IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 6.252
Volume 2, Issue 1, August 2022

Advanced Blockchain-Based Framework for Enhancing Security, Transparency, and Integrity in Decentralised Voting System

Suhag Pandya
Independent Researcher
spandya5886@ucumberlands.edu

Abstract: *The modern challenges of supply chain control arising from globalisation, decentralisation, and modernisation are rapidly exposed to data leakage, network attacks, and software flaws. Business stakeholders are turning to blockchain technology as a possible solution to improve modern supply chains' reliability, integration, and visibility. Blockchain is an elaborate structure that remains relevant when managing product traceability, integration, and increasing general transparency. This article explores the possibility of blockchain technology enhancing the transparency, integrity, and security of decentralised voting systems. Blockchain, which is decentralised, irreversible and fully transparent, is an alternative solution to the world's problems described by manipulation, fraud and lack of transparency inherent in the globalisation of voting systems. The paper considers several models of voting on the basis of blockchain technology, comparing their advantages, which consist of providing the inviolability of the election results as well as minimising the usage of the intermediaries' services. Evaluating blockchain technology using election procedures as a perspective, this article explores its foundational features, such as cryptographic protections, consensus processes, and ever-executable contracts. Other issues that are named by the study as the challenges for implementing blockchain technology in voting include scalability, energy consumption, and legal issues. This research aims to respond to these questions for enhancing election systems in the digital world by reviewing the literature comprehensively on blockchain technology for decentralised voting and providing a brief overview of the current trend. The results highlight the need for more study into blockchain-based voting systems to resolve the technological and ethical issues that have been raised.*

Keywords: Blockchain Technology, Decentralized Voting Systems, Data Integrity, Transparency, Security, Cryptographic

I. INTRODUCTION

The introduction of distributed, transparent, and secure methods for data management brought about by blockchain technology has caused a revolution in a number of sectors [1]. In essence, blockchain acts as a distributed ledger platform enabling the provision of provable, tamper-proof records uniquely suited to services that need trust and integrity. That said, one domain where these attributes can play a huge role in voting systems, in which openness and the lack of vulnerability threaten the democratic processes.

Improving security, transparency, and integrity is now considered an important objective in the development of new models of voting systems [2]. Paper-based voting or a central electronic voting system is most common and causes many problems like fraud, no trust, manipulation, etc. These challenges reduces confidence of the public in the retrieved election results, this calls for more strategies that can mitigate such problems[3]. Blockchain provides an innovative solution to this problem since it facilitates the casting of votes, stores them in a decentralised manner and protects them from tampering.

In order to eliminate the intermediaries in a decentralised voting system, blockchain technology makes it impossible for one entity to monopolise the decision-making process. It is intrinsically auditable; viewers need not invade voters' privacy to scrutinise and timestamp votes, which has been a major problem in establishing voting protocols that are

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 6.252
Volume 2, Issue 1, August 2022

both secure and private[4][5]. In addition, the application of cryptographic methods, namely zero-knowledge proofs and blind signatures, increases the privacy of voters and, at the same time, preserves the possibility of checking the results of elections[6].

A. Paper structure

This paper is structured into several sections: Section II, Blockchain Technology Overview, its features, and applications. Blockchain's role in enhancing transparency is provided in section III. Section IV provides the blockchain in data integrity and its application and challenges. Section V explained the Decentralized Voting System in Blockchain. Previous research on the Blockchain-Based Framework for Enhancing Security, Transparency, and Integrity in Decentralized Voting Systems is provided in section VI. lastly, section VII provides the conclusion and future study.

II. OVERVIEW OF ADVANCED BLOCKCHAIN TECHNOLOGY

Blockchain technology is an advanced security mechanism and it has secured reasonable attention from cloud users. The blockchain is considered an accounting book and a digital database that works as a distributed and decentralised ledger. Blockchain technology is continuously enhancing to improve data security and privacy, maintaining data integrity and reducing the computational cost of data transmission. Blockchain architecture Figure 1 consists of a set of blocks, every of which comprises a block header and transaction history.

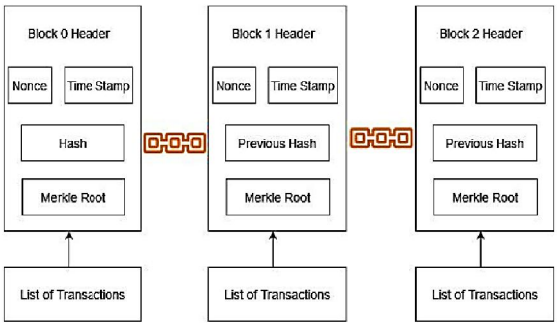

Figure 1: Blockchain architecture

Figure 1 represents the components of blockchain architecture. Throughout a network transaction, a sequence of transactions is recorded into blocks and uploaded sequentially to a blockchain network[7]. The block header provides the following verifiable facts:

- **Previous Hash:** The heading of the block before this one is hashed 256 bits in the previous block.
- **Merkle Root:** This field stores a 256-bit hash of the Merkle tree root across all transactions in the current block.
- **Time Stamp:** This field includes the actual block's timestamp, which is used to locate it chronologically on the blockchain.
- **Nonce:** It contains a 32-bit value that a miner was permitted to modify in order to correctly solve the computational challenge of the current block.

A. Blockchain features and Characteristics

There are many ways in which blockchain technology might improve operational procedures for companies. There are a lot of cool things about blockchain technology that may make it replace current systems [8].

Decentralization

The Peer-to-Peer (P2P) techniques used by blockchain contribute significantly to user protection by enhancing the decentralised apps that are loaded on a large number of devices. Due to its P2P nature, it is not limited by a single unifying factor. Thus, digital money is just one of many possible applications of this technology. Cryptography, distributed norms, and information hoarding are the three main features of blockchain that demonstrate innovation.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 6.252
Volume 2, Issue 1, August 2022

Blockchain technology is based on these interconnected features, which, when used together, gradually decentralise its applications [9].

Shared and public

Blockchain is analogous to a world where immutable data is encoded in computer code and kept in transparent, public databases. The information provided by the controlling party guides a set of rules that anybody may follow in order to join the system and publish a transaction. In order to prevent any loss of data, blockchain technology will provide an enhanced and unique record for each alteration[10]. The more space something takes up, the less reliable it gets and the more likely it is to be lost forever. This is one of the drawbacks of blockchain technology [11].

Trust

Considering that trust is crucial to all human relationships, blockchain technology raises important questions about the current state of affairs. Blockchain technology fosters trust by going directly to the source, eliminating intermediaries.

Immutability

The importance of blockchain, according to Crosby and Nachiappan, is in the security and safety it offers, enabling users to produce decentralised proof of records that are impenetrable by third parties. Blockchain's distinctiveness lies in its immutability and unchanging character, which makes it an ideal option for digital currency transactions [12].

Redundancy

The immutability of the record is ensured by its replication on the blockchain. For instance, to transmit data to each of the N locations where an element is stored, the total stockpile and system transmission speed must be N times. There is no evidence that adding redundancy improves system transfer speed, cost, or capacity [13].

B. Blockchain Security

The phrase "blockchain security" encompasses all the methods and tools used to ensure the reliability and authenticity of blockchain networks. Distributed digital ledgers that record transactions across several computers in an immutable way are the core concept underlying blockchain [14][15]. A high degree of trust and security is an intrinsic goal of this architecture, and it is essential for use in many fields, including healthcare, supply chain management, and financial services. Another advantage of blockchain is the enhanced security it provides; this is highly valuable in the current world, where cyber risks are ever-changing [16]. There are various benefits of blockchain security that are listed below:

Trust and Transparency

The consensus makes blockchain have a distributed ledger with past transaction records that are secure and open. Lack of such control reduces central authority risks and it fits nicely such business segments like supply chain and healthcare that need safe and provable data [17][18].

Reduction in Fraud and Theft

The cryptographic nature of the blockchain ensures that neither identity theft nor any form of fraud or financial theft is committed. Smart contracts go a step further to ensure that security is achieved through unalterable agreements, thereby minimising manipulation-related issues [19][20].

Enhanced Data Integrity

Blockchain provides data authenticity independently stored in registers using a cryptographic hash. It mitigates misuse, making the capture of data for healthcare, finance, and legal industries accurate, besides institutional strategies against legal provisions such as GDPR [21].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 6.252
Volume 2, Issue 1, August 2022

III. BLOCKCHAIN'S ROLE IN ENHANCING TRANSPARENCY

While the immutability of blockchain transactions is undeniably a notable characteristic, the consequences of this immutability go much beyond that. All the nodes in a blockchain network can view the same distributed ledger that stores every transaction that takes place. This means that each participant may input data to the pool and may also verify input data using other input data received from the central authority. Banks and payment processors, which have long been needed to keep and validate information in centralised systems, are rendered unnecessary by the decentralised verification process[22]. The technology of the blockchain straightens and minimises transaction costs through the removal of these middlemen.[23] This article aims to provide a thorough overview of the possible advantages of blockchain technology across different businesses by analysing its ability to increase openness in data privacy. Readers may learn how blockchain technology can change data security methods by reading an unbiased review of its features and uses

A. Blockchain Enhance Transparency

This paper shows that due to its properties, blockchain is an effective means of increasing the level of transparency in various fields [24]. The following sections detail its impact on key areas:

Financial Transparency

The financial sector often grapples with issues like fraudulent activities, hidden fees, and opaque transactions[25]. Blockchain provides a real-time, tamper-proof ledger that records all transactions:

- **Fraud Prevention:** Blockchain's immutability ensures that records cannot be tampered with, reducing fraudulent activities in financial systems[26].
- **Auditability:** Every transaction is documented, making it easy for regulators, auditors, and stakeholders to trace financial flows.
- **Smart Contracts:** There is no need for intermediaries with these self-executing contracts that have predetermined terms, which makes agreements and payments more transparent.

Supply Chain Transparency

Supply chain systems involve multiple stakeholders, from manufacturers to consumers[27]. The inability of traditional methods to provide insight into the movement of products often results in problems like counterfeiting and unethical behaviour. Blockchain transforms this by:

- **End-to-end Tracking:** Each transaction in the supply chain is recorded on the blockchain, allowing stakeholders to trace products from origin to destination[28].
- **Ethical Sourcing:** Consumers can verify claims about sustainability or fair trade by accessing blockchain records.
- **Inventory Management:** Real-time data ensures accurate tracking and efficient inventory control.

Governance and Public Administration

Governments worldwide face criticism for lack of transparency and corruption. Blockchain can transform governance by ensuring accountability and providing a clear audit trail:

- **Transparent Elections:** Blockchain-based voting systems record each vote immutably, reducing election fraud and enhancing voter confidence.
- **Public Fund Tracking:** Blockchain ensures that taxpayer money is used effectively by making expenditure records accessible to the public[29].
- **Identity Management:** In welfare programs, blockchain-based secure digital identities eliminate the possibility cases of fraud and enhance the delivery of services.

Healthcare Transparency

The healthcare sector needs efficient and safe solutions regarding data handling, medication identification, and billing [30]. One will want to secure patient information, enable people to own their health information, and let them decide on

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 6.252
Volume 2, Issue 1, August 2022

which provider can have access to the records, all of which explain blockchain technology. This will enhance the implementation of care coordination and patient versatility while at the same time achieving data security [31].

Media and Information Transparency

To wit, the rampant circulation of fake news and piracy have emerged as major threats to the media business in the decentralised digital world. This is especially a formidable solution since blockchain technology enhances content verification, making it possible to determine the origin and timestamp of articles or multimedia. This checks on fake news and brings credibility to the news being shared online. In addition, it has an application in digital rights management, which allows owners to protect content and record the payment of royalties credibly [32].

IV. BLOCKCHAIN'S ROLE IN ENSURING INTEGRITY

Data integrity, therefore, refers to the fact of maintaining integrity of the data within its lifecycle. Here, blockchain technology does a great job because it creates a record that cannot be changed. The data's reliability and purity are preserved by the built-in cryptographic hash that goes with every block of the blockchain. It is instantly obvious whether there has been any manipulation since the hash will change with even the smallest alteration to the data [33]. Some industries, such as health, financial, and supply chain sectors, are interested in blockchain since they require the assurance of a data source. Adding on Blockchain with master data management (MDM) enhances data reliability by ensuring all systems depend on reliable data [34].

Applications of Blockchain in Data Integrity

Blockchain or distributed ledger technology is now being discussed as revolutionising the way data is secured in several fields [35][36]. The ledgers are decentralised, fixed and clear, allowing data to be protected from alteration, theft and loss and, therefore, suitable for handling sensitive data. Some important uses of blockchain technology for data integrity assurance are as follows:

- **Supply Chain Management:** Blockchain technology captures actions and transactions, and supply chains retain uncompromised visibility, ranging from initiation to completion. This has the advantage of defending against counterfeiting, ensuring that product information is correct and establishing goodwill among its stakeholders [37][38].
- **Digital Identity Verification:** The use of blockchain-based services provides a decentralised and permanent means of identification. Controlling one's identity in cyberspace and securely sharing information helps reduce instances of identity theft and unauthorised access [39].
- **Financial Transactions:** Cryptocurrencies built on the blockchain, such as Ethereum and Bitcoin, allow for decentralised, auditable, and safe financial transactions. By automating and enforcing transaction rules, smart contracts help decrease fraud and guarantee the accuracy of financial data[40].
- **Healthcare Records:** Electronic health records (EHRs) may be safely stored and managed using blockchain technology [41], which guarantees the privacy and integrity of patient data. Fewer data breaches and better healthcare results are possible because patients may manage their data and authorise healthcare professionals to access it as required[42].

Challenges of Blockchain in Data Integrity

Scalability

The efficiency and speed of a blockchain network could degrade as its transaction volume increases. It is still quite difficult to achieve scalability while keeping security in mind [43].

Energy Consumption

Certain blockchain networks, especially those that use proof-of-work, like Bitcoin, consume a significant amount of electricity. More energy-efficient consensus processes are being sought as a result of this, which has sparked environmental concerns [44].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 6.252
Volume 2, Issue 1, August 2022

Regulatory Hurdles

The decentralised nature of blockchain technology often causes friction with preexisting regulatory systems. Legislation addressing issues with taxes, compliance, and fraud is currently in the works by many governments and agencies [45].

Interoperability

Achieving compatibility across various blockchain networks and existing systems is no easy task. We need these different systems to be able to communicate and transmit data seamlessly for blockchain to be used widely.

Data Privacy

Blockchain offers transparency, but it also has the potential to make sensitive data accessible to a large audience. The difficulty of balancing openness and data privacy is one that organisations must face [46].

Smart Contract Vulnerabilities

Smart contracts, which are decentralised agreements that run on the blockchain, might have vulnerabilities. The security of these agreements must be ensured.

V. BLOCKCHAIN-BASED VOTING FRAMEWORKS (DECENTRALIZED VOTING SYSTEM)

Numerous security and administrative concerns have prevented online voting systems using electronic voting gear from gaining unwavering confidence despite their widespread usage in certain nations. One widely held belief is that the much-discussed trust in electronic voting might be significantly enhanced by incorporating blockchain technology into online voting [47][48]. A growing body of literature suggests that blockchain technology might revolutionise online voting. In addition to allowing voters to modify their votes (within the allotted time), it provides a small degree of decentralisation.

Using biometric information encoded by the Message-digest version 5 (MD5) method to validate the user is one of three modules that make up a decentralised e-voting system that uses blockchain for elections (see Figure 2). Elections using dynamic ballot loading take into account voters' actual locations while casting their ballots. The voter is acknowledged with a vote ID after casting their ballot. To cast an eligible vote and pay the associated costs, voters must provide the Election Authority (EA) with their public key. The EA will then provide an address to receive the automatically generated Bitcoin. In addition, the EA's own bitcoin address is used for publishing results. It is necessary for both voters and candidates to register with the Registration Authority (RA) so that an identification number may be generated for each[49]. There is no way to cast a second, third, or even fourth vote since the voting costs for the Bitcoin address for voters are immediately zero.

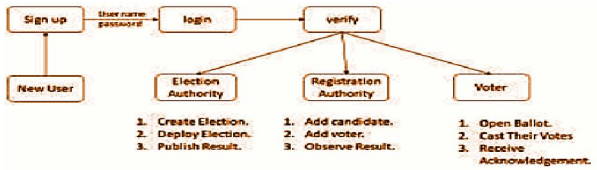

Fig. 1. Decentralized e-voting system flow diagram

An use of a centralised third party has been key to many electronic voting protocols, which has made the implementation and operation of these systems much easier. However, there are also disadvantages to utilising a centralised trusted party since it might make the whole system more susceptible [13]. Therefore, it is safe to employ a decentralised electronic voting protocol that offers a flexible and safe voting process that reduces the authority of an election organiser. Blind signatures and blockchain are the two primary methods utilised to protect voters' selections. Voters, organisers, and inspectors are the three groups of participants in decentralised electronic voting systems.

- A group of voters who are qualified to cast ballots are included in the voters.
- To the voters, the organiser is the official individual to deal with and responsible for confirmation of the eligible voters and their details.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 6.252
Volume 2, Issue 1, August 2022

- It is the responsibility of inspectors to engage with voters and check and restrict the organiser's authority. As e-voting becomes increasingly decentralised, it is preferable to have many inspectors.

VI. LITERATURE REVIEW

Blockchain technology has been hailed as a game-changer in the field of voting systems among the breakthroughs created in the last 10 years. Voting and counting might be conducted in a manner that is secure and easily auditable. A few earlier studies are as follows:

This study, Bhattacharya, Zavarsky and Butakov (2020) explored potential situations where personal data may be exposed via the exchange of credentials across these identities, as well as the dangers of man-in-the-middle attacks inside the Hyperledger Indy blockchain-based identification system. A study suggests a following improvements based on the results: 1) A novel approach to assessing the sensitivity of attributes communicated in credential exchanges employing autonomous identity agents 2) A strategy for protecting peer self-sovereign identities against man-in-the-middle attacks and 3) Here we provide a novel quantitative approach to determining an issuer's overall confidence level score by looking at their reputation and the amount of credentials they issued within a certain time frame [50].

This paper, Al Barghuthi et al. (2019) unveiling a blockchain-based prototype for the UAE' electronic voting system. Blockchain uses distributed and immutable databases as the fundamental components that manage distributed data storage and delivery to all the related users in the network. Among the many possible uses for its numerous advantages are electronic voting systems. To keep election expenses down and voter confidence high, use the blockchain-based electronic voting system. By requiring users to verify their identity before casting a ballot, it has the ability to reduce instances of voter fraud while also making all ballots trackable and verifiable[39].

In this paper, Liang et al. (2019) suggest a novel security architecture that relies on distributed ledger technology to strengthen the capacity of contemporary power systems to defend themselves against cyberattacks. They provide an in-depth analysis of how smart meters may be integrated into a distributed network that stores meter readings as blocks, so strengthening the reliability and safety of the power grid. Simulation studies on the IEEE-118 benchmark system show that the suggested protection architecture is effective [51].

This paper, Kost'Al et al. (2019) provide a blockchain-based electronic voting platform suitable for all types of votes. Utilising it to its fullest potential, blockchain allows for the management of all processes inside. Once voting has begun, the platform acts autonomously and decentrally, removing any possibility of interference. Voters' identities are protected by homomorphic encryption, but the data are completely visible. Our system has been thoroughly tested and evaluated across three distinct blockchains. The findings demonstrate that there is minimal difference in speed between using public and private blockchains. The main innovation of our system is the use of blockchain technology to operate the e-voting platform in a completely decentralised manner, transparency throughout the whole process, and homomorphic encryption to protect voter security and privacy[52].

This paper, Patidar and Jain (2019) suggests a blockchain-based electronic voting system that might solve some of the problems with current voting processes. Additionally, the paper presents the stance of certain blockchain frameworks with regard to electronic voting. For smaller-scale elections that take place in settings like boardrooms and corporate offices, the proposed implementation is suitable. The implementation makes advantage of Ethereum's smart contract. This article develops, tests, and implements smart contracts using the Truffle framework. As an Ethereum client, Ganache is used for testing purposes. This is when Meta-mask becomes the browser's wallet [53].

In this paper, Rawat and Alshaikhi (2018) intend to set up VWNs using a distributed blockchain, additionally known as a public ledger, where PWROs sublease their wireless resources (like infrastructure or a portion of RF spectrum) to MVNOs via machine-to-machine communication, in compliance with the SLAs between the two parties. Participating PWROs and MVNOs are protected by the proposed distributed Blockchain-based method, which also aids MVNOs in meeting customer QoS standards and inhibits PWROs from overcommitting resources (thus stopping double spending). This basically aids customers in satisfying their preferred quality of service criteria while also meeting the standards set by the government. Numerical findings are used to assess performance [54].

In this paper, Le et al. (2018) To improve the acquired evidence's integrity, validity, and non-repudiation qualities, we suggest a permissioned blockchain-based IoT forensics system. Our formal definition of the system architecture includes providing specifics about the framework and proposing a cryptographic-based strategy to address the problem

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 6.252
Volume 2, Issue 1, August 2022

of identity privacy [55].

Table I provides a clear comparison of each paper's contributions, technologies used, proposed solutions, and their specific applications. It should help shed light on where many fields' blockchain-based security system research is right now.

Table 1: Summary Of Background Study On Blockchain Solutions Across Different Domains

Ref	Contributions	Focus Area	Technologies	Proposed Solutions/	Applications
Bhattacharya, Zavarsky, and Butakov (2020)	Examines risks of man-in-the-middle attacks in Hyperledger Indy blockchain identity system.	Blockchain -Based Identity Systems	Hyperledger Indy, Self-sovereign Identity	1) Attribute Sensitivity Score Model, 2) Mitigation of Man-in-the-Middle Attacks, 3) Quantitative Reputation Model for Issuers	Identity Management
Al Barghuthi et al. (2019)	Proposes a blockchain-based e-voting system for UAE elections to ensure transparency, security, and cost-effectiveness.	Electronic Voting Systems	Blockchain, Decentralized Ledger	Blockchain-based system for voter authentication, traceability, and fraud prevention	Electoral Systems
Liang et al. (2019)	Proposes a blockchain-based protection framework to enhance the cybersecurity of power systems against cyber-attacks.	Cybersecurity for Power Systems	Blockchain, Distributed Network, Power Grid	Blockchain-based system for secure data transmission between meters and protection against cyber-attacks	Power Systems Cybersecurity
Kost'Al et al. (2019)	Presents a fully decentralised blockchain-based e-voting platform	E-Voting Platform	Blockchain, Homomorphic Encryption	1) Decentralized e-voting management, 2) Transparency of voting process, 3) Voter privacy via encryption	Electoral Systems
Patidar and Jain (2019)	Blockchain-based e-voting system for small-scale elections using Ethereum and smart contracts.	Small-Scale E-Voting	Blockchain (Ethereum), Truffle Framework, Ganache, Meta-mask	Ethereum smart contracts, Truffle for development, Meta-mask for wallet management	Corporate or Small-Scale Elections
Rawat and Alshaikhi (2018)	Proposes a distributed blockchain-based scheme for wireless virtual networks (VWNs) to secure wireless resource allocation.	Wireless Resource Management	Blockchain, Machine-to-Machine Communication	Blockchain-based scheme to secure resource allocation and prevent over-commitment by resource owners	Wireless Networks (Spectrum Management)
Le et al. (2018)	permissioned blockchain-based IoT forensics framework to ensure integrity, authenticity, and non-repudiation of IoT evidence.	IoT Forensics and Evidence Integrity	Blockchain, Cryptographic Techniques	1) Blockchain framework for IoT forensics, 2) Cryptographic approach to mitigate identity privacy concerns	IoT Forensics

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 6.252
Volume 2, Issue 1, August 2022

VII. CONCLUSION AND FUTURE WORK

The security of blockchain is driving its fast development in many fields. Internet security is becoming among the most important basic issues. Blockchain technology offers a fresh approach to strengthening the safety of apps running on networks. Decentralised voting systems stand to benefit tremendously from blockchain technology's revolutionary capacity to increase data integrity, transparency, and security. Its decentralised nature ensures tamper-proof records, mitigating the risks of fraud and manipulation in elections. Blockchain, with its smart contracts and cryptographic security, removes middlemen, which increases confidence among participants and verifies the legitimacy of the voting process. Full effectiveness and widespread use of blockchain-based voting systems are contingent upon resolving issues with scalability, energy consumption, data privacy, and regulatory considerations. To ensure future elections are conducted on a secure, efficient, and transparent platform, more study is necessary to refine the integration of blockchain technology into voting systems. The integration of blockchain could ultimately transform electoral processes, offering a more reliable and democratic alternative to traditional voting methods.

REFERENCES

[1] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *Int. J. Prod. Res.*, 2019, doi: 10.1080/00207543.2018.1533261.

[2] M. Gopalsamy, "Advanced Cybersecurity in Cloud Via Employing AI Techniques for Effective Intrusion Detection," *Int. J. Res. Anal. Rev.*, vol. 8, no. 1, 2021.

[3] M. Z. Hasan, R. Fink, M. R. Suyambu, M. K. Baskaran, D. James, and J. Gamboa, "Performance evaluation of energy efficient intelligent elevator controllers," in *IEEE International Conference on Electro Information Technology*, 2015. doi: 10.1109/EIT.2015.7293320.

[4] U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system—review and open research challenges," 2021. doi: 10.3390/s21175874.

[5] M. R. Kishore Mullangi, Vamsi Krishna Yarlagadda, Niravkumar Dhameliya, "Integrating AI and Reciprocal Symmetry in Financial Management: A Pathway to Enhanced Decision-Making," *Int. J. Reciprocal Symmetry Theor. Phys.*, vol. 5, no. 1, pp. 42–52, 2018.

[6] A. Dhillon, G. Kotsialou, P. McBurney, and L. Riley, "Voting over a distributed ledger: An interdisciplinary perspective," 2021. doi: 10.1561/0700000071.

[7] T. Ali Syed, A. Alzahrani, S. Jan, M. S. Siddiqui, A. Nadeem, and T. Alghamdi, "A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations," *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2957660.

[8] V. V. Kumar, F. W. Liou, S. N. Balakrishnan, and V. Kumar, "Economical impact of RFID implementation in remanufacturing: a Chaos-based Interactive Artificial Bee Colony approach," *J. Intell. Manuf.*, vol. 26, no. 4, pp. 815–830, Aug. 2015, doi: 10.1007/s10845-013-0836-9.

[9] S. Meunier, "Blockchain 101: What is Blockchain and How Does This Revolutionary Technology Work?. What is Blockchain and How Does This Revolutionary Technology Work?," in *Transforming Climate Finance and Green Investment with Blockchains*, 2018. doi: 10.1016/B978-0-12-814447-3.00003-3.

[10] M. Iansiti and K. R. Lakhani, "The truth about blockchain," 2017.

[11] S. K. R. Anumandla, V. K. Yarlagadda, S. C. R. Vennapusa, and K. R. V Kothapalli, "Unveiling the Influence of Artificial Intelligence on Resource Management and Sustainable Development: A Comprehensive Investigation," *Technol. \& Manag. Rev.*, vol. 5, no. 1, pp. 45–65, 2020.

[12] M. L. Marsal-Llacuna, "Future living framework: Is blockchain the next enabling network?," *Technol. Forecast. Soc. Change*, 2018, doi: 10.1016/j.techfore.2017.12.005.

[13] M. Z. Hasan, R. Fink, M. R. Suyambu, and M. K. Baskaran, "Assessment and improvement of intelligent controllers for elevator energy efficiency," in *IEEE International Conference on Electro Information Technology*, 2012. doi: 10.1109/EIT.2012.6220727.

[14] Ramesh Bishukarma, "Scalable Zero-Trust Architectures for Enhancing Security in Multi-Cloud SaaS Platforms," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 3, pp. 1308–1319, Jul. 2023, doi: 10.48175/IJARSCT-14000S.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 6.252
Volume 2, Issue 1, August 2022

[15] N. G. Singh, Abhinav Parashar A, "Streamlining Purchase Requisitions and Orders : A Guide to Effective Goods Receipt Management," *J. Emerg. Technol. Innov. Res.*, vol. 8, no. 5, 2021.

[16] V. V. Kumar and F. T. S. Chan, "A superiority search and optimisation algorithm to solve RFID and an environmental factor embedded closed loop logistics model," *Int. J. Prod. Res.*, 2011, doi: 10.1080/00207543.2010.503201.

[17] R. Arora, S. Gera, and M. Saxena, "Mitigating security risks on privacy of sensitive data used in cloud-based ERP applications," in *Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development, INDIACom 2021*, 2021. doi: 10.1109/INDIACom51348.2021.00081.

[18] V. Kumar, V. V. Kumar, N. Mishra, F. T. S. Chan, and B. Gnanasekar, "Warranty failure analysis in service supply Chain a multi-agent framework," in *SCMIS 2010 - Proceedings of 2010 8th International Conference on Supply Chain Management and Information Systems: Logistics Systems and Engineering*, 2010.

[19] R. A. Anoop Kumar, Ramakrishna Garine, Arpita Soni, "Leveraging AI for E-Commerce Personalization : Insights and Challenges from 2020," pp. 1–6, 2020.

[20] S. Bauskar and S. Clarita, "AN ANALYSIS: EARLY DIAGNOSIS AND CLASSIFICATION OF PARKINSON'S DISEASE USING MACHINE LEARNING TECHNIQUES," *Int. J. Comput. Eng. Technol.*, vol. 12, no. 01, pp. 54-66., 2021, doi: 10.5281/zenodo.13836264.

[21] S. K. R. A. Sai Charan Reddy Vennapusa, Takudzwa Fadziso, Dipakkumar Kanubhai Sachani, Vamsi Krishna Yarlagadda, "Cryptocurrency-Based Loyalty Programs for Enhanced Customer Engagement," *Technol. Manag. Rev.*, vol. 3, no. 1, pp. 46–62, 2018.

[22] M. A. Shajahan, N. Richardson, N. Dhameliya, B. Patel, S. K. R. Anumandla, and V. K. Yarlagadda, "AUTOSAR Classic vs. AUTOSAR Adaptive: A Comparative Analysis in Stack Development," *Eng. Int.*, vol. 7, no. 2, pp. 161–178, Dec. 2019, doi: 10.18034/ei.v7i2.711.

[23] R. Goyal, "THE ROLE OF REQUIREMENT GATHERING IN AGILE SOFTWARE DEVELOPMENT: STRATEGIES FOR SUCCESS AND CHALLENGES," *Int. J. Core Eng. Manag.*, vol. 6, no. 12, pp. 142–152, 2021.

[24] D. J. Ghode, R. Jain, G. Soni, S. K. Singh, and V. Yadav, "Architecture to enhance transparency in supply chain management using blockchain technology," in *Procedia Manufacturing*, 2020. doi: 10.1016/j.promfg.2020.10.225.

[25] V. K. Yarlagadda and R. Pydipalli, "Secure Programming with SAS: Mitigating Risks and Protecting Data Integrity," *Eng. Int.*, vol. 6, no. 2, pp. 211–222, Dec. 2018, doi: 10.18034/ei.v6i2.709.

[26] S. G. Thomas Jubin, Kirti Vinod Vedi, "Enhancing Supply Chain Resilience Through Cloud-Based SCM and Advanced Machine Learning: A Case Study of Logistics," *J. Emerg. Technol. Innov. Res.*, vol. 8, no. 9, 2021.

[27] A. S. Ramakrishna Garine, Rajeev Arora, Anoop Kumar, "Advanced Machine Learning for Analyzing and Mitigating Global Supply Chain Disruptions during COVID-19," *Available SSRN 4937475*, pp. 1–6, 2020.

[28] V. V Kumar, M. Tripathi, S. K. Tyagi, S. K. Shukla, and M. K. Tiwari, "An integrated real time optimization approach (IRTO) for physical programming based redundancy allocation problem," *Proc. 3rd Int. Conf. Reliab. Saf. ...*, 2007.

[29] V. V. Kumar, M. K. Pandey, M. K. Tiwari, and D. Ben-Arieh, "Simultaneous optimization of parts and operations sequences in SSMS: A chaos embedded Taguchi particle swarm optimization approach," *J. Intell. Manuf.*, 2010, doi: 10.1007/s10845-008-0175-4.

[30] B. Boddu, "Serverless Databases Are the Future of Database Management," *https://jsaer.com/download/vol-6-iss-1-2019/JSAER2019-6-1-277-282.pdf*, vol. 6, no. 1, p. 5, 2020.

[31] M. S. Rajeev Arora, Sheetal Gera, "Impact of Cloud Computing Services and Application in Healthcare Sector and to provide improved quality patient care," *IEEE Int. Conf. Cloud Comput. Emerg. Mark. (CCEM), NJ, USA, 2021*, pp. 45–47, 2021.

[32] J. R. Sunkara, S. Bauskar, C. Madhavaram, E. P. Galla, and H. K. Gollangi, "Data-Driven Management: The Impact of Visualization Tools on Business Performance," *https//iaeme.com/Home/journal/IJM 1290 Ed. Int. J. Manag.*, vol. 12, no. 3, pp. 1290–1298, 2021.

[33] X. Wang, "Research on data integrity verification technology based on blockchain," in *Journal of Physics:*

Conference Series, 2021. doi: 10.1088/1742-6596/2035/1/012017.

[34] N. Richardson, R. Pydipalli, S. S. Maddula, S. K. R. Anumandla, and V. K. Yarlagadda, "Role-Based Access Control in SAS Programming: Enhancing Security and Authorization," *Int. J. Reciprocal Symmetry Theor. Phys.*, 2019.

[35] Y. Gajmal and R. Udayakumar, "A Bibliometric Analysis of Authentication based Access Control in Cloud using Blockchain," *Libr. Philos. Pract.*, 2021.

[36] B. Boddu, "Data Governance and Quality in Data Warehousing and Business Intelligence," *https://www.ijfmr.com/research-paper.php?id=10876*, vol. 3, no. 6, p. 8, 2021.

[37] W. Lin *et al.*, "Blockchain Technology in Current Agricultural Systems: From Techniques to Applications," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3014522.

[38] S. G. Jubin Thomas, Kirti Vinod Vedi, "The Effect and Challenges of the Internet of Things (IoT) on the Management of Supply Chains," *Int. J. Res. Anal. Rev*, vol. 8, no. 3, pp. 874–878, 2021.

[39] N. B. Al Barghuthi *et al.*, "An Analytical View on Political Voting System using Blockchain Technology-UAE Case Study," in *ITT 2019 - Information Technology Trends: Emerging Technologies Blockchain and IoT*, 2019. doi: 10.1109/ITT48889.2019.9075074.

[40] P. C. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, "Blockchain data-based cloud data integrity protection mechanism," *Futur. Gener. Comput. Syst.*, 2020, doi: 10.1016/j.future.2019.09.028.

[41] S. Pandya, "Predictive Analytics in Smart Grids : Leveraging Machine Learning for Renewable Energy Sources," *Int. J. Curr. Eng. Technol.*, vol. 11, no. 6, pp. 677–683, 2021, doi: https://doi.org/10.14741/ijcet/v.11.6.12.

[42] V. K. Yarlagadda, "Harnessing Biomedical Signals: A Modern Fusion of Hadoop Infrastructure, AI, and Fuzzy Logic in Healthcare," vol. 8, 2021.

[43] V. V Kumar, M. Tripathi, M. K. Pandey, and M. K. Tiwari, "Physical programming and conjoint analysis-based redundancy allocation in multistate systems: A Taguchi embedded algorithm selection and control (TAS&C) approach," *Proc. Inst. Mech. Eng. Part O J. Risk Reliab.*, vol. 223, no. 3, pp. 215–232, Sep. 2009, doi: 10.1243/1748006XJRR210.

[44] R. Bishukarma, "The Role of AI in Automated Testing and Monitoring in SaaS Environments," *Int. J. Res. Anal. Rev.*, vol. 8, no. 2, pp. 846–851, 2021.

[45] Rajesh Goyal, "THE ROLE OF BUSINESS ANALYSTS IN INFORMATION MANAGEMENT PROJECTS," *Int. J. Core Eng. Manag.*, vol. 6, no. 9, 2020.

[46] V. N. Boddapati, E. P. Galla, J. R. Sunkara, S. Bauskar, and R. Madhavaram, "Harnessing the Power of Big Data: The Evolution of AI and Machine Learning in Modern Times," *ESP J. Eng. Technol. Adv.*, vol. 1, pp. 134–146, 2021, doi: 10.56472/25832646/JETA-V1I2P116.

[47] G. Han, Y. Li, Y. Yu, K. K. R. Choo, and N. Guizani, "Blockchain-based self-tallying voting system with software updates in decentralized IoT," *IEEE Netw.*, 2020, doi: 10.1109/MNET.001.1900439.

[48] B. Boddu, "The Quantum Edge: How Quantum Computing Will Transform Databases," *https://www.ijirmps.org/research-paper.php?id=231462*, vol. 9, no. 3, p. 5, 2021.

[49] K. Patel, "Quality Assurance In The Age Of Data Analytics: Innovations And Challenges," *Int. J. Creat. Res. Thoughts*, vol. 9, no. 12, pp. f573–f578, 2021.

[50] M. P. Bhattacharya, P. Zavarsky, and S. Butakov, "Enhancing the security and privacy of self-sovereign identities on hyperledger indy blockchain," in *2020 International Symposium on Networks, Computers and Communications, ISNCC 2020*, 2020. doi: 10.1109/ISNCC49221.2020.9297357.

[51] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed Blockchain-Based Data Protection Framework for Modern Power Systems Against Cyber Attacks," *IEEE Trans. Smart Grid*, 2019, doi: 10.1109/TSG.2018.2819663.

[52] K. Kost'Al, R. Bencel, M. Ries, and I. Kotuliak, "Blockchain e-voting done right: Privacy and transparency with public blockchain," in *Proceedings of the IEEE International Conference on Software Engineering and Service Sciences, ICSESS*, 2019. doi: 10.1109/ICSESS47205.2019.9040770.

[53] K. Patidar and S. Jain, "Decentralized E-Voting Portal Using Blockchain," in *2019 10th International*

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 6.252
Volume 2, Issue 1, August 2022

Conference on Computing, Communication and Networking Technologies, ICCCNT 2019, 2019. doi: 10.1109/ICCCNT45670.2019.8944820.

[54] D. B. Rawat and A. Alshaikhi, "Leveraging Distributed Blockchain-based Scheme for Wireless Network Virtualization with Security and QoS Constraints," in *2018 International Conference on Computing, Networking and Communications, ICNC 2018*, 2018. doi: 10.1109/ICCNC.2018.8390344.

[55] D. P. Le, H. Meng, L. Su, S. L. Yeo, and V. Thing, "BIFF: A Blockchain-based IoT Forensics Framework with Identity Privacy," in *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, 2018. doi: 10.1109/TENCON.2018.8650434.