International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Blockchain-Based Secure Data Sharing for Smart Cities: Challenges, Solutions, and Future Directions

Md Nyem Hasan Bhuiyan [1, *], Samya Datta [2], Touhidul Arefin [3], Mohammad Quayes Bin Habib [4] and Shuvo Chakroborti [5]

[1] *BSc in CSE, Dhaka International University.*
[2] *CSE, Leading University.*
[3] *Department of Business Administration, East West University.*
[4] *CSE, Daffodil International University.*
[5] *BSc in Microelectronics science and engineering, Yangzhou university, China.*

International Journal of Science and Research Archive, 2025, 17(01), 1109-1122

Publication history: Received on 21 September 2025; revised on 25 October 2025; accepted on 27 October 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.17.1.2931

Abstract

Blockchain technology plays a pivotal role in enabling secure, transparent, and decentralized data sharing in smart city environments. This paper explores the challenges associated with data privacy, interoperability, and scalability in smart cities and investigates blockchain-based solutions that leverage features such as immutability, smart contracts, and decentralized consensus to address these issues. Furthermore, it highlights future research directions to enhance blockchain integration for efficient and trustworthy data exchange among diverse urban stakeholders, ensuring the resilience and sustainability of smart city ecosystems.

Keywords: Blockchain; Smart Cities; Secure Data Sharing; Privacy; Interoperability; Scalability

1. Introduction

Smart cities represent an amalgamation of advanced information and communication technologies, the Internet of Things (IoT), and robust urban infrastructure designed to improve the quality of life for their inhabitants. These complex ecosystems generate, collect, and process vast quantities of data from diverse sources, including sensors, smart devices, vehicles, and citizen interactions. Effective management and secure sharing of this data are paramount for optimizing urban services, enhancing decision-making, and fostering innovation. However, the centralized nature of many traditional data management systems introduces significant vulnerabilities concerning security, privacy, and trust. A decentralized approach to data sharing offers considerable advantages in mitigating these risks.

1.1. Background and Motivation

The proliferation of IoT devices within smart city frameworks has led to an exponential increase in data volume and velocity (Nartey et al., 2021). This data encompasses sensitive personal information, critical infrastructure metrics, and operational insights, making its secure handling a non-trivial undertaking (Ali et al., 2022). Centralized data repositories are susceptible to single points of failure, cyberattacks, and unauthorized access, eroding public trust and compromising the integrity of urban services(Raiyan et al., 2025)(Yu et al., 2021)(Kasera et al., 2023). Issues such as data tampering, privacy breaches, and lack of transparency hinder the full realization of smart city potential (Alasbali et al., 2022).

Blockchain technology, a distributed ledger system, presents a compelling solution to these challenges (Dahiya et al., 2022). Its inherent characteristics of decentralization, immutability, transparency, and cryptographic security provide

* Corresponding author: Md Nyem Hasan Bhuiyan.

a robust foundation for building trustworthy data-sharing mechanisms (Hakak et al., 2020)(Raiyan et al., 2025a)(Trivedi et al., 2023). By distributing data across multiple nodes and securing transactions with cryptographic proofs, blockchain can foster a more resilient and verifiable data ecosystem within smart cities (Trivedi et al., 2023). This shift towards a blockchain-enabled infrastructure can address critical gaps in existing smart city standards, facilitating connections between various stakeholders while ensuring autonomous, immutable, and non-repudiated transactions (Alasbali et al., 2022).

1.2. Objectives and Research Questions

This paper systematically analyzes the integration of blockchain technology for secure data sharing within smart city environments. The primary objective is to evaluate how blockchain can enhance data security, privacy, and integrity, thereby fostering trust among diverse urban stakeholders. A further objective involves identifying and discussing the associated technical, legal, and ethical challenges, along with potential solutions and future research trajectories. This analysis is structured around the following research questions:

- How do blockchain's fundamental principles contribute to improving data security, privacy, and integrity in smart city data-sharing ecosystems?
- What are the prevalent architectural models and integration strategies for deploying blockchain in smart cities, particularly in conjunction with IoT and edge computing?
- Which empirical applications and case studies demonstrate the practical utility and performance characteristics of blockchain-based secure data sharing in urban contexts?
- What are the primary opportunities, advantages, and persistent challenges associated with implementing blockchain for secure data sharing in smart cities?
- What directions for future research and standardization are relevant for advancing blockchain adoption in smart city data management?

1.3. Scope and Structure of the Paper

This document presents a comprehensive review of blockchain-based secure data sharing within smart city paradigms. The scope encompasses the theoretical foundations of blockchain, its application in urban data management, and an assessment of its practical implications. We consider various aspects, including data security mechanisms, privacy-preserving techniques, architectural designs, and real-world implementations. The discussion extends to current limitations and emerging research avenues.

The paper is organized into several sections. Following this introduction, the Methodology section details the systematic approach employed for this research. The Literature Review / Thematic Analysis section delves into blockchain fundamentals, smart city data characteristics, security and privacy concerns, architectural models, and existing applications. The Analysis / Discussion section then critically evaluates the opportunities and challenges, conducts a comparative analysis of different approaches, and outlines future research directions. Finally, the Conclusion summarizes key findings, provides recommendations for practitioners and policymakers, and identifies limitations for subsequent investigations.

2. Methodology

2.1. Research Design and Approach

This study adopts a systematic literature review methodology to synthesize existing knowledge regarding blockchain-based secure data sharing in smart cities. This approach involves a structured and comprehensive search, selection, and critical appraisal of relevant academic literature.(Raiyan, Shaif, et al., 2025a) The goal is to provide a holistic understanding of the subject, identify recurring themes, evaluate proposed solutions, and highlight research gaps. This systematic process ensures rigor and replicability in the findings presented (Zheng & Lu, 2021).

The methodology integr-ates qualitative synthesis of conceptual frameworks with quantitative analysis of empirical results where available. Emphasis is placed on identifying peer-reviewed articles from reputable scientific databases. The review process involved a multi-stage filtering system to ensure the relevance and quality of selected sources, focusing on publications that directly address the intersection of blockchain, secure data sharing, and smart city applications. This structured approach allows for a comprehensive assessment of the technological advancements and implementation considerations.

2.2. Data Sources and Selection Criteria

Electronic databases were systematically searched using a combination of keywords to identify pertinent literature. Primary databases included Scopus, IEEE Xplore, ACM Digital Library, and Web of Science. Search terms encompassed "blockchain," "distributed ledger technology," "smart city," "data sharing," "security," "privacy," "integrity," "IoT," and "urban computing," along with their various permutations and synonyms. Boolean operators (AND, OR) were utilized to refine search queries and capture a broad yet focused range of publications.

Inclusion criteria for selecting articles mandated that studies must be peer-reviewed, published in English, and directly address blockchain applications for data sharing or security within smart city contexts.(Yu et al., 2021) Publications focusing solely on cryptocurrency or general blockchain theory without specific smart city applications were excluded. Additionally, works primarily concerned with non-data-sharing aspects of smart cities (e.g., smart grid optimization without data security focus) were filtered out. The initial search yielded several hundred results, which were subsequently refined through title, abstract, and full-text screening to ensure alignment with the research questions. Ultimately, 17 related articles were obtained and analyzed in detail(Raiyan Haider et al., 2025).

2.3. Analytical Framework

The analytical framework for this review is structured to categorize and evaluate the selected literature across several dimensions. Initially, articles are classified based on their primary focus: foundational blockchain principles, security and privacy mechanisms, architectural models, or practical applications and case studies. This categorization aids in organizing the vast body of knowledge and identifying thematic clusters. A critical evaluation then assesses the proposed solutions, methodologies, and findings within each category.

For security and privacy aspects, the framework scrutinizes the specific cryptographic techniques employed, the extent of decentralization achieved, and the mechanisms for ensuring data integrity and confidentiality. Architectural models are analyzed for their scalability, interoperability, and integration with existing smart city infrastructure, particularly IoT devices. Performance metrics, such as transaction throughput, latency, and resource consumption, are extracted from empirical studies to benchmark the effectiveness of different blockchain implementations. Finally, legal, ethical, and regulatory considerations are examined to understand the broader societal implications. This multi-faceted analytical approach facilitates a robust understanding of the subject matter and informs the subsequent discussion of opportunities, challenges, and future research directions.(Raiyan Haider, Wahida Ahmed Megha, et al., 2025)

3. Literature Review / Thematic Analysis

3.1. Blockchain Fundamentals and Its Role in Smart Cities

Blockchain technology, initially conceptualized for decentralized digital currency, has evolved into a foundational framework for secure and transparent data management across various sectors (Dahiya et al., 2022)(Zheng & Lu, 2021). Its application in smart cities is particularly compelling given the intricate web of data exchanges and the imperative for trust and security (Hakak et al., 2020). The integration of blockchain offers a paradigm shift from centralized data governance to a distributed, verifiable, and immutable record-keeping system (Alasbali et al., 2022)(Trivedi et al., 2023).

Smart cities, by their very nature, rely on interconnected systems and data from diverse sources, including transportation, energy, healthcare, and public safety (Yu et al., 2021). This interdependence necessitates a robust, secure, and transparent data-sharing infrastructure (Alasbali et al., 2022). Blockchain addresses many of the inherent vulnerabilities of traditional centralized systems, which are prone to data silos, single points of failure, and susceptibility to malicious attacks (Kasera et al., 2023). The unique technical characteristics of blockchain, such as distributed storage, transparency, and trust mechanisms, significantly contribute to resolving security and privacy issues prevalent in IoT-based smart city development (Yu et al., 2021).

3.1.1. Core Principles: Decentralization, Immutability, and Consensus Mechanisms

Blockchain technology is predicated on several core principles that collectively establish its utility for secure data sharing. Decentralization ensures that no single entity controls the network, distributing data and operational control across multiple nodes (Dahiya et al., 2022). This architecture removes single points of failure, making the system more resilient to attacks and censorship(Raiyan Haider, Wahida Ahmed Megha, et al., 2025)(Trivedi et al., 2023). In a smart city context, decentralization allows various municipal departments, private service providers, and citizens to interact

and share data without relying on a central authority, fostering a more collaborative and trustworthy environment (Alasbali et al., 2022).

Immutability refers to the inability to alter or delete data once it has been recorded on the blockchain (Dahiya et al., 2022). Each block contains a cryptographic hash of the previous block, creating an unbroken chain of records that is resistant to tampering (Trivedi et al., 2023). This characteristic is crucial for maintaining the integrity and auditability of sensitive smart city data, such as public records, sensor readings, or transaction logs. Data authenticity and historical accuracy are thus guaranteed. Consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), enable distributed nodes to agree on the validity of new transactions and blocks (Trivedi et al., 2023). These protocols ensure that all participants maintain a consistent and synchronized copy of the ledger, preventing fraudulent activities and ensuring data consistency across the network (Wu et al., 2022)(Md Shafin & Reno, 2024). For instance, a novel group-weighted-decay Practical Byzantine Fault Tolerance (gwd-PBFT) consensus algorithm has been proposed to enhance efficiency and security in vehicle-to-vehicle communication within smart cities (Wu et al., 2022).

3.1.2. Smart City Data Ecosystems: Characteristics and Needs

Smart city data ecosystems are characterized by their immense volume, variety, velocity, and veracity (the "4 Vs" of big data) (Kasera et al., 2023). Data originates from heterogeneous sources, including IoT sensors monitoring traffic, environmental conditions, and utility consumption, as well as citizen-generated data from mobile applications and social platforms (Khan et al., 2023). The real-time nature of many smart city services demands high-velocity data processing and analysis. Ensuring the veracity, or trustworthiness, of this data is a critical requirement for accurate decision-making and effective service delivery (Alasbali et al., 2022).

The diverse nature of smart city data also necessitates interoperability among different systems and platforms (Alasbali et al., 2022). Data silos, where information is confined within specific departments or service providers, impede comprehensive urban planning and integrated service provision. Secure and controlled data sharing is essential for fostering innovation, enabling collaborative urban management, and delivering personalized citizen services (Kasera et al., 2023)(Raiyan Haider, Wahida Ahmed Megha, Jafia Tasnim Juba, Aroa Alamgir, et al., 2025). The needs of smart city data ecosystems extend beyond mere storage and retrieval to include robust access control, verifiable data provenance, and mechanisms for anonymization and privacy preservation, especially for sensitive personal data (Ali et al., 2022). The challenge lies in creating a data infrastructure that supports these requirements while balancing innovation with security and privacy mandates (Yu et al., 2021).

3.2. Security, Privacy, and Integrity in Blockchain-Based Data Sharing

Security, privacy, and integrity are foundational pillars for any data-sharing framework, particularly within the sensitive and interconnected environment of smart cities (Yu et al., 2021)(Ali et al., 2022). Blockchain technology offers distinct advantages in these areas by design, moving beyond traditional perimeter-based security models to a trustless, cryptographically secured approach (Dahiya et al., 2022)(Trivedi et al., 2023). However, the specific implementation choices and integration strategies determine the ultimate level of protection achieved.

The inherent vulnerabilities of IoT devices, often deployed at scale with limited processing capabilities, necessitate lightweight and robust security solutions for smart cities (Trivedi et al., 2023)(Khalil et al., 2022). Blockchain's ability to provide a tamper-proof ledger and verifiable transactions directly addresses concerns about data authenticity and integrity. Moreover, its decentralized nature reduces reliance on central servers, mitigating risks associated with single points of attack and unauthorized data manipulation (Alasbali et al., 2022).

3.2.1. Confidentiality, Integrity, and Availability: Definitions and Requirements

The "CIA triad" (Confidentiality, Integrity, and Availability) forms the cornerstone of information security. Confidentiality ensures that sensitive data is accessible only to authorized entities (Dayong et al., 2023). In smart cities, this is paramount for personal citizen data, proprietary business information, and critical infrastructure control signals. Blockchain, while inherently transparent in its ledger, can support confidentiality through cryptographic techniques that encrypt data entries or store only hashes on-chain, with actual data residing off-chain in encrypted form (Dayong et al., 2023).

Integrity guarantees that data remains unaltered and accurate throughout its lifecycle, preventing unauthorized modification or corruption (Dahiya et al., 2022). The immutable nature of blockchain, secured by cryptographic linking of blocks and consensus mechanisms, inherently provides a high degree of data integrity (Trivedi et al., 2023). Any attempt to tamper with recorded data would be detectable and rejected by the network. Availability ensures that

authorized users can access information and resources when needed (Raiyan Haider, Md Farhan Abrar Ibne Bari, Osru, Nishat Afia, et al., 2025). The distributed architecture of blockchain networks, where data is replicated across multiple nodes, enhances availability by eliminating single points of failure often found in centralized systems (Trivedi et al., 2023). Even if some nodes fail, the network can continue to operate, preserving access to the ledger (Wu et al., 2022).

3.2.2. Cryptographic Methods and Privacy-Preserving Solutions

Cryptography is fundamental to blockchain's security model, underpinning its ability to ensure data integrity and authenticity (Dayong et al., 2023). Hash functions, public-key cryptography, and digital signatures are standard components used to secure transactions and link blocks. For instance, elliptic curve cryptography and Schnorr verifiable random functions contribute to robust security in blockchain architectures (Md Shafin & Reno, 2024).

Beyond basic security, privacy-preserving solutions are crucial for smart cities, especially when handling personal data. Techniques such as zero-knowledge proofs (ZKPs) allow one party to prove knowledge of a piece of information without revealing the information itself, enabling verification without compromising privacy . Homomorphic encryption enables computations on encrypted data without decryption, preserving confidentiality during processing (Ali et al., 2022)(Jia et al., 2022). Differential privacy adds statistical noise to datasets, making it difficult to re-identify individuals while still allowing for aggregate analysis (Jia et al., 2022). Multi-party computation (MPC) allows multiple parties to jointly compute a function over their private inputs without revealing those inputs to each other (Khan et al., 2023). These methods are vital for maintaining user privacy while facilitating data validation, such as in mobility data sharing within smart cities (Khan et al., 2023). A blockchain-based Healthcare Privacy Protection Model (BC-HCPPM) leverages an integrated encoder to cryptographically secure Electronic Medical Records (EMRs), obscuring confidential data to safeguard patient privacy (Saini et al., 2024). Furthermore, a lightweight message-sharing strategy with a (t, n)-threshold is introduced to rebuild EMRs with a minimum of 't' portions, enhancing security and storage efficiency (Saini et al., 2024).

3.2.3. Legal and Ethical Considerations (e.g., GDPR, Data Protection)

The deployment of blockchain for smart city data sharing must navigate a complex landscape of legal and ethical considerations. Regulations such as the General Data Protection Regulation (GDPR) in the European Union impose strict requirements on the collection, processing, and storage of personal data, including principles of data minimization, purpose limitation, and the right to be forgotten (Kasera et al., 2023). The immutable nature of blockchain can conflict with the "right to erasure" (right to be forgotten) mandated by GDPR, as data once recorded is difficult to remove (Kasera et al., 2023). Solutions often involve storing only encrypted data or hashes on-chain, with the actual data stored off-chain where it can be managed and potentially deleted in compliance with regulations.

Ethical considerations extend to algorithmic bias, surveillance risks, and equitable access to smart city services. The transparency of public blockchains, while beneficial for auditability, could inadvertently expose sensitive patterns or behaviors if not managed carefully. Data governance frameworks are essential to define roles, responsibilities, and access policies for various stakeholders. These frameworks must balance the need for data utility with the imperative to protect individual rights and ensure fair and ethical use of technology (Raiyan Haider, 2025)(Dahiya et al., 2022).

3.3. Architectures and Models for Blockchain-Based Data Sharing in Smart Cities

The effective implementation of blockchain in smart cities necessitates careful consideration of architectural designs that can accommodate the scale, diversity, and specific security needs of urban environments. Various models have emerged, each offering distinct advantages and trade-offs concerning decentralization, performance, and access control (Hakak et al., 2020)(Trivedi et al., 2023). The choice of architecture significantly influences the system's ability to support real-time data processing, integrate with existing infrastructure, and comply with regulatory requirements.

A hybrid blockchain IoT integration architecture leveraging containerization has been proposed to address key challenges in smart city applications (Nartey et al., 2021). This model emphasizes enhanced security and traceability, aligning with the requirements for managing vast amounts of data from diverse IoT devices. The architecture allows for flexible deployment and management of blockchain components within a dynamic urban landscape.

3.3.1. Types of Blockchains: Public, Consortium, and Private

Blockchain networks can be broadly categorized into three types, each with implications for smart city applications:

- **Public Blockchains:** These are permissionless networks, open to anyone to join, participate, and validate transactions. Examples include Bitcoin and Ethereum. They offer the highest degree of decentralization and

immutability but often struggle with scalability and transaction throughput, which can be limiting for high-volume smart city data (Trivedi et al., 2023). Their transparency also presents challenges for privacy-sensitive data (Dayong et al., 2023).

- **Consortium Blockchains:** Also known as federated blockchains, these are partially decentralized. A group of pre-selected organizations or nodes controls the consensus process. This model offers a balance between decentralization and performance, making it suitable for inter-organizational data sharing in smart cities, such as between municipal departments and utility companies. They provide more control over participants and data access than public blockchains, addressing some privacy concerns.
- **Private Blockchains:** These are permissioned networks controlled by a single organization. While they offer high transaction speeds and scalability, they sacrifice decentralization, resembling distributed databases with cryptographic security features. Private blockchains might be suitable for internal data management within a specific smart city department where high performance and strict access control are paramount, but they may not fully capture the trust benefits of true decentralization. Hyperledger Fabric is a prominent example of a private/permissioned blockchain often used in enterprise contexts (Ali et al., 2022).

The selection of blockchain type depends on the specific use case, data sensitivity, required transaction volume, and the desired level of decentralization and trust among participants (Hakak et al., 2020).

3.3.2. Integration with IoT and Edge Devices

The integration of blockchain with IoT and edge devices is critical for processing the massive data streams generated in smart cities (Khalil et al., 2022)(Nartey et al., 2021). IoT devices, ranging from environmental sensors to smart meters and connected vehicles, often have limited computational and storage capabilities, making direct on-chain processing impractical (Trivedi et al., 2023). Edge computing emerges as a complementary solution, allowing data to be processed closer to the source, reducing latency, and offloading the main blockchain network (Medhane et al., 2020).

In this integrated model, edge devices can perform initial data filtering, aggregation, and cryptographic hashing before sending summarized, privacy-preserved data or transaction proofs to the blockchain. This approach ensures that the immutability and security of blockchain are extended to the data collected at the network's periphery (Medhane et al., 2020). For instance, a blockchain-enabled distributed security framework using edge cloud and Software-Defined Networking (SDN) has been proposed to enhance data confidentiality and detect security attacks in IoT networks (Medhane et al., 2020). The SDN-enabled gateway contributes to attack recognition and mitigates threats by hindering suspicious traffic flows (Medhane et al., 2020). Such integration also addresses issues of authentication for IoT-enabled smart devices, which is critical given the vulnerability of unauthenticated assets (Khalil et al., 2022).

3.3.3. Cross-Chain Interoperability and Data Governance Frameworks

Smart cities often involve multiple, disparate blockchain networks or distributed ledgers operated by different entities for various services (e.g., one for energy, another for transportation) (Biswas et al., 2023). Cross-chain interoperability is a significant architectural challenge, aiming to enable seamless communication and data exchange between these independent blockchain systems (Biswas et al., 2023). Protocols and technologies that facilitate cross-chain atomic swaps, sidechains, or relay networks are essential for creating a truly integrated smart city data ecosystem. Interoperability is crucial for overcoming protocol variances and managing local transactions without overloading the main blockchain network (Biswas et al., 2023).

Complementing this, robust data governance frameworks are necessary to define rules for data ownership, access, usage, and sharing across the blockchain network (Dahiya et al., 2022). These frameworks typically involve smart contracts to automate and enforce governance policies, ensuring transparency and accountability. A well-designed governance model specifies roles and permissions for data producers, consumers, and network validators, thus maintaining a balance between data utilization and privacy protection. Such frameworks ensure that the benefits of blockchain's distributed trust are maximized while mitigating potential risks associated with data misuse (Alasbali et al., 2022).

3.4. Current Applications, Case Studies, and Performance Metrics

The theoretical benefits of blockchain for secure data sharing in smart cities are increasingly being substantiated by practical applications and case studies across various urban sectors. These implementations demonstrate the technology's capacity to enhance trust, transparency, and efficiency in complex data ecosystems. Examining these real-world scenarios provides insights into the functional viability and performance characteristics of blockchain-enabled solutions.

The literature highlights several key application areas where blockchain addresses critical challenges, particularly concerning data integrity, privacy, and the secure exchange of information among multiple stakeholders (Yu et al., 2021)(Chentouf & Bouchkaren, 2023). The distributed nature of smart city operations makes blockchain a natural fit for managing transactions and interactions among diverse IoT devices and service providers (Nartey et al., 2021).

3.4.1. Smart Healthcare, Transportation, Energy, and E-Government Use Cases

In **smart healthcare**, blockchain offers a solution for secure and interoperable Electronic Medical Record (EMR) management. Centralized healthcare platforms face challenges with isolated data, patient privacy, and cross-institutional data exchange (Saini et al., 2024). A Blockchain-based Healthcare Privacy Protection Model (BC-HCPPM) has been proposed to maintain anonymity by cryptographically securing EMRs, obscuring confidential data, and enabling secure message sharing with a (t, n)-threshold scheme. This model streamlines sharing procedures while safeguarding EMRs, showing improved power usage and storage efficiency compared to existing methods (Saini et al., 2024).

For **smart transportation**, blockchain addresses issues in Internet of Vehicles (IoV) data management, message credibility assessment, and security of centralized data storage (Wu et al., 2022). A trusted paradigm based on a vehicle–road–cloud architecture leverages blockchain to evaluate message credibility and store data securely. A system called BELIEVE (Blockchain-Enabled Location Identification and Efficient Validation with Encryption) utilizes blockchain and multi-party computation (MPC) to securely validate mobility data from sources without violating user privacy (Khan et al., 2023). This platform enables mobile peers to reach consensus on data validation using MPC, with validated spatio-temporal data updated on a distributed ledger. Simulations in a portion of New York City's transportation network demonstrated lower delays and overhead (Khan et al., 2023).

In **smart energy** grids, blockchain can facilitate secure energy trading, demand-response management, and transparent carbon credit tracking. It enables peer-to-peer energy transactions, fostering microgrids and enhancing energy independence while ensuring the integrity of consumption and production data. While specific detailed case studies are less represented in the provided sources, the principles of immutable record-keeping and decentralized control are highly applicable.

For **e-government services**, blockchain offers enhanced transparency, auditability, and security for public records, digital identity, and electronic voting (Chentouf & Bouchkaren, 2023). Implementing an electronic voting model using smart contracts on the Ethereum blockchain exemplifies how this technology can promote security and trust in civic processes (Chentouf & Bouchkaren, 2023). Blockchain can also streamline public service delivery by ensuring the authenticity of documents and reducing bureaucratic overhead. A framework for interoperability across various blockchain-based smart city services has been proposed to manage local transactions efficiently without overloading the blockchain network, demonstrating scalability and memory optimization (Biswas et al., 2023).

3.4.2. Empirical Results: Efficiency, Scalability, and Adoption Statistics

Empirical studies on blockchain implementations in smart cities reveal varying performance metrics, primarily focusing on efficiency, scalability, and aspects of adoption. A blockchain architecture designed to transcend the trilemma of decentralization, security, and scalability reported a throughput of over 1700 transactions per second (TPS) . This level of performance was achieved while maintaining robust security and decentralization, with an average CPU usage of 16.1% for validators and affordable hardware costs .

For IoT data sharing, a Payment Channel Network (PCN)-extended blockchain approach, combined with homomorphic hashing-based transaction segmentation and Multi-point Relay (MPR)-based multi-path routing, outperformed baseline methods in transaction efficiency and success ratio (Zhang et al., 2022). This demonstrates solutions addressing the high-frequency data sharing requirements of IoT devices within smart cities. In the medical blockchain system (BC-HCPPM), simulation findings showed improvements in power usage and storage space efficiency compared to similar literature, indicating strong stability (Saini et al., 2024). The BELIEVE platform for mobility data validation achieved lower delays and overhead in simulated environments for New York City, suggesting practical efficiency (Khan et al., 2023).

Despite these promising results, scalability remains a frequently cited concern for blockchain implementations, especially in public or highly decentralized networks (Trivedi et al., 2023). Solutions often involve off-chain transactions, layered architectures, or more efficient consensus mechanisms to handle the sheer volume of data generated by smart city IoT devices. Adoption statistics are still nascent, reflecting the technology's relative youth and

the complexities of integrating it into established urban infrastructures. However, the continuous innovation in consensus protocols and smart contract designs provides optimism for broader adoption (Trivedi et al., 2023).

4. Analysis / Discussion

The integration of blockchain technology into smart city data sharing architectures represents a transformative shift from traditional centralized models. This section critically examines the opportunities and advantages that blockchain presents, alongside the significant challenges and barriers that must be addressed for its widespread and effective implementation. A comparative analysis of various approaches from the literature further refines understanding of the current state of the art, paving the way for future research directions.

4.1. Opportunities and Advantages of Blockchain-Based Secure Data Sharing

Blockchain technology offers compelling opportunities for enhancing secure data sharing in smart cities, primarily by fundamentally altering the trust model and improving data quality and transparency. Its inherent design addresses many vulnerabilities prevalent in existing centralized data management systems, offering a robust foundation for a new generation of urban services (Hakak et al., 2020).

4.1.1. Trust Infrastructure and Decentralized Governance

One of the foremost advantages of blockchain in smart cities is its capacity to establish a decentralized trust infrastructure (Alasbali et al., 2022). Unlike traditional systems that rely on a central authority for trust, blockchain distributes trust across a network of participants through cryptographic validation and consensus mechanisms (Dahiya et al., 2022). This attribute is particularly significant in multi-stakeholder smart city environments, where various municipal departments, private entities, and citizens interact and exchange sensitive data (Alasbali et al., 2022). By removing the need for a single trusted intermediary, blockchain mitigates risks associated with corruption, single points of failure, and data manipulation (Trivedi et al., 2023).

Decentralized governance, facilitated by blockchain's distributed nature and smart contracts, enables more transparent and equitable data management. Smart contracts can automate and enforce predefined rules for data access, usage, and sharing, ensuring adherence to agreed-upon policies without human intervention or bias (Chentouf & Bouchkaren, 2023). This promotes accountability among all participants and fosters a cooperative environment where data can be shared securely and verifiably. For example, in IoV, blockchain-enabled solutions can assess message credibility in untrusted environments and provide secure, efficient data storage, improving overall system efficiency and security (Wu et al., 2022).

4.1.2. Enhancing Data Quality, Transparency, and Citizen Services

Blockchain's immutable ledger ensures the integrity and authenticity of data, directly enhancing data quality within smart cities (Dahiya et al., 2022). Once data is recorded on the blockchain, it cannot be altered or deleted, providing an auditable and tamper-proof history of all transactions and events (Trivedi et al., 2023). This verifiability is crucial for critical urban applications, such as environmental monitoring, infrastructure maintenance, and public safety, where data accuracy directly impacts decisions and outcomes. The transparent nature of blockchain, where all network participants can view transaction records (though content can be encrypted for privacy), promotes greater accountability and trust among stakeholders (Alasbali et al., 2022)(Chentouf & Bouchkaren, 2023).

By securing data and fostering trust, blockchain significantly improves citizen services. For instance, secure management of Electronic Medical Records (EMRs) via blockchain ensures patient privacy and efficient data exchange between healthcare providers (Saini et al., 2024). In transportation, platforms like BELIEVE allow for privacy-preserving validation of mobility data, leading to safer and more intelligent transportation systems (Khan et al., 2023). E-government services can leverage blockchain for secure digital identity management and transparent voting systems, increasing citizen participation and trust in public institutions (Chentouf & Bouchkaren, 2023). The ability to track data provenance and ensure its authenticity also empowers citizens with greater control over their personal data, fostering a more privacy-aware smart city environment (Kasera et al., 2023).

4.2. Challenges and Barriers to Implementation

Despite its numerous advantages, the deployment of blockchain for secure data sharing in smart cities faces considerable technical, security, legal, and ethical hurdles. These challenges require innovative solutions and collaborative efforts across various domains to achieve widespread adoption and effective integration.

4.2.1. Technical Challenges: Scalability, Interoperability, and Efficiency

The technical demands of smart city data ecosystems often strain current blockchain capabilities. Scalability remains a primary concern; public blockchains, while offering strong decentralization, typically exhibit low transaction throughput (e.g., Bitcoin ~7 TPS, Ethereum ~15-30 TPS), which is insufficient for the high-frequency, high-volume data generated by millions of IoT devices (Trivedi et al., 2023). While solutions like sharding, layer-2 protocols, and improved consensus mechanisms are being developed, achieving high TPS without compromising decentralization is a complex engineering task .

Interoperability between different blockchain networks and with existing legacy smart city systems presents another significant barrier (Alasbali et al., 2022). Smart cities are characterized by diverse platforms and data formats, making seamless cross-chain communication and data exchange difficult (Biswas et al., 2023). The lack of standardized protocols for inter-blockchain communication hinders the creation of a unified smart city data fabric. Efficiency, particularly concerning energy consumption (especially for Proof of Work systems) and computational overhead, can be prohibitive for resource-constrained IoT devices and large-scale deployments (Trivedi et al., 2023). More lightweight cryptographic schemes and efficient consensus algorithms are necessary to overcome these limitations (Khalil et al., 2022).

4.2.2. Security Risks: Attacks, Vulnerabilities, and Key Management Issues

While blockchain offers enhanced security, it is not impervious to attacks and vulnerabilities. Common threats include 51% attacks, where a single entity gains control of more than half of the network's computing power, potentially manipulating transactions (Trivedi et al., 2023). Smart contracts, if poorly coded, can harbor vulnerabilities that lead to exploits and financial losses. Furthermore, the integration of IoT devices introduces a broader attack surface, as these devices can be compromised, leading to the injection of malicious data into the blockchain (Yu et al., 2021)(Khalil et al., 2022).

Key management poses a substantial challenge. Securely generating, storing, and managing cryptographic keys for millions of devices and users is complex. Loss of a private key can lead to irreversible loss of access to assets or data, while compromise of a key can grant unauthorized access. Robust key management strategies, including hardware security modules (HSMs) and multi-signature schemes, are essential but add complexity and cost. Additionally, quantum computing advancements present a future threat to current cryptographic algorithms, necessitating quantum-resistant cryptographic solutions (Dayong et al., 2023).

4.2.3. Legal, Regulatory, and Ethical Constraints

The legal and regulatory landscape surrounding blockchain and data privacy remains largely undefined or inconsistent across jurisdictions. Compliance with data protection regulations, such as GDPR, is difficult due to blockchain's immutability, which conflicts with the 'right to be forgotten' (Kasera et al., 2023). Determining data ownership and liability in a decentralized network, especially when data crosses national borders, introduces legal ambiguities. Furthermore, the legal status of smart contracts in many jurisdictions is still evolving, posing challenges for their enforceability in real-world disputes.

Ethical considerations are equally pressing. The potential for ubiquitous surveillance through interconnected smart city sensors and immutable data records raises significant privacy concerns, even with privacy-preserving technologies (Kasera et al., 2023). Ensuring equitable access to blockchain-enabled services and preventing digital divides is important. The transparency of public blockchains, while beneficial for accountability, could also lead to unintended exposure of sensitive information if not carefully managed. Establishing clear ethical guidelines and robust governance models is crucial to foster public trust and ensure that blockchain technology serves the collective good rather than exacerbating existing societal inequalities (Dahiya et al., 2022).

4.3. Comparative Analysis of Approaches in Literature

The literature presents a diverse array of approaches for integrating blockchain into smart city data sharing. These vary primarily in how data is stored (on-chain vs. off-chain), the design of smart contracts, and the overall network architecture. A comparative analysis highlights the trade-offs and suitability of different solutions for specific smart city contexts.

4.3.1. Synthesis of Solutions: On-Chain vs. Off-Chain Storage, Smart Contracts Models

The choice between on-chain and off-chain storage is fundamental. Storing all data directly on a blockchain (on-chain) offers maximum immutability and transparency but significantly impacts scalability and cost due to storage limitations and transaction fees. For instance, an immutable transaction updated on a distributed ledger like InterPlanetary File System (IPFS) allows for secure spatio-temporal validation without storing raw data directly on the blockchain (Khan et al., 2023). This approach is generally reserved for critical metadata, hashes, or transaction proofs. Conversely, storing data off-chain in traditional databases or decentralized storage solutions like IPFS, with only cryptographic hashes or pointers recorded on the blockchain, addresses scalability and privacy concerns (Khan et al., 2023). This hybrid approach allows for large data volumes while maintaining blockchain's integrity benefits. A notable example is a Payment Channel Network (PCN)-extended blockchain, which, alongside homomorphic hashing, offers efficient IoT data sharing by segmenting transactions and utilizing multi-path routing (Zhang et al., 2022).

Smart contract models vary in complexity and functionality. Simple smart contracts can automate basic agreements, such as granting data access based on predefined conditions. More sophisticated models incorporate privacy-enhancing technologies like zero-knowledge proofs (ZKPs) or multi-party computation (MPC) to allow verified data usage without revealing underlying sensitive information (Khan et al., 2023) . The design of effective smart contracts for resource-constrained IoT environments requires careful consideration of computational overhead and gas costs (Trivedi et al., 2023). An effective view of consensus and smart contract design is considered an open problem for meeting end application requirements in blockchain-IoT ecosystems (Trivedi et al., 2023).

4.3.2. Evaluation of Experimental Platforms and Prototypes

Experimental platforms and prototypes demonstrate the practical feasibility of blockchain solutions. Hyperledger Fabric is a prominent permissioned blockchain framework often used in enterprise and smart city contexts due to its modular architecture, privacy features (channels), and high transaction throughput compared to public chains (Ali et al., 2022). Its application in secure searchable blockchains for PHR management showcases its ability to integrate homomorphic encryption and secure key revocation policies (Ali et al., 2022).

Other prototypes focus on specific smart city domains. The BELIEVE framework for mobility data validation, simulated in a New York City transportation network segment, achieved reduced delays and overhead, validating the utility of MPC with blockchain for privacy-preserving real-time data validation (Raiyan Haider & Jasmima Sabatina, 2025)(Khan et al., 2023). Similarly, a blockchain-enabled federated learning model for Industrial IoT (IIoT) integrates differential privacy and homomorphic encryption to protect sensitive data during sharing, showing improved performance in selected indicators (Jia et al., 2022). An infinite loop model for a standardized, intermediary cloud-based blockchain for IoT networking is proposed to resolve critical gaps in distributed IoT-based smart cities, drawing connections between nodes, users, and service providers (Alasbali et al., 2022). These evaluations indicate that while challenges persist, targeted architectural designs and cryptographic integrations can yield efficient and secure smart city data-sharing solutions.

4.4. Future Research Directions

The field of blockchain for smart cities is still in its early stages of development, with numerous avenues for further exploration. Addressing the identified challenges and capitalizing on the opportunities requires sustained research and innovation across multiple disciplines. Future research should concentrate on enhancing core technological capabilities, fostering standardization, and informing policy development.

4.4.1. Innovative Architectures and Privacy-Preserving Technologies

Future research should prioritize the development of innovative blockchain architectures that concurrently address scalability, security, and decentralization. Solutions include novel consensus mechanisms optimized for IoT environments, sharding techniques for parallel transaction processing, and layered architectures that offload heavy computations from the main chain (Trivedi et al., 2023) . Research into more efficient data storage solutions, combining on-chain and off-chain elements seamlessly, is also critical. For instance, further refinement of payment channel networks and homomorphic hashing for high-frequency IoT data sharing could yield substantial benefits (Zhang et al., 2022).

Advancements in privacy-preserving technologies are essential to balance data utility with individual rights. This includes enhancing zero-knowledge proofs for real-time applications, developing more practical homomorphic encryption schemes, and exploring federated learning integrated with blockchain for distributed data analysis without centralizing raw data (Ali et al., 2022)(Jia et al., 2022). Research into quantum-resistant cryptography is also important

to future-proof blockchain security against emerging threats (Dayong et al., 2023). Furthermore, creating lightweight authentication mechanisms for IoT devices that integrate robustly with blockchain without excessive computational overhead presents a significant area for investigation (Khalil et al., 2022).

4.4.2. Standardization Efforts and Policy Recommendations

Standardization is pivotal for achieving interoperability and widespread adoption of blockchain in smart cities. Research should contribute to developing common protocols, data formats, and API standards that enable seamless communication between diverse blockchain networks and legacy systems (Alasbali et al., 2022). This includes establishing benchmarks for performance metrics, security audits, and privacy compliance. An infinite loop model for establishing a standardized, intermediary cloud-based blockchain for IoT networking provides a conceptual framework for such efforts (Alasbali et al., 2022).

Policy recommendations are necessary to address the legal and ethical complexities. This involves developing clear regulatory frameworks that reconcile blockchain's immutability with data protection laws like GDPR, defining legal liability in decentralized autonomous organizations (DAOs), and establishing clear guidelines for data ownership and governance (Kasera et al., 2023). Policies should also encourage public-private partnerships to pilot and scale blockchain solutions, foster innovation, and ensure equitable access to smart city services. Research into the socio-economic impact of blockchain deployment, including its effects on employment, governance structures, and citizen engagement, will also be vital for informed policy-making.

5. Conclusion

The transformation of urban centers into smart cities necessitates robust and secure data-sharing mechanisms to unlock the full potential of interconnected technologies. Traditional centralized systems present inherent vulnerabilities, underscoring the appeal of decentralized solutions. Blockchain technology, with its intrinsic properties of decentralization, immutability, and cryptographic security, offers a compelling framework for establishing trustworthy and resilient data ecosystems within smart cities. This comprehensive analysis has explored the foundations, applications, challenges, and future trajectories of blockchain-based secure data sharing in this domain.

Summary of Key Findings

This investigation confirms that blockchain's core principles significantly bolster data security, privacy, and integrity in smart city data sharing. Decentralization eliminates single points of failure, while immutability ensures data authenticity and an unalterable audit trail. Advanced cryptographic methods, including homomorphic encryption, zero-knowledge proofs, and multi-party computation, are pivotal in preserving confidentiality and enabling privacy-aware data validation.

Various architectural models, spanning public, consortium, and private blockchains, cater to different smart city requirements, with hybrid approaches often integrating IoT and edge computing to manage data at the periphery of the network. Empirical case studies in smart healthcare, transportation, and e-government demonstrate the practical utility of blockchain, showcasing enhancements in efficiency, scalability, and security through systems like BC-HCPPM for EMRs and BELIEVE for mobility data. Notably, some advanced architectures have achieved throughputs exceeding 1700 transactions per second while maintaining strong security and decentralization . The overall findings suggest that blockchain offers a robust mechanism for building trust infrastructure, enhancing data quality, and improving citizen services through transparent and verifiable processes.

Recommendations for Practice and Policy Makers

To effectively leverage blockchain in smart cities, practitioners and policymakers should consider the following recommendations:

- **Adopt Hybrid Architectures:** Prioritize hybrid blockchain models that combine on-chain immutability for metadata and integrity checks with off-chain storage for large datasets, particularly those from IoT devices. This balances scalability, cost, and privacy.
- **Invest in Privacy-Preserving Technologies:** Implement solutions utilizing homomorphic encryption, zero-knowledge proofs, and differential privacy to ensure compliance with data protection regulations while enabling data utility for urban planning and services.
- **Develop Interoperability Standards:** Actively participate in and promote the development of open standards for cross-chain communication and data exchange protocols to foster a cohesive smart city data ecosystem.

- **Establish Robust Governance Frameworks:** Create clear legal and ethical guidelines for data ownership, access control, and liability within decentralized networks, potentially leveraging smart contracts for automated enforcement.
- **Pilot and Scale Solutions Strategically:** Initiate pilot projects in less sensitive domains to gain experience, then gradually scale to critical infrastructure, learning from empirical results regarding efficiency and security.
- **Foster Public-Private Partnerships:** Encourage collaboration between municipal governments, technology providers, and academic institutions to drive innovation, share expertise, and address implementation challenges collectively.

These actions can mitigate risks, enhance public trust, and accelerate the secure integration of blockchain within smart city initiatives.

Limitations and Suggestions for Future Work

This review, while comprehensive, is subject to certain limitations. The rapidly evolving nature of blockchain technology means that new solutions and challenges emerge continuously. The selection of literature, though systematic, might not encompass every relevant publication, particularly those in nascent stages of research or specialized conference proceedings not indexed in the primary databases. Furthermore, detailed quantitative comparisons across all presented solutions are challenging due to varied experimental setups and reporting metrics. The token budget also constrained the depth of discussion on certain sub-topics.

Future work should focus on several critical areas. Continued research into novel consensus mechanisms and layer-2 scaling solutions is essential to meet the high transaction demands of smart cities. Exploring the long-term sustainability and energy efficiency of blockchain deployments, especially in the context of increasing computational power, warrants further investigation. Developing standardized benchmarks and metrics for evaluating blockchain performance in smart city contexts would facilitate more robust comparative analyses. Additionally, addressing the legal ambiguities surrounding data ownership, smart contract enforceability, and GDPR compliance within decentralized systems remains a priority for academic and legal scholars. Finally, comprehensive studies on the socio-economic impacts and governance models for citizen-centric blockchain applications are necessary to ensure inclusive and ethical smart city development.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Nartey, C., Tchao, E. T., Gadze, J. D., Keelson, E., Klogo, G. S., Kommey, B., & Diawuo, K. (2021). On Blockchain and IoT Integration Platforms: Current Implementation Challenges and Future Perspectives. In M. Fazio (Ed.), *Wireless Communications and Mobile Computing* (Vol. 2021, Issue 1). Wiley. https://doi.org/10.1155/2021/6672482

[2] Ali, A., Pasha, M. F., Ali, J., Fang, O. H., Masud, M., Jurcut, A. D., & Alzain, M. A. (2022). Deep Learning Based Homomorphic Secure Search-Able Encryption for Keyword Search in Blockchain Healthcare System: A Novel Approach to Cryptography. In *Sensors* (Vol. 22, Issue 2, p. 528). MDPI AG. https://doi.org/10.3390/s22020528

[3] Raiyan, H., Shaif, Md. F. I., Ahmed, R., Nafi, N. H., Sumon, M. R., & Rahman, M. (2025a). Assessing the impact of influencer marketing on brand value and business revenue: An empirical and thematic analysis. *International Journal of Science and Research Archive*, *16*(02), 471–482. https://doi.org/10.30574/ijsra.2025.16.2.2355

[4] Yu, Z., Song, L., Jiang, L., & Khold Sharafi, O. (2021). Systematic literature review on the security challenges of blockchain in IoT-based smart cities. In *Kybernetes* (Vol. 51, Issue 1, pp. 323–347). Emerald. https://doi.org/10.1108/k-07-2020-0449

[5] Kasera, S., Gehlot, A., Uniyal, V., Pandey, S., Chhabra, G., & Joshi, K. (2023). Right to Digital Privacy: A Technological Intervention of Blockchain and Big Data Analytics. In *2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA)* (pp. 1122–1127). IEEE. https://doi.org/10.1109/icidca56705.2023.10100229

[6] Alasbali, N., Azzuhri, S. R. B., Salleh, R. B., Kiah, M. L. M., Shariffuddin, A. A. A. S. A., Kamel, N. M. I. bin N. M., & Ismail, L. (2022). Rules of Smart IoT Networks within Smart Cities towards Blockchain Standardization. In H. A. Khattak (Ed.), *Mobile Information Systems* (Vol. 2022, pp. 1–11). Wiley. https://doi.org/10.1155/2022/9109300

[7] Dahiya, A., Gupta, B. B., Alhalabi, W., & Ulrichd, K. (2022). A comprehensive analysis of blockchain and its applications in intelligent systems based on IoT, cloud and social media. In *International Journal of Intelligent Systems* (Vol. 37, Issue 12, pp. 11037–11077). Hindawi Limited. https://doi.org/10.1002/int.23032

[8] Hakak, S., Khan, W. Z., Gilkar, G. A., Imran, M., & Guizani, N. (2020). Securing Smart Cities through Blockchain Technology: Architecture, Requirements, and Challenges. In *IEEE Network* (Vol. 34, Issue 1, pp. 8–14). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/mnet.001.1900178

[9] Raiyan, H., Shaif, Md. F. I., Ahmed, R., Nafi, N. H., Sumon, M. R., & Rahman, M. (2025b). The influence of social media branding on consumer purchase behavior: A comprehensive empirical and thematic analysis. *International Journal of Science and Research Archive*, *16*(02), 460–470. https://doi.org/10.30574/ijsra.2025.16.2.2354

[10] Trivedi, C., Rao, U. P., Parmar, K., Bhattacharya, P., Tanwar, S., & Sharma, R. (2023). A transformative shift toward blockchain-basedIoTenvironments: Consensus, smart contracts, and future directions. In *SECURITY AND PRIVACY* (Vol. 6, Issue 5). Wiley. https://doi.org/10.1002/spy2.308

[11] Raiyan, H., Jafia Tasnim, J., & Satu, C. (2025). Exploring the link between suicidal ideation and digital environments: The hidden impact of marketing content. *International Journal of Science and Research Archive*, *16*(02), 607–614. https://doi.org/10.30574/ijsra.2025.16.2.2353

[12] Zheng, X. R., & Lu, Y. (2021). Blockchain technology – recent research and future trend. In *Enterprise Information Systems* (Vol. 16, Issue 12). Informa UK Limited. https://doi.org/10.1080/17517575.2021.1939895

[13] Raiyan Haider, Wahida Ahmed Megha, Jafia Tasnim Juba, Aroa Alamgir, & Labib Ahmad. (2025). The conversational revolution in health promotion: Investigating chatbot impact on healthcare marketing, patient engagement, and service reach. In *International Journal of Science and Research Archive* (Vol. 15, Issue 3, pp. 1585–1592). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.3.1937

[14] Raiyan Haider, Farhan Abrar Ibne Bari, Osru, Nishat Afia, & Mohammad Abiduzzaman khan Mugdho. (2025). Leveraging internet of things data for real-time marketing: Opportunities, challenges, and strategic implications. In *International Journal of Science and Research Archive* (Vol. 15, Issue 3, pp. 1657–1663). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.3.1936

[15] Raiyan Haider, Md Farhan Abrar Ibne Bari, Md. Farhan Israk Shaif, Mushfiqur Rahman, Md. Nahid Hossain Ohi, & Kazi Md Mashrur Rahman. (2025). Quantifying the Impact: Leveraging AI-Powered Sentiment Analysis for Strategic Digital Marketing and Enhanced Brand Reputation Management. In *International Journal of Science and Research Archive* (Vol. 15, Issue 2, pp. 1103–1121). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.2.1524

[16] Wu, Y., Wu, L., & Cai, H. (2022). A Trusted Paradigm of Data Management for Blockchain-Enabled Internet of Vehicles in Smart Cities. In *ACM Transactions on Sensor Networks*. Association for Computing Machinery (ACM). https://doi.org/10.1145/3572841

[17] Md Shafin, K., & Reno, S. (2024). Breaking the Blockchain Trilemma: A Comprehensive Consensus Mechanism for Ensuring Security, Scalability, and Decentralization. In N. Sarwar (Ed.), *IET Software* (Vol. 2024, Issue 1). Institution of Engineering and Technology (IET). https://doi.org/10.1049/2024/6874055

[18] Khan, J. A., Wang, W., & Ozbay, K. (2023). BELIEVE: Privacy-Aware Secure Multi-Party Computation for Real-Time Connected and Autonomous Vehicles and Micro-Mobility Data Validation Using Blockchain—A Study on New York City Data. In *Transportation Research Record: Journal of the Transportation Research Board* (Vol. 2678, Issue 3, pp. 410–421). SAGE Publications. https://doi.org/10.1177/03611981231180200

[19] Raiyan Haider, Md Farhan Abrar Ibne Bari, Md. Farhan Israk Shaif, & Mushfiqur Rahman. (2025). Engineering hyper-personalization: Software challenges and brand performance in AI-driven digital marketing management: An empirical study. In *International Journal of Science and Research Archive* (Vol. 15, Issue 2, pp. 1122–1141). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.2.1525

[20] Khalil, U., Malik, O. A., Uddin, M., & Chen, C.-L. (2022). A Comparative Analysis on Blockchain versus Centralized Authentication Architectures for IoT-Enabled Smart Devices in Smart Cities: A Comprehensive Review, Recent Advances, and Future Research Directions. In *Sensors* (Vol. 22, Issue 14, p. 5168). MDPI AG. https://doi.org/10.3390/s22145168

[21] Dayong, Z., Wahab, N. H. A., Kadir, K. A., Aldhaqm, A., Nasir, H. M., & Wong, K. Y. (2023). Research on Blockchain: Privacy Protection of Cryptography Blockchain-Based Applications. In *2023 3rd International Conference on Emerging Smart Technologies and Applications (eSmarTA)* (pp. 1–6). IEEE. https://doi.org/10.1109/esmarta59349.2023.10293507

[22] Raiyan Haider, Md Farhan Abrar Ibne Bari, Osru, Nishat Afia, & Tanjim Karim. (2025). Illuminating the black box: Explainable AI for enhanced customer behavior prediction and trust. In *International Journal of Science and Research Archive* (Vol. 15, Issue 3, pp. 247–268). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.3.1674

[23] Jia, B., Zhang, X., Liu, J., Zhang, Y., Huang, K., & Liang, Y. (2022). Blockchain-Enabled Federated Learning Data Protection Aggregation Scheme With Differential Privacy and Homomorphic Encryption in IIoT. In *IEEE Transactions on Industrial Informatics* (Vol. 18, Issue 6, pp. 4049–4058). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/tii.2021.3085960

[24] Saini, Dr. M., Himanshi, Dr., & Sanju Saini, Dr. (2024). Privacy-enhancing Blockchain Solutions for the Healthcare Sector: Efficient Message Sharing and Robust Big Data Protection. In *Journal of Internet Services and Information Security* (Vol. 14, Issue 3, pp. 85–97). SASA Publications. https://doi.org/10.58346/jisis.2024.i2.006

[25] Raiyan Haider. (2025). Navigating the digital political landscape: How social media marketing shapes voter perceptions and political brand equity in the 21st Century. In *International Journal of Science and Research Archive* (Vol. 15, Issue 1, pp. 1736–1744). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.1.1217

[26] Medhane, D. V., Sangaiah, A. K., Hossain, M. S., Muhammad, G., & Wang, J. (2020). Blockchain-Enabled Distributed Security Framework for Next-Generation IoT: An Edge Cloud and Software-Defined Network-Integrated Approach. In *IEEE Internet of Things Journal* (Vol. 7, Issue 7, pp. 6143–6149). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/jiot.2020.2977196

[27] Biswas, S., Yao, Z., Yan, L., Alqhatani, A., Bairagi, A. K., Asiri, F., & Masud, M. (2023). Interoperability Benefits and Challenges in Smart City Services: Blockchain as a Solution. In *Electronics* (Vol. 12, Issue 4, p. 1036). MDPI AG. https://doi.org/10.3390/electronics12041036

[28] Chentouf, F. zahrae, & Bouchkaren, S. (2023). Security and privacy in smart city: a secure e-voting system based on blockchain. In *International Journal of Electrical and Computer Engineering (IJECE)* (Vol. 13, Issue 2, p. 1848). Institute of Advanced Engineering and Science. https://doi.org/10.11591/ijece.v13i2.pp1848-1857

[29] Zhang, Y., Gai, K., Xiao, J., Zhu, L., & Choo, K.-K. R. (2022). Blockchain-Empowered Efficient Data Sharing in Internet of Things Settings. In *IEEE Journal on Selected Areas in Communications* (Vol. 40, Issue 12, pp. 3422–3436). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/jsac.2022.3213353

[30] Raiyan Haider, & Jasmima Sabatina. (2025). Harnessing the power of micro-influencers: A comprehensive analysis of their effectiveness in promoting climate adaptation solutions. In *International Journal of Science and Research Archive* (Vol. 15, Issue 2, pp. 595–610). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.2.1448