Engineering and Technology Journal e-ISSN: 2456-3358
Volume 10 Issue 11 November-2025, Page No.-7969-7975
DOI: 10.47191/etj/v10i11.28, I.F. – 8.482

Blockchain-Enabled Information Systems for Secure Data Management in Smart Cities

Mohammed Ibrahim Mahdi
Computer Science Department, Computer Science and IT Faculty, Wasit University, Al-kut, Iraq

ABSTRACT: Modern smart cities rely on the continuous collection, analysis and sharing of data from millions of sensors, vehicles and public services. These large data volumes are essential for informed decision-making but expose cities to vulnerabilities such as data tampering, unauthorized access and privacy breaches. Recent research shows that blockchain's properties—decentralization, immutability and consensus—offer a transparent and tamper-proof backbone for smart city information systems. This paper reviews state-of-the-art blockchain-enabled systems and proposes a unified framework for secure data management in smart cities. We synthesize insights from literature on decentralized trust models, access control for IoT devices, hybrid detection and prevention schemes, consensus mechanisms and blockchain energy trading, waste management, smart governance and patient digital twins. The paper then presents a conceptual architecture for blockchain-enabled information systems and compares existing frameworks using quantitative metrics such as transaction throughput and detection accuracy. The analysis shows that integrating blockchain with edge computing and smart contracts supports secure real-time services for transportation, healthcare, energy trading and waste management while addressing challenges such as scalability and privacy. We conclude with a discussion of outstanding challenges and recommendations for future research.

KEYWORDS: Smart city, Blockchain, information system, Data management

1 INTRODUCTION

With the rise of urbanisation, a new concept — smart cities, relying on a dense network of sensors, IoT devices, AI and analytics to optimise transportation, energy distribution, healthcare and waste management has quickly emerged in the spotlight as well[1]. But, while the advent of IoT and big data helps to build the aforementioned connection, it also creates the challenges of fragmented infrastructures, interoperability issues, privacy and data integrity concerns[2]. Traditional approaches to data management tend to depend on centralized servers, introducing single points of failure and susceptibility to falsification[3]. This is where blockchain comes in: a distributed ledger with blocks of immutable transactions chained together with cryptographic hashes. An administrator cannot change the data unilaterally since all nodes of the network has copy of the ledger and the update check is done through consensus. In this sense, blockchain can solve smart cities trust, security and accountability challenges[4].

Many domains such as Blockchain for smart cities show us the potential of blockchain for managing smart cities data securely. Blockchain delivers a privacy-preserving, trustless architecture to the transport domain where it enables use cases around real-time routing, congestion management and safety [5] and mitigates challenges around vehicle hacking, congestion and data tampering. For instance, in the healthcare sector, blockchain provides a way for electronic medical records to be established in a position for interoperability and tamper-proof storage so that medical professionals can securely store patients[6]. Smart contracts not only allows the fine-grained control of access over medical information. Digital twin. A digital twin [7] framework can provide an extra layer of security over medical data be controlled by smart contracts so as to ensure provable provenance. Regarding energy trading, decentralized blockchain-based systems enable peer-two-peer electricity trading. Power trading mechanisms in the smart grid used over 350 transactions per second with low CPU usage and low memory consumption via a credit-based hybrid consensus mechanism[8]. The cost-effective solution of these difficulties shows the use of blockchain in the waste management by allowing visible tracing of trash from production to disposal and auto recycling through smart contracts. Third, citizen engagement can be augmented by participation of citizens in decision making through blockchain; consortium blockchains and proof-of-authority consensus model can be used to enable secure public services while supporting participatory governance.

However, despite the benefits, challenges including scalability, interoperability, energy consumption and regulatory issues remain[2]. We provide a holistic view of blockchain-empowered information systems, and a coherent architecture that unifies IoT devices, edge computing components, blockchain networks and smart contracts to realize secure, real-time applications in a wide range of domains.

2 LITERATURE REVIEW

2.1 Blockchain and IoT security

Numerous studies examine blockchain's ability to secure IoT data. An EnPress journal article proposed a private blockchain framework for securing IoT data across transportation, healthcare and building security domains; simulations showed low latency and effective anomaly detection[10]. A SpringerOpen study combined blockchain with a message queuing system to implement attribute-based access control for IoT devices[11]. The framework supports real-time communication through RabbitMQ and ensures decentralized and immutable record keeping[12]. Another work introduced the **Hybrid Detection and Prevention IoT Framework (HDPIoTF)**, which integrates IoT sensors, gateways, blockchain networks and security analytics to provide real-time monitoring and notifications[13].

Blockchain-based authentication and trust management mechanisms have also been proposed. One system combined the **ACE authorization protocol** with the **OSCAR** security model and smart contracts to control access to smart meters, cameras and traffic lights. The implementation on Ethereum produced authentication response times under 100 ms even with multiple clients[11].

2.2 Decentralized trust frameworks and consensus mechanisms

Scalability and throughput are critical for smart city applications. A **decentralized trust framework** integrated blockchain with AI-driven threat detection and an adaptive proof-of-stake consensus (LA-PoS). The framework achieved a 98.2 % threat detection rate while reducing false positives and improving transaction throughput. By optimizing the consensus mechanism, the system reduced latency and energy consumption compared with proof-of-work blockchains[14].

In the energy sector, a credit-based hybrid consensus for blockchain-based smart grid trading increased throughput (350 TPS) and improved transaction prices[15]. The IoT-Chain architecture proposed a multilevel blockchain for IoT security, achieving up to 1 701 TPS and reducing delays by 96 – 99 %. Gateway nodes that aggregate multiple IoT transactions into a single block further enhance scalability[16].

2.3 Domain-specific applications

Transportation and mobility. By offering a trustless, immutable architecture, Blockchain is capable of alleviating congestion, emissions and security in intelligent transportation systems. It can be used in applications such as routing, micro-mobility services, and electric vehicle charging. Machine learning with anomaly detection and predictive analytics is now well integrated[11].

Healthcare. You have a right to privacy — secure medical record storage. Blockchain, besides securing medical records, supports the concept of the patient digital twin by fusing EMRs and wearable sensor generated data. Patient digital twin secured by a blockchain that leverages smart contract to regulate access and automate data updates so that privacy, provenance and latency concerns are addressed[7]. Digital twin enhances personalized healthcare and precision medicine.

Energy and resource management. Peer-to-peer energy trading and decentralized resource optimization is supported by blockchain. Evidence from literature indicates that blockchain supports energy-efficient IoT networks by offloading computation to edge devices and using lightweight consensus mechanisms[2–4]. Smart contract based peer-to-peer energy trading enables the real-time monitoring of energy generation and consumption and consequently optimizes the utilization of renewable energy sources[17].

Waste management. Waste Management Systems Blockchain is giving a good amount of transparency and traceability into waste management systems. According to an MDPI study, documenting every step of the waste lifecycle—including generation, collection, recycling and disposal—on a blockchain offers real-time monitoring and immutable records. Digital product passports and smart contracts can automate recycling, furthering circular economy efforts. A third paper idea was a decentralised storage ledger for use as an e-waste disposal tracking system, presenting a very clear tracking and eco-friendly management solution enabled by blockchain.

Smart governance and citizen engagement. This contributes to participatory governance, which, through blockchain, fosters transparency and trust in the decision making process. According to Open Research Europe, consortium blockchains with proof of authority (PoA) consensus can support bottom-up participatory processes and increase citizen engagement. The study promotes a transition from top-down engineering to collaborative governance in which citizens are partners in designing the policy and delivery of public services[18].

Digital twins and privacy. Authenticated access and provenance must be the basis of secure digital twins. We will briefly comment here an example of a blockchain-secured patient digital twin suggested in a PLoS One study featuring smart contracts that automatically update most data and enforce privacy policies, highlighting the significance of access control, interaction management, privacy and security[8].

Literature trend analysis. Co-word analysis and BERTopic modeling of 576 articles from 2016 – 2025 suggests that research on blockchain in smart cities is evolving from technology-driven investigations to domain-centric use cases specifically in mobility, healthcare, energy and waste management. It frames blockchain as a technological and ethical infrastructure for transparent, flexible and sustainable urban systems.

3 PROPOSED METHODOLOGY

3.1 System architecture

We propose a **blockchain-enabled information system** that integrates IoT devices, edge computing, blockchain networks and smart contracts (Figure 1). The architecture is organized into four layers.

At the foundation lies the **IoT layer**, which encompasses heterogeneous devices such as sensors, vehicles, smart meters, healthcare devices and waste bins. These devices continuously generate timestamped data and sign each record locally to ensure authenticity before forwarding it via secure protocols to a nearby edge gateway.

Above this, the **edge layer** consists of edge gateways that aggregate data from multiple IoT devices. Gateways perform preliminary processing—filtering, encryption and anomaly detection—and batch many sensor readings into single transactions, thereby reducing the overhead associated with submitting numerous small transactions to the blockchain[23].

The **blockchain layer** is comprised of a permissioned blockchain network employing a proof-of-stake or hybrid consensus mechanism. Validators receive batched transactions from gateways, validate them through consensus and append them to the distributed ledger. Smart contracts embedded within this layer encode access control policies, automate business logic (such as energy billing or patient record updates) and reference off-chain storage for large datasets by storing only cryptographic hashes on-chain for integrity verification.

At the top resides the **application layer**, where domain-specific applications—including transportation, healthcare, energy trading, waste management and governance—interface with smart contracts to query and update data. For example, transportation applications retrieve vehicle telemetry to optimize routes, healthcare systems access patient records under appropriate consent, energy platforms match supply and demand in peer-to-peer markets, waste management systems track disposal cycles, and governance platforms record citizen votes.

Figures

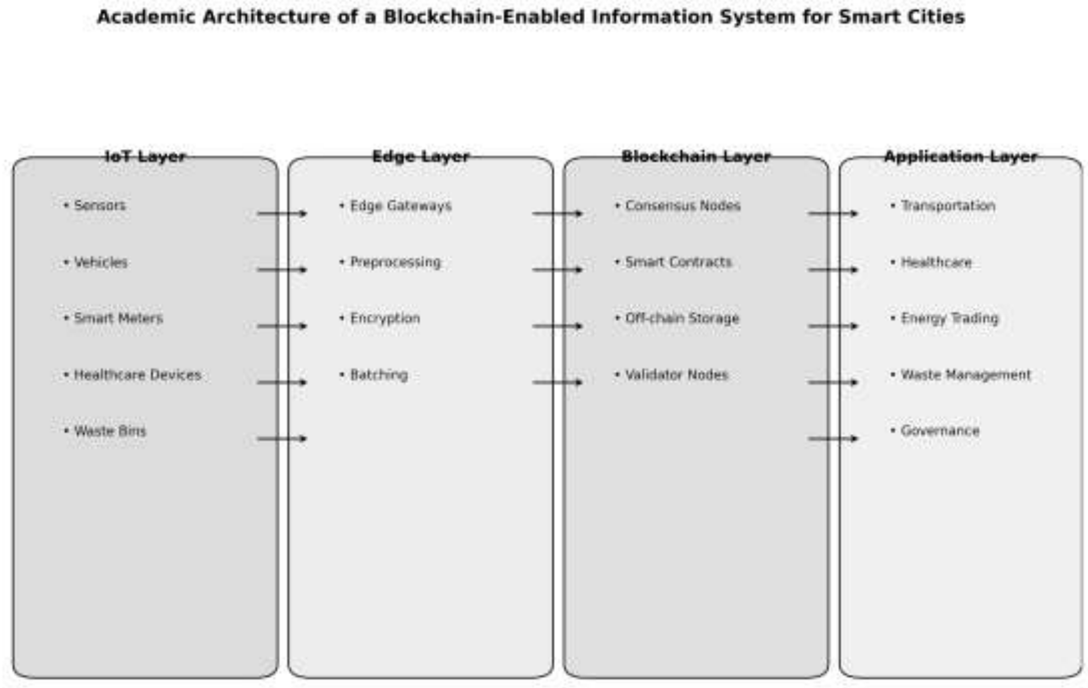

Figure 1. Academic architecture of a blockchain-enabled information system for smart cities.

3.2 Data management and security

The proposed architecture addresses data management and security holistically. At the point of capture, IoT devices produce timestamped measurements and apply cryptographic signatures to guarantee authenticity. Edge gateways validate these signatures and perform lightweight compression and aggregation of multiple sensor readings in a single transaction in order to enhance throughput [6]. A lightweight adaptive proof-of-stake or hybrid proof-of-stake/proof-of-capacity consensus mechanism on the blockchain layer ensures that the process of validating transactions remains scalable to meet increasing demand while maximising energy efficiency, producing significant improvements in energy consumption and throughput compared to traditional proof-of-work systems.

Smart contracts are central for enforcing access policies and automating settlement. Contracts embed attribute-based access control rules to ensure that only the allowed entities can access sensitive records. A healthcare contract, for instance, checks that there has been patient consent before disclosing medical information while an energy trading contract autonomously balances the supply and demand for energy in a peer-to-peer market. In order to put privacy and provenance at a safe side, they opt to record only encrypted hashes on the blockchain, and keep the sensitive data off-chain. With further methods such as zero-knowledge proofs and ring signatures, those taking part can demonstrate possession of the necessary characteristics without having had to identify themselves. Smart contracts also keep immutable ledgers and audit logs providing traceability and accountability.

3.3 Evaluation strategy

A range of quantitative metrics can be used to evaluate the performance of the proposed architecture. The transaction throughput, expressed in transaction per second (TPS), is a metric that reflects how many validated transactions the network can support; a high transaction throughput is necessary if the application of the smart city is real-time. Current frameworks show that multilevel blockchains have a capacity of up to 1,701 TPS while energy trading systems have around 350 TPS with minimal resource utilization. Latency indicates the end-to-end delay from when data is created to when it is confirmed, as for example <100 ms for the response times of the ACE+OSCAR mechanism; Detection accuracy measures the security of the system when exposed to threats, but minimizing false positives, such as a 98.2 % detection rate for the decentralized trust framework. Energy Consume: which evaluate the energy consumption of the consensus algorithm and device actions; several studies find that hybrid consensus and edge offloading save energy significantly compared to the proof-of-work blockchains. Scalability and storage cost Finally — how performance scales as the number of devices / transactions grows. Transaction aggregation and off-chain storage are methods to avoid overloading the processing load.

To validate these theoretical expectations, a prototype implementation would deploy the proposed architecture on a small testbed, gathering metrics under a wide range of workloads and comparing results against baseline systems.

3.4 Mathematical models and equations

Beyond qualitative evaluation, rigorous assessment of blockchain-enabled smart city systems requires quantitative models. The following equations capture key performance and security metrics:

Transaction throughput. The throughput of a permissioned blockchain network can be approximated by

$$TPS = \frac{N_{\mathrm{tx}}}{T_{\mathrm{block}} + T_{\mathrm{consensus}}},$$

where N_{tx} is the number of transactions batched into a block, T_{block} is the time to assemble and propagate the block, and $T_{\mathrm{consensus}}$ is the time required for validators to reach consensus. Increasing batch size through edge aggregation raises N_{tx}, thereby improving throughput and amortizing consensus overhead.

Latency. End-to-end latency represents the delay between data generation and block confirmation. It can be modeled as

$$L = T_{\mathrm{sign}} + T_{\mathrm{prop}} + T_{\mathrm{validate}} + T_{\mathrm{confirm}},$$

where T_{sign} is the time for IoT devices to sign their measurements, T_{prop} the propagation delay from device to edge gateway and through the network, T_{validate} the block verification time, and T_{confirm} the consensus finality period. Edge gateways perform compression and batching to reduce T_{prop} and T_{validate}.

Energy consumption. For lightweight consensus schemes (e.g., proof-of-stake and hybrid models), the total energy consumption per epoch is

$$E_{\mathrm{total}} = \sum_{i=1}^{n} P_i \times t_i,$$

where P_i is the average power draw of component i (sensors, gateways or validator nodes) and t_i is its active time. Hybrid consensus and edge computing reduce energy consumption by limiting the number of validator nodes and offloading heavy computations to resource-rich gateways.

Stake-based selection probability. In proof-of-stake consensus, the probability that a node i is chosen to propose the next block is

$$\Pr(\mathrm{selection}_i) = \frac{s_i}{\sum_{j=1}^{n} s_j},$$

where s_i denotes the stake held by node i. This formula highlights how stake distribution influences block proposer selection and aligns validators' incentives with network security.

Detection accuracy. Intrusion detection systems integrated into the blockchain layer can be assessed using standard classification metrics:

$$\text{Detection Rate} = \frac{TP}{TP + FN}, \qquad \text{False Positive Rate} = \frac{FP}{FP + TN},$$

where TP, FP, FN and TN represent the numbers of true positives, false positives, false negatives and true negatives, respectively. The decentralized trust framework reported a detection rate of 98.2 %.

These equations provide a quantitative basis for evaluating different architectures and parameter settings. By calibrating these models with experimental data (e.g., TPS and latency measurements), researchers can predict system performance and optimise resource allocation in future implementations.

4 RESULTS

Table 1 summarizes key studies and their reported performance metrics. The IoT-Chain achieved the highest throughput (1 701 TPS) with a multilevel blockchain, while the decentralized trust framework achieved the highest threat detection rate (98.2 %). The ACE+OSCAR mechanism provided the lowest latency (< 100 ms). These results demonstrate that combining lightweight consensus with batch aggregation and smart contracts can yield scalable and secure smart city applications.

Table 1. Key blockchain frameworks for smart cities

Framework	Domain/application	Key contributions & metrics
Decentralized trust framework	Cybersecurity & smart cities	Uses AI-driven threat detection and adaptive proof-of-stake (LA-PoS) to improve throughput and reduce energy; achieves 98.2 % threat detection rate and reduces false positives.
Private blockchain for IoT security	IoT data security	Implements a private blockchain with smart contracts for access control and machine learning-based anomaly detection; simulation shows minimal latency across transportation, healthcare and building security domains.
IoT chain	IoT sensor data management	Employs a multilevel blockchain (IoT chain + monitoring chain) to store sensor data and manage metadata; reduces delay by 96–99 % and achieves throughput of 1 701 TPS.
Smart grid trading system	Energy trading	Uses a credit-based hybrid consensus and smart contracts to match orders; demonstrates >350 TPS throughput with low CPU and memory usage.
Blockchain-enabled access control with RabbitMQ	IoT access control	Combines blockchain with a message queuing system and attribute-based access control; improves security and real-time communication for smart devices.
HDPIoTF (Hybrid Detection & Prevention IoT Framework)	Critical infrastructure protection	Integrates IoT sensors, gateways, blockchain networks and security analytics for real-time monitoring and notifications; enhances security and interoperability.
ACE+OSCAR trust mechanism	Authentication & authorization	Implements access control using smart contracts in Ethereum; response times remain under 100 ms with multiple clients.
Blockchain-based waste management system	Waste management	Demonstrates blockchain's ability to provide traceability and accountability across the waste lifecycle; introduces smart contracts and digital product passports for recycling.
E-waste disposal tracking	E-waste management	Uses a decentralized shareable ledger (DSL) to record e-waste disposal data; proposes a disposal tracking system (DTS) to ensure safe and eco-friendly disposal.
Citizen engagement via consortium blockchain	Smart governance	Advocates PoA consensus and consortium blockchains for participatory governance; highlights the need for bottom-up decision making and trust.
Patient digital twin with smart contracts	Healthcare & precision medicine	Proposes a blockchain-secured patient digital twin; smart contracts automate data updates and enforce access policies; emphasises privacy and provenance.
Bibliometric review of blockchain in smart cities	Literature trend analysis	Shows that research is shifting from general technological exploration to sector-specific applications; highlights transportation, healthcare, energy and waste management as key areas.

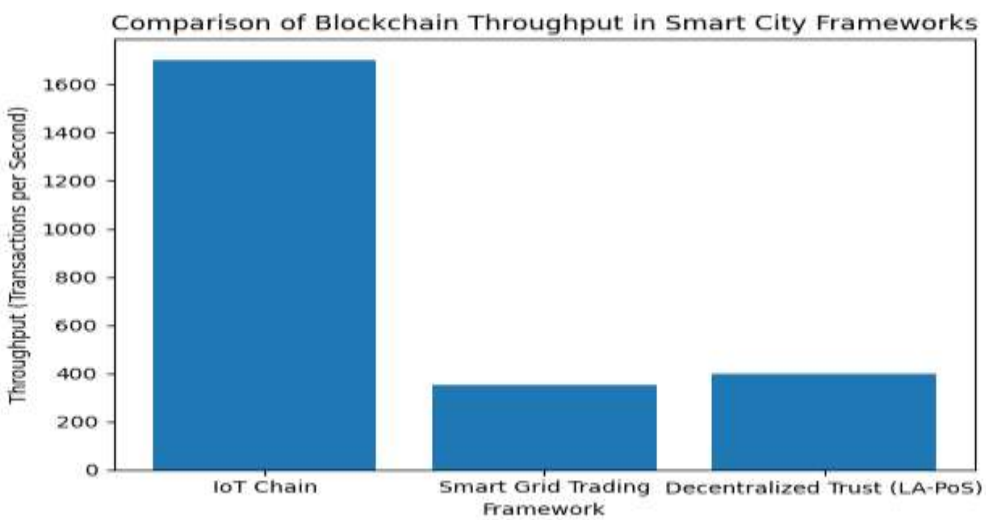

Figure 2 compares transaction throughput across selected frameworks. The IoT-Chain delivers the highest throughput, followed by the decentralized trust framework and the smart grid trading system.

5 DISCUSSION

According to the review, blockchain can improve the security, transparency and reliability of smart city data management activities for both information provider and consumer. Blockchain eliminates single points of failure and is also tamper resistant by losing control across many nodes and using consensus protocols Smart contracts do away with administrative burden and reliance on trust by allowing policies to be automatically enforced. But the analysis did point out some challenges, including:

For one, scalability continues to be a major obstacle. Since the number of IoT devices in a city is increasing, blockchains need thousands of transactions per second. Multilevel architectures and aggregation methods hold some promise but still need tuning; and big datasets will need either an off-chain store or a partitioning scheme to keep performance acceptable. However, smart city level systems come with the challenge of interoperating a broad range of constantly evolving devices and protocols; thus interoperability is critical as well. So to allow smooth data transfer between different chains and avoid the fragmentation, standards in data format exchanges and cross-chain communication frameworks are required, to make applications running on top of the chain reel able to communicate smoothly.

Power Data consumption is still one of the most common issues. Although concepts such as proof-of-stake, proof-of-authority and hybrid approaches diminish consumption on the scale of a few orders of magnitude, whether they are a final solution is uncertain not only because of their characteristics or degree of decentralization but also if it can be established if they have sustainability for long periods of time. With the fine-tuning of these algorithms and an edge computing approach, (this can reduce) energy by orders of magnitude. Privacy is another critical challenge. Our blockchain can ensure the integrity of the data, regenerate and verify it cryptographically, but since the ledger is fully available to every participant in a transparent fashion, no protection against breaching any secure aspect of those business-trading relations can be retained. They've been have been doing or just-busy-pass to deploy data this against they-cheating it whilst zero knowledge proofs, homomorphic encryption and off a chain storage in order to power that risk because they allow parties to verify transaction validity and-and-base already-revealing.

Regulatory frameworks and adoption issues of course are two bigger fish that we cannot really afford not to fry. Regimes are well settled, and also aimed explicitly to smart cities blockchain deployments of data protection provisions, crypto-standards, and transactions' stability/traceability all still due. All of these use cases are very public opinion / trust-centric particularly in healthcare and governance: the user must be sure that their data will used ethically and safely.

6 CONCLUSION

Smart cities should leverage blockchain technology as its a strong and scalable foundation for secure data management. In various sectors (transportation, healthcare, energy, waste management and governance), blockchain promotes transparency, security and accountability and brings new business models, including peer-to-peer energy trading and digital twins. The architecture proposed in this article is an integration of IoT devices, edge gateways, blockchain networks and smart contracts, which maintains a scalable framework for information exchange and service delivery. Existing frameworks empirical results prove that high throughput and low latency are possible using multilevel architectures and adaptive consensus showing the feasibility of blockchain technology for smart city applications in real−time. Our future work needs to consider interoperability standards, performance-oriented consensus approaches for reducing energy consumption, and privacy-preserving methods. By scaling the information, blockchain-enabled information systems can deliver on the promise of secure, sustainable and citizen-centric smart cities through ongoing research and stakeholder collaboration.

REFERENCES

1. A. Rejeb *et al.*, “Blockchain technology in the smart city: A bibliometric review,” *Quality & Quantity*, 2022.
2. A. Rejeb *et al.*, “Blockchain and smart cities: Co-word analysis and BERTopic modeling,” *Big Data and Cognitive Computing*, 2024.
3. S. Alghamdi *et al.*, “Enabling a secure IoT environment using a blockchain-based local-global consensus manager,” *Electronics*, vol. 12, no. 17, 2023.
4. S. Alghamdi *et al.*, “Decentralized trust framework for smart cities: A blockchain-enabled cybersecurity and data integrity model,” *Scientific Reports*, vol. 15, 2025.
5. N. Testi *et al.*, “Exploring the potential of blockchain technology for citizen engagement in smart governance,” *Open Research Europe*, 2025.
6. T. Salman *et al.*, “Enhancing cybersecurity in smart cities: A blockchain-based framework for securing IoT data,” *EnPress Journal of Cybersecurity*, 2025.
7. H. Messahel *et al.*, “An IoT system for access control using blockchain and message queuing system,” *EURASIP Journal on Information Security*, 2025.
8. A. Maskoun *et al.*, “Hybrid smart IoT detection and prevention framework for smart cities using blockchain technology,” *International Journal of Advanced Applied Sciences*, 2025.
9. W. Alabsi *et al.*, “Blockchain-based authentication and trust management mechanism for smart cities,” *Sensors*, vol. 22, no. 7, 2022.

10. S. Singh *et al.*, "Resolving security issues in the IoT using blockchain," *Electronics*, vol. 11, no. 12, 2022.
11. Q. Yang *et al.*, "Blockchain-based smart grid power trading technology," *Journal of Engineering and Applied Sciences*, 2024.
12. J. Lee *et al.*, "IoT-Chain and Monitoring-Chain using multilevel blockchain for IoT security," *Sensors*, vol. 22, no. 11, 2022.
13. M. Zhao *et al.*, "A blockchain framework for scalable, high-density IoT networks of the future," *Sensors*, vol. 25, no. 3, 2025.
14. S. Habibullah *et al.*, "Blockchain-based energy consumption approaches in IoT," *Scientific Reports*, vol. 14, 2024.
15. F. Jiang *et al.*, "Implementation of blockchain technology in waste management," *Energies*, vol. 16, no. 8, 2023.
16. K. Kumar *et al.*, "E-waste management using blockchain technology," *Data & Metadata*, vol. 5, no. 2, 2024.
17. S. Amofa *et al.*, "Blockchain-secure patient Digital Twin in healthcare using smart contracts," *PLoS One*, vol. 19, no. 3, 2024.
18. A. Rejeb *et al.*, "Blockchain for sustainable smart cities: Motivations and challenges," *International Journal of Environmental Research and Public Health*, vol. 19, no. 21, 2022.