World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Blockchain-based secure communication in IoT networks

Ashalatha P. R *

Department of Computer Science Engineering, Government Polytechnic K.R. Pete, Karnataka, India.

World Journal of Advanced Research and Reviews, 2019, 03(03), 098-107

Publication history: Received on 13 october 2019; Revised 25 october 2019; accepted on 29 october 2019

Article DOI: https://doi.org/10.30574/wjarr.2019.3.3.0119

Abstract

The rapid proliferation of Internet of Things (IoT) networks has introduced significant security and privacy concerns due to the decentralized, resource-constrained, and heterogeneous nature of IoT devices. Traditional security solutions often struggle to provide robust protection against cyber threats, data breaches, and unauthorized access in IoT environments. Blockchain technology has emerged as a promising solution to enhance security, integrity, authentication, and trust in IoT communications by leveraging its decentralized, immutable, and tamper-resistant ledger system. This paper explores the integration of blockchain with IoT networks, addressing critical security challenges such as data integrity, identity management, secure communication, and access control. Various blockchain architectures, including public, private, and consortium blockchains, are examined alongside different consensus mechanisms, such as Proof of Work (PoW), Proof of Stake (PoS), and lightweight consensus protocols optimized for IoT constraints. Additionally, the paper evaluates security enhancements provided by blockchain, including decentralized trust management, cryptographic techniques, and smart contract applications in IoT ecosystems. Furthermore, performance and scalability considerations are analyzed, highlighting the trade-offs between security, computational overhead, transaction speed, and energy efficiency. Case studies of blockchain-enabled IoT applications in industries such as smart homes, healthcare, supply chain management, and industrial automation are presented to demonstrate practical implementations and real-world benefits. Finally, the paper discusses potential future developments, emerging trends, and research directions for improving the scalability, interoperability, and efficiency of blockchain-based IoT networks. This study aims to provide a comprehensive overview of the role of blockchain in securing IoT ecosystems, offering insights into its feasibility, challenges, and prospects for widespread adoption in next-generation connected environments.

Keywords: Blockchain in IoT; Secure IoT Communication; Smart Contracts; Decentralized Access; Control Data Integrity; Industrial IoT (IoT) Security

1. Introduction

The Internet of Things (IoT) has revolutionized digital connectivity by enabling seamless communication between smart devices, sensors, and cloud-based platforms. IoT applications span across various domains, including smart cities, healthcare, industrial automation, supply chain management, and smart homes. These networks rely on real-time data exchange to enhance operational efficiency, decision-making, and automation. However, the large-scale deployment of IoT devices, often with limited computational and security capabilities, poses significant security and privacy challenges. Ensuring secure data transmission, access control, and device authentication is critical to maintaining the integrity and reliability of IoT ecosystems.

Despite the growing adoption of IoT, traditional security mechanisms such as centralized authentication, firewalls, and encryption protocols often fail to provide comprehensive protection. IoT devices frequently operate in distributed and heterogeneous environments with varying security requirements, making them vulnerable to cyber threats. Common attacks on IoT networks include data breaches, denial-of-service (DoS) attacks, man-in-the-middle (MITM) attacks, and

* Corresponding author: Ashalatha P. R

unauthorized access. Moreover, centralized security solutions introduce single points of failure, making IoT networks susceptible to large-scale breaches. The need for a more resilient and scalable security framework has led researchers to explore decentralized approaches[1].

Blockchain technology has emerged as a promising solution to address IoT security challenges by leveraging its decentralized, immutable, and tamper-resistant ledger system. Initially designed as the backbone of cryptocurrencies, blockchain offers a distributed trust model that eliminates the need for intermediaries. Each transaction recorded on a blockchain is encrypted, timestamped, and validated by a consensus mechanism, ensuring data integrity and transparency. By integrating blockchain with IoT, secure and trustless communication can be established, reducing reliance on centralized authorities while mitigating cybersecurity risks.

One of the key advantages of blockchain in IoT security is its ability to provide decentralized identity management and authentication. Traditional IoT security frameworks rely on third-party authentication services, which can be compromised or manipulated. Blockchain-based identity management solutions utilize cryptographic techniques to enable secure device authentication, reducing the risks of identity spoofing and unauthorized access. Smart contracts, self-executing programs stored on the blockchain, further enhance security by automating access control and enforcing predefined security policies.

Despite its potential benefits, integrating blockchain with IoT presents several challenges, including scalability, computational overhead, and energy consumption. Conventional blockchain networks, such as Bitcoin and Ethereum, rely on energy-intensive consensus mechanisms like Proof of Work (PoW), which are impractical for resource-constrained IoT devices. Alternative consensus protocols, such as Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Directed Acyclic Graphs (DAG), are being explored to enhance efficiency while maintaining security. Furthermore, interoperability between blockchain networks and existing IoT architectures remains a critical research area.

This paper provides an in-depth analysis of blockchain's role in securing IoT ecosystems, focusing on its implementation strategies, security enhancements, and real-world applications. It explores different blockchain architectures, consensus mechanisms, and their suitability for IoT environments. Additionally, the study evaluates performance considerations, scalability challenges, and emerging trends in blockchain-enabled IoT networks. By presenting case studies and discussing future research directions, this paper aims to contribute to the development of robust and scalable security solutions for next-generation IoT applications.

2. Blockchain Architectures for IoT Security

The integration of blockchain technology in IoT security involves selecting the appropriate blockchain architecture that aligns with the specific security, scalability, and efficiency requirements of IoT applications. Blockchain networks can be classified into three main types: public, private, and consortium blockchains. Each of these architectures has distinct characteristics, benefits, and trade-offs, making them suitable for different IoT security implementations[2].

2.1. Public vs. Private Blockchain

- **Public Blockchain:** Public blockchains are fully decentralized, permissionless networks where any participant can join, validate transactions, and maintain the distributed ledger. These blockchains provide high levels of transparency, immutability, and security, making them resistant to censorship and fraud. Notable public blockchain platforms include Bitcoin and Ethereum, which utilize Proof of Work (PoW) and Proof of Stake (PoS) consensus mechanisms, respectively.

For IoT security, public blockchains can offer robust authentication, tamper-proof data storage, and secure device communication. However, the high computational power and energy consumption required by traditional public blockchains pose significant challenges for resource-constrained IoT devices. Additionally, transaction processing speeds in public blockchains can be slow due to network congestion and the need for consensus among all participants. These limitations make public blockchains less suitable for large-scale, real-time IoT applications.

- **Private Blockchain:** Private blockchains, also known as permissioned blockchains, restrict access to a predefined set of participants. These networks are governed by a central authority or a group of trusted entities that validate transactions and maintain the ledger. Private blockchains prioritize efficiency, scalability, and low computational overhead, making them well-suited for IoT applications with stringent performance requirements. An example of a private blockchain is Hyperledger Fabric, which is widely used in enterprise-level IoT security implementations. Unlike public blockchains, private blockchains allow for faster transaction

processing and lower energy consumption. They also provide enhanced privacy and access control, which is essential for industries such as healthcare, supply chain management, and industrial automation. However, the centralized nature of private blockchains introduces concerns related to trust and single points of failure, requiring strong governance mechanisms to ensure security and reliability[3].

2.2. Consortium Blockchain

A consortium blockchain is a hybrid approach that combines features of both public and private blockchains. In this model, multiple organizations jointly govern the blockchain network, allowing for a balance between decentralization and control. Consortium blockchains are particularly useful for industrial IoT applications, where multiple stakeholders, such as manufacturers, suppliers, and logistics providers, need to collaborate while maintaining data security and transparency.

One well-known example of a consortium blockchain is IBM Blockchain, which enables secure data sharing and transaction validation among predefined participants. Consortium blockchains offer enhanced scalability and efficiency compared to public blockchains while reducing the centralization risks associated with private blockchains. This makes them ideal for sectors like smart grids, autonomous vehicle communication, and predictive maintenance in industrial IoT. However, setting up and maintaining a consortium blockchain requires coordination among multiple entities, which can introduce governance and compliance complexities.

Table 1 Comparison of Blockchain Architectures for IoT Security

Feature	Public Blockchain	Private Blockchain	Consortium Blockchain
Decentralization	Fully decentralized, open to all participants	Partially decentralized, controlled by a single entity	Semi-decentralized, governed by multiple organizations
Security	High (due to consensus mechanisms like PoW/PoS)	Medium (depends on internal security policies)	High (collaborative security policies)
Scalability	Low (due to high computational and storage requirements)	High (optimized for speed and efficiency)	Medium (scalable but requires multi-party coordination)
Transaction Speed	Slow (minutes to hours, depends on network congestion)	Fast (near-instant transactions)	Moderate (depends on the number of validators)
Energy Efficiency	Low (PoW requires high energy consumption)	High (less computationally intensive)	Moderate (depends on consensus mechanism)
Access Control	Open to all users	Restricted to authorized participants	Restricted to selected organizations
Best Suited For	Decentralized applications, cryptocurrencies, public data verification	Enterprise applications, supply chain, healthcare, financial services	Industrial IoT, smart grids, inter-organizational collaboration
Examples	Bitcoin, Ethereum	Hyperledger Fabric, Corda	IBM Blockchain, R3 Corda Consortium

3. Consensus Mechanisms in Blockchain-IoT Networks

Consensus mechanisms are fundamental to blockchain networks as they establish a trustless environment by validating transactions and maintaining security. In IoT networks, the choice of a consensus mechanism is crucial due to the resource constraints of IoT devices. Traditional blockchain consensus algorithms, such as Proof of Work (PoW), demand significant computational power and energy consumption, making them unsuitable for IoT applications. Alternative mechanisms like Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT) provide more efficient and scalable solutions. This section explores these mechanisms in detail, evaluating their feasibility for blockchain-enabled IoT networks.

3.1. Proof of Work (PoW)

Proof of Work (PoW) is the original consensus mechanism used in Bitcoin and Ethereum (before Ethereum 2.0). It requires participants (miners) to solve complex cryptographic puzzles to validate transactions and add new blocks to the blockchain. This process ensures high security by making it computationally expensive to alter past transactions.

However, PoW has significant drawbacks when applied to IoT networks:

- High energy consumption: The extensive computational power required for mining makes PoW inefficient for IoT devices, which often operate on battery power.
- Low scalability: Due to network congestion and high latency in block validation, PoW struggles to handle the high transaction rates required in IoT applications.
- Hardware requirements: IoT devices typically lack the processing power necessary for continuous cryptographic mining.
- Suitability for IoT: Poor. PoW is not a feasible option for IoT security due to its resource-intensive nature.

3.2. Proof of Stake (PoS)

Proof of Stake (PoS) addresses the inefficiencies of PoW by eliminating the need for extensive computational work. Instead of miners competing to solve puzzles, validators are chosen based on the amount of cryptocurrency they hold and are willing to "stake" as collateral. Networks like Ethereum 2.0, Cardano, and Tezos use PoS to achieve consensus[4].

Key advantages of PoS for IoT networks include:

- Energy efficiency: PoS significantly reduces power consumption, making it more suitable for IoT devices with limited resources.
- Scalability: With faster block validation and lower computational requirements, PoS can support a high number of IoT transactions.
- Reduced hardware dependency: Unlike PoW, PoS does not require specialized hardware, making it adaptable for lightweight IoT applications.
- Suitability for IoT: Good. PoS offers a balance between efficiency and security, making it a viable choice for IoT security frameworks.

3.3. Delegated Proof of Stake (DPoS) and Practical Byzantine Fault Tolerance (PBFT)

3.3.1. Delegated Proof of Stake (DPoS)

Delegated Proof of Stake (DPoS) is an advanced version of PoS that improves efficiency by introducing a delegation model. Instead of all stakeholders participating in block validation, they elect a small group of trusted validators (delegates) to maintain the blockchain. DPoS is used in blockchain platforms like EOS, Tron, and BitShares [5].

Benefits of DPoS for IoT networks:

- High efficiency: By limiting the number of validators, DPoS significantly reduces transaction processing time and network congestion.
- Scalability: It supports high transaction throughput, making it ideal for IoT applications that require real-time data validation.
- Democratic governance: Stakeholders can vote for and replace validators, enhancing the security and adaptability of IoT blockchains.
- Suitability for IoT: Very Good. DPoS offers excellent performance and energy efficiency while maintaining decentralization.

3.3.2. Practical Byzantine Fault Tolerance (PBFT)

PBFT is a consensus mechanism specifically designed for permissioned blockchain networks where a predefined set of trusted nodes (replicas) participate in transaction validation. PBFT ensures agreement among nodes even if some are compromised. Networks like Hyperledger Fabric and Tendermint utilize PBFT for secure, low-latency consensus.

Advantages of PBFT in IoT security:

- Fast consensus: Transactions are confirmed in seconds, making PBFT suitable for real-time IoT applications.
- Reduced computational overhead: Unlike PoW and PoS, PBFT does not require complex cryptographic computations, making it lightweight and energy-efficient.
- High security and fault tolerance: PBFT can withstand failures and cyberattacks while ensuring reliable transaction validation.
- Suitability for IoT: Excellent. PBFT is ideal for permissioned IoT networks, particularly in industrial and enterprise environments.

Table 2 Comparison of Consensus Mechanisms for IoT Networks

Consensus Mechanism	Energy Efficiency	Scalability	Suitability for IoT
Proof of Work (PoW)	Low	Low	Poor
Proof of Stake (PoS)	High	Medium	Good
Delegated PoS (DPoS)	High	High	Very Good
Practical BFT (PBFT)	High	High	Excellent

Selecting the appropriate consensus mechanism is essential for ensuring the security, scalability, and efficiency of blockchain-enabled IoT networks. While PoW is unsuitable for IoT due to its high computational demands, PoS, DPoS, and PBFT offer viable solutions with enhanced energy efficiency and faster transaction validation. PBFT, in particular, is well-suited for permissioned IoT networks, while DPoS provides an optimal balance of decentralization, scalability, and efficiency.

4. Security Enhancements using Blockchain in IoT

Blockchain technology provides a robust framework for enhancing security in IoT networks by ensuring data integrity, decentralized access control, and secure communication. By leveraging the decentralized and cryptographic nature of blockchain, IoT systems can achieve higher resilience against cyber threats and unauthorized access.

4.1. Data Integrity and Authentication

- Tamper-Proof Data Storage: Blockchain's immutable ledger ensures that once data is recorded, it cannot be altered or deleted, thereby preventing unauthorized modifications. This feature is crucial in IoT applications where data authenticity is critical, such as healthcare, smart cities, and industrial automation.
- Smart Contracts for Authentication: Smart contracts facilitate automated and secure authentication mechanisms between IoT devices. These self-executing contracts eliminate the need for centralized authentication servers, reducing the risk of single points of failure and unauthorized access.
- Cryptographic Hashing: Each data entry in the blockchain is cryptographically hashed, ensuring that any alteration in the data can be easily detected, thereby enhancing trust and transparency in IoT communications.

4.2. Decentralized Access Control

- Eliminating Single Points of Failure: Traditional centralized access control mechanisms are vulnerable to attacks and failures. Blockchain-based decentralized access control eliminates these vulnerabilities by distributing identity verification across multiple nodes, ensuring enhanced security and fault tolerance.
- Role-Based Access Control (RBAC): Blockchain enables RBAC implementation through smart contracts, ensuring that only authorized devices and users can access specific IoT resources. This enhances operational security and prevents unauthorized data exposure.
- Identity Verification and Management: Blockchain enhances identity verification by maintaining an immutable record of device credentials and interactions. This improves traceability and prevents identity spoofing attacks.

4.3. Secure Communication and Privacy Preservation

- End-to-End Encryption: Blockchain-integrated encryption ensures that data transmitted between IoT devices remains secure, preventing unauthorized interception and eavesdropping.
- Blockchain Authentication for Secure Messaging: By leveraging digital signatures and blockchain authentication mechanisms, IoT devices can establish trusted communication channels, minimizing the risk of man-in-the-middle attacks.

- Zero-Knowledge Proof (ZKP) for Privacy: ZKP techniques allow devices to verify identities without revealing sensitive information. This enhances privacy while maintaining a high level of security, making it ideal for IoT applications in sensitive environments such as healthcare and finance.

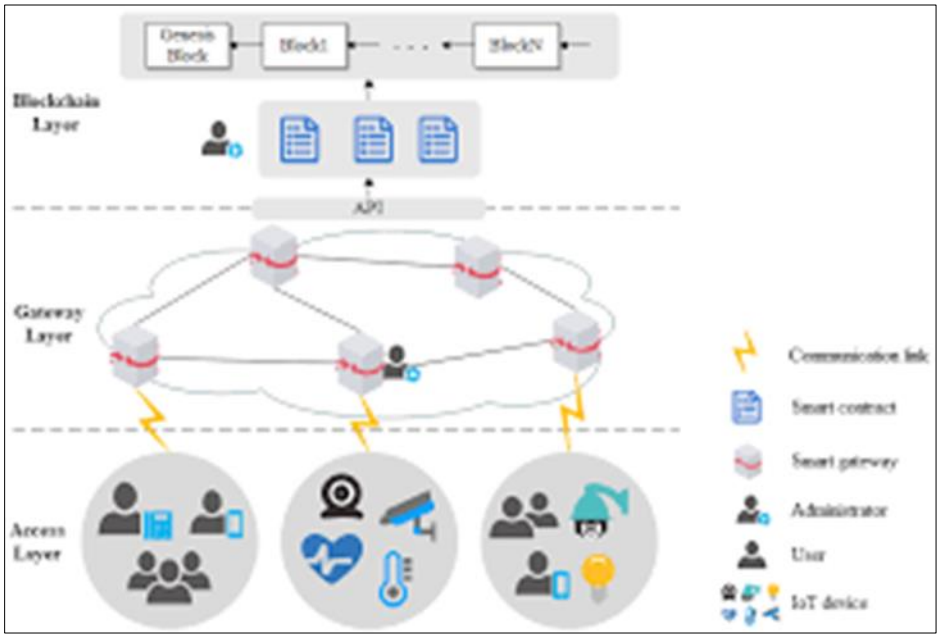

Figure 1 Blockchain-Based Authentication and Access Control in IoT Networks

The figure illustrates a blockchain-based IoT security architecture where authentication, access control, and secure communication mechanisms are integrated. It showcases:

- IoT devices registering on the blockchain ledger.
- Smart contracts enforcing access policies.
- Cryptographic techniques ensuring data integrity and secure communication.
- A decentralized consensus mechanism for verifying transactions and identities.
- By integrating blockchain with IoT security mechanisms, organizations can significantly mitigate cybersecurity risks, ensuring a secure, transparent, and scalable IoT ecosystem.

5. Performance and Scalability Challenges

Despite the significant security enhancements blockchain brings to IoT ecosystems, its integration presents several performance and scalability limitations. These challenges arise due to the resource-constrained nature of IoT devices and the computational overhead of blockchain operations. Addressing these issues is critical to ensuring blockchain's seamless adoption in IoT networks.

5.1. Transaction Latency

One of the primary performance challenges is high transaction latency, which affects real-time IoT applications. Public blockchain networks, such as Bitcoin and Ethereum, require multiple confirmations before finalizing a transaction, leading to delays that are impractical for time-sensitive IoT operations.

Causes of Transaction Latency:

- Consensus Mechanisms: Proof-of-Work (PoW) and Proof-of-Stake (PoS) protocols introduce delays due to mining and validation processes.
- Network Congestion: High transaction volume increases wait times, making real-time IoT data processing inefficient.
- Block Size Limitations: Fixed block sizes constrain the number of transactions that can be processed per block, further slowing the system.

Solutions to Reduce Transaction Latency:

- To overcome transaction delays and improve efficiency, several blockchain scaling techniques have been proposed:
- Off-Chain Scaling: Transactions are processed outside the main blockchain, reducing on-chain congestion. Example: Lightning Network for micropayments.
- Sharding: The blockchain is partitioned into smaller "shards", allowing parallel transaction processing. Example: Ethereum 2.0.
- Sidechains: Separate chains operate alongside the main blockchain, handling specific transactions to reduce load. Example: Plasma sidechains.

These techniques aim to enhance transaction throughput while maintaining decentralization and security, making blockchain more viable for real-time IoT applications.

5.2. Storage Overhead

Another critical challenge in blockchain-IoT integration is storage overhead, as IoT devices typically have limited processing power and memory capacity. Storing an entire blockchain ledger on constrained devices is impractical, leading to scalability concerns.

Causes of Storage Overhead:

- Full Nodes: Traditional blockchain networks require full nodes to store and validate all transactions, consuming substantial memory.
- Data Redundancy: Each node in a blockchain network must store the complete ledger, leading to unnecessary duplication.
- Continuous Growth: Blockchain size increases exponentially, making it unmanageable for IoT devices with restricted storage.

Solutions to Minimize Storage Overhead:

Several lightweight blockchain implementations are being explored to optimize storage use in IoT networks:

- Lightweight Nodes (SPV Nodes): IoT devices can operate as Simplified Payment Verification (SPV) nodes, storing only block headers instead of the entire blockchain.
- Distributed Ledger Pruning: Redundant and outdated transaction records are periodically removed, reducing storage demands while preserving security. Example: Ethereum State Pruning.
- Interplanetary File System (IPFS): Instead of storing all transaction data on-chain, IPFS enables off-chain decentralized storage, significantly reducing storage requirements.

These approaches aim to reduce blockchain storage footprints while ensuring IoT devices can participate in blockchain networks without excessive computational overhead.

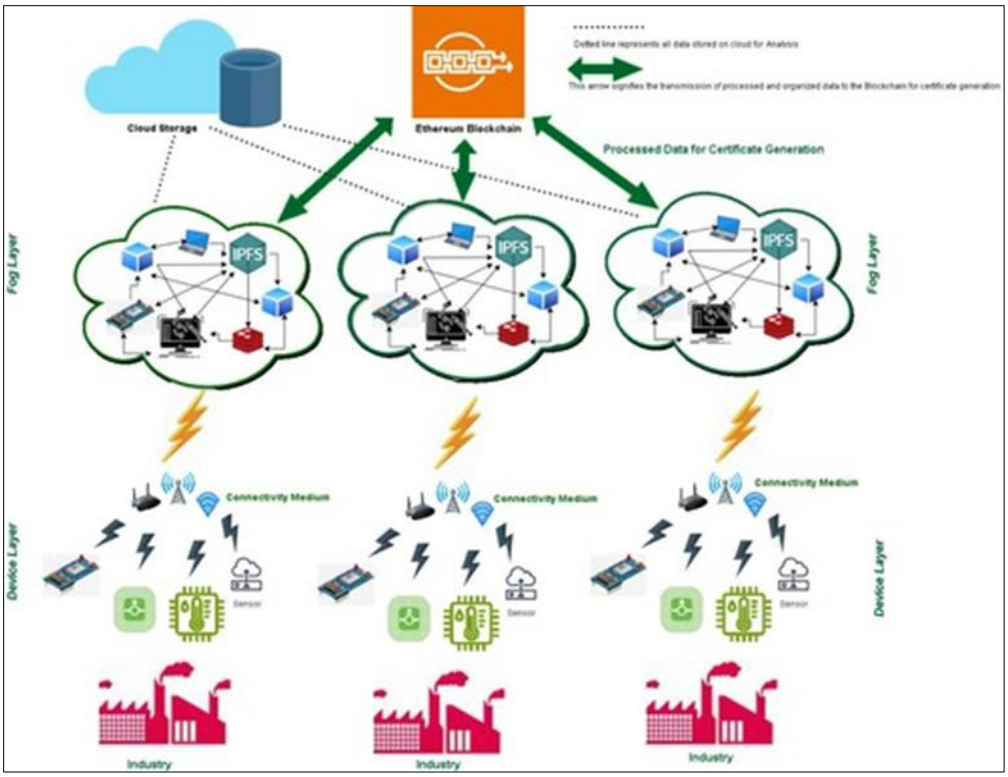

Figure 2 Scalability Optimization Techniques in Blockchain-IoT Integration

By addressing these performance and scalability challenges, blockchain can be efficiently integrated into IoT networks, unlocking its full potential for secure, decentralized, and real-time IoT applications.

6. Case Studies

The integration of blockchain in IoT has been successfully implemented across various industries, improving security, data integrity, and automation. The following case studies highlight key applications of blockchain technology in IoT-driven sectors.

6.1. Smart Healthcare

Healthcare systems generate vast amounts of sensitive patient data, requiring strong security measures to ensure privacy and prevent unauthorized access. Blockchain provides a tamper-proof and decentralized way to store and share patient records.

6.1.1. Key Benefits

- Enhanced Data Security: Blockchain encrypts patient records, ensuring that medical data remains immutable and untraceable to unauthorized parties.
- Decentralized Patient Records: Patients can own and control access to their medical history, reducing risks of data breaches.
- Fraud Prevention: Eliminates counterfeit drugs and medical fraud by enabling secure tracking of pharmaceuticals through the supply chain.
- *Example:* Estonia has implemented a blockchain-based eHealth system, allowing secure patient record management and real-time access to medical history by authorized healthcare providers.

6.2. Industrial IoT (IIoT) Security

In industrial applications, supply chain transparency and access control are crucial for efficient and secure operations. Blockchain enables smart contracts that automate business processes while ensuring data integrity.

6.2.1. Key Benefits

- Supply Chain Traceability: Blockchain tracks product movement from manufacturers to consumers, ensuring authenticity and reducing fraud.
- Automated Contract Execution: Smart contracts enforce pre-set conditions for secure and transparent industrial transactions.
- Access Control & Device Authentication: Ensures only authorized devices and personnel can interact with IoT-enabled industrial equipment.
- *Example:* Walmart and IBM have adopted blockchain-based supply chain tracking systems to improve food traceability, reducing fraud and contamination risks.

Table 2 Blockchain Use Cases in IoT Domains

Application	**Benefits**
Smart Healthcare	Secure patient data, fraud prevention
Industrial IoT	Supply chain tracking, access control
Smart Cities	Secure communication, decentralized identity

7. Future Directions

As blockchain adoption in IoT expands, future research and development efforts must address challenges related to scalability, security, and interoperability. Key areas of innovation include:

7.1. Integration with AI

- AI-driven anomaly detection can enhance blockchain-based IoT security by identifying malicious activities and predicting cyber threats.
- Machine learning algorithms can optimize blockchain transactions, reducing latency and improving efficiency.

7.2. Quantum-Resistant Cryptography

- The rise of quantum computing poses potential threats to current blockchain encryption standards.
- Post-quantum cryptography (PQC) methods, such as lattice-based encryption and quantum key distribution (QKD), are being explored to ensure blockchain resilience against quantum attacks.

7.3. Interoperability Solutions

- Current blockchain networks operate independently, limiting cross-platform functionality.
- Cross-chain communication protocols will enable seamless data exchange between different blockchain ecosystems, ensuring better integration in IoT frameworks.

8. Conclusion

Blockchain technology presents a transformative approach to enhancing IoT security by ensuring data integrity, secure communication, and decentralized control. By leveraging smart contracts, cryptographic authentication, and immutable ledgers, blockchain mitigates many security vulnerabilities inherent in IoT networks. However, despite its advantages, blockchain faces challenges such as high energy consumption, transaction latency, and scalability constraints. Solutions like off-chain processing, optimized consensus mechanisms, and AI-driven automation will be key to improving blockchain's efficiency for large-scale IoT deployments.

Future research should focus on:

- Developing lightweight blockchain protocols for IoT devices.
- Enhancing AI integration to improve security and performance.
- Implementing quantum-resistant cryptographic techniques to future-proof blockchain security.

By addressing these challenges and leveraging emerging technologies, blockchain will play a crucial role in next-generation IoT security frameworks, ensuring secure, scalable, and autonomous IoT ecosystems.

References

[1]. Fan, Kai, Shangyang Wang, Yanhui Ren, Kan Yang, Zheng Yan, Hui Li, and Yintang Yang. "Blockchain-based secure time protection scheme in IoT." IEEE Internet of Things Journal 6, no. 3 (2018): 4671-4679.

[2]. Fakhri, Dinan, and Kusprasapta Mutijarsa. "Secure IoT communication using blockchain technology." In 2018 international symposium on electronics and smart devices (ISESD), pp. 1-6. IEEE, 2018.

[3]. Patil, Akash Suresh, Bayu Adhi Tama, Youngho Park, and Kyung-Hyune Rhee. "A framework for blockchain based secure smart green house farming." In Advances in Computer Science and Ubiquitous Computing: CSA-CUTE 17, pp. 1162-1167. Springer Singapore, 2018.

[4]. Krishnan, K. Navaneeth, Roopesh Jenu, Tintu Joseph, and M. L. Silpa. "Blockchain based security framework for IoT implementations." In 2018 international CET conference on control, communication, and computing (IC4), pp. 425-429. IEEE, 2018.

[5]. Pulkkis, Göran, Jonny Karlsson, and Magnus Westerlund. "Blockchain-Based Security Solutions for IoT Systems." Internet of things A to Z: technologies and applications (2018): 255-274.