International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Decentralized and Trustworthy Connectivity in IoT through Blockchain-Enabled Secure Data Sharing over Wireless Networks

Dr. K Seshadri Ramana[1], Dr. Veera Talukdar[2,*], Manisha Mittal[3], Elangovan Muniyandy[4], V V S Sasank[5], Amit Verma[6], Dharmesh Dhabliya[7]

Submitted: 06/02/2024 **Revised**: 14/03/2024 **Accepted**: 20/03/2024

Abstract: The proliferation of Internet of Things (IoT) devices has led to an exponential increase in data generated and shared over wireless networks, posing significant challenges in terms of security, privacy, and trustworthiness. This paper proposes a novel approach to address these challenges by leveraging blockchain technology for secure data sharing in IoT ecosystems. By decentralizing data storage and enabling tamper-resistant transaction records, blockchain provides a robust framework for ensuring the integrity, confidentiality, and accountability of IoT data. This paper outlines the key principles and mechanisms underlying blockchain-enabled secure data sharing in IoT networks, including cryptographic techniques, consensus algorithms, and smart contracts. Furthermore, it discusses the potential benefits and challenges of adopting blockchain in IoT deployments, as well as future research directions to overcome existing limitations and realize the full potential of decentralized and trustworthy connectivity in IoT environments.

Keywords: *IoT , Blockchain, secure data sharing, Wireless network, Machine learning, decentralization*

1. Introduction

Numerous sectors, ranging from healthcare to manufacturing, have been revolutionized as a result of the spread of Internet of Things (IoT) devices for secure data sharing. These devices have enabled networked systems that collect and share data in real time. On the other hand, this expanded connectedness brings with it a greater danger of security breaches, data manipulation, and privacy violations. When it comes to efficiently addressing these difficulties, traditional centralized ways to safeguarding industrial Internet of Things networks often suffer. The technology known as blockchain, which was first designed as the foundational framework for cryptocurrencies, has recently emerged as a potentially useful solution for improving the security, integrity, and trustworthiness of data that is transferred over Internet of Things networks. A solid basis for maintaining the confidentiality, integrity, and accountability of Internet of Things (IoT) data is provided by blockchain technology. This is accomplished via the decentralization of data storage and the facilitation of tamper-resistant transaction records. The idea of decentralized and trustworthy connection in the Internet of Things (IoT) is investigated in this article via the use of blockchain technology to allow safe data exchange across wireless networks. An outline of the fundamental ideas and procedures that underpin blockchain technology and its implementation in Internet of Things contexts is presented at the beginning of the article. Subsequently, it illustrates the potential advantages of implementing blockchain-based solutions and explores the constraints and limits of current centralized methods to Internet of Things (IoT) security. In addition, the article goes into the technical elements of blockchain-enabled safe data sharing in Internet of Things networks. These aspects include cryptographic approaches, consensus algorithms, and smart contracts. This paper investigates the ways in which these methods may be used to construct secure communication channels, authenticate devices, and implement access control rules in decentralized Internet of Things ecosystems. Real-world use cases and applications of blockchain technology in the Internet of Things are discussed in the paper.

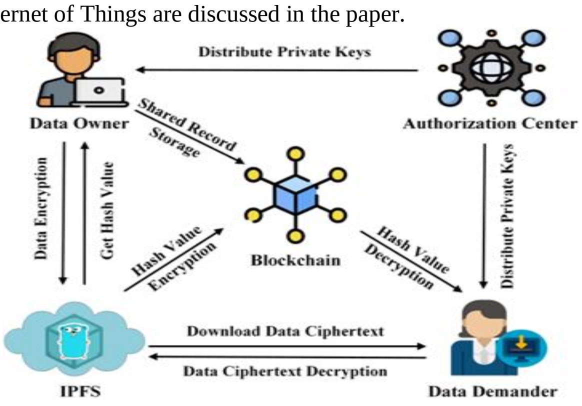

Fig 1. Precision Farming and Crop management [13]

These applications and use cases range from supply chain management to smart cities and autonomous cars. It investigates

[1]Professor, Department of Computer Science and Engineering, Ravindra College of Engineering for Women, Kurnool, Andhra Pradesh, India Email: ramana.kothapalli@gmail.com
[2]Professor, Department of Computer Science, D Y Patil International University, Akurdi Pune, Maharashtra, India Email: bhaskarveera95@gmail.com
[3]Associate Professor, Department of Electronics and Communication Engineering, Guru Tegh Bahadur Institute of Technology, GGSIPU, New Delhi, India Email: manumanisha22@gmail.com
[4]Department of Biosciences, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India Email: muniyandy.e@gmail.com
[5]Assistant Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India Email: sasank64@gmail.com
[6]University Centre for Research and Development, Chandigarh University, Gharuan Mohali, Punjab, India Email: amit.e9679@cumail.in
[7]Professor, Department of Information Technology, Vishwakarma Institute of Information Technology, Pune, Maharashtra, India Email: dharmesh.dhabliya@viit.ac.in
[*]Corresponding Author: - Dr. Veera Talukdar (bhaskarveera95@gmail.com)

the ways in which blockchain technology might allow new business models, improve transparency, and safeguard the exchange of data across a variety of businesses that are enabled by the Internet of Things. Purpose of this study is to provide the groundwork for a more in-depth investigation into the decentralized and trustworthy connection of the Internet of Things (IoT) via the use of blockchain technology to allow safe data exchange across wireless networks.

Through the use of the inherent characteristics of blockchain technology, enterprises have the capacity to improve the security, privacy, and dependability of Internet of Things deployments, therefore paving the path for a digital future that is both more linked and safe.

2. Evaluation of IoT devices with blockchain technology

The historical evolution of decentralized and trustworthy connectivity in IoT through blockchain-enabled secure data sharing over wireless networks can be traced through several key stages:

1. Early Adoption of IoT Devices:

The early 2000s saw the emergence of Internet of Things (IoT) devices, including sensors, actuators, and smart devices, capable of gathering and transmitting data over wireless networks. These devices revolutionized various industries, from healthcare to agriculture, by enabling real-time monitoring, automation, and optimization of processes.

2. Rise of Blockchain Technology:

In 2008, Bitcoin was introduced as the first decentralized cryptocurrency, utilizing blockchain technology to enable secure and transparent transactions without the need for intermediaries. The underlying principles of blockchain, including decentralization, cryptographic security, and immutability, laid the foundation for enhancing trust and transparency in digital transactions.

3. Integration of Blockchain with IoT:

Recognizing the potential synergies between blockchain and IoT, researchers and industry practitioners began exploring ways to integrate blockchain technology into IoT deployments. Blockchain offered a decentralized and tamper-resistant framework for securing IoT data, transactions, and communication channels, addressing key security and trust challenges inherent in centralized IoT architectures.

4. Proof of Concept and Early Implementations:

In the mid-2010s, proof of concept projects and early implementations of blockchain-enabled IoT solutions began to emerge. These projects demonstrated the feasibility of using blockchain for secure data sharing, device authentication, and decentralized control in IoT ecosystems. Examples include supply chain tracking, energy management, and smart city initiatives leveraging blockchain technology.

5. Emergence of Blockchain Platforms and Protocols:

With the growing interest in blockchain-enabled IoT applications, various blockchain platforms and protocols tailored for IoT use cases started to emerge. Platforms like Ethereum, Hyperledger, and IOTA offered features such as smart contracts, permissioned blockchains, and feeless transactions, catering to the diverse needs of IoT deployments.

6. Standardization Efforts and Consortia:

Standardization bodies and industry consortia, such as the Industrial Internet Consortium (IIC) and the Trusted IoT Alliance, played a pivotal role in driving the adoption of blockchain-enabled IoT standards and best practices. These efforts aimed to promote interoperability, security, and scalability in blockchain-enabled IoT deployments, fostering collaboration among stakeholders across different sectors.

7. Maturation and Diversification of Use Cases:

In recent years, blockchain-enabled IoT deployments have matured and diversified across various industries and domains. Use cases span supply chain management, healthcare, energy, transportation, agriculture, and environmental monitoring, among others. These deployments leverage blockchain technology to enhance data integrity, provenance, and security in IoT ecosystems, enabling new business models and value propositions.

8. Ongoing Research and Innovation:

Research and innovation in blockchain-enabled IoT continue to evolve, addressing challenges such as scalability, interoperability, privacy, and energy efficiency. Emerging technologies such as sharding, sidechains, zero-knowledge proofs, and consensus algorithms aim to improve the performance and resilience of blockchain-enabled IoT networks, paving the way for broader adoption and impact in the future.

In conclusion, the historical evolution of decentralized and trustworthy connectivity in IoT through blockchain-enabled secure data sharing over wireless networks reflects a convergence of technological advancements, industry collaborations, and evolving use cases. By leveraging the combined strengths of blockchain and IoT, organizations can unlock new possibilities for secure, transparent, and decentralized data exchange in the digital age.

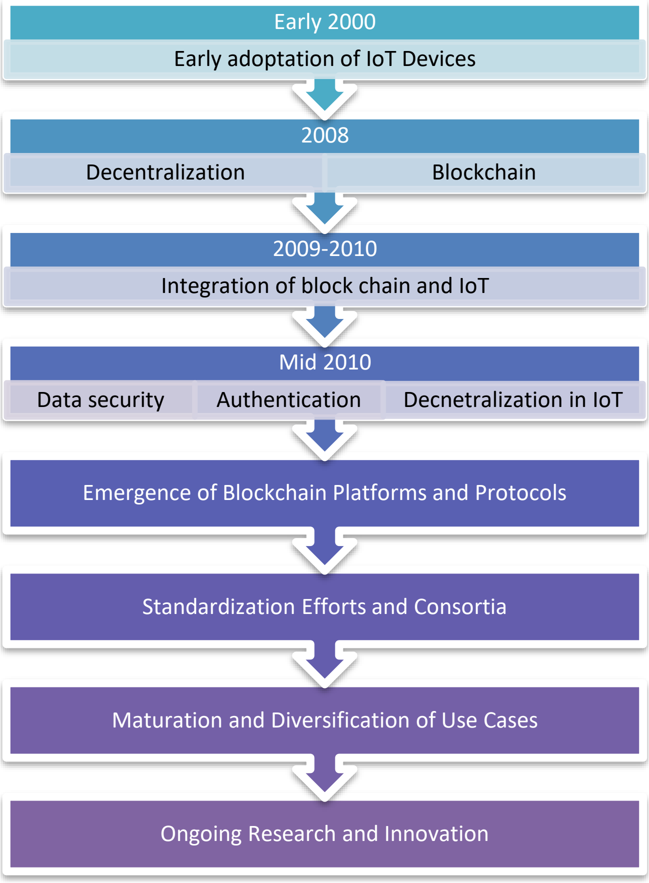
Early 2000
Early adoptation of IoT Devices
2008
Decentralization
Blockchain
2009-2010
Integration of block chain and IoT
Mid 2010
Data security
Authentication
Decnetralization in IoT
Emergence of Blockchain Platforms and Protocols
Standardization Efforts and Consortia
Maturation and Diversification of Use Cases
Ongoing Research and Innovation

Fig 2. Historical Evolution

3. Literature review

The work that was done on blockchain based NFT Culture by Gupta, M., and others was given as a proposal for the new age [1]. Here NFT are secured digitally over blockchain and could be used in IoT based ecosystem when required. M. Gupta has examined the connection between blockchain technology and non-fungible tokens (NFT) from the perspective of well-known NFT market places [2]. Study of web 3.0 environment has been conducted where web application authenticates user considering status of NFT holding in digital wallet. D. Gupta et al. [4] focused on exploring the function of blockchain in developing greetings valuable by making use of blockchain technology, while R. Gupta studied the role of liquidity pool in stabilizing the value of tokens [3]. Role of blockchain based smart contract has been considered in greeting people on IoT platform [4]. R. Issalh [5] described the PI network revolution as well as the NFT that is associated with it. An investigation was carried out by A. Duggal in order to demonstrate the relevance of NFT avatars in the metaverse that could be used for authentication in IoT environment, and a case study was conducted on the subject [6]. M. Gupta [7] conducted research in the field of finance in order to argue that there should be no speculation in the cryptocurrency market during NFT exchanges or transactions conduction in decentralized manner for data security.The influence that the Bitcoin halving has had on the cryptocurrency market was explored by A. Singla [8].Researchers I.Gupta and P. Jain[9] conducted study on the anticipated effects of decentralization via the use of technologies based on blockchain. World-famous NFT Scripts were investigated by D. Gupta and S. Gupta throughout their research. There is a paper that was written by M. Gupta [11] to show the integration of Blockchain technology with the Internet of Things for user authentication.

4. Problem statement

Decentralized and trustworthy connectivity in IoT through blockchain-enabled secure data sharing over wireless networks faces several issues and challenges:

1. Scalability: When it comes to transaction throughput and latency, blockchain networks, especially public ones like Ethereum and Bitcoin, have scaling issues. A major obstacle to rapid processing and validation of transactions is scalability, which is exacerbated by the massive volumes of data generated by IoT networks.
2. Network Congestion: High transaction volumes and limited network bandwidth can lead to network congestion and increased transaction fees in blockchain-enabled IoT networks. This congestion can hinder the real-time communication and responsiveness required for IoT applications, particularly in mission-critical scenarios.
3. Interoperability: Achieving interoperability between different blockchain platforms and IoT devices remains a challenge. Lack of standardized protocols and data formats for blockchain integration with IoT devices can hinder seamless communication and data exchange across heterogeneous networks.
4. Security Risks: While decentralisation and cryptography make blockchain technology more secure, it is still susceptible to assaults and flaws. The security and dependability of blockchain-enabled Internet of Things networks are at danger from smart contract vulnerabilities, faults in consensus algorithms, and 51% assaults.
5. Privacy Concerns: Blockchain's transparency and immutability features can raise privacy concerns, particularly in IoT applications where sensitive data is involved.
6. Energy Consumption: All too often, blockchain networks resort to the resource- and energy-intensive Proof-of-Work (PoW) consensus methods. Internet of Things (IoT) devices often have limited computing power and battery life, making PoW consensus an unsustainable option.
7. Regulatory Compliance: Deploying blockchain technology for the Internet of Things (IoT) isn't without its share of legal hurdles, including data protection regulations and industry standards.
8. Adoption Barriers: Despite the potential benefits of blockchain-enabled IoT, adoption barriers such as lack of awareness, expertise, and infrastructure persist. Organizations may hesitate to invest in blockchain technology due to perceived complexity, uncertainty, and the need for specialized skills.
9. Cost and Resource Constraints: There may be substantial initial expenditures and resource commitments required to implement blockchain-enabled Internet of Things solutions. Because of limited resources and manpower, small and medium-sized businesses (SMEs) and other organisations may struggle to use blockchain technology.

Addressing these issues and challenges requires collaboration between stakeholders in the blockchain and IoT ecosystems, as well as ongoing research, innovation, and standardization efforts. By mitigating these challenges, organizations can unlock the full potential of decentralized and trustworthy connectivity in IoT through blockchain-enabled secure data sharing over wireless networks..

5. Research Motivation

The motivation for research on decentralized and trustworthy connectivity in IoT through blockchain-enabled secure data sharing over wireless networks stems from several key factors:

1. Security Concerns in IoT: Significant security issues, such as data breaches, device tampering, and unauthorised access, have emerged due to the growth of Internet of Things (IoT) devices. Innovative solutions are needed to improve the security and integrity of IoT data, as traditional centralised techniques are vulnerable to cyber assaults and single points of failure.
2. Need for Decentralization and Trust: Centralized architectures pose risks in terms of data privacy, trustworthiness, and resilience. Decentralized approaches, enabled by blockchain technology, offer a promising alternative by distributing data storage and control among network participants, thereby reducing vulnerabilities and enhancing trust in IoT ecosystems.
3. Data Privacy and Ownership: IoT devices generate vast amounts of sensitive data, raising concerns about privacy, ownership, and control over personal information. Blockchain's immutable ledger and cryptographic security features provide a transparent and tamper-resistant framework for ensuring data privacy, ownership rights, and auditability in IoT data sharing scenarios.
4. Transparency and Accountability: Blockchain's transparency and auditability features promote accountability and transparency in IoT data transactions. By recording transactional data on a distributed ledger, blockchain enables verifiable and immutable records of data exchanges, facilitating accountability and dispute resolution in IoT networks.
5. Interoperability and Integration: Integrating diverse IoT devices and platforms in a seamless and interoperable manner remains a challenge. Blockchain-based solutions offer

standardized protocols, smart contracts, and decentralized identifiers (DIDs) for facilitating secure and interoperable communication among heterogeneous IoT devices, enabling seamless integration and collaboration.

6. Regulatory Compliance and Governance: Internet of Things (IoT) installations must adhere to all applicable regulations, including data protection legislation (such as GDPR) and industry standards (such as ISO 270001). With blockchain technology, data transactions can be verified and audited, which helps with regulatory compliance and governance. This technology also ensures that data protection standards are followed.

7. Resilience to Cyber Attacks: IoT networks are vulnerable to various cyber threats, including DDoS attacks, malware infections, and data breaches. Blockchain's distributed and consensus-driven architecture enhances resilience to cyber attacks by eliminating single points of failure, mitigating the risk of data manipulation, and ensuring the integrity and availability of IoT data.

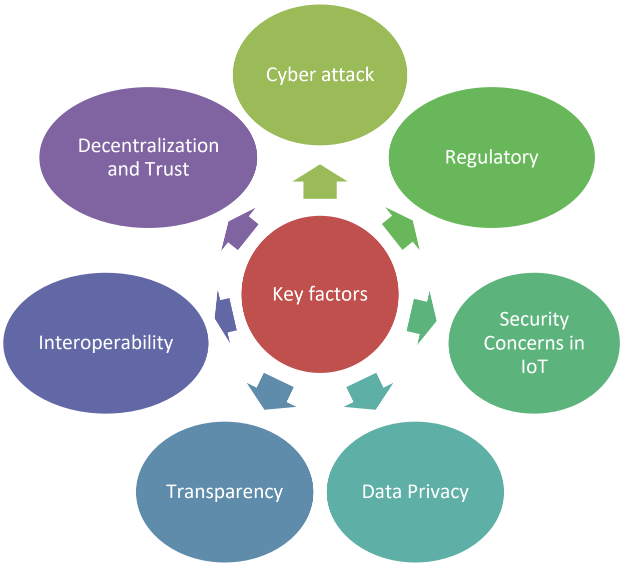

Fig 3 Key factors for motivation

The motivation for research on decentralized and trustworthy connectivity in IoT through blockchain-enabled secure data sharing over wireless networks arises from the pressing need to address security, privacy, interoperability, and regulatory compliance challenges in IoT deployments. By leveraging blockchain technology's decentralized and immutable properties, researchers aim to enhance the security, integrity, and trustworthiness of IoT data sharing, thereby unlocking the full potential of IoT applications in diverse industries.

6. Proposed work

Designing a model for decentralized and trustworthy connectivity in IoT through blockchain-enabled secure data sharing over wireless networks involves several key steps. Below is a process flow outlining these steps:

1. Problem Identification and Requirements Gathering:

- Identify the specific challenges and requirements of decentralized and trustworthy connectivity in IoT deployments.
- Define the objectives, scope, and stakeholders involved in the design process.
- Gather input from domain experts, stakeholders, and end-users to understand their needs and priorities.

2. Literature Review and Research:

- Conduct a comprehensive review of existing literature, research papers, and industry best practices related to blockchain-enabled IoT solutions.
- Explore relevant technologies, protocols, and frameworks for decentralized connectivity, secure data sharing, and wireless communication in IoT environments.
- Identify successful use cases, implementation strategies, and lessons learned from previous deployments.

3. System Architecture Design:

- Design the overall architecture of the decentralized IoT system, incorporating blockchain technology for secure data sharing and wireless communication protocols for connectivity.
- Define the roles and responsibilities of different network participants, including IoT devices, blockchain nodes, and data consumers.
- Determine the components, interfaces, and communication protocols required to facilitate interoperability and integration within the system.

4. Blockchain Selection and Configuration:

- Select a suitable blockchain platform or protocol based on the requirements of the IoT application, considering factors such as scalability, consensus mechanism, and smart contract support.
- Configure the blockchain network parameters, including block size, block interval, consensus algorithm, and network governance model.
- Determine the deployment model (public, private, or consortium blockchain) based on the desired level of decentralization and trust among network participants.

5. Data Model and Smart Contract Development:

- Define the data model for representing IoT data on the blockchain, specifying the structure, format, and metadata associated with each data record.
- Develop smart contracts to govern data sharing, access control, and incentive mechanisms within the blockchain network.
- Implement functions for data validation, authorization, and encryption to ensure the integrity and confidentiality of IoT data stored on the blockchain.

6. Integration with IoT Devices and Gateways:

- Integrate IoT devices and gateways with the blockchain network, enabling secure communication and data exchange over wireless networks.
- Implement communication protocols (e.g., MQTT, CoAP) and cryptographic mechanisms (e.g., SSL/TLS, HMAC) to facilitate secure data transmission between IoT devices and blockchain nodes.
- Configure IoT devices to interact with smart contracts, submit data transactions, and respond to commands and queries from the blockchain network.

7. Testing and Evaluation:

- Conduct comprehensive testing of the decentralized IoT system to validate its functionality, performance, and security.
- Perform unit testing, integration testing, and end-to-end testing to identify and resolve any issues or vulnerabilities.
- Evaluate the system against predefined criteria and metrics,

such as data integrity, latency, scalability, and resource utilization.

8. Deployment and Deployment:
- Deploy the decentralized IoT system in a production environment, considering factors such as scalability, reliability, and availability.
- Configure network nodes, deploy smart contracts, and establish communication channels between IoT devices and blockchain network.
- Monitor system performance, collect feedback from users, and iterate on the design based on real-world usage and experiences.

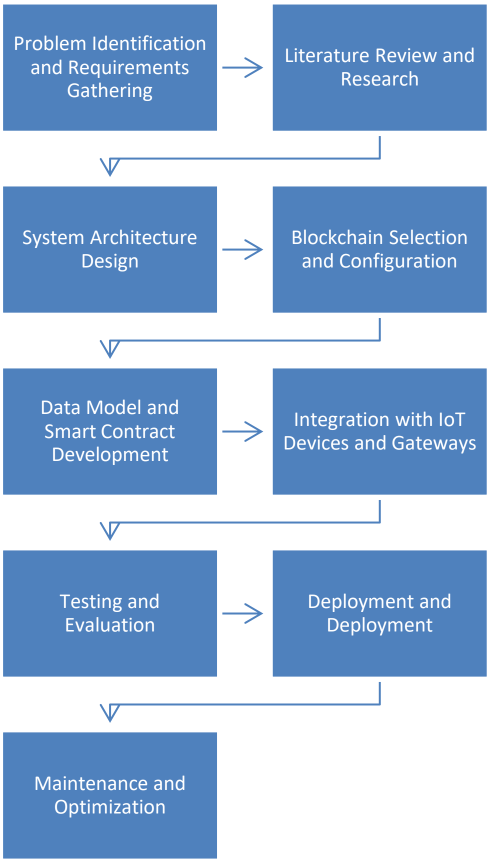
Problem Identification and Requirements Gathering
Literature Review and Research
System Architecture Design
Blockchain Selection and Configuration
Data Model and Smart Contract Development
Integration with IoT Devices and Gateways
Testing and Evaluation
Deployment and Deployment
Maintenance and Optimization

Fig. 4. Process flow of work

9. Maintenance and Optimization:
- Continuously monitor and maintain the decentralized IoT system to ensure its reliability, security, and performance.
- Implement updates, patches, and enhancements to address emerging threats, vulnerabilities, and evolving user requirements.
- Optimize system parameters, configurations, and algorithms to maximize efficiency, scalability, and cost-effectiveness over time.

By following this process flow, "researchers and practitioners can design and implement a model for decentralized and trustworthy connectivity in IoT through blockchain-enabled secure data sharing over wireless networks, addressing key challenges and requirements in IoT deployments.

7. Simulation Results

Simulation of NFT transaction has been made on IoT based decentralized environment to evaluate the failure rate on Core block chain.

7.1. Blockchain based NFT transaction simulation

Confusion matrix obtained in the case of conventional research is shown in Table 1.

Table 1. NFT transaction status for non optimized blockchain

Transaction No	NFT Name	Blockchain	Status
1	NFT GIRL	Core	Success
2	KAIGEN	Core	Success
3	UNIGECKO	Core	Failure
4	NFT GIRL	Core	Success
5	KAIGEN	Core	Success
6	UNIGECKO	Core	Success
7	NFT GIRL	Core	Success
8	KAIGEN	Core	Failure
9	UNIGECKO	Core	Failure
10	NFT GIRL	Core	Success
11	KAIGEN	Core	Success
12	UNIGECKO	Core	Success
13	NFT GIRL	Core	Success
14	KAIGEN	Core	Failure
15	NFT GIRL	Core	Success
16	KAIGEN	Core	Success
17	KAIGEN	Core	Success
18	KAIGEN	Core	Success
19	KAIGEN	Core	Success
20	AVENGERS	Core	Success
21	AVENGERS	Core	Success
22	AVENGERS	Core	Success
23	AVENGERS	Core	Success
24	AVENGERS	Core	Success
25	AVENGERS	Core	Success

It has been observed that in case of standard blockchain success rate of blockchain transaction is
(21 (Successful transaction)/25 (Total Transaction)) *100 = 84%

Where as failure rate is
(4 (Successful transaction)/25 (Total Transaction)) *100 =16%.

Optimized blockchain has been proposed in this work to process the block at rapid rate. It has reduced waiting time of transaction moreover the transaction rate is also improved. Table 2 is resenting NFT transaction status for 25 transactions.

Table 2. NFT transaction status for proposed optimized approach

Transaction No	NFT Name	Blockchain	Status
1	NFT GIRL	Core	Success
2	KAIGEN	Core	Success
3	UNIGECKO	Core	Success
4	NFT GIRL	Core	Success
5	KAIGEN	Core	Success
6	UNIGECKO	Core	Success
7	NFT GIRL	Core	Success
8	KAIGEN	Core	Success
9	UNIGECKO	Core	Failure
10	NFT GIRL	Core	Success
11	KAIGEN	Core	Success
12	UNIGECKO	Core	Success
13	NFT GIRL	Core	Success
14	KAIGEN	Core	Failure
15	NFT GIRL	Core	Success
16	KAIGEN	Core	Success
17	KAIGEN	Core	Success
18	KAIGEN	Core	Success
19	KAIGEN	Core	Success
20	AVENGERS	Core	Success
21	AVENGERS	Core	Success
22	AVENGERS	Core	Success
23	AVENGERS	Core	Success
24	AVENGERS	Core	Success
25	AVENGERS	Core	Success

Thus, improved approach is providing transaction success rate of (23 (Successful transaction)/25 (Total Transaction)) *100 = 92%

Where as failure rate is
(2 (Successful transaction)/25 (Total Transaction)) *100 =8%

Table 3 Comparison of success rate and failure rate is show below

Table 3. NFT transaction status comparison

Approach	Success Rate	Failure rate
Previous	84	16
Proposed	92	8

Considering table 3, success rate is shown below in figure 4

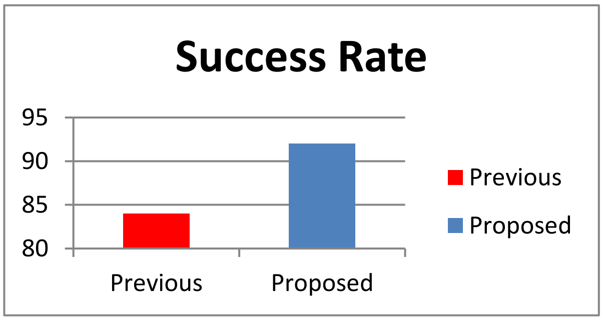

Fig. 5. Comparative analysis of conventional and proposed work to evaluate success rate

Considering table 3, Failure rate comparison is shown in case of conventional and proposed work in following figure

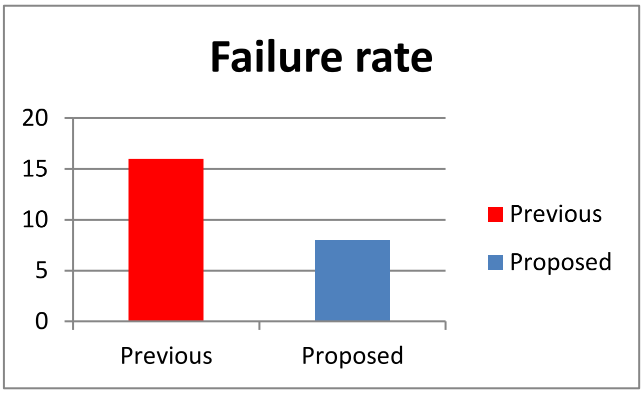

Fig.6. Comparative analysis of conventional and proposed work to evaluate Failure rate

8. Conclusion

In conclusion, the integration of blockchain technology with Internet of Things (IoT) devices holds tremendous promise for achieving decentralized and trustworthy connectivity in IoT deployments, particularly for secure data sharing over wireless networks. This paper has explored the various aspects and implications of this integration, highlighting both its potential benefits and challenges.

1. Benefits of Decentralized Connectivity: Blockchain technology offers a decentralized and tamper-resistant framework for securing IoT data, transactions, and communication channels. By distributing data storage and control among network participants, blockchain enhances the security, privacy, and reliability of IoT ecosystems.

2. Applications and Use Cases: Blockchain-enabled IoT solutions have a wide range of applications across diverse industries, including supply chain management, healthcare, energy, transportation, and smart cities.

3. Challenges and Considerations: Despite its potential, integrating blockchain with IoT poses several challenges, including scalability, interoperability, security, privacy, and regulatory compliance.

4. Future Directions: Future research and development efforts should focus on addressing the scalability, interoperability, and security challenges of blockchain-enabled IoT deployments. Emerging technologies such as sharding, sidechains, zero-knowledge proofs, and consensus algorithms hold promise for improving the performance and resilience of decentralized IoT systems.

5. Conclusion: Decentralized and trustworthy connectivity in IoT through blockchain-enabled secure data sharing over wireless networks represents a significant paradigm shift in how data is managed and exchanged in IoT ecosystems”.

Decentralized and trustworthy connectivity in IoT through blockchain-enabled secure data sharing over wireless networks offers a transformative approach to enhancing the security, privacy, and reliability of IoT deployments. By embracing this integration and addressing its associated challenges, organizations can pave the way for a more secure, transparent, and interconnected IoT ecosystem..

9. Future Scope

The future scope for decentralized and trustworthy connectivity in IoT through blockchain-enabled secure data sharing over wireless networks is vast and promising. Several key areas of future development and opportunities include:

1. Scalability Solutions: Research and innovation efforts will focus on addressing scalability challenges associated with blockchain-enabled IoT deployments. Technologies such as sharding, sidechains, and off-chain scaling solutions will be explored to increase transaction throughput and reduce latency, enabling blockchain networks to support larger-scale IoT applications.

2. Interoperability Standards: Standardization bodies and industry consortia will work towards establishing interoperability standards and protocols for blockchain-enabled IoT ecosystems. Common data formats, communication protocols, and interoperability frameworks will facilitate seamless integration and collaboration among heterogeneous IoT devices and blockchain platforms.

3. Privacy-Preserving Techniques: Safe multi-party computing, zero-knowledge proofs, and homomorphic encryption are some of the privacy-preserving approaches that will allow for the secret and secure sharing of IoT data over blockchain networks. Data integrity and auditability will be preserved while sensitive information is protected using these strategies.

4. Energy-Efficient Solutions: For IoT devices with limited resources, energy consumption is a major issue in blockchain-enabled installations. To address the issue of blockchain networks' energy footprint without sacrificing security or scalability, research will concentrate on creating algorithms for energy-efficient consensus, cryptography that is lightweight, and optimization strategies.

5. Edge and Fog Computing Integration: Integration of blockchain with edge and fog computing technologies will enable distributed processing and storage of IoT data closer to the network edge. Edge-based blockchain nodes will facilitate real-time data processing, local decision-making, and secure data sharing in latency-sensitive IoT applications.

6. Regulatory Compliance Frameworks: Regulatory compliance frameworks and governance models will evolve to address the unique legal and regulatory challenges of blockchain-enabled IoT deployments. Compliance with data protection laws, industry standards, and regulatory requirements will be ensured through transparent governance mechanisms and regulatory sandboxes.

7. AI and Machine Learning Integration: Integration of artificial intelligence (AI) and machine learning (ML) techniques with blockchain-enabled IoT systems will enable predictive analytics, anomaly detection, and autonomous decision-making. AI-driven smart contracts and autonomous agents will enhance the intelligence and automation capabilities of decentralized IoT networks.

8. Industry-Specific Applications: Industry-specific applications of blockchain-enabled IoT will continue to emerge across sectors such as supply chain management, healthcare, energy, transportation, and smart cities. These applications will leverage blockchain technology to enhance data integrity, traceability, and transparency in various business processes and value chains.

9. Social Impact and Sustainability: Blockchain-enabled IoT solutions have the potential to address social and environmental challenges, such as supply chain transparency, renewable energy trading, and environmental monitoring. These solutions will contribute to sustainability, social responsibility, and inclusive development by empowering communities and stakeholders with transparent and decentralized access to resources and information.

The future scope for decentralized and trustworthy connectivity in IoT through blockchain-enabled secure data sharing over wireless networks is characterized by ongoing innovation, collaboration, and convergence of technologies. By leveraging blockchain's decentralized architecture, cryptographic security, and immutable ledger, organizations can unlock new opportunities for secure, transparent, and interoperable IoT deployments, paving the way for a more connected and trustworthy digital future..

References

[1] Gupta, M., Gupta, D., & Duggal, A. (2023). NFT Culture: A New Era. Scientific Journal of Metaverse and Blockchain Technologies, 1(1), 57–62. https://doi.org/10.36676/sjmbt.v1i1.08.

[2] M. Gupta, “Reviewing the Relationship Between Blockchain and NFT With World Famous NFT Market Places”, SJMBT, vol. 1, no. 1, pp. 1–8, Dec. 2023..

[3] R. Gupta, M. Gupta, and D. Gupta, “Role of Liquidity Pool in Stabilizing Value of Token”, SJMBT, vol. 1, no. 1, pp. 9–17, Dec. 2023.

[4] M. GUPTA and D. Gupta, “Investigating Role of Blockchain in Making your Greetings Valuable”, URR, vol. 10, no. 4, pp. 69–74, Dec. 2023..

[5] R. Issalh, A. Gupta, and M. Gupta, “PI NETWORK : A REVOLUTION”, SJMBT, vol. 1, no. 1, pp. 18–27, Dec. 2023

[6] A. Duggal, M. Gupta, and D. Gupta, “SIGNIFICANCE OF NFT AVTAARS IN METAVERSE AND THEIR PROMOTION: CASE STUDY”, SJMBT, vol. 1, no. 1, pp. 28–36, Dec. 2023.

[7] M. Gupta, “Say No to Speculation in Crypto market during NFT trades: Technical and Financial Guidelines”, SJMBT, vol. 1, no. 1, pp. 37–42, Dec. 2023..

[8] A. Singla, M. Singla, and M. Gupta, “Unpacking the Impact of Bitcoin Halving on the Crypto Market: Benefits and Limitations”, SJMBT, vol. 1, no. 1, pp. 43–50, Dec. 2023..

[9] Gupta and P. Jain, “EXPECTED IMPACT OF DECENTRALIZATION USING BLOCKCHAIN BASED TECHNOLOGIES”, SJMBT, vol. 1, no. 1, pp. 51–56, Dec. 2023.

[10] D. Gupta and S. Gupta, “Exploring world famous NFT Scripts: A Global Discovery”, SJMBT,vol. 1, no. 1, pp. 63–71, Dec. 2023..

[11] M.Gupta, “Integration of IoT and Blockchain for user Authentication”,SJMBT, vol. 1, no. 1,pp. 72–84, Dec. 2023..

[12] A. Gupta, D. Kaushik, M. Garg and A. Verma, "Machine Learning model for Breast Cancer Prediction," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2020, pp. 472-477, doi: 10.1109/I-SMAC49090.2020.9243323

[13] https://dfzljdn9uc3pi.cloudfront.net/2023/cs-1337/1/fig-1-full.png

[14] V. Veeraiah, K. R. Kumar, P. Lalitha Kumari, S. Ahamad, R. Bansal and A. Gupta, "Application of Biometric System to Enhance the Security in Virtual World," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2022, pp. 719-723, doi: 10.1109/ICACITE53722.2022.9823850.

[15] V. Veeraiah, G. P, S. Ahamad, S. B. Talukdar, A. Gupta and V. Talukdar, "Enhancement of Meta Verse Capabilities by IoT Integration," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2022, pp. 1493-1498, doi: 10.1109/ICACITE53722.2022.9823766.

[16] Kaushik Dushyant; Garg Muskan; Annu; Ankur Gupta; Sabyasachi Pramanik, "Utilizing Machine Learning and Deep Learning in Cybesecurity: An Innovative Approach," in Cyber Security and Digital Forensics: Challenges and Future Trends , Wiley, 2022, pp.271-293, doi: 10.1002/9781119795667.ch12.

[17] V. Veeraiah, H. Khan, A. Kumar, S. Ahamad, A. Mahajan and A. Gupta, "Integration of PSO and Deep Learning for Trend Analysis of Meta-Verse," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2022, pp. 713-718, doi: 10.1109/ICACITE53722.2022.9823883.

[18] V. Talukdar, D. Dhabliya, B. Kumar, S. B. Talukdar, S. Ahamad and A. Gupta, "Suspicious Activity Detection and Classification in IoT Environment Using Machine Learning Approach," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 531-535, doi: 10.1109/PDGC56933.2022.10053312.

[19] V. Jain, S. M. Beram, V. Talukdar, T. Patil, D. Dhabliya and A. Gupta, "Accuracy Enhancement in Machine Learning During Blockchain Based Transaction Classification," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 536-540, doi: 10.1109/PDGC56933.2022.10053213.

[20] P. R. Kshirsagar, D. H. Reddy, M. Dhingra, D. Dhabliya and A. Gupta, "A Review on Comparative study of 4G, 5G and 6G Networks," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1830-1833, doi: 10.1109/IC3I56241.2022.10073385.

[21] P. Venkateshwari, V. Veeraiah, V. Talukdar, D. N. Gupta, R. Anand and A. Gupta, "Smart City Technical Planning Based on Time Series Forecasting of IOT Data," 2023 International Conference on Sustainable Emerging Innovations in Engineering and Technology (ICSEIET), Ghaziabad, India, 2023, pp. 646-651, doi: 10.1109/ICSEIET58677.2023.10303480.

[22] V. Veeraiah, J. Kotti, V. Jain, T. Sharma, S. Saini and A. Gupta, "Scope of IoT in Emerging Engineering Technology during Online Education," 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1-6, doi: 10.1109/ICCCNT56998.2023.10308107.

[23] Bijender Bansal; V. Nisha Jenipher; Rituraj Jain; R. Dilip; Makhan Kumbhkar; Sabyasachi Pramanik; Sandip Roy; Ankur Gupta, "Big Data Architecture for Network Security," in Cyber Security and Network Security , Wiley, 2022, pp.233-267, doi: 10.1002/9781119812555.ch11.

[24] K. A. Shukla, S. Almal, A. Gupta, R. Jain, R. Mishra and D. Dhabliya, "DL Based System for On-Board Image Classification in Real Time, Applied to Disaster Mitigation," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 663-668, doi: 10.1109/PDGC56933.2022.10053139.

[25] R. Bansal, A. Gupta, R. Singh and V. K. Nassa, "Role and Impact of Digital Technologies in E-Learning amidst COVID-19 Pandemic," 2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT), Sonepat, India, 2021, pp. 194-202, doi: 10.1109/CCICT53244.2021.00046.

[26] A. Gupta, R. Singh, V. K. Nassa, R. Bansal, P. Sharma and K. Koti, "Investigating Application and Challenges of Big Data Analytics with Clustering," 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), Coimbatore, India, 2021, pp. 1-6, doi: 10.1109/ICAECA52838.2021.9675483.

[27] Mamta, V. Veeraiah, D. N. Gupta, B. S. Kumar, A. Gupta and R. Anand, "Prediction of Health Risk Based on Multi-Level IOT Data Using Decision Trees," 2023 International Conference on Sustainable Emerging Innovations in Engineering and Technology (ICSEIET), Ghaziabad, India, 2023, pp. 652-656, doi: 10.1109/ICSEIET58677.2023.10303560.

[28] V. Veeraiah, N. B. Rajaboina, G. N. Rao, S. Ahamad, A. Gupta and C. S. Suri, "Securing Online Web Application for IoT Management," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2022, pp. 1499-1504, doi: 10.1109/ICACITE53722.2022.9823733.

[29] K. A. Shukla, S. Ahamad, G. N. Rao, A. J. Al-Asadi, A. Gupta and M. Kumbhkar, "Artificial Intelligence Assisted IoT Data Intrusion Detection," 2021 4th International Conference on Computing and Communications Technologies (ICCCT), Chennai, India, 2021, pp. 330-335, doi: 10.1109/ICCCT53315.2021.9711795.

[30] P. R. Kshirsagar, D. H. Reddy, M. Dhingra, D. Dhabliya and A. Gupta, "A Scalable Platform to Collect, Store, Visualize and Analyze Big Data in Real- Time," 2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM), Uttar Pradesh, India, 2023, pp. 1-6, doi: 10.1109/ICIPTM57143.2023.10118183.

[31] P. R. Kshirsagar, D. H. Reddy, M. Dhingra, D. Dhabliya and A. Gupta, "Detection of Liver Disease Using Machine Learning Approach," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1824-1829, doi: 10.1109/IC3I56241.2022.10073425.

[32] P. R. Kshirsagar, D. H. Reddy, M. Dhingra, D. Dhabliya and A. Gupta, "A Review on Application of Deep Learning in Natural Language Processing," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1834-1840, doi: 10.1109/IC3I56241.2022.10073309.

[33] V. Veeraiah, V. Talukdar, S. B. Talukdar, J. Kotti, M. K. Dharani and A. Gupta, "IoT Framework in a Blockchain dependent Cloud Environment," 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1-6, doi: 10.1109/ICCCNT56998.2023.10308158.

[34] M. Dhingra, D. Dhabliya, M. K. Dubey, A. Gupta and D. H. Reddy, "A Review on Comparison of Machine Learning Algorithms for Text Classification," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1818-1823, doi: 10.1109/IC3I56241.2022.10072502.

[35] D. Mandal, K. A. Shukla, A. Ghosh, A. Gupta and D. Dhabliya, "Molecular Dynamics Simulation for Serial and Parallel Computation Using Leaf Frog Algorithm," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 552-557, doi: 10.1109/PDGC56933.2022.10053161

[36] K. A. Shukla, V. Juneja, S. Singh, U. Prajapati, A. Gupta and D. Dhabliya, "Role of Hybrid Optimization in Improving Performance of Sentiment Classification System," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC),

Solan, Himachal Pradesh, India, 2022, pp. 541-546, doi: 10.1109/PDGC56933.2022.10053333.

[37] V. V. Chellam, S. Praveenkumar, S. B. Talukdar, V. Talukdar, S. K. Jain and A. Gupta, "Development of a Blockchain-based Platform to Simplify the Sharing of Patient Data," 2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM), Uttar Pradesh, India, 2023, pp. 1-6, doi: 10.1109/ICIPTM57143.2023.10118194.

[38] Borkar, P., Wankhede, V. A., Mane, D. T., Limkar, S., Ramesh, J. V. N., & Ajani, S. N. (2023). Deep learning and image processing-based early detection of Alzheimer disease in cognitively normal individuals. Soft Computing, 1-23.

[39] Reddy, B. N. K., Suresh, N., Ramesh, J. V. N., Pavithra, T., Bahulya, Y. K., Edavoor, P. J., & Ram, S. J. (2015, August). An efficient approach for design and testing of FPGA programming using Lab VIEW. In 2015 international conference on advances in computing, communications and informatics (ICACCI) (pp. 543-548). IEEE.

[40] Rao, K. R., Rao, P. P., Ramesh, J. V. N., Reddy, P. S., Velivela, S. S. K., & Rajesh, T. (2015). Development of RLS algorithm for localization in wireless sensor networks. Procedia Computer Science, 65, 58-64.

[41] Ramesh, J. V. N., Reddy, B. N. K., Krishna, V. M., Gandhi, B. K., Shiva, V., & Devi, M. D. (2015). An Effective Self-test Scheduling for Realtime Processor based System. International Journal of Smart Home, 9(3), 101-112.

[42] Bhanu, B. B., Rao, K. R., Ramesh, J. V. N., & Hussain, M. A. (2014, September). Agriculture field monitoring and analysis using wireless sensor networks for improving crop production. In 2014 Eleventh international conference on wireless and optical communications networks (WOCN) (pp. 1-7). IEEE.

[43] B. S. Rawat, D. Gangodkar, V. Talukdar, K. Saxena, C. Kaur and S. P. Singh, "The Empirical Analysis of Artificial Intelligence Approaches for Enhancing the Cyber Security for Better Quality," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 247-250, doi: 10.1109/IC3I56241.2022.10072877.

[44] Dwarakanath, D. B., Shrivastava, D. G. ., Bansal, D. R. ., Nandankar, P. ., Talukdar , D. V. ., & Usmani, M. A. . (2023). Explainable Machine Learning Techniques in Medical Image Analysis Based on Classification with Feature Extraction. International Journal of Communication Networks and Information Security (IJCNIS), 14(3), 342–357.