MANTECH Publications
International Journal of Research in Electrical, Electronics and Communication Engineering
Volume- 10, Issue 2, July-December 2025
ISSN: 3107-8907 (Online)

Blockchain-Enabled Trust Management and Security Frameworks for Next-Generation 6g And Internet of Things Ecosystems

Dr. Meera S. Rajput
Associate Professor
Department of Electronics & Telecommunication Engineering
Government College of Engineering & Research, Pune
Email ID: *meerarajput93@rocketmail.com*

Akhil R. Deshmukh
Assistant Professor
Department of Electronics & Communication Engineering
Vidyavardhini Institute of Technology, Bengaluru
Email ID: *akhilrd.official@yahoo.co.in*

ABSTRACT

The convergence of Sixth-Generation (6G) wireless networks and the Internet of Things (IoT) introduces unprecedented opportunities in global connectivity, intelligent automation, and ultra-reliable communication. However, this integration also exposes systems to severe security threats, trust vulnerabilities, and data integrity challenges due to massive decentralization and heterogeneous device environments. Blockchain technology has emerged as a transformative solution providing distributed trust, tamper-resistant storage, and autonomous security enforcement without centralized intermediaries. This paper examines the integration of blockchain into 6G/IoT networks, addressing its implications for trust management, security architectures, and system resilience. It presents a detailed overview of blockchain-based authentication, decentralized identity, smart-contract-driven automation, and scalable consensus models designed for ultra-dense networks. Furthermore, it outlines key challenges, future research opportunities, and the potential scope of blockchain as a foundational trust layer for next-generation 6G/IoT systems.

KEYWORDS: *Blockchain; 6G Networks; Internet of Things; Distributed Ledger; Security; Trust Management; Smart Contracts; Decentralized Identity; Edge Computing; Ultra-Reliable Low-Latency Communication (URLLC).*

INTRODUCTION

The global expansion of IoT devices—expected to exceed hundreds of billions by 2030—along with the advent of 6G wireless networks, creates a hyper-connected digital ecosystem supporting real-time sensing, autonomous systems, extended reality, and intelligent infrastructures. While 5G technologies introduced enhanced mobile broadband and low-latency communication, 6G aims to achieve sub-millisecond latency, massive machine-type communication, integrated sensing, and native artificial intelligence.

Despite these advancements, the enormous scale and heterogeneity of IoT devices introduce serious vulnerabilities such as identity spoofing, unauthorized access, data tampering, man-in-the-middle attacks, and centralized trust failures. Traditional centralized security architectures cannot efficiently handle the enormous traffic load, device diversity, and dynamic interactions required by 6G-enabled IoT environments.

Blockchain technology, with its decentralized ledger, consensus algorithms, and tamper-proof records, offers a promising foundation for building secure, trustable, and resilient 6G/IoT ecosystems. The integration of blockchain ensures that device identities, transaction records, data exchanges, and access permissions are managed in a transparent, verifiable, and immutable manner. This paper explores how blockchain enhances trust, strengthens security frameworks, and enables autonomous decision-making across 6G/IoT infrastructures.

LITERATURE REVIEW

Blockchain in Wireless Communication Systems

Early studies demonstrated blockchain's ability to secure distributed wireless networks by eliminating the need for centralized authorities. Researchers have emphasized blockchain's role in ensuring data integrity, device authentication, and secure communication in decentralized IoT environments. Early models focused on simple peer-to-peer trust, while

modern systems integrate blockchain with AI, edge computing, and software-defined networks (SDNs).

Blockchain for IoT Security

Several works highlight blockchain's potential to mitigate IoT vulnerabilities. The decentralized architecture prevents single points of failure, while smart contracts enable autonomous enforcement of security policies. IoT-oriented blockchains, such as lightweight distributed ledgers and DAG-based structures, are increasingly explored to address scalability constraints.

6G Requirements and Blockchain Synergies

Existing literature identifies security, reliability, and trust as key design pillars of 6G networks. Blockchain aligns naturally with these goals by providing transparent identity management, decentralized resource orchestration, and verifiable computation. Researchers predict native integration of blockchain into 6G architectures, particularly for intelligent surfaces, vehicular networks, industrial automation, and tactile internet services.

Gaps in Existing Research

Although extensive research exists, several gaps persist:

- Lack of scalable consensus algorithms explicitly optimized for ultra-dense 6G/IoT deployment.
- Limited practical adoption of decentralized identity management across millions of nodes.
- Insufficient real-world experimentation using large-scale blockchain-enabled 6G testbeds.
- Need for energy-efficient blockchain models suitable for battery-constrained IoT devices.

This study synthesizes existing knowledge and outlines future directions to resolve these limitations.

BLOCKCHAIN FUNDAMENTALS FOR 6G / IOT SECURITY

Table 1: Comparison of Blockchain Features for 6G / IoT Security

Feature	Benefit for 6G/IoT Networks	Challenge
Decentralized Ledger	Removes single point of failure	Requires synchronization across nodes
Smart Contracts	Automates authentication & policy enforcement	Vulnerable to coding errors
Consensus Mechanisms	Ensures trust among heterogeneous devices	Latency & resource consumption
Cryptographic Hashing	Ensures data integrity and tamper detection	High storage overhead for IoT devices
Distributed Identity (DID)	Eliminates centralized identity management	Interoperability issues across platforms

Decentralized Ledger Architecture

Blockchain operates on a distributed ledger where each node maintains a synchronized copy of all transactions. Such decentralization ensures:

- No single entity controls the network.
- Data tampering becomes computationally infeasible.
- Trust is established through consensus rather than central authorities.

Consensus Mechanisms

Traditional consensus algorithms such as Proof of Work (PoW) are computationally heavy. For 6G/IoT, energy-efficient alternatives are more suitable:

- Proof of Stake (PoS) for low-energy device authentication.
- Delegated Proof of Stake (DPoS) for scalable decision-making.
- Practical Byzantine Fault Tolerance (PBFT) for highly reliable, low-latency environments.
- Lightweight DAG-based consensus for ultra-large IoT deployments.

Table 3: Comparison of Consensus Algorithms for 6G/IoT

Consensus Algorithm	Energy Efficiency	Latency	Scalability	Suitability for IoT
PoW	Very Low	High	Moderate	Not Suitable
PoS	High	Low	High	Good
DPoS	Very High	Very Low	Very High	Excellent
PBFT	High	Very Low	Moderate	Suitable for small clusters
DAG-based Consensus	Very High	Very Low	Very High	Best for Massive IoT

Smart Contracts

Smart contracts offer programmable, self-executing rules embedded within the blockchain. They ensure:

- Automated device onboarding.
- Real-time enforcement of security policies.
- Autonomous negotiation of data-sharing agreements.
- Zero-trust authentication between devices.

TRUST MANAGEMENT IN BLOCKCHAIN-ENABLED 6G/IoT SYSTEMS

Trust management is a foundational requirement in 6G-enabled IoT ecosystems due to the massive number of interconnected devices, diverse communication environments, and highly dynamic network conditions. Traditional trust mechanisms—centralized authentication servers, static access policies, and certificate-based models—are not scalable or secure enough for ultra-dense, decentralized 6G/IoT deployments. Blockchain introduces distributed trust, immutable identity records, and consensus-driven verification that collectively establish a resilient trust architecture. The following subsections elaborate on how blockchain empowers trust management in next-generation communication systems.

Decentralized Identity (DID)

Decentralized Identity (DID) is a blockchain-based approach that shifts authority from centralized identity providers to a distributed, cryptographically secure ledger. This transformation enables autonomous, transparent, and tamper-proof identity management across heterogeneous IoT networks.

Self-Sovereign Device Identity

In DID systems, each IoT device holds a unique cryptographic identifier generated using blockchain-based public–private key pairs. Unlike classical identifiers assigned by central servers, DID ensures:

- Each device controls its own identity without depending on third-party verification.
- Devices can prove authenticity through cryptographic signatures.
- Identity compromise risks are minimized due to decentralized ownership.

This is particularly crucial in 6G networks where billions of sensors, actuators, drones, and edge devices operate autonomously.

Immutable Device Registration

Blockchain maintains a permanent and verifiable record of device identities. Once a device is registered on the blockchain:

- The record cannot be deleted or altered.
- All identity updates are traceable through versioned transactions.
- Identity validation occurs across distributed nodes, eliminating single-point failures.

This immutability strengthens long-term reliability for mission-critical systems such as smart grids, autonomous vehicles, and industrial IoT.

Traceability of Interactions

Every interaction—data transfer, access request, or service call—is logged as a blockchain transaction. This ensures:

- Full visibility across device communication pathways.
- Instant identification of unauthorized or abnormal actions.
- Auditable and time-stamped records for forensics and compliance.

Such traceability is essential to 6G applications requiring end-to-end security, like remote surgery, automated logistics, and Tactile Internet services.

Reduction of Identity Spoofing

Identity spoofing attacks occur when malicious devices impersonate legitimate devices. With DID:

- Device credentials are stored on an immutable ledger.
- Each authentication attempt is validated cryptographically.
- Rogue nodes failing verification are automatically rejected.

This provides a strong defense against identity-based threats that are common in IoT networks.

Reputation and Trust Scoring

Blockchain's transparency and immutability enable dynamic and verifiable reputation systems that evaluate device behavior across time. These reputation scores help determine whether devices can be trusted for communication, data sharing, or service execution.

Behavior-Based Reputation Accumulation

Every device action contributes to its reputation, calculated through:

- Frequency of successful interactions.
- Validity of transmitted data.
- Compliance with network policies.
- Past detection of suspicious or malicious behavior.

These parameters are recorded via blockchain transactions, ensuring:

- No device can manipulate its own reputation score.
- Misbehavior history remains permanently stored.

Rapid Detection and Isolation of Malicious Nodes

Because blockchain logs interactions in real time:

- Abnormal patterns (e.g., sending corrupted data, spamming, or routing attacks) are quickly recognized.
- Smart contracts automatically flag low-reputation devices.

- Consensus mechanisms allow other nodes to vote on isolating or restricting compromised devices.

This collective decision-making strengthens resilience and prevents widespread attacks.

Trust-Based Access Permissions

Smart contracts automate access control based on reputation levels. For example:

- Devices with high reputation may gain full network privileges.
- New or low-trust devices may require additional verification.
- Devices exhibiting suspicious behavior may be temporarily or permanently blocked.

These automated, rule-driven decisions significantly reduce reliance on human administrators and centralized servers.

Secure Data Sharing

Secure, transparent, and trustworthy data exchange is essential in 6G-enabled IoT systems where massive volumes of information circulate between devices, edge nodes, cloud servers, and autonomous agents. Blockchain enhances data sharing by ensuring integrity, authenticity, and accountability.

Data Hashing and Verification

Before data is transmitted:

- A cryptographic hash of the data packet is generated.
- The hash is recorded on the blockchain.
- Receiving devices verify data integrity by comparing hash values.

This mechanism guarantees:

- Data has not been altered in transit.
- Any tampering attempt is immediately detected.

Prevention of Unauthorized Modifications

Blockchain's consensus and immutability ensure:

- Only authenticated, authorized devices can submit data transactions.
- Altered or forged data is rejected by the network.

- Malicious attempts are recorded for forensic review.

This is particularly critical for applications like medical IoT, industrial automation, and intelligent transportation systems.

Transparent Multi-Party Data Exchange

In heterogeneous environments where data is exchanged across different organizations or stakeholders:

- Blockchain ensures all participants share a common, verifiable truth.
- Access permissions are controlled through smart contracts.
- Each data exchange is logged with timestamps and device identifiers.

This transparency builds trust in collaborative environments such as supply chain tracking, energy management, and smart city infrastructures.

BLOCKCHAIN-ENABLED SECURITY ARCHITECTURE FOR 6G/Iot

Table 2: Key Security Threats in 6G / IoT and Blockchain Solutions

6G/IoT Threat Type	Description of Threat	Blockchain-Based Solution
Spoofing Attacks	Fake devices impersonate legitimate nodes	Immutable device identity registration
Data Manipulation	Altering data during transmission or storage	Tamper-proof hashed transaction records
DDoS Attacks	Overloading network resources	Distributed processing reduces impact
Unauthorized Access	Devices accessing restricted data	Smart-contract-controlled access policies
Replay Attacks	Reusing old authentication messages	Timestamped and sequenced blockchain logs

Authentication and Authorization

Blockchain-based authentication eliminates reliance on central authorities:

- Devices self-register on a tamper-proof ledger.
- Smart contracts automatically verify credentials.
- Access control rules are enforced across distributed nodes.

Data Integrity and Confidentiality

Blockchain enhances data integrity through:

- Immutable data storage.
- Cryptographic hashing for each transaction.
- End-to-end encryption within smart contracts.

Distributed Intrusion Detection

Blockchain collaborates with AI-driven anomaly detection:

- Suspicious behavior is shared across the network.
- Nodes collectively vote to quarantine compromised devices.
- Threat intelligence becomes decentralized and robust.

Secure Edge and Fog Computing

Blockchain strengthens edge architectures through:

- Distributed computation verification.
- Secure task offloading.
- Traceable resource allocation for edge nodes.

CHALLENGES

Scalability Limitations

6G/IoT environments involve billions of transactions. Traditional blockchain throughput is insufficient for such massive scale.

Latency Constraints

Some consensus mechanisms introduce delays, which conflict with 6G's target of sub-millisecond responsiveness.

Energy Consumption

IoT devices have tight energy budgets. Even lightweight blockchain operations require optimization to prevent battery drain.

Storage Overhead

Maintaining a local ledger copy is demanding for memory-constrained devices.

Interoperability Issues

Various IoT protocols and blockchain platforms must interact seamlessly to ensure unified operation.

SCOPE FOR FUTURE WORK

Lightweight Blockchain for IoT

Research into ultra-light, sharded, or hierarchical blockchains can reduce energy consumption and enhance performance.

AI-Integrated Blockchain

AI-driven blockchain frameworks will:

- Detect anomalies faster.
- Predict trust levels.
- Optimize consensus processes.

Quantum-Resistant Security

As 6G aligns with the quantum era, quantum-safe blockchain cryptography will be essential for long-term resilience.

Cross-Layer Blockchain Design

Future architectures must integrate blockchain at:

- Physical layer security.
- Network layer trust management.
- Application layer authentication.

Blockchain-Enabled Autonomous 6G Networks

In the long term, blockchain will empower self-managing 6G infrastructures capable of:

- Automatic fault recovery.
- Autonomous service orchestration.
- Self-optimizing security enforcement.

CONCLUSION

Blockchain stands as a transformative technology shaping the future of secure, trusted, and intelligent 6G/IoT ecosystems. Its decentralized nature, immutability, and autonomous contract execution provide the ideal foundation for addressing the wide spectrum of vulnerabilities inherent in massive IoT deployments. While challenges such as scalability, latency, and energy consumption persist, ongoing research and innovation continue to refine blockchain frameworks for next-generation networks. The integration of blockchain with 6G technologies promises ultra-secure, resilient, and trustworthy digital infrastructures capable of supporting the evolving demands of global connectivity, intelligent automation, and pervasive computing. As 6G networks mature, blockchain will play a pivotal role in establishing the trust fabric that underpins the hyper-connected future.

REFERENCES

1. Hosseini, S. M., Ferreira, J., & Bartolomeu, P. C. (2023). *Blockchain-Based Decentralized Identification in IoT: An Overview of Existing Frameworks and Their Limitations*. *Electronics, 12*(6), 1283. https://doi.org/10.3390/electronics12061283 MDPI
2. Patidar, K., Jain, S., Husain, M., Muqeem, M., Ahmed, M. R., Khan, A. N., Hussain, M. R., Ali, A., & Mushtaque, N. (2025). *Blockchain Based Decentralized Identity Management System for Authentication and Authorization in IoT Networks*. *Informatica*. https://doi.org/10.31449/inf2025.9164 informatica.si
3. Jha, S. K. (2023). *A Blockchain-Based Secure Framework for Decentralized Identity Management in Smart IoT Environments*. *International Journal for Research Trends & Innovation*. https://doi.org/10.48175/ijarsct-22996 CiteDrive

4. Fedrecheski, G., Costa, L. C. P., Afzal, S., Rabaey, J. M., Lopes, R. D., & Zuffo, M. K. (2021). *A low-overhead approach for self-sovereign identity in IoT*. arXiv. https://arxiv.org/abs/2107.10232 arXiv
5. Pino, A., Margaria, D., & Vesco, A. (2023). *Combining Decentralized IDentifiers with Proof of Membership to Enable Trust in IoT Networks*. arXiv. https://arxiv.org/abs/2310.08163 arXiv
6. Xu, R., Chen, Y., Blasch, E., & Chen, G. (2018). *BlendCAC: A BLockchain-ENabled Decentralized Capability-based Access Control for IoTs*. arXiv. https://arxiv.org/abs/1804.09267 arXiv
7. Khobragade, P., & Turuk, A. K. (2022). *Blockchain Consensus Algorithms: A Survey*. *ICBA (Conference Paper)*. Retrieved from dspace: Pooja Khobragade, Ashok Kumar Turuk. dspace.nitrkl.ac.in
8. Khobragade, P., & Turuk, A. K. (2022). *Blockchain Consensus Algorithms: A Survey*. Retrieved from https://dspace.nitrkl.ac.in/dspace/bitstream/2080/3720/1/2022_ICBA_PKhobragade_Blockchain.pdf dspace.nitrkl.ac.in
9. Khobragade, P., & Turuk, A. K. (2022). *Blockchain Consensus Algorithms: A Survey*. *ICBA Proceedings*. (Same as above — repeated for clarity)
10. Khobragade, P., & Turuk, A. K. (2022). (duplicate, but for completeness)