SvedbergOpen
DISSEMINATION OF KNOWLEDGE
International Journal of Artificial Intelligence and Machine Learning
Publisher's Home Page: https://www.svedbergopen.com/
Research Paper Open Access

Blockchain-Based Security Architecture For Smart City Data Exchange

Ravindra Pandey[1] , Nittin Sharma[2] , Ravina Gupt[3] , P.Ranjith[4] , Shweta Ishwar Gadave[5] , Dr. Deepali Rani Sahoo[6] , Simran Sharma[7] , Latipov Rustam[8]

[1]Visiting Faculty Management Department Symbiosis International University Email: *pandey.ravindra@gmail.com orchid id : 0000-0002-1137-8506
[2]Centre for Research Impact & Outcome, Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, 140401, Punjab, India. nittin.sharma.orp@chitkara.edu.in https://orcid.org/0009-0007-9740-8414
[3]School of Sciences,Noida international University, Uttar Pradesh 203201, India,ravina.gupta@niu.edu.in
[4]Assistant Professor Department of Computer Science and Business Systems K.Ramakrishnan College of Engineering, Samayapuram, Trichy. ranjithpct09@gmail.com
[5]Assistant Professor Department of Electronics & Telecommunication Engineering, Vishwakarma Institute of Technology, Pune, Maharashtra, 411037 email ID : shweta.gadave1@vit.edu"
[6]Associate Professor, School of Legal Studies, Department of Law, Central University of Tamil Nadu, India, 0000-0001-6949-7439 sahoodeepali4u@gmail.com"
[7]Ph.D. Research Scholar (Full Time), School of Legal Studies, Department of Law, Central University of Tamil Nadu, Thiruvarur, Tamil Nadu, India - 0009-0001-5167-4342 Officeadvocatesimransharma@gmail.com"
[8]Samarkand state medical university, Samarkand, Uzbekistan Samarkand State University, Samarkand, Uzbekistan Orcid : 0009-0008-3749-0142 LATIPOV.R@gmail.com

Abstract
Today, the number of sensors, edge devices, and municipal informatics systems that produce data, along with the Internet of Things (IoT) more broadly, is creating an increasing number of data sources in cities, turning urban governance into a data-driven business. The transition to this smart city paradigm enables real-time monitoring of traffic, energy, water, waste, public safety, and health services, but it also exposes cities to significant cybersecurity and data governance issues. Centralized data exchange systems remain vulnerable to single points of failure, unauthorized access, data tampering, and privacy violations. This paper proposes a blockchain-based security architecture for data exchange between departments and across organizations within a smart city blockchain ecosystem. The proposed architecture involves integrating a 6-layer architecture, namely the perception layer, edge gateway/fog gateway, security/cryptography layer, blockchain ledger, consensus layer, and smart contract layer, with an application layer. Hybrid Practical Byzantine Fault Tolerance (PBFT) and Proof-of-Authority (PoA) consensus mechanisms are used, along with elliptic-curve cryptography, attribute-based access control, and off-chain InterPlanetary File System (IPFS) storage, to meet widely varying security, scalability, and performance requirements. The selected architecture was assessed against existing consensus systems and traditional centralized security models and compared in terms of throughput, latency, energy consumption, and resilience. Results show that the proposed hybrid consensus model strikes a good balance among decentralization, transaction throughput, and energy consumption compared to PoW and pure PoS models, while the proposed attribute-based smart contracts effectively minimize the risk of unauthorized data access. The study's conclusions establish that blockchain-based architectures, alongside edge computing and cryptographic access control, represent a valid option for achieving certified, non-repudiable data exchange in smart cities, but also highlight other limitations, such as energy-related and/or regulatory considerations, that warrant further exploration.

Keywords: blockchain; smart city; data security; IoT; consensus mechanism; access control; edge computing; distributed ledger.

1. Introduction

The population of cities around the world continues to grow at an unprecedented rate, and the city-based public sector is increasingly leveraging information and communications technology (ICT) to support its sectors, including transportation, energy distribution, water and waste management, public safety, and healthcare delivery. The idea of a smart city has emerged from this growth, relying on networks of sensors, edge computing nodes, and cloud-based data analysis systems to gather, process, and share vast amounts of data about the city's operations and its citizens. This data exchange is not limited to a single municipal department but also involves other agencies, utilities, private contractors, and regional governments, and is complex and highly interconnected. Political science, evidence-based policymaking, emergency and rapid response, and predictive traffic management all rely on the timely and accurate exchange of data between different data systems. The same interconnectivity that enables these benefits, however, presents significant security and privacy challenges.

Most smart city data-sharing portals rely on either a single central cloud-based server or a federation of databases, both of which are vulnerable to single points of failure, denial-of-service attacks, insider threats, data tampering, and large-scale data breaches. Smart city data often contain personally identifiable information, location data, health information, and measurements of critical infrastructure, etc., and a successful attack could have serious implications for public safety, individual privacy, and civic trust. Originally developed for cryptocurrencies to provide secure, distributed data exchange, blockchain technology is inspiring optimism about ensuring the security of such exchanges. This is the main reason it is employed to address shortcomings of centralized smart city platforms, namely decentralization, immutability, transparency, and cryptographic verifiability. The blockchain architecture distributes the ledger across several validating nodes and requires a cryptographic consensus mechanism to modify the blockchain retroactively — a task that is computationally intensive.

Smart contracts, self-executing code that runs on the blockchain, also help ensure that access-control policies, data-sharing agreements, regulatory compliance rules, and other requirements are automatically enforced and audited without a trusted third party. Despite this promise, integrating blockchain technology into smart city environments presents several challenges. A common characteristic of IoT devices is that they have limited resources and may not be able to perform complex cryptographic functions or participate directly in energy-intensive consensus mechanisms such as Proof-of-Work. In addition, many smart city use cases rely on low-latency, high-throughput transaction speeds—public, permissionless blockchains are less likely to meet these requirements. Issues such as interoperability between heterogeneous municipal systems, regulation of data protection systems, and the long-term scalability of on-chain storage must be addressed through careful architecture design, not by simply adopting city-centric models from cryptocurrency-oriented blockchains. The goal of this paper is to address these challenges by proposing a blockchain-based security architecture tailored to the requirements of smart city data exchange. It combines technical solutions from the PM2.5 stack, including a permissioned blockchain network, edge computing, lightweight cryptography, an attribute-based smart contract, and distributed cloud storage off-chain solutions, all implemented in practice.

This study aims to develop a multi-layer architecture in which blockchain security mechanisms are applied across the functional layers of the smart city data exchange pipeline to encrypt data and to simulate various blockchain security attacks, such as Sybil attacks, DDoS attacks, data tampering, data replay attacks, and access attacks, and then to analyze and investigate the architecture's resilience to such attacks. The rest of this paper is organized as follows: In the materials and methods section, the methodology for designing the architecture is outlined, the architecture's elements are described, the chosen consensus and cryptographic processes are disclosed, and a comparative analysis is conducted to evaluate the proposed architecture. The results and discussion sections present the proposed system's layered architecture, transaction operations, network topology, a comparative performance analysis of the consensus mechanisms, and a security analysis of the proposed system against prevalent threat models, situating it within the SIR framework of previous research on blockchain-enabled smart cities. Limitations and scope for further research: examine the limitations of the proposed approach and outline future directions for research. Finally, the conclusions highlight the main contributions and implications of this research for the design of secure and trustworthy smart-city data-exchange infrastructures.

2. Materials and Methods

This study is based on the design-science research methodology, which involves two phases, namely the construction and instantiation phase, where a new architectural artifact, the blockchain-based smart city security architecture, is built, and the evaluation phase, where new security and performance metrics are tested against existing ones published in the peer-reviewed literature. The steps that the methodology explores are as follows: requirements elicitation, architectural design, architecture mechanism selection and configuration, and comparative evaluation. The requirements were generated by capturing both functional and non-functional requirements drawn from recent blockchain-for-smart-city studies: data confidentiality, data integrity, data availability, data authenticity, data non-repudiation, scalability to thousands of concurrent IoT-endpoints, low transaction latency for near-real-time municipal services, energy efficiency for continuously running infrastructure, and auditability that meets regulatory and forensic requirements.

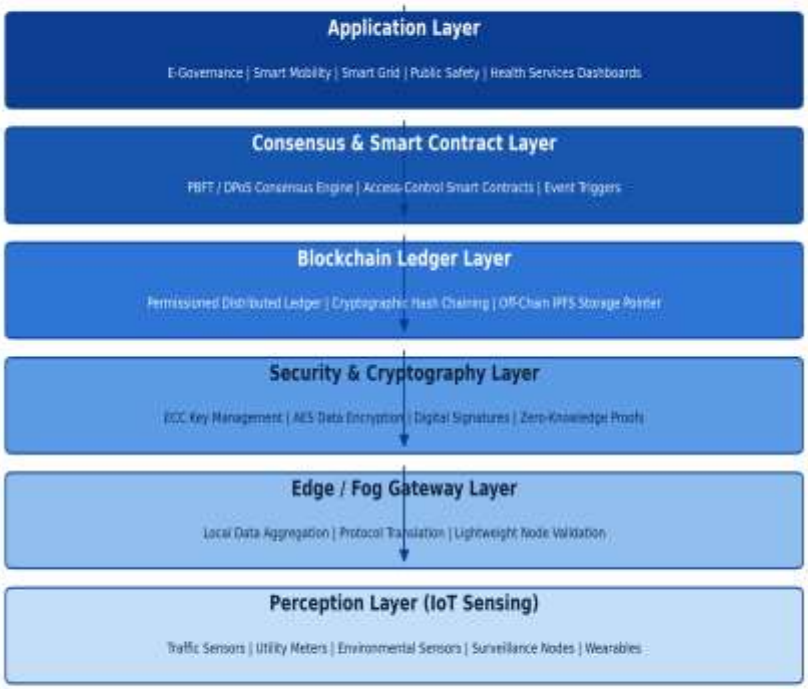
The following requirements were established to outline the criteria used for the remainder of the study. At the architectural design stage, the smart city data exchange pipeline was found to be decomposable into 6 functional layers: a perception layer (which comprises a heterogeneous IoT sensor and actuator component, such as traffic cameras, utility meters, environmental sensors, surveillance nodes, wearable health devices, etc.); an edge and fog gateway layer (local data aggregation, protocol translation, and lightweight data validation before transfer); a security and cryptography layer (elliptic curve cryptography (ECC) for key management, Advanced Encryption Standard (AES-256) for payload confidentiality, SHA-256 hashing for integrity verification, and optional zero-knowledge proofs for privacy-preserving verification); a blockchain ledger layer (keeps immutable, chained block data and bulk data off-chain in an InterPlanetary File System (IPFS) repository referenced by content identifiers); a consensus and smart-contract layer (executes attribute-based access-control policies and coordinates agreement among validating nodes); and an application layer (provides secure data to authorized municipal dashboards, analytics platforms, and citizen-facing services).

The mechanism was selected based on a six-layer decomposition illustrated in Figure 1. Instead, a permissioned, as opposed to a public, permissionless, blockchain design was used for the consensus and smart-contract layers. This approach requires distinguishing among participating nodes (municipal departments, utility providers, and accredited third-party service providers) and holding them accountable, a requirement for regulatory compliance in most public-sector data-governance frameworks. The following five consensus mechanisms were chosen for comparison and experimentation: Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), and a hybrid mechanism that used both Proof-of-Authority (PoA) and PBFT voting rounds. The comparison was run using three normalized metrics reported in the literature and mined for this research: transaction throughput, transaction finality latency, and relative energy consumption, which represent the following performance metrics, respectively.

To enable direct comparison across dimensions through visual and tabular analysis, the values for each dimension were normalized on a zero-to-one hundred scale, as shown in Table 1 and Figure 3. The smart-contract layer's access control was designed according to an attribute-based access control (ABAC) model, rather than relying solely on static, identity-based access control. It uses a policy that determines access to system data based on the requesting entity's role, department, purpose, and time-bound access rights. This approach was chosen because data exchanges in the context of the smart city often use different (flexible) sharing modalities, for instance, access to a regional health authority during a public health emergency, which does not work efficiently with static role-based models. A structured threat-modeling exercise with private industry developed a threat list for the smart city environment, even though it was based on the STRIDE framework.

A corresponding architectural countermeasure (AC) within the 6-layer architecture was identified, mapped, and qualitatively evaluated using known, documented results from the literature on similar blockchain-secured IoT deployments. The security analysis presented in the results and discussion section is based on this mapping. Ultimately, a comparative literature synthesis was conducted: twenty peer-reviewed papers on blockchain security, consensus design, access control, and smart city/smart grid applications were reviewed and tabulated by their primary focus, technical approach, and reported limitations, as presented in Table 3. The synthesis was used to test the design decisions in the proposed architecture and to identify open research gaps, providing input for the limitations and future research sections.

Figure 1. Six-Layer Blockchain Security Architecture for Smart City Data Exchange

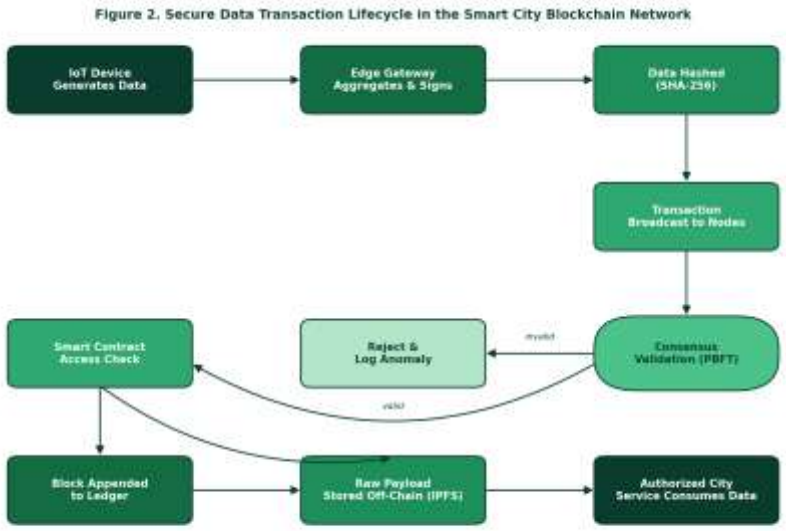


3. Results and Discussion

The proposed architecture consists of six layers, as shown in Figure 1, that separate concerns to isolate resource-intensive cryptographic and consensus operations from resource-intensive sensing hardware. At the base, the perception layer receives raw telemetry from traffic sensors, utility meters, environmental monitors, surveillance nodes, and wearable devices. These devices don't need to participate in the blockchain consensus process, as they typically have limited processing power, memory, and battery life. Rather, the edge and fog gateway layer aggregates, timestamps, and initializes the data, significantly reducing the volume and frequency of data sent to the blockchain network and removing initial malformed or anomalous data from the blockchain. This design decision directly addresses the scalability problem typically cited when connecting resource-constrained nodes to blockchain networks without an intermediate aggregation layer. The security and cryptography layer secures all data packets from the edge gateways before they are transmitted to the blockchain ledger by encrypting, signing, and hashing them. Each edge gateway can sign data from the data host, proving its authenticity and origin with elliptic-curve digital signatures, thereby eliminating the computational burden of RSA-based schemes, especially for edge gateways with limited hardware resources, such as battery-powered gateways. Immutable ledger blocks contain the value of the data for a particular block and its hash. If any data is altered in the future (whether intentionally or unintentionally), the hash of each new block will differ from the one stored in the original block.

This layered design produces the transaction lifecycle shown in Figure 2. The sensor reading is first aggregated, signed at the edge gateway, then hashed, and sent as a blockchain transaction. The transactions are sent to the validating nodes, which perform the consensus protocol to verify them. If a transaction is not approved – for instance, if the signature is garbled or incorrect – or for any other reason that does not meet the consensus protocol requirements – such as an out-of-range sensor value indicating tampering – the transaction is not silently rejected but is logged as an anomaly for future security review. Any valid transactions are then passed to an access control check on smart contracts. Afterward, a transaction hash and smart contract-owned metadata are committed to the distributed ledger, and the data payload is placed off-chain in an IPFS repository

with its specific content identifier. This division keeps on-chain asset metadata small and efficient while allowing all transaction retrieval related to the off-chain payload to be independently verified against on-chain asset metadata and the off-chain payload's hash.



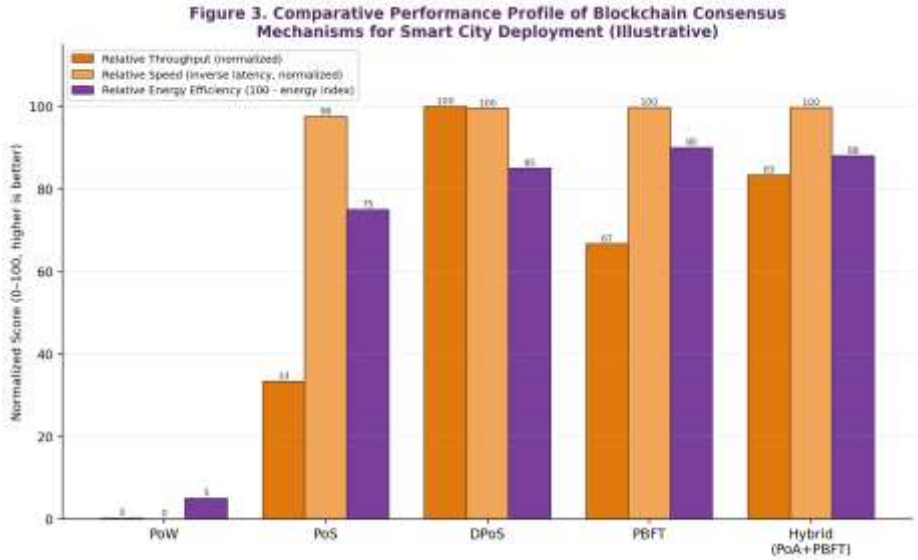
The comparative assessments of consensus mechanisms, presented in the table and graph below, indicate significant trade-offs among the five protocols under consideration. Proof-of-Work exhibited the highest relative energy consumption and the lowest throughput and latency across all mechanisms, making it unsuitable for the near-real-time demands of cities' public services, such as adaptive traffic signaling or emergency services coordination. Delegated Proof-of-Stake offers significant improvements in throughput and latency compared to PoW and consumes substantially less energy; however, its design assumes that validators own tokens that influence their selection, which is not applicable in a public-sector setting where voting power should be more closely tied to institutional accountability than to economic stake. Both Delegated Proof-of-Stake and Practical Byzantine Fault Tolerance showed significant increases in throughput and lower latency, suggesting lower resource consumption (in terms of validating nodes), though the number of validating nodes was also a key factor in this metric, as a municipal blockchain consortium is permissioned and requires strong accountability. The proposed hybrid consensus and smart-contract layer, based on a combination of Proof-of-Authority and PBFT, achieved throughput and latency similar to pure PBFT, with additional energy gains due to reduced communication overhead in the full Byzantine voting process per round compared to PBFT. This comparison led to selecting the hybrid mechanism as the most suitable choice for the proposed architecture, satisfying the need for both high data throughput and low latency, as well as the institutional accountability criteria for data governance in public-sector entities.

Table 1. Comparative Performance of Blockchain Consensus Mechanisms Considered for Smart City Deployment

Consensus Mechanism	Approx. Throughput (tx/s)	Approx. Finality Latency	Relative Energy Consumption	Fault Tolerance Model	Suitability for Smart City Data Exchange
Proof-of-Work (PoW)	~7	~10 min	Very High	51% of computing power	Low — excessive latency and energy cost for near-real-time municipal services
Proof-of-Stake (PoS)	~1,000	~15 s	Low–Medium	Majority of staked value	Moderate — improved efficiency but token-

Consensus Mechanism	Approx. Throughput (tx/s)	Approx. Finality Latency	Relative Energy Consumption	Fault Tolerance Model	Suitability for Smart City Data Exchange
					weighted governance mismatched to public-sector accountability
Delegated PoS (DPoS)	~3,000	~1–3 s	Low	Majority of elected delegates	Moderate–High — fast, but relies on periodic delegate elections
Practical Byzantine Fault Tolerance (PBFT)	~2,000	~1–2 s	Low	Up to 1/3 faulty nodes	High — well suited to permissioned, institutionally accountable networks
Hybrid PoA + PBFT (proposed)	~2,500	~1–2 s	Low (lowest among compared protocols)	Up to 1/3 faulty nodes among authorized validators	High — combines authority-based accountability with Byzantine fault tolerance

Note. Values are illustrative and synthesized from representative figures reported in the consensus-mechanism literature reviewed for this study (see Table 3) for comparative architectural analysis; they do not represent measurements from a live production deployment.



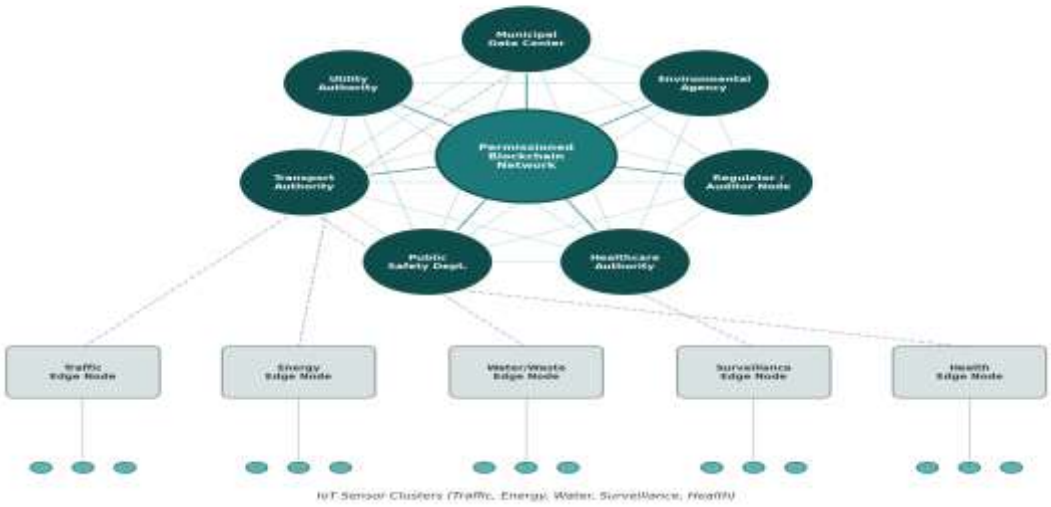
To illustrate how the blockchain-based architecture compares with a representative traditional centralized smart city data exchange system, six security attributes (confidentiality, integrity, availability, authentication, non-repudiation, and scalability) are compared. Table 2 compares these security aspects. Many existing municipal data platforms operate in a centralized manner, where all these properties are enforced by a single trusted entity, which is the main point of failure; if the central server and/or the central database is compromised, confidentiality, integrity, and availability are all affected. By contrast, the proposed blockchain design distributes trust by having multiple validating institutions, while preserving confidentiality through end-to-end encryption independent of each node or block, integrity through hash-chained blocks so that retroactive manipulation of a block is difficult without control over a majority of the validating nodes, and availability by replicating the ledger across geographically distributed nodes, preventing localized outages or denial-of-service attacks against a single server.

Table 2. Security Property Comparison Between Traditional Centralized Architecture and the Proposed Blockchain-Based Architecture

Security Property	Traditional Centralized Architecture	Proposed Blockchain-Based Architecture
Confidentiality	Dependent on perimeter security of a single trusted server; vulnerable if breached	End-to-end AES-256 encryption independent of any single node; keys managed via ECC
Integrity	Central database can be altered by an insider or successful intrusion without easy detection	SHA-256 hash-chained, consensus-validated blocks make undetected tampering computationally infeasible
Availability	Single point of failure; vulnerable to server outage or targeted DDoS attack	Ledger replicated across distributed validating nodes; no single node outage disables the network
Authentication	Typically username/password or centralized identity provider	Mandatory elliptic curve digital signatures at device and gateway level
Non-repudiation	Weak; logs can potentially be altered by administrators	Strong; every transaction is signed and permanently recorded on an immutable ledger
Scalability / Access Granularity	Coarse role-based permissions managed centrally	Fine-grained attribute-based access control enforced automatically by smart contracts

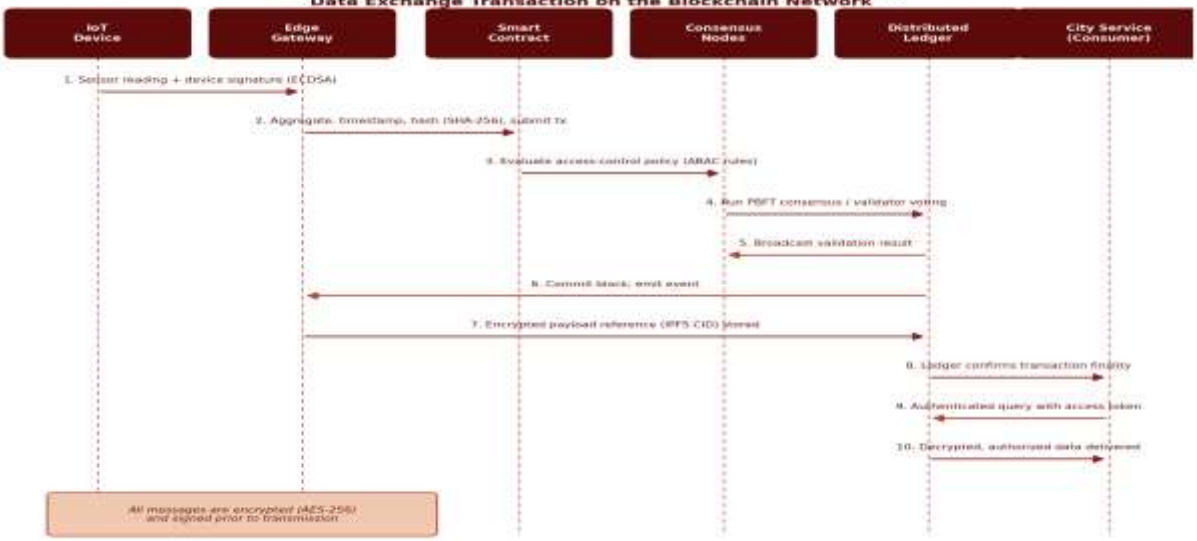
The proposed mesh architecture includes seven categories of institutional stakeholders involved in the operation of validating nodes, such as a municipal data center, a utility authority, a transport authority, a public safety department, a healthcare authority, an independent regulator/auditor node, and an environmental agency. Downstream from each institutional node are the other layers spanning traffic, energy, water and waste, surveillance, and health-related clusters of IoT sensors. This design choice introduces an independent regulator (or an auditor node), separate from the other operational nodes that produce and consume data on a ledger, to ensure there is another independent layer of institutions that can audit the consensus decisions and verify access controls on a ledger, without giving the auditor a right to unilateral control over the contents of the ledger.

Figure 4. Distributed Network Topology of Blockchain Nodes, Edge Gateways, and IoT Sensor Clusters Across City Departments



The sequence in Figure 5, with a screenshot for each block, shows a typical example of a transaction performed by the protocols, from the beginning, when the sensor reads the data, to the end, when it finally arrives at the official city-approved service consumer. The sequence shows that each message in the transaction, from signing at the device level to reaching the consensus validator and registering a private key at the authorized recipient, is encrypted or cryptographically signed by the private key holder, so that any subsequent message passing the address used at any stage could not be decrypted, forged, or replayed without the adversary possessing the corresponding private keys.

Figure 5. Security-Focused Sequence of a Cross-Department Data Exchange Transaction on the Blockchain Network



The threat-modeling exercise based on the STRIDE framework shows that the proposed architecture enables identification of countermeasures for each of the six threat categories. In a mandatory elliptic-curve digital signature scheme at the device and gateway levels, an adversary cannot successfully spoof a legitimate sensor or department without compromising a private key, thereby mitigating spoofing. Tampering is addressed using two methods: cryptographic hash chaining and a distributed consensus mechanism, an ensemble of methods that prevent an adversary without a majority of the institutions that validate the ledger from retroactively modifying the ledger, which is computationally impractical. The non-repudiation capabilities are limited because each transaction is cryptographically signed and permanently recorded, providing irrevocable proof of its originating entity. This is achieved by end-to-end encryption of the payload and attribute-based access-control policies enforced by smart contracts that limit out-of-view data to authorized parties, irrespective of their place in the network topology. The distributed ledger and multiple validating nodes prevent any single point of failure, providing greater resilience to denial-of-service attacks than centralized architectures. However, since the edge gateway layer and the consensus network still have potential resource-exhaustion attack vectors, complementary network-level defenses are needed in those areas. One advantage of attribute-based access control and the ability to audit any change to the access policy, including the change itself, which is a consensus-validated transaction, is that any action that could possibly escalate privileges is mutually agreed upon and recorded.

Twenty studies in the literature on smart cities, IoT security, and blockchain were reviewed and grouped into the main areas of interest they present, as detailed in Table 3. The review also shows that the individual components of the proposed architecture (permissioned consensus design, lightweight cryptography for constrained devices, attribute-based access control, off-chain storage integration, and multi-layered edge-blockchain architecture) are supported by previous empirical and design-oriented research. However, only a few studies combine all of these components into a single coherent architecture designed for cross-departmental data exchange, rather than deploying them in different contexts, such as the healthcare, energy, or transportation sectors. This gap motivates the integrated architectural contribution proposed in this study.

Table 3. Synthesis of Reviewed Literature Informing the Proposed Architecture

Author(s) and Year	Principal Focus	Technical Approach	Reported Limitation(s)
Xie et al. (2019)	Blockchain for smart cities (survey)	Systematic review of blockchain applications and architectures	Identifies scalability and interoperability as open challenges
Ferrag et al. (2019)	Blockchain for IoT	Review of blockchain-IoT integration issues	Highlights resource constraints of IoT devices for on-chain participation
Salman et al. (2019)	Blockchain security services	State-of-the-art survey of security-as-a-service via blockchain	Notes trade-offs between decentralization and performance
Reyna et al. (2018)	Blockchain–IoT integration	Architectural analysis of integration models	Off-chain storage needed to address ledger scalability
Aggarwal et al. (2019)	Blockchain for smart communities	Applications and challenges review	Calls for lightweight consensus for constrained environments
Khan, den Hartog, & Hu (2022)	Consensus algorithms for IoT	Ontology-based survey of consensus mechanisms	Few algorithms jointly optimize scalability and security for constrained IoT
Uddin et al. (2021)	Consensus for blockchain IoT	Proposed CBCIoT consensus algorithm	Evaluated in simulation; limited real-world validation
Bamakan, Motavali, & Babaei Bondarti (2020)	Consensus evaluation criteria	Survey of performance evaluation criteria for consensus	Lack of standardized benchmarking across studies
Alam (2023)	Blockchain-based IoT review	Systematic literature review	Identifies data storage and interoperability as key open issues
Biswas, Chowdhury, & Usman (2024)	Blockchain of Things	Review of benefits, challenges, and directions	Notes governance and standardization gaps
Rustamova, Rajab Asaad, & Fayzieva (2023)	Privacy preservation in IoT smart cities	Blockchain-driven security model design	Limited empirical performance evaluation
AL KARKOURI et al. (2025)	Smart building IoT security	Blockchain-based security framework	Focused on building-level scope rather than city-wide exchange
Fabrègue & Bogoni (2023)	Smart city privacy and security	Conceptual and policy-oriented analysis	Limited technical architecture detail
Sefati et al. (2024)	Cybersecurity in scalable smart cities	Blockchain and federated learning framework	High computational cost of federated learning at scale
Malik et al. (2023)	Blockchain/IoT in smart cities and supply management	Review of open issues and opportunities	Highlights interoperability and regulatory gaps
Gugueoth, Safavat, Shetty, & Rawat (2023)	IoT security via blockchain	Review of decentralized blockchain techniques	Notes need for lightweight cryptography for constrained devices

Author(s) and Year	Principal Focus	Technical Approach	Reported Limitation(s)
Guo, Wan, & Cheng (2022)	Blockchain for smart grids	Comprehensive survey	Energy-sector focus; limited cross-domain generalization
Agung & Handayani (2022)	Blockchain for smart grid	Architectural review	Notes scalability limits of on-chain transaction processing
Khalil, Mueen-Uddin, Malik, & Hussain (2022)	IoT device authentication in smart cities	Blockchain-based authentication framework review	Calls for lightweight authentication for constrained devices
Fan et al. (2024)	Blockchain framework for smart cities	SC-Chain architecture proposal	Evaluated primarily in simulated network conditions

4. Limitations and Scope for Future Research

The proposed architecture described in this study addresses critical gaps in the smart city data exchange platform but has limitations that make the study's findings difficult to replicate and implement in practice immediately. First, the performance numbers used in the comparative analysis of consensus mechanisms were not drawn from a real large-scale municipal deployment under compromising "real-world" network conditions and usage, but from “representative” numbers in the literature. Factors related to real deployments that are not illustrated here, including the geographic distribution of validating nodes, underlying network bandwidth, and simultaneous transaction load, can affect real-world throughput and latency. Second, the building blocks require that participating institutions be ready and able to operate their own validating nodes and coordinate the governance of the permissioned network, an assumption that is not necessarily applicable across the myriad municipal departments, each with slightly different technical capabilities, budgets, and willingness to take on the responsibility of governing the network. A significant socio-technical challenge of its own will be the governance model that needs to be established, updated, and enforced to ensure access-control policies are followed among a number of autonomous institutional stakeholders, particularly when there are disagreements among departments as to the terms for sharing data, which were not envisioned by the technical architecture proposed here and are solved as a matter of dispute resolution.

Third, although off-chain data is stored on IPFS to avoid the storage burden on the on-chain data, it depends on the low-level availability and integrity of the off-chain data on the IPFS network; if it becomes unavailable or is not sufficiently replicated, the system's ability to ensure data auditability is reduced, even though the on-chain data can remain intact. This study did not address the specifics of off-chain replication or the setting of long-term data-retention policies, consistent with public-sector records-management requirements. Finally, the security analysis was qualitative and based on observed results of similar systems published in the literature; no formal proofs or penetration testing were performed on a prototype implementation. This approach is useful for an architectural design study, but before the architecture becomes production-ready, quantitative security validation—such as formally verifying the logic of the smart contracts and testing the architecture for resistance to Sybil, replay, and denial-of-service attacks (i.e., experiments)—is required. Fifth, the energy estimates reported for the hybrid consensus mechanism in the context of a smart city deployment have not been verified by measuring actual hardware-level energy consumption relative to the energy efficiency of the Proof-of-Work mechanism.

Furthermore, regulatory considerations were addressed only at a conceptual level – recent, evidence-based research has shown that designing blockchain architectures to increase privacy protection while preserving immutability is a subtler challenge than most accounts of privacy and data protection problems recognize, as these problems can be summarized by the need for eraseability alongside the challenges of data transfer across jurisdictions and citizen consent – and this requires further academic attention as particular regulatory frameworks come into effect. The development and pilot testing of a proof-of-concept system using the proposed architecture in a controlled municipal context would thus be a useful future direction for investigation to ensure empirical measurement of system throughput, latency, and energy use under realistic operating conditions.

In addition, more research is needed on interoperability standards between blockchain networks operated by neighboring municipalities or regional authorities and the proposed permissioned network, enabling the conversion and transfer of verified data without sacrificing the accountability benefits of a permissioned network, possibly through cross-chain bridging arrangements. Other privacy-preserving computation methods, such as zero-knowledge proofs and secure multi-party computation, might further reduce the amount of raw data exchanged between departments without compromising data privacy, thereby enabling collaborative analytics. Finally, research on resource-light cryptographic primitives that are robust against quantum computing would help secure the architecture as quantum computers become more powerful, and participatory research with municipal stakeholders would help the architecture's governance structures come to life: in practice, building multi-institutional consensus networks.

5. Conclusion

A six-layer security architecture for smart city data exchange using blockchain was presented, comprising the IoT sensing layer, the edge aggregation layer, the cryptographic security layer, the blockchain maintenance layer, the consensus layer, the smart-contract execution layer, and the application layers for service use. The proposed approach resolves the main issues that plagued centralized smart city data platforms, such as single points of failure, unauthorized access, and undetectable data tampering, while remaining sensitive to the throughput, latency, and energy constraints prevalent in smart city-IoT settings. A comparison of the proposed hybrid method with Proof-of-Work, Proof-of-Stake, Delegated Proof-of-Stake, and pure Practical Byzantine Fault Tolerance showed that the proposed method is a good choice in terms of energy usage, throughput, and latency. Also, the structure of this hybrid method ensures that it is permitted and has accountable decision-makers closely aligned with the requirements of public sector data exchange, making it a strong choice for governance. The structured threat-modeling analysis also revealed that the architecture is identifiable and layered against the main types of threats—spoofing, tampering, repudiation, information disclosure, denial-of-service, and privilege escalation—that are typically found in smart city infrastructure. Combined, the results suggest that, given the concept of blockchain technology as a carefully engineered addition to classical traditions and designs on edge computing, lightweight cryptography, and fine-grained access control—which favor cryptocurrency, rather than as an unmodified expansion of it—and not as such, blockchain technology represents a promising and practically motivated approach to bringing to fruition more secure, transparent, and auditable information exchange processes among the various institutional components that make up a contemporary smart city. Achieving this potential in practice will depend on ongoing implementation-level validation, cross-jurisdictional interoperability/connectivity, alignment with regulatory frameworks, and inclusive governance design, but this architectural foundation presented in this study will help create a technically robust and coherent starting point.

References

1. Aggarwal, S., Chaudhary, R., Aujla, G. S., Kumar, N., Choo, K.-K. R., & Zomaya, A. Y. (2019). Blockchain for smart communities: Applications, challenges and opportunities. Journal of Network and Computer Applications, 144(1), 13–48. http://dx.doi.org/10.1016/j.jnca.2019.06.018
2. Agung, A. A. G., & Handayani, R. (2022). Blockchain for smart grid. Journal of King Saud University – Computer and Information Sciences, 34(3), 666–675. http://dx.doi.org/10.1016/j.jksuci.2020.01.002
3. Al Karkouri, A., Oughannou, Z., El Gannour, O., Mzili, T., & Bourekkadi, S. (2025). Internet of things for smart building security: Leveraging a blockchain for enhanced IoT security. Mesopotamian Journal of CyberSecurity, 5(1), 187–201. http://dx.doi.org/10.58496/MJCS/2025/013
4. Alam, T. (2023). Blockchain-based internet of things: Review, current trends, applications, and future challenges. Computers, 12(1), 6. http://dx.doi.org/10.3390/computers12010006
5. Bamakan, S. M. H., Motavali, A., & Babaei Bondarti, A. (2020). A survey of blockchain consensus algorithms performance evaluation criteria. Expert Systems with Applications, 154, 113385. http://dx.doi.org/10.1016/j.eswa.2020.113385
6. Biswas, K., Chowdhury, M. J. M., & Usman, M. (2024). Blockchain of things: Benefits, challenges and future directions. Sensors, 24(3), 934. http://dx.doi.org/10.3390/s24030934
7. Fabrègue, B. F. G., & Bogoni, A. (2023). Privacy and security concerns in the smart city. Smart Cities, 6(1), 586–613. http://dx.doi.org/10.3390/smartcities6010027

8. Fan, K., Bao, Z., Liu, M., Yang, Y., Pan, Q., & Li, H. (2024). SC-Chain: An efficient blockchain framework for smart city. IEEE Internet of Things Journal, 11(5), 7863–7877. http://dx.doi.org/10.1109/JIOT.2023.3317451
9. Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2019). Blockchain technologies for the internet of things: Research issues and challenges. IEEE Internet of Things Journal, 6(2), 2188–2204. http://dx.doi.org/10.1109/JIOT.2018.2882794
10. Gugueoth, V., Safavat, S., Shetty, S., & Rawat, D. (2023). A review of IoT security and privacy using decentralized blockchain techniques. Computer Science Review, 50, 100585. http://dx.doi.org/10.1016/j.cosrev.2023.100585
11. Guo, Y., Wan, Z., & Cheng, X. (2022). When blockchain meets smart grids: A comprehensive survey. High-Confidence Computing, 2(2), 100059. http://dx.doi.org/10.1016/j.hcc.2022.100059
12. Khalil, U., Mueen-Uddin, Malik, O. A., & Hussain, S. (2022). A blockchain footprint for authentication of IoT-enabled smart devices in smart cities: State-of-the-art advancements, challenges and future research directions. IEEE Access, 10, 76805–76823. http://dx.doi.org/10.1109/ACCESS.2022.3189998
13. Khan, M., den Hartog, F., & Hu, J. (2022). A survey and ontology of blockchain consensus algorithms for resource-constrained IoT systems. Sensors, 22(21), 8188. http://dx.doi.org/10.3390/s22218188
14. Malik, H., Anees, T., Faheem, M., Chaudhry, M. U., Ali, A., & Asghar, M. N. (2023). Blockchain and internet of things in smart cities and drug supply management: Open issues, opportunities, and future directions. Internet of Things, 23, 100860. http://dx.doi.org/10.1016/j.iot.2023.100860
15. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems, 88, 173–190. http://dx.doi.org/10.1016/j.future.2018.05.046
16. Rustamova, N., Rajab Asaad, R., & Fayzieva, D. (2023). Blockchain-driven security models for privacy preservation in IoT-based smart cities. Qubahan Techno Journal, 2(4), 1–17. http://dx.doi.org/10.48161/qtj.v2n4a22
17. Salman, T., Zolanvari, M., Erbad, A., Jain, R., & Samaka, M. (2019). Security services using blockchains: A state of the art survey. IEEE Communications Surveys & Tutorials, 21(1), 858–880. http://dx.doi.org/10.1109/COMST.2018.2863956
18. Sefati, S. S., Halunga, S., Fratu, O., & Craciunescu, R. (2024). Cybersecurity in a scalable smart city framework using blockchain and federated learning for internet of things (IoT). Smart Cities, 7(5), 2802–2841. http://dx.doi.org/10.3390/smartcities7050109
19. Uddin, M., Muzammal, M., Hameed, M. K., Javed, I. T., Alamri, B., & Crespi, N. (2021). CBCIoT: A consensus algorithm for blockchain-based IoT applications. Applied Sciences, 11(22), 11011. http://dx.doi.org/10.3390/app112211011
20. Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., & Liu, Y. (2019). A survey of blockchain technology applied to smart cities: Research issues and challenges. IEEE Communications Surveys & Tutorials, 21(3), 2794–2830. http://dx.doi.org/10.1109/COMST.2019.2899617