. Blockchain allows us to distribute and preserve digital information, but once recorded, it cannot be altered. An immutable ledger, consisting of data about transactions that cannot be erased, may be built on top of blockchain technology. Because of this, DLT is a common way to describe Blockchain.

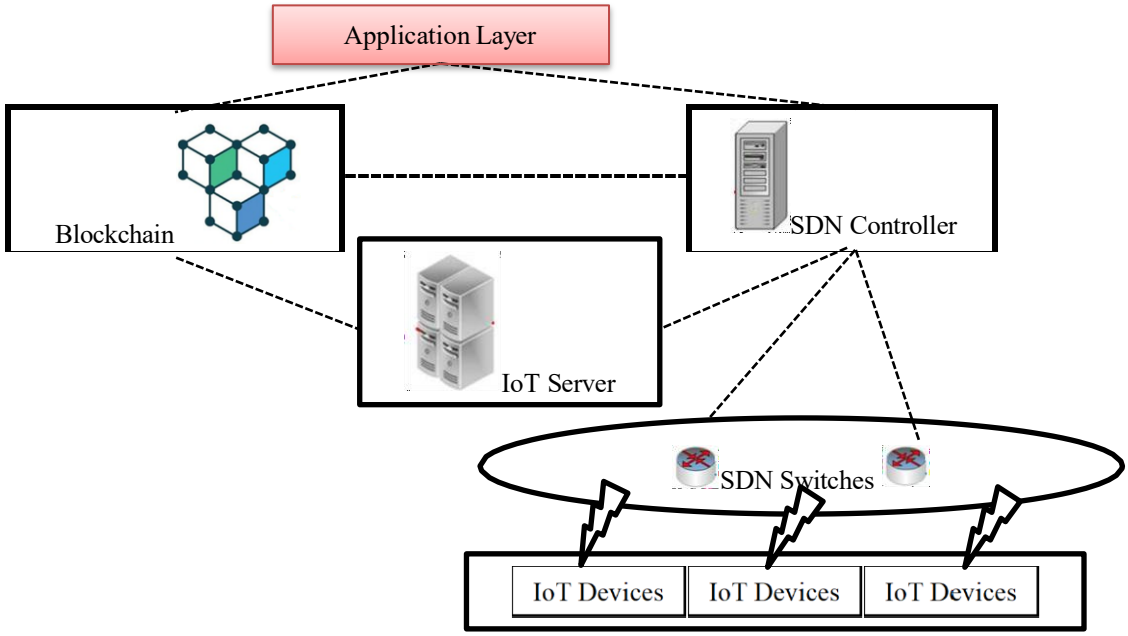

Fig 2. Data Transmission using Blockchain

The key aspects of Blockchain technology that we have already discussed are:

- Immutability: This is a state that cannot be changed. It is very useful feature of Blockchain and it make sures the long stay of the technology as it is immutable and stable.
- Decentralization: Since the network is decentralized, that's why, for infrastructure nobody is responsible and it means that privacy and security will not affect.
- Improved security: In Blockchain, all data is hashed and encrypted using encryption algorithms. Unauthorized access of our data is provided by this.
- Distributed ledger: All citizens can access this information through the public ledger. There is no escape because everything is revealed.
- Consensus: To achieve the consensus tools are very important for block chain. This architecture is built on a smart design consensus algorithm. Consensus is needed for every Blockchain to work correctly.
- Quicker Settlement: The Transactions which are created using the old-style banking systems takes long time.

Significant attention has been gained by Blockchain technology which provides the possible answer to increase the integrity and security of e-voting systems. Unique features of Blockchain can address some of the main security risks related with e-voting during the COVID-19 pandemic and beyond. Here are the roles that blockchain can play in securing e-voting:

- Tamper-Resistant Ledger: All the transactions in Blockchain are recorded in a secure and immutable manner and it is a distributed ledger technology.

- Transparency: Transactions are transparent in Blockchain and all the participants in the network can view the transactions.
- Decentralization: A decentralized network of nodes is used to operate the Blockchain, this makes it extremely resistant to single points of attacks and failures.
- Security through Cryptography: Cryptographic techniques are used to secure the transactions.
- Audibility: Blockchain enables a complete and auditable trail of votes, from the moment a voter submits their ballot to the final tally.
- Redundancy: across multiple nodes, Copies of the blockchain ledger are distributed in the network.
- Resilience to Cyberattacks: Blockchain's distributed and encrypted nature makes it resilient to various cyberattacks.
- Smart Contracts: These are automatically-executing contracts with already defined conditions and rules, which may be used to automate the election process aspects.

[3] Literature Review

M. Picchio et al. (2022) [1] raised the stakes for public gatherings and elections. For every one percentage point increase in mortality among the elderly, voter participation fell half a percentage point. A study conducted by L. Baccini et al. (2021) [2] examined the impact of COVID-19 cases and deaths on the voting patterns of counties in relation to Trump from 2016 to 2020. Using demographic and socioeconomic data, among other COVID-19-related variables, they attempted to eliminate confounding factors. After the French town hall elections in mid-March 2020, L. Bach et al. (2021) [3] looked at the mortality rates of 163,000 male candidates aged 60 and over. People 'rally-around-the-flag' for political leaders during global crises, according to M. Baekgaard et al. (2023) [4]. They raised doubts about the applicability of studies on the impact of rallies to COVID-19 social lockdowns. This COVID-19 pandemic lockdown is different from other academic emergencies. African electoral democracy may be affected by factors such as PU, trust tendency, attitudes towards using/adopting, and willingness to adopt financial resources; sectarian divides; election fraud; perceived threat; and political and economic conditions. This research was conducted under COVID-19 restricted criteria (P. D. Ntale et al., 2021) [5]. S. Bertoli et al. (2020) [6] investigated the potential effects on mortality rates at the local level of the French government's sponsorship of the first round of municipal elections on March 15, 2020. The transmission and death rates of COVID-19 in India were studied by A. Bhadra et al. (2020) [7], who took population density into account. Extensive correlation and regression studies were conducted to correlate district-level COVID-19 transmission to mortality rates. The study by T. S. James et al. (2020) [8] examined the basis of democracy, which is the frequency of elections. This research looked at the humanitarian reasons for postponing natural disasters. The impact of natural disasters on the credibility of elections was the subject of this retrospective analysis. T. Bigger [9] The public's perception of important institutions determines whether a crisis is decisive or maintains the status quo. Before and after nationwide lockdowns, we want to compare the level of political support among survey takers.

T. Landman et al. (2020) [10] investigated the risks of COVID-19 to credible national elections. We start by talking about how elections are essential to democracies. In their study, A. Leininger et al. (2020) [11] looked at how the COVID-19 pandemic has affected voting behaviour in Germany. During the early phases of the outbreak, municipal elections were held in Bavaria. To find out how the virus affected the election outcomes, we may use the within-county estimate of impacts and differences as there is no pattern. Examining the effects of COVID-19 on voting was done by A. Noury et al. (2021) [12]. During the course of the epidemic, almost nine thousand municipalities in France participated in the local elections that took place on March 15, 2020. Through the use of several estimating methodologies and complicating factors, our study revealed that the closer a city was near COVID-19 clusters, the lower the participation rates. These problems were solved and a reliable voting system was established by M. S. Peelam in 2024. For secure online voting, we suggest Democracy Guard, which is built on Ethereum. Voters' faces may be recognised by the gadget. Online voting is now more secure and widely accepted because to Democracy Guard, which is changing the face of politics [13]. Before describing blockchain's problems, S. Tanwar (2023) hurriedly presented it. There has to be a change to our electoral voting system because of cases of incompetence and vote manipulation on a national level. Last but not least, more open and secure voting might lead to more equitable results [14]. An electronically trustworthy, publicly traceable, self-tallying system was developed by Y. Lu (2024) using blockchain technology. Transparency, self-tallying, anonymity, confidentiality, time-limited ballot secrecy, and excludability are all guaranteed by our physical technique. By creating prototypes both on and off the blockchain and then measuring the step time overhead, we are able to confirm our technique [15]. M. Rachwał (2024) highlighted the importance of pandemic voting systems in meeting the standards for global elections. While other voting procedures might achieve universal suffrage in the event of a pandemic, their veracity is uncertain [16]. W. Wojtasik (2024) thinks that the 2020 COVID-19 epidemic might lead to more representative elections. In the name of pandemic, politicians are able to spread lies via the internet and social media [17].

[3] Problem Statement

In times of crisis, when large-scale gatherings pose health dangers, standard voting procedures have their drawbacks, as the COVID-19 epidemic demonstrated. Online voting systems provide an opportunity, but they face significant obstacles that prevent them from being widely used. These include safeguarding voters' identities, keeping votes anonymous and uncompromised, and avoiding hacking, tampering, or illegal access. There are worries about the trustworthiness and dependability of the

election process since current online voting technologies do not always have the appropriate security measures to protect against these dangers. There are serious concerns over the viability of moving to digital democracy due to the lack of a strong, scalable, and secure system for online voting, especially in times of crisis.

[4] Research Methodology

Research adopts experimental methodology to propose, and evaluate blockchain-based E-voting framework that ensures secure, transparent, and reliable elections. The methodology consists of the following stages:

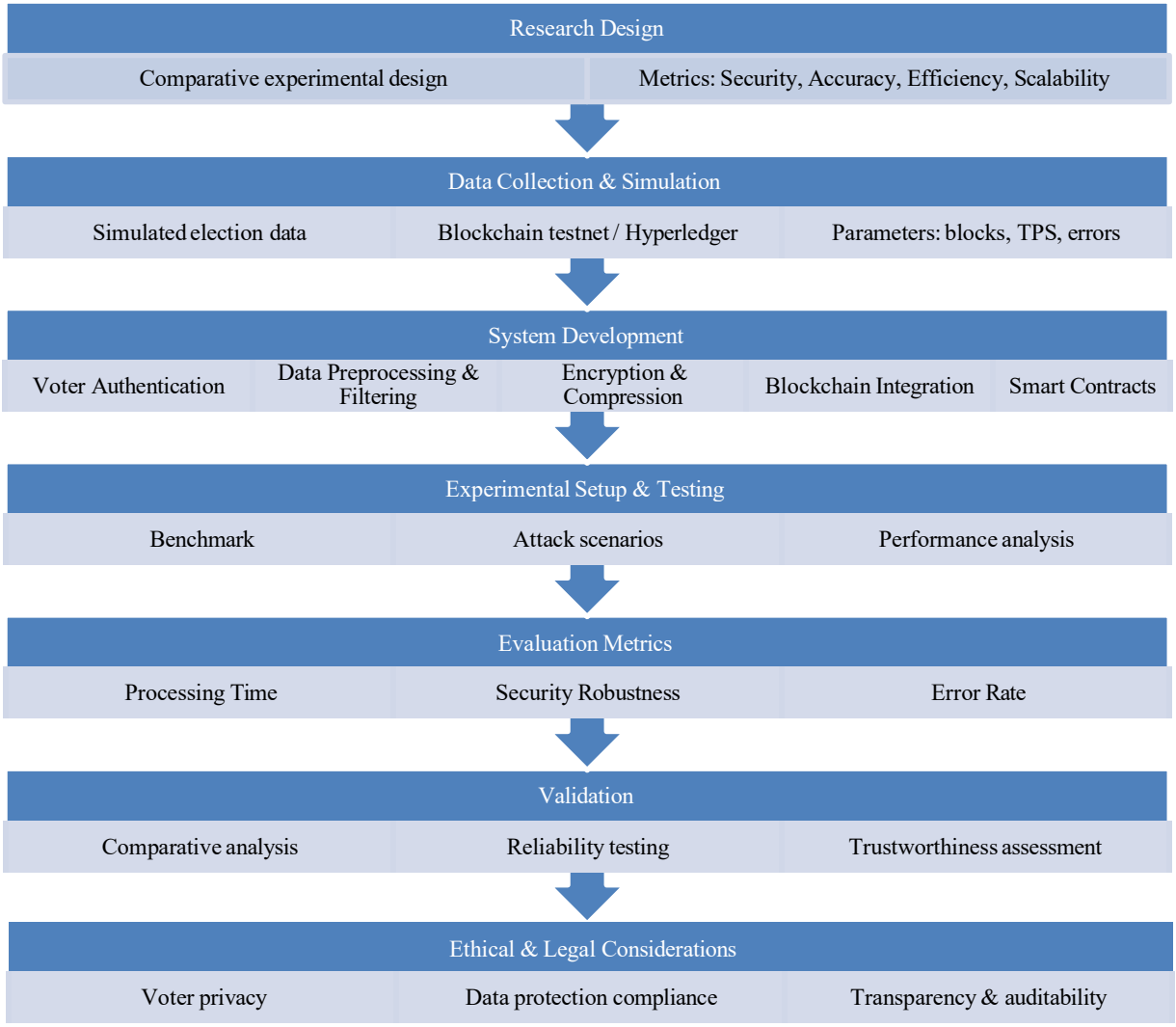

Figure 2 Research Methodology

The study's main goal is to use a comparative experimental method to see how well a blockchain-based voting system works compared to more traditional electronic voting methods. The design is based on four main criteria for evaluation: Efficient processing speed and the ability to handle huge volumes of data; Accuracy in filtering and validating to cut down on mistakes; Scalability in adding more voter data without slowing down; and Security in keeping out assaults, tampering, and fraud.

[5] Proposed Work

The proposed research intends to make blockchain-based systems more efficient, accurate, and safe by integrating the latest data processing and filtering techniques with compression and encryption. To solve the current problems with accuracy, effectiveness, and protection from outside threats, the project looks at important topics such cryptography security, identity management, and blockchain technology. Data processing and filtering approaches employ pretreatment operations to sort and clean the data. This makes the input data more dependable and accurate. It filters out duplicates and undesirable noise from the input, which makes it simpler to connect to the blockchain system. The built-in compression and encryption technologies employ data compression methods to make the blockchain less busy. Encryption keeps the data secure and confidential while it is being sent and stored. Blockchain integration takes use of blockchain's decentralized and unchangeable nature to manage data and identities well. Using cryptography algorithms makes blockchain a lot better and safer. Modern cryptography uses both encryption and compression to make it harder for hackers to get into. These kinds of adjustments are called "performance and security improvements." They also make it easier to do

business on the blockchain, which makes it safer and less likely to be hacked. Research may check error rate to see how filtering, compression, and encryption affect the correctness of data. It also tests the suggested model's effectiveness in cybersecurity by seeing how well it protects packets from outside attackers.

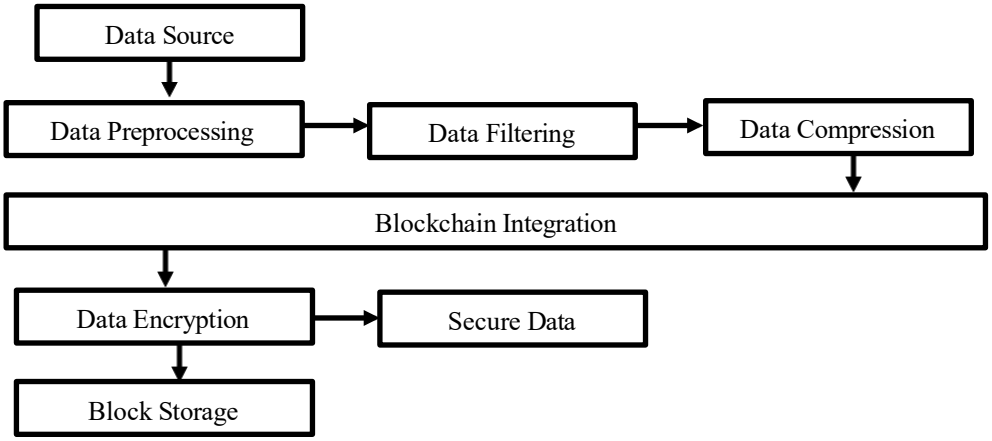

Fig 3 Proposed Work

The recommended integration is expected to make the system work better by using data compression to make it smaller and data filtering and encryption methods to make it more accurate and reliable. Strengthen the security of blockchain systems to make them harder to hack. This will show that the suggested model is better than other solutions in terms of performance, mistake rate, and security measures. It will also provide a full framework for evaluating them. The suggested architecture tries to solve these big problems in order to make blockchain technology more useful in sectors that need high performance and security. Figure 4 shows the Research Model.

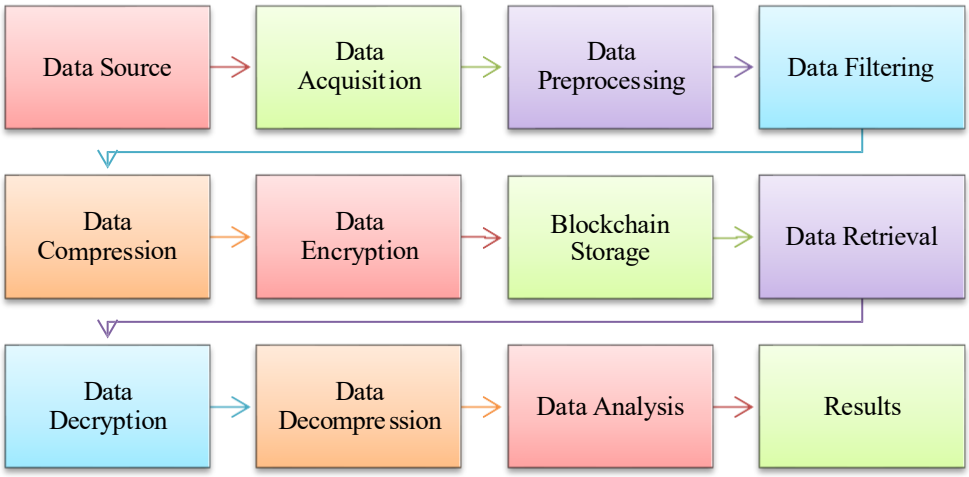

Fig 4 Process flow of Research Model

Work Model of Blockchain-Based Online Voting System

People may register to vote on a safe government website. Only eligible voters may vote with multi-factor authentication. The blockchain generates a unique voter token for each voter, which keeps their identity secret. After the user has been verified, a digital ballot is made. Public-key cryptography is used to encrypt ballots. To make sure that each vote is real and correct, it is digitally signed. The voter sends in their ballot in an encrypted form via a desktop program or a mobile device. The blockchain network gets a message when this encrypted ballot is sent. Before a vote is added to the block, it is checked for validity by a consensus process. The vote is kept on an unchangeable distributed ledger. Blockchain maintains transparency while preserving voter anonymity using hashing and pseudonymization. Smart contracts automatically tally encrypted votes once voting ends. Results are self-verifiable and auditable without revealing voter identities. Data compression and encryption minimize latency and improve efficiency. External attack simulations are mitigated through distributed consensus and encryption. Final results are published in real time on the blockchain. Independent auditors and the public can verify results without compromising voter privacy.

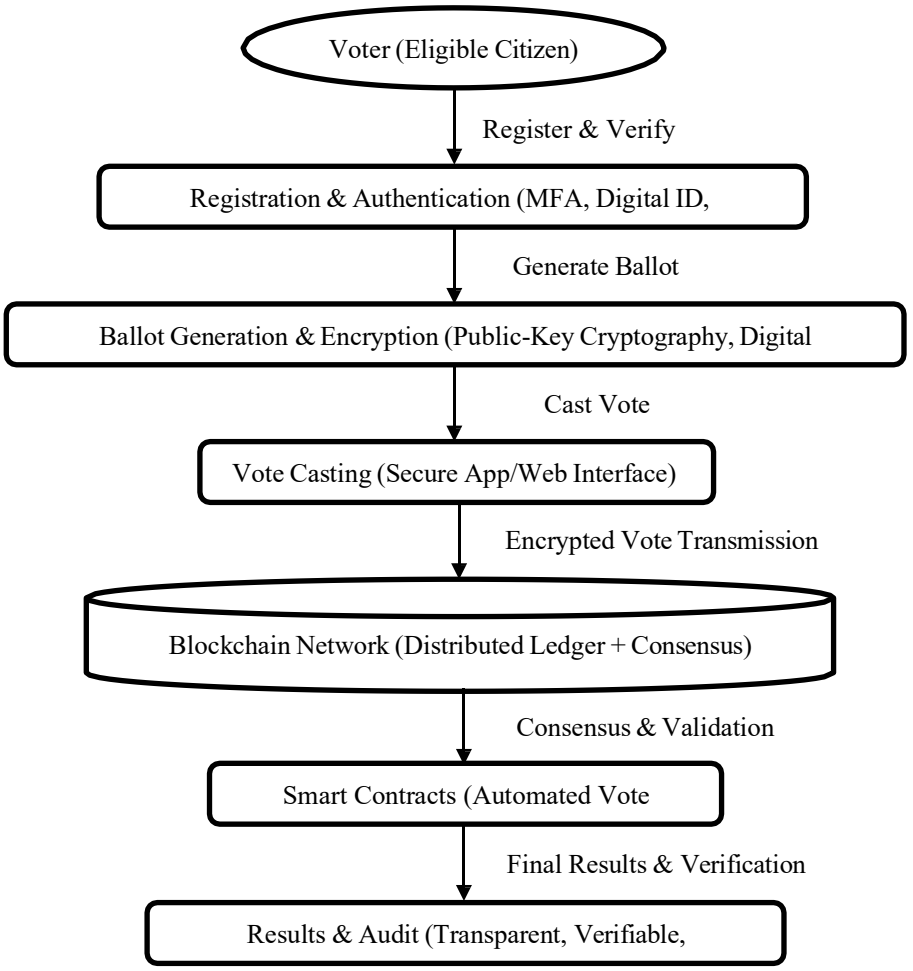

Figure 5 Work Model Flow (Diagram Representation)

Algorithm: Secure E-Voting with Blockchain (End-to-End)

Input: Voter set V, Candidate set C, ElectionParams (T_start, T_end, Chain, PoA/PoS)
Output: Final tally T over C, public audit artifacts
Setup()
CA ← initElectionCA()
Chain ← initBlockchain(Consensus=PoA|PoS, SmartContracts={BallotSC, TallySC})
publish(ElectionParams, Chain.genesis, SC addresses)

For each voter v ∈ V do
IssueCredential(v)

Input: v's government ID attributes; CA
Output: credential Cred_v, unlinkable UTOKEN_v
(pk_v, sk_v) ← KeyGen()
D ECC recommended
Cred_v ← CA.SignSelectiveDisclosure(pk_v, attrs_v)
UTOKEN_v ← IssueBlindSignatureToken(v)
D prevents linkability
Store {pk_v, Cred_v}; deliver sk_v to v securely (HSM/secure enclave)
Return Cred_v, UTOKEN_v

IssueEligibilityToken(v)
D one-time, unlinkable token (UTOKEN)

While now ∈ [T_start, T_end] do in parallel
For any authenticated voter v:
b ← GenerateEncryptedBallot(v, C)

Input: Cred_v, UTOKEN_v, candidate set C
Output: encrypted ballot B*, proof π_priv
AuthZ ← Verify(Cred_v, UTOKEN_v)
D zk-proof / selective disclosure
choices ← GetBallotFromUI(C)
D UX enforces valid format
r ← Random()
D fresh nonce
B ← EncodeBallot(choices, r)
B* ← Enc_pk_Election(B)
D ElGamal/Paillier/ECC-based
σ ← Sign(sk_v, H(B* || UTOKEN_v))
D integrity & non-repudiation
π_priv ← ZKP_prove(valid ballot, 1 vote, within

```
        domain C)
        Return (B*, σ, UTOKEN_v, π_priv)

    tx ← CastVote(b)

        Input: tuple (B*, σ, UTOKEN_v, π_priv)
        Output: tx receipt on Chain
        require BallotSC.IsOpen() == true
        assert ZKP_verify(π_priv) == true
        assert BallotSC.IsSpent(UTOKEN_v) == false
                        D one-vote guarantee
        tx ← BallotSC.Submit(B*, σ, UTOKEN_v)
                        D emits event VoteSubmitted
        Chain.ConsensusAppend(tx)
                        D PoA/PoS finality
        BallotSC.MarkSpent(UTOKEN_v)
        Return tx.receipt

    submit tx to Chain
```

After T_**end**

```
    seal voting in BallotSC
    T ← SmartTally()

    Pick (A) Homomorphic tallying (fast, on-chain proof)
    or (B) Mix-net (strong unlinkability). Both yield
    public proofs.
    (A) SmartTally (Homomorphic)
        Input: all B* on Chain, election private tally key
        sk_T (threshold-shared)
        Output: tally T over C, proof π_tally
        Ctxt ← ProductHomomorphic(B* for all votes)
                        D on-chain aggregation
        Shares ← ThresholdDecrypt(Ctxt, sk_T_shares)
                        D distributed trustees
        T ← DecodeTally(Shares)
        π_tally ← ZKP_prove(correct decryption &
        aggregation)
        TallySC.Publish(T, π_tally)
        Return T
    (B) SmartTally (Mix-net)
        Input: ciphertexts set {B*}
        Output: tally T, proofs π_mix
        For each trustee i:
            ({B*}_i,                π_i)              ←
        ShuffleAndReencrypt({B*}_{i-1})
        After final shuffle: Decrypt all and count
        π_mix ← product of verifiable shuffle proofs
        Publish T and π_mix
        Return T

    publish(T, AuditBundle)

        Input: Chain state, SC logs, proofs {π_priv,
        π_tally|π_mix}, Merkle roots
        Output: boolean Verified
        VerifyEvery(π_priv)
                        D each ballot well-formed
        VerifyOneVotePerUTOKEN()
                        D nullifier set no duplicates
        VerifyTallyProof(π_tally | π_mix)
        VerifyImmutability(MerkleRoots,
        BlockHeaders)
        Return true if all checks pass else false
```

Return T

[6] Result and discussion

The planned research was going to look at a lot of different things. Encryption and compression are two really good ways to make things smaller. Encryption, on the other hand, made things safer and faster. Research looked at how well the recommended model worked, how many mistakes it made, and how well it held up to outside attachments compared to the standard model Research have utilized three main metrics to compare the recommended model's simulation results to those of more traditional approaches. Regarding security, error rate, and processing speed, the proposed model performs better than the others. This section deepens the findings by using tables and figures displaying the outcomes of the comparisons.

6.1 Comparative Analysis of Performance

The proposed model drastically reduces block processing times when compared to conventional methods. This advantage shows itself as the number of blocks increases, therefore demonstrating the efficiency of the model in handling vast amounts of data. Table 2 and Figure 5 demonstrate the performance comparison; at every interval the proposed model regularly beats the conventional system. At 50 blocks, for instance, a significant improvement in computation speed results from a reduction in processing time from 4.92 seconds to 3.16 seconds.

Table 2 Comparison of performance

Blocks vs Processing Time	Conventional	Proposed
10	1.27	0.60
20	2.35	1.24
30	3.10	1.85
40	4.61	2.45
50	5.35	3.08
60	6.72	3.83
70	7.96	4.33
80	7.98	5.20
90	8.99	5.72
100	10.36	6.58

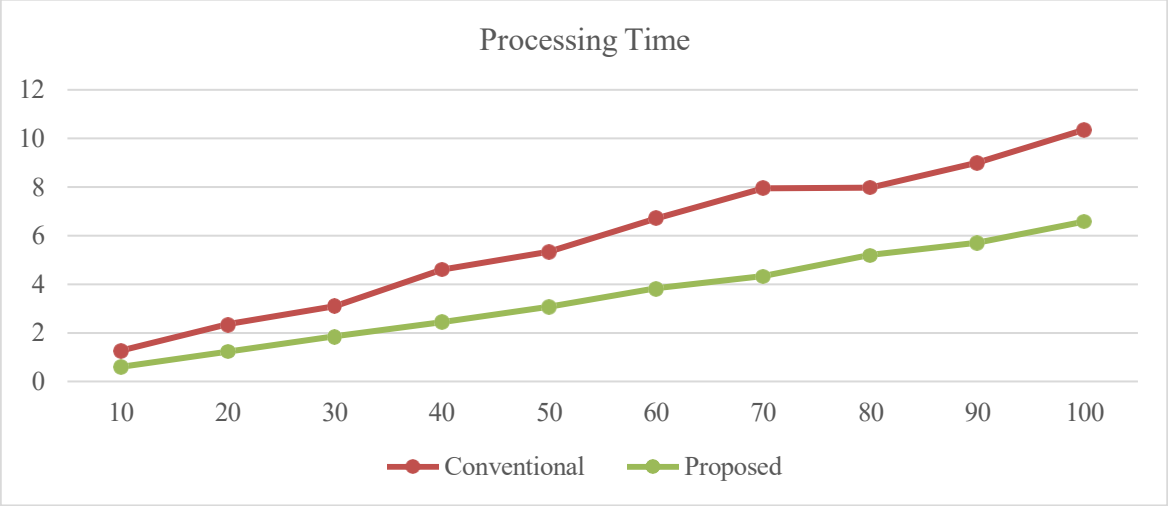

Fig 5 comparative analysis of performance

6.2 Comparative Analysis of Error Rate

The proposed model demonstrates a quite good accuracy gain when compared with more conventional approaches. Consistently showing a reduction in errors, Table 3 and Figure 6 illustrate the findings of the examination of simulated data errors. Things have become much better because to innovative data processing and filtering techniques, which greatly reduce errors and increase data dependability. Here we have addressed the simulated errors. Comparatively to the usual method, the frequency of errors has dropped by considering block numbers every 10 blocks.

Table 3 Comparative analysis of error rate

Packets	Conventional	Proposed
1	4	2
2	6	2
3	9	3
4	11	4
5	14	4
6	16	5
7	19	5
8	21	6
9	24	7
10	26	7

Fig 6 Comparative analysis of error rate

6.3 Comparative Analysis of Blocks Affected by External Attacks

Under outside threats, the proposed approach performs far better. Table 4 and Figure 7 illustrate the outcomes of the simulations, which consistently demonstrate that the suggested approach produces a lesser number of blocks affected by these attacks. This development emphasises the dependability of the encryption methods and the power of the combined security elements of the paradigm. Here, one has modelled an external assault. Studies have shown that counting blocks in increments of 10 lowers the number of blocks vulnerable to an external assault when

compared to a typical system.

Table 4 Comparative analysis of Blocks affected by external attacks

Blocks	Conventional	Proposed
10	3	3
20	5	4
30	6	6
40	9	8
50	9	8
60	13	11
70	13	12
80	15	14
90	17	15
100	20	17

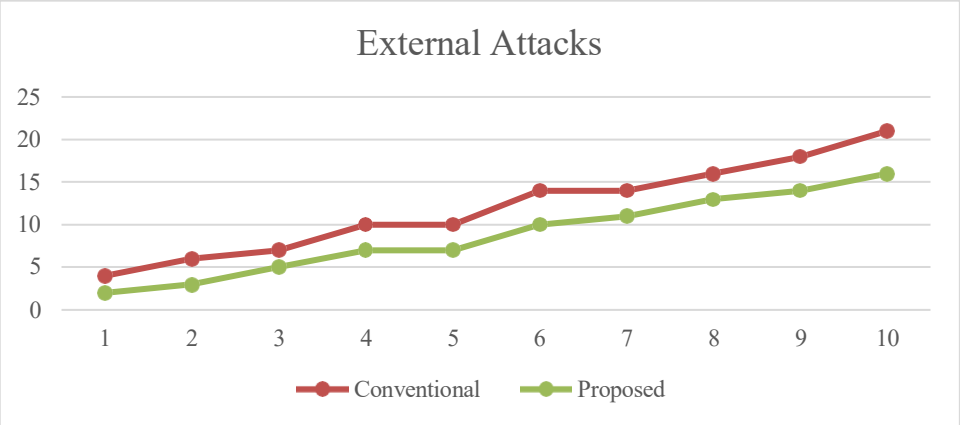

Fig 7 Comparative analysis of Blocks affected by external attacks

The proposed method is shown to be more effective and efficient in addressing important issues than more traditional blockchain methods. Modern data processing techniques ensure a low error rate by combining compression with encryption, therefore improving speed and security. The proposed paradigm may help blockchain applications in fields where performance and security are top priorities to gain from.

[7] Novelty of the Research

The present research introduces a unique integration of blockchain technology, encryption, and data compression for securing online voting systems in pandemic times. The main goals of research on blockchain-based electronic voting have been immutability and transparency. Here are the origins of new ideas:

- **Combining Compression with Blockchain Voting:** The suggested system uses data compression methods before storing and sending data, which is different from traditional blockchain e-voting systems.
- **Better Security with Dual Protection:** The study combines encryption methods with the unchangeable and consensus-building features of blockchain.
- **Accurate and Reliable Hybrid Framework:** The system cuts down on duplicate data and mistakes in voting processes by combining data pretreatment and filtering steps.
- **Validation by Comparative Simulations:** The suggested work is grounded in theory and substantiated by comprehensive simulations and comparisons.
- **Democratic Resilience in Pandemic Scenarios:** The system is meant to work when there is a crisis or pandemic and people can't vote in person. This makes sure that democracy stays strong. It assures that democratic processes will continue while keeping openness, voter privacy, and trust intact, which is not the case with current systems.

To emphasize the uniqueness of our approach, we juxtapose it with existing studies on blockchain-based electronic voting systems and their conclusions. Previous research has mostly overlooked essential factors such as scalability, efficiency, and crisis resilience, focusing instead on immutability and transparency. The suggested technique fixes these problems by combining blockchain technology with algorithms for filtration, encryption, and compression. This makes the system faster and safer at the same time. The table below shows the main differences between the current research and the current procedure. Table 5 shows how the intended study is different from earlier studies.

Table 5 Comparison of Proposed Work with Existing Studies

Aspect	Existing Studies	Proposed Work
Primary Focus	Emphasis on transparency, immutability, and decentralizatio	Focus on security, efficiency, accuracy, and scalability using blockchain with compression & encryption.

	n of blockchain voting.	
Data Handling	Votes stored directly on blockchain without optimization.	Data preprocessing and compression applied before blockchain storage, reducing size and latency.
Security Approach	Standard encryption or blockchain immutability alone.	Dual-layer protection: Encryption + Blockchain consensus ensures confidentiality and tamper-resistance.
Error Managemen t	Limited error handling, prone to redundancy and invalid packets.	Filtering algorithms reduce redundancy and lower error rates, improving accuracy and reliability.
Scalability	Performance degrades with large-scale elections due to block size growth.	Compression + optimized block processing improve throughput and scalability for national-level voting.
Validation Method	Mostly conceptual or small pilot studies.	Comparative simulation-based validation against conventional models, proving reduced processing time, lower error rate, and higher attack resistance.
Crisis Readiness	General e-voting solutions without pandemic-specific resilience.	Explicitly designed for pandemic/emergenc y situations, ensuring democratic continuity with trust and anonymity.

[8] Conclusion and Future Scope

Proposed blockchain-enabled compression and encryption methods, backed by cutting-edge data processing and filtering algorithms, efficiently addressed issues of performance, accuracy, and security. They work significantly better than older systems when it comes to speed, mistake rate, and how easily they can be attacked from the outside. These changes show how the proposed paradigm might make blockchain-based systems better for real-world uses that need high levels of security and efficiency. Blockchain technology may be utilized in situations where both speed and security are very important because of how it is set up. This makes the system work better while lowering the risks. This kind of research builds on past efforts and opens doors for next developments that would make blockchain technology more dependable and effective in many diverse environments. Distributed ledger technology (blockchain) makes immutable storage and exchange of digital information feasible. Unchangeable ledgers, permanent records of transactions, are built on a blockchain. Blockchains also go under DLT. One cannot change or undo a hexadecimal hash. Maintaining data security is an ongoing effort needing regular attention. Encryption of data and key management are aspects of data security. The term "access management" refers to the steps taken by a business to limit access to its internal and outside systems and services (IAM) to only authorised staff only. Their immutability makes distributed ledgers unsuitable for storing important patient data. Blockchain technology's basic component for identity management is a distributed ledger. Individuals may regain control of their personal information and administer their own identities by generating a multi-purpose universal ID on the blockchain. If blockchain technology is used, voters' identities would remain hidden until they provide their consent, which might solve the problems mentioned before. It is possible to safely move user data across systems and platforms with the help of blockchain technology. A safe and efficient way to create an immutable record of sensitive transactions is by using the blockchain. Because of these characteristics, it is perfect for Bitcoin payments and international money transfers..

REFERENCES

[1] Picchio, M., & Santolini, R. (2022). The COVID-19 pandemic's effects on voter turnout. European Journal of Political Economy, 73, 102161. https://doi.org/10.1016/j.ejpoleco.2021.102161

[2] Baccini, L., Brodeur, A., & Weymouth, S. (2021). The COVID-19 pandemic and the 2020 US presidential election. Journal of Population Economics, 34(2), 739–767. https://doi.org/10.1007/s00148-020-00820-3

[3] Bach, L., Guillouzouic, A., & Malgouyres, C. (2021). Does holding elections during a Covid-19 pandemic put the lives of politicians at risk? Journal of Health Economics, 78, 102462. https://doi.org/10.1016/j.jhealeco.2021.102462

[4] Bækgaard, M., Christensen, J., Madsen, J. K., & Mikkelsen, K. S. (2023). Rallying Around the Flag in Times of COVID-19: Societal Lockdown and Trust in Democratic Institutions. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4318576

[5] Ntale, P. D., & Ngoma, M. (2021). Is COVID-19 threatening electoral democracy in Uganda? Readiness to accept 'scientific voting' (electronic voting) amidst the COVID-19 pandemic. Digital Policy, Regulation and Governance, 23(4), 377–397. https://doi.org/10.1108/dprg-01-2021-0025

[6] Bertoli, S., Guichard, L., & Marchetta, F. (2020). Turnout in the Municipal Elections of March 2020 and Excess Mortality During the Covid-19 Epidemic in France. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3627035

[7] Bhadra, A., Mukherjee, A., & Sarkar, K. (2020). Impact of population density on Covid-19 infected and mortality rate in India. Modeling Earth Systems and Environment, 7(1), 623–629. https://doi.org/10.1007/s40808-020-00984-7

[8] James, T. S., & Alihodzic, S. (2020). When Is It Democratic to Postpone an Election? Elections During Natural Disasters, COVID-19, and Emergency Situations. Election Law Journal: Rules, Politics, and Policy, 19(3), 344–362. https://doi.org/10.1089/elj.2020.0642

[9] Landman, T., & Splendore, L. D. G. (2020). Pandemic democracy: elections and COVID-19. Journal of Risk Research, 23(7–8), 1060–1066. https://doi.org/10.1080/13669877.2020.1765003

[10] Leininger, A., & Schaub, M. (2020). Strategic Alignment in Times of Crisis: Voting at the Dawn of a Global Pandemic. Center for Open Science. https://doi.org/10.31235/osf.io/a32r7

[11] Noury, A., François, A., Gergaud, O., & Garel, A. (2021). How does COVID-19 affect electoral participation? evidence from the French municipal elections. PLOS ONE, 16(2), e0247026. https://doi.org/10.1371/journal.pone.0247026

[12] Peelam, M. S., Kumar, G., Shah, K., & Chamola, V. (2024). DemocracyGuard: Blockchain-based Secure Voting Framework for Digital Democracy. Authorea. https://doi.org/10.22541/au.171933260.05961056/v1

[13] Tanwar, S., Gupta, N., Kumar, P., & Hu, Y.-C. (2023). Implementation of blockchain-based e-voting system. Multimedia Tools and Applications, 83(1), 1449–1480. https://doi.org/10.1007/s11042-023-15401-1

[14] Lu, Y., Li, H., Gao, L., Yu, J., Yu, Y., & Su, H. (2024). Self-tallying e-voting with public traceability based on blockchain. Computer Standards & Interfaces, 88, 103795. https://doi.org/10.1016/j.csi.2023.103795

[15] Rachwał, M. (2024). Alternative Voting Procedures and Universal Suffrage during a Pandemic. In BRILL eBooks (pp. 105–118). https://doi.org/10.1163/9789004690622_009

[16] Wojtasik, W., & Pluszczyk, A. (2024). Elections in Times of a Pandemic – the Context of Political Disinformation. In BRILL eBooks (pp. 56–67). https://doi.org/10.1163/9789004690622_006

[17] Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021). Blockchain for Electronic Voting System—Review and Open Research Challenges. Sensors, 21(17), 5874. https://doi.org/10.3390/s21175874

[18] Shahzad, B., & Crowcroft, J. (2019). Trustworthy Electronic Voting Using Adjusted Blockchain Technology. IEEE Access, 7, 24477–24488. https://doi.org/10.1109/ACCESS.2019.2895670

[19] Schinckus, C. (2020). The good, the bad and the ugly: An overview of the sustainability of blockchain technology. Energy Research & Social Science, 69, 101614. https://doi.org/10.1016/j.erss.2020.101614

[20] Basin, D., Gersbach, H., Mamageishvili, A., Schmid, L., & Tejada, O. (2017). Election Security and Economics: It's All About Eve. In Electronic Voting (pp. 1–20). Springer International Publishing. https://doi.org/10.1007/978-3-319-68687-5_1

[21] Wolchok, S., et al. (2010). Security analysis of India's electronic voting machines. In Proceedings of the 17th ACM conference on Computer and communications security. https://doi.org/10.1145/1866307.1866309

[22] Gao, S., Zheng, D., Guo, R., Jing, C., & Hu, C. (2019). An Anti-Quantum E-Voting Protocol in Blockchain With Audit Function. IEEE Access, 7, 115304–115316. https://doi.org/10.1109/ACCESS.2019.2935895

[23] Kim, T., et al. (2022). An Overview of Cyber-Physical Security of Battery Management Systems and Adoption of Blockchain Technology. IEEE Journal of Emerging and Selected Topics in Power Electronics, 10(1), 1270–1281. https://doi.org/10.1109/JESTPE.2020.2968490

[24] Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., & Arami, M. (2020). How Blockchain can impact financial services – The overview, challenges and recommendations from expert interviewees. Technological Forecasting and Social Change, 158, 120166. https://doi.org/10.1016/j.techfore.2020.120166

[25] Ometov, A., et al. (2020). An Overview on Blockchain for Smartphones: State-of-the-Art, Consensus, Implementation, Challenges and Future Trends. IEEE Access, 8, 103994–104015. https://doi.org/10.1109/ACCESS.2020.2998951.