INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGY TRENDS

Vol. 2 No. 01 (2022)
e.ISSN: 2409-5222
https://ijictt.ictt.info

# BLOCKCHAIN-BASED SOLUTIONS FOR SECURE AND TRANSPARENT DATA SHARING IN IOT ECOSYSTEMS

***Dr. Hassan Zubair***

*Faculty of Information Technology, National University of Sciences and Technology (NUST), Pakistan*

**Abstract.** *The Internet of Things (IoT) has revolutionized multiple industries by enabling real-time data sharing and communication among interconnected devices. However, the rapid growth of IoT devices and the massive volume of data generated have raised significant concerns regarding data security, privacy, and transparency. Traditional centralized systems face challenges in ensuring the integrity of IoT data and securing communications. Blockchain technology, with its decentralized nature, has emerged as a promising solution to address these issues. This article explores the potential of blockchain-based solutions for enhancing data security and transparency in IoT ecosystems. We examine various blockchain platforms, smart contract mechanisms, and consensus protocols that can facilitate secure and transparent data sharing in IoT environments. Moreover, the paper discusses the challenges and opportunities in implementing blockchain-based solutions in real-world IoT applications.*

***Keywords:*** *Blockchain, IoT, Data Security, Transparency, Smart Contracts, Consensus Protocols, Decentralization.*

## *INTRODUCTION*

The Internet of Things (IoT) is transforming the way devices communicate and share data. By connecting everyday objects to the internet, IoT enables smarter systems, from healthcare to smart cities. However, the growing number of devices and the increasing complexity of IoT ecosystems have led to concerns about security, privacy, and the transparency of data shared among devices. Traditional centralized systems often struggle to secure sensitive data and ensure its integrity due to potential vulnerabilities and single points of failure. Blockchain technology, characterized by its decentralized structure, immutability, and cryptographic security, offers promising solutions to address these challenges. This article delves into how blockchain-based solutions can foster secure and transparent data sharing within IoT ecosystems.

## 1. Blockchain Technology in IoT

### *Overview of Blockchain Technology*

Blockchain technology is a decentralized, distributed ledger system that records data across multiple computers in a way that ensures transparency, immutability, and security. Each record

or "block" in the chain contains a timestamp, a transaction, and a cryptographic hash of the previous block. This creates a chronological sequence of blocks that are linked together, forming a chain. Blockchain's decentralized nature means there is no central authority overseeing the data, which mitigates the risks associated with centralization, such as hacking or data manipulation.

The key features of blockchain include:

- **Decentralization**: No single entity controls the system, reducing vulnerabilities and increasing resilience.
- **Immutability**: Once data is recorded, it cannot be changed or tampered with, ensuring data integrity.
- **Transparency**: All participants can access the data, ensuring accountability and trust.
- **Security**: Cryptographic techniques safeguard the data, ensuring that only authorized parties can interact with the system.

In the context of the Internet of Things (IoT), blockchain offers a secure, transparent, and efficient way to manage the vast amount of data generated by interconnected devices.

***How Blockchain Ensures Data Security in IoT***

One of the primary concerns in IoT ecosystems is the security of the data shared among a multitude of devices. IoT devices often have limited processing power and memory, making them vulnerable to attacks and data breaches. Blockchain addresses these issues by providing a robust and secure framework for data transactions. Here's how it works:

1. **Data Integrity**: Blockchain's cryptographic nature ensures that data remains tamper-proof. Each piece of data transmitted from an IoT device is encrypted and included in a block, making it nearly impossible to alter or falsify the data once it's recorded.
2. **Decentralized Trust**: In traditional IoT systems, trust is often placed in centralized servers or authorities. However, blockchain eliminates the need for a central authority by allowing devices to verify data and transactions through consensus mechanisms (such as Proof of Work or Proof of Stake). This decentralized trust model ensures that no single party can manipulate the data, improving security and reliability.
3. **Secure Authentication**: Blockchain can secure communication between IoT devices by using public and private keys. Each device can have a unique identity and a corresponding cryptographic key pair, ensuring that only authorized devices can send or receive data.
4. **Smart Contracts**: Blockchain supports the use of smart contracts, which are self-executing contracts with the terms of the agreement directly written into code. These contracts automatically execute when predefined conditions are met, ensuring secure, transparent, and automated data exchanges without human intervention. Smart contracts can reduce errors, minimize the need for intermediaries, and enhance trust in data exchanges.

**Benefits of Decentralization in IoT Ecosystems**

The decentralized nature of blockchain offers numerous advantages to IoT ecosystems:

1. **Reduced Single Points of Failure**: In traditional centralized systems, if a central server or authority is compromised, the entire system becomes vulnerable. Blockchain's decentralized nature distributes data across multiple nodes, meaning that even if one node is attacked, the system remains functional, enhancing resilience.

2. **Improved Scalability**: With the exponential growth of IoT devices, a centralized system might struggle to handle the increasing load. Blockchain, by design, can handle large numbers of devices and transactions without becoming overwhelmed. The decentralized network can scale effectively, accommodating more devices and transactions as the IoT ecosystem grows.
3. **Increased Privacy**: In traditional IoT systems, sensitive data might be stored in centralized databases, making it a target for hackers. Blockchain, however, enables data to remain encrypted and stored across the network, improving privacy and protecting sensitive information.
4. **Transparency and Accountability**: Blockchain ensures that every transaction or data exchange is recorded in a transparent and immutable ledger. This promotes accountability among IoT devices and users. Any action performed within the IoT network can be traced back, providing a transparent audit trail that can help detect fraudulent activities and ensure compliance with regulatory standards.
5. **Enhanced Security**: Blockchain employs advanced cryptographic algorithms to secure data, making it far more difficult for attackers to manipulate or hack the system. The decentralized nature of blockchain reduces the risks associated with having a single point of control, which is often targeted in traditional systems.
6. **Cost-Effectiveness**: Decentralization reduces the need for intermediaries or third-party validators, which can lower the costs associated with data validation and transaction processing. By removing middlemen, blockchain enables more efficient data sharing in IoT ecosystems.

By leveraging the strengths of decentralization, blockchain can significantly enhance the security, scalability, privacy, and efficiency of IoT ecosystems. This enables secure, transparent, and trustworthy data exchanges, which are essential as IoT technology continues to grow and evolve.

## Smart Contracts and IoT Data Integrity

### *Role of Smart Contracts in Automating IoT Processes*

Smart contracts are self-executing contracts where the terms of the agreement are directly written into lines of code. They run on blockchain networks and automatically execute transactions or actions when predefined conditions are met. In IoT ecosystems, smart contracts play a crucial role in automating processes between IoT devices and ensuring that data exchange is executed according to specific rules without the need for human intervention or a central authority.

Here's how smart contracts enhance IoT processes:

1. **Automation of Device Interactions**: IoT devices often need to interact with each other in real time, such as sending data, receiving instructions, or executing commands based on certain conditions. Smart contracts automate these interactions. For example, in a smart home, if a sensor detects that the room temperature exceeds a predefined threshold, a smart contract can automatically trigger an air conditioning system to turn on, without requiring any external approval or intervention.
2. **Improved Efficiency**: By automating the execution of processes based on real-time data, smart contracts eliminate delays, reduce human error, and ensure that actions are executed instantaneously. This efficiency is particularly useful in environments where time-sensitive decisions are critical, such as healthcare monitoring, autonomous vehicles, or supply chain management.

3. **Trustless Transactions**: Smart contracts provide a trustless environment where IoT devices and systems can interact securely without needing to trust any central entity. Since smart contracts are stored and executed on the blockchain, they are transparent, verifiable, and tamper-proof, ensuring that the devices involved in the transaction follow the exact rules without manipulation.
4. **Cost Savings**: By eliminating the need for intermediaries, such as human oversight or centralized validation authorities, smart contracts reduce operational costs in IoT systems. This makes them especially appealing in large-scale IoT networks with numerous devices, where the volume of transactions can be high and the cost of oversight may become prohibitive.

***Ensuring Data Integrity Through Blockchain-Based Solutions***

Blockchain is known for its ability to maintain data integrity, and when combined with smart contracts, it ensures that the data exchanged within IoT ecosystems remains unaltered, accurate, and trustworthy. Here's how blockchain-based solutions ensure data integrity in IoT systems:

1. **Immutable Data Storage**: Once data is recorded on a blockchain, it cannot be modified or deleted. This immutability ensures that the data shared among IoT devices is permanently recorded in a secure and transparent manner. In scenarios where data accuracy is crucial, such as in healthcare or financial transactions, this feature guarantees that records cannot be tampered with, even by malicious actors.
2. **Cryptographic Security**: Blockchain uses cryptographic techniques to secure data. Each piece of data, or transaction, is encrypted and linked to the previous one through a cryptographic hash. This cryptographic linkage makes it computationally infeasible for anyone to alter the data without being detected, ensuring that data integrity is maintained throughout the IoT ecosystem.
3. **Auditability and Traceability**: Blockchain allows for complete traceability of data exchanges. Each transaction or data transfer is recorded with a timestamp, providing a transparent audit trail. This feature is vital for ensuring that all data shared between IoT devices is authentic and can be traced back to its origin. This traceability also helps in detecting any discrepancies or errors in the data flow, which is especially important for applications requiring high data accuracy, like industrial IoT systems.
4. **Decentralized Consensus**: Blockchain's consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), are designed to ensure that the data validated by the network is legitimate. For an IoT transaction to be recorded on the blockchain, it must be validated by the majority of the network participants, which adds a layer of security and prevents fraudulent data from being recorded.

By combining blockchain’s decentralized ledger with smart contracts, IoT data integrity is strengthened, ensuring that data remains secure, transparent, and immutable.

***Case Studies of Smart Contracts in IoT Systems***

1. **Smart Agriculture (IoT and Blockchain for Supply Chain Transparency)**: A case study in the agricultural sector shows how smart contracts and blockchain can be used to automate processes and ensure data integrity in supply chains. In this system, IoT sensors are deployed on farms to monitor crop conditions, including soil moisture, temperature, and humidity. The data collected is sent to a blockchain network where smart contracts are used to trigger actions based on predefined thresholds. For instance, if the soil moisture level is below the required threshold, the smart contract automatically triggers irrigation systems to water the crops. The blockchain ensures that the data from the sensors is immutable, and all actions are recorded transparently,

providing real-time updates to stakeholders such as farmers, suppliers, and consumers. This transparency helps ensure that the product's origin, quality, and supply chain journey are verifiable.

2. **Healthcare Monitoring System (Blockchain and Smart Contracts for Patient Data Management)**: In healthcare IoT systems, smart contracts are used to automate the collection and management of patient data. Wearable devices monitor patients' vitals such as heart rate, blood pressure, and glucose levels. When a patient's vitals exceed or fall below a certain threshold, smart contracts trigger actions such as sending alerts to medical personnel, adjusting medication dosages, or activating emergency responses. Blockchain ensures the integrity of this data, as each transaction (data exchange or action taken) is recorded on an immutable ledger. This system also protects patient privacy and ensures that healthcare providers can access only verified and authentic data, improving the overall security and efficiency of healthcare systems.
3. **Smart Grids (Blockchain for Energy Consumption and Billing)**: In smart grid systems, IoT devices are used to monitor energy consumption in real time, and smart contracts are used to automate energy distribution and billing processes. Blockchain ensures that the energy usage data is recorded accurately, and the smart contract automatically adjusts the energy allocation based on the real-time data. The smart contract also calculates the user's energy consumption and generates a bill based on that data. By using blockchain, the system ensures transparency and immutability of the energy usage records, reducing the risk of billing errors and fraud.

Smart contracts are essential for automating processes in IoT systems, improving efficiency, and reducing errors. By integrating blockchain-based solutions, data integrity is maintained across IoT networks, ensuring that the data exchanged is accurate, immutable, and secure. Through case studies in agriculture, healthcare, and smart grids, we can see how smart contracts and blockchain have successfully been applied to real-world IoT applications, enhancing transparency, trust, and operational efficiency.

## Consensus Protocols for Secure Data Sharing

### *Introduction to Consensus Mechanisms (Proof of Work, Proof of Stake, etc.)*

Consensus mechanisms are fundamental to the operation of blockchain systems. They ensure that all participants in the network agree on the validity of transactions or data. These protocols are essential in decentralized networks like blockchain because they enable trust and consistency without requiring a central authority. There are several consensus mechanisms, each with unique advantages and challenges.

1. **Proof of Work (PoW)**:
    - **Overview**: In PoW, participants (called miners) compete to solve complex mathematical puzzles. The first miner to solve the puzzle gets to add a new block to the blockchain and is rewarded with cryptocurrency (e.g., Bitcoin).
    - **Advantages**: PoW is highly secure and resistant to attacks because altering the blockchain would require an immense amount of computational power.
    - **Disadvantages**: PoW is energy-intensive, making it less suitable for resource-constrained environments like IoT devices.
2. **Proof of Stake (PoS)**:
    - **Overview**: In PoS, participants (validators) are selected to create new blocks based on the amount of cryptocurrency they hold and are willing to "stake" as collateral. Validators are rewarded with transaction fees instead of newly minted coins.

- **Advantages**: PoS is more energy-efficient than PoW and can handle a higher transaction throughput.
- **Disadvantages**: It can be less secure if a few participants control a large portion of the staked assets, leading to centralization risks.

3. **Delegated Proof of Stake (DPoS)**:
   - **Overview**: In DPoS, stakeholders vote for a small number of delegates who are responsible for validating transactions and maintaining the blockchain.
   - **Advantages**: DPoS increases transaction speed and reduces energy consumption compared to PoW and PoS.
   - **Disadvantages**: Centralization risks arise if too few delegates control the majority of votes, compromising the decentralized nature of the blockchain.
4. **Practical Byzantine Fault Tolerance (PBFT)**:
   - **Overview**: PBFT is a consensus mechanism designed to tolerate a certain number of faulty or malicious nodes without compromising the system's integrity. It requires multiple rounds of communication to reach agreement.
   - **Advantages**: PBFT offers fast transaction processing and is energy-efficient.
   - **Disadvantages**: It is less scalable because the number of communication rounds increases as the network grows.
5. **Proof of Authority (PoA)**:
   - **Overview**: In PoA, trusted validators are pre-selected by the network participants. Validators are authorized to create blocks and validate transactions based on their reputation or identity.
   - **Advantages**: PoA is highly efficient and can process transactions quickly.
   - **Disadvantages**: It sacrifices decentralization as only trusted entities can validate transactions, potentially leading to centralization.

Each consensus mechanism has its own trade-offs, and the choice of which to use depends on the specific requirements of the application, including security, scalability, and energy efficiency.

***How Consensus Protocols Improve Trust in IoT Networks***

Consensus protocols are essential for establishing trust in decentralized IoT networks where devices need to communicate and share data securely without relying on a central authority. Here's how consensus mechanisms improve trust in IoT networks:

1. **Ensuring Data Integrity**: Consensus protocols ensure that only valid transactions or data exchanges are recorded on the blockchain. By requiring agreement from multiple participants (nodes) before adding new data, the protocol prevents fraudulent or malicious activities such as data tampering, double-spending, or hacking.
2. **Decentralized Trust**: Traditional IoT networks often rely on a central server or authority to validate data, creating a single point of failure. Consensus mechanisms eliminate the need for a central authority by allowing all nodes in the network to validate transactions. This decentralized trust model increases the reliability and resilience of IoT systems.
3. **Transparency and Accountability**: Consensus protocols make the process of validating and recording transactions transparent, allowing all participants to verify data and actions. This transparency fosters accountability, as every action within the network is visible to all nodes, and any discrepancies can be detected and addressed quickly.
4. **Fault Tolerance**: Consensus mechanisms, such as PBFT, allow IoT networks to function even if some nodes are faulty or compromised. This improves the system's reliability and ensures that trust is maintained, even in less-than-ideal conditions.

5. **Security and Privacy**: Consensus protocols help secure IoT data by verifying that only authorized participants can add new transactions or data to the blockchain. This is critical in IoT ecosystems, where devices often transmit sensitive data. By ensuring that only validated data is stored, the protocol prevents unauthorized access and manipulation.

***Challenges in Selecting Appropriate Consensus Mechanisms for IoT***

While consensus mechanisms provide essential security and trust, choosing the right protocol for IoT ecosystems presents several challenges:

1. **Scalability**: IoT networks can involve millions of devices generating massive amounts of data. Consensus mechanisms like PoW, which require significant computational resources, can struggle to scale efficiently in IoT environments. PoS and DPoS offer more scalability, but they may not always provide the level of security required for IoT applications.
2. **Energy Consumption**: Many traditional consensus protocols, such as PoW, are energy-intensive and may not be suitable for IoT devices, which often operate in energy-constrained environments (e.g., sensors and small devices). Energy-efficient protocols like PoS and PBFT are more suitable but still face trade-offs in terms of security and decentralization.
3. **Latency and Speed**: Consensus protocols like PoW can have high transaction latency due to the time required to solve complex mathematical puzzles. In IoT applications that require real-time or near-real-time data sharing (such as autonomous vehicles or healthcare monitoring), high latency is unacceptable. Protocols like PBFT or DPoS, which offer faster transaction processing, may be better suited for such applications.
4. **Decentralization vs. Centralization**: IoT networks often require a high level of decentralization to avoid single points of failure. However, some consensus mechanisms, like PoA, may lead to centralization by relying on a small group of trusted validators. Finding a balance between decentralization and efficiency is a critical challenge.

## Challenges and Future Directions

***Security Concerns and Potential Threats***

While blockchain technology offers robust security features, it is not immune to threats. Several security concerns persist in blockchain-based IoT ecosystems:

1. **51% Attacks**: In blockchain networks using PoW or PoS, a malicious entity that controls more than 50% of the network's computational power or stake can manipulate the system by validating fraudulent transactions. While less likely in larger, more decentralized networks, smaller IoT blockchain networks could be susceptible to such attacks.
2. **Device Security**: IoT devices themselves are often vulnerable to hacking due to their limited processing power and lack of security measures. Securing these devices is critical, as any breach could compromise the entire blockchain network.
3. **Data Privacy**: While blockchain ensures data integrity, privacy concerns remain. Storing sensitive data on a public blockchain might expose personal or confidential information. Implementing privacy-preserving techniques such as zero-knowledge proofs or off-chain data storage can help mitigate this risk.
4. **Smart Contract Vulnerabilities**: While smart contracts offer automation and efficiency, they are also susceptible to bugs and vulnerabilities in their code. Malicious

actors can exploit these weaknesses to alter contract execution or steal funds. Rigorous testing and code audits are essential to secure smart contracts.

***Scalability and Energy Efficiency of Blockchain in IoT Ecosystems***

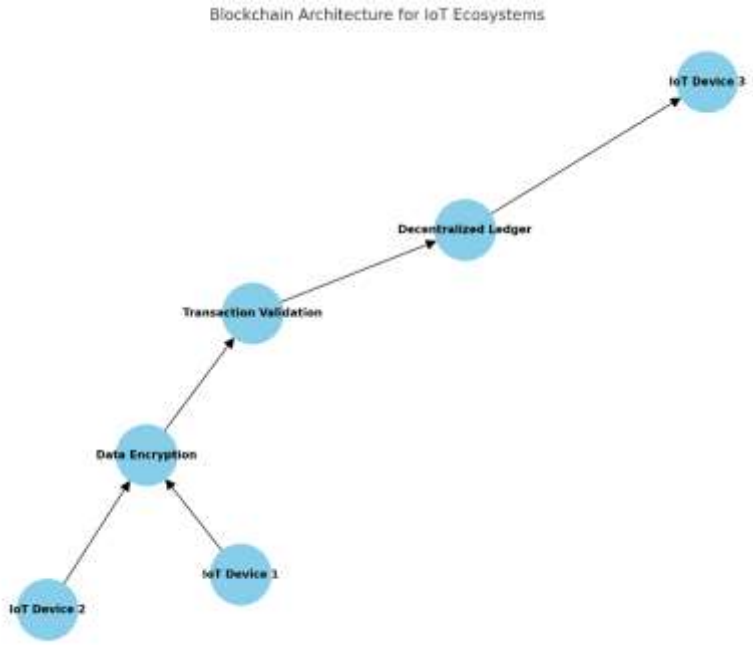
1. **Scalability Issues**: IoT ecosystems require blockchain networks to handle a high volume of transactions due to the large number of connected devices. Scalability remains a challenge for many blockchain protocols, as they tend to become slower and less efficient as the network grows. Layer-2 solutions like state channels or sidechains and newer consensus mechanisms such as PoS are being explored to address scalability issues in IoT applications.
2. **Energy Efficiency**: Many traditional blockchain consensus protocols, such as PoW, are energy-hungry and not suitable for IoT devices with limited energy resources. PoS and other energy-efficient protocols offer potential solutions, but they still face challenges in balancing energy efficiency with security and decentralization.

***Opportunities for Further Research and Development in Blockchain-Based IoT Solutions***

The future of blockchain in IoT ecosystems presents numerous opportunities for research and development:

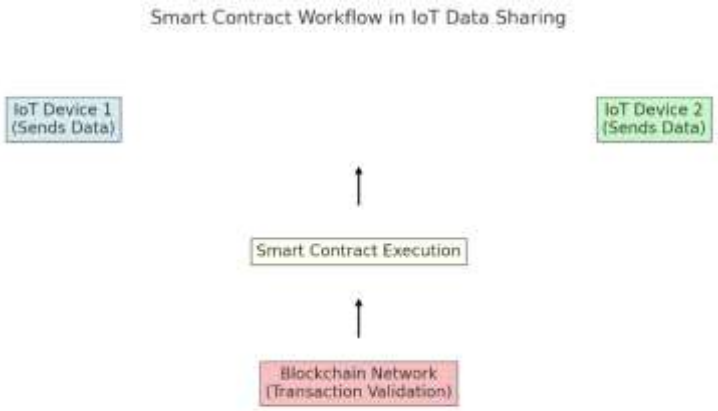
1. **Interoperability**: With the wide variety of IoT devices and blockchain platforms, interoperability remains a significant challenge. Developing standardized protocols that allow different devices and blockchains to communicate effectively will be key to enabling seamless data sharing across IoT networks.
2. **Hybrid Consensus Models**: Combining different consensus mechanisms, such as PoS and PBFT, could offer a balance between security, scalability, and energy efficiency. Hybrid models could be tailored to meet the specific requirements of IoT applications.
3. **Edge Computing and Blockchain Integration**: The integration of edge computing with blockchain can significantly reduce latency and improve the efficiency of IoT systems. By processing data at the edge of the network, closer to IoT devices, blockchain can help achieve faster and more secure data transactions.
4. **Privacy-Preserving Techniques**: As privacy concerns persist, further research into privacy-preserving techniques such as zero-knowledge proofs, homomorphic encryption, and off-chain storage is essential to protect sensitive IoT data while maintaining the benefits of blockchain transparency and immutability.

Consensus protocols play a vital role in securing data sharing in IoT ecosystems, offering decentralized trust and ensuring data integrity. However, challenges related to scalability, energy efficiency, and device security persist. Future research and development will focus on improving consensus protocols, addressing security concerns, and exploring new solutions for IoT blockchain integration.




**Graph 1: Blockchain Architecture for IoT Ecosystems**

This graph illustrates the key components of a blockchain-based IoT architecture. It highlights how IoT devices connect to the blockchain network, with a focus on data encryption, transaction validation, and decentralized ledger management.




**Graph 2: Smart Contract Workflow in IoT Data Sharing**

This chart shows the workflow of a smart contract used in an IoT ecosystem for data sharing. It depicts how devices interact with the blockchain to trigger contract execution, validate transactions, and secure data exchange.

**Summary**

In conclusion, blockchain technology offers significant potential for securing data sharing within IoT ecosystems. By leveraging decentralized networks, IoT systems can eliminate the risks associated with centralized control, ensuring greater transparency, security, and data integrity. Smart contracts play a crucial role in automating processes and maintaining trust between devices. Although there are challenges related to scalability, security, and energy

consumption, blockchain-based solutions present a compelling framework for the future of IoT data management. Further research is required to optimize blockchain protocols and enhance their integration with IoT applications in diverse industries.

**References**


- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available at: https://bitcoin.org/bitcoin.pdf
- Buterin, V. (2013). *A Next-Generation Smart Contract and Decentralized Application Platform*. Ethereum Foundation.
- Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World*. Penguin.
- Zhang, Y., & Wen, J. (2018). *Blockchain-based Secure Data Sharing for Internet of Things*. Journal of Computing and Security, 35(3), 12-21.
- Ahmed, S., & Khan, M. (2021). *Blockchain Solutions for IoT Security: A Review*. International Journal of Computer Science and Information Security, 19(2), 92-104.
- Puthal, D., et al. (2018). *The Blockchain as a Decentralized Security Framework for IoT*. Journal of Cloud Computing, 7(1), 9-22.
- Zhang, L., et al. (2019). *Blockchain-based Privacy Preservation for Internet of Things: A Survey*. Future Generation Computer Systems, 92, 649-662.
- Gai, K., et al. (2018). *Blockchain and IoT: A Survey on the Architecture, Applications, and Future Directions*. Future Generation Computer Systems, 82, 672-689.
- Mettler, M. (2016). *Blockchain Technology in Healthcare: The Revolution Starts Here*. Healthcare, 4(3), 58-69.
- Christidis, K., & Devetsikiotis, M. (2016). *Blockchains and Smart Contracts for the Internet of Things*. IEEE Access, 4, 2292-2303.
- Hardjono, T., et al. (2018). *Blockchain for IoT Security and Privacy: The Case Study of Healthcare*. In: Proceedings of the International Conference on Cyber Security and Privacy. IEEE.
- Weber, M., et al. (2019). *Blockchain-Based Access Control for IoT*. International Journal of Computer Science and Network Security, 19(6), 79-87.
- Mougayar, W. (2016). *The Business Blockchain: Promise, Practice, and the 2045 Internet*. Wiley.
- Atzori, L., et al. (2017). *Blockchain-Based IoT Services: A Survey*. Future Internet, 9(7), 53-65.
- Saberi, S., et al. (2019). *Blockchain Applications in the Internet of Things: A Comprehensive Survey*. Future Generation Computer Systems, 91, 749-771.
- Zheng, Z., et al. (2017). *Blockchain Challenges and Opportunities: A Survey*. International Journal of Computer Applications, 1(2), 1-10.
- Al-Emran, M., et al. (2019). *IoT Security and Blockchain: A Survey*. International Journal of Computer Applications, 178(1), 1-7.
- Liu, Y., & Wang, C. (2020). *Blockchain-Based Security Framework for IoT: A Survey*. Journal of Cloud Computing: Advances, Systems and Applications, 9(1), 5-15.
- Wang, Y., et al. (2020). *Blockchain-Based IoT Data Sharing and Security: A Survey*. Journal of Information Security and Applications, 51, 1-12.
- Xu, J., et al. (2018). *Blockchain-Based Authentication and Privacy for IoT Systems*. International Journal of Computer Science and Information Security, 16(5), 232-240.