# The SynapticCity Phenomenon: When All Foundation Models Marry Federated Learning and Blockchain

**Sergio Zaera Mata**
Department of Artificial Intelligence
HI Iberia (HIB)
szaera@hi-iberia.es

**Roberto Gómez-Espinosa**
Department of Artificial Intelligence
HI Iberia (HIB)
robertogemartin@hi-iberia.es

## Abstract

Our work proposes an innovative framework for smart cities that integrates Foundation Models (FMs), Federated Learning (FL), and Blockchain to address key challenges in urban data management, such as privacy, scalability, and predictive accuracy. By combining the predictive power of FMs with the privacy-preserving capabilities of FL and the secure, transparent governance provided by Blockchain, we create a robust, decentralized solution for managing diverse urban data. Our approach enables real-time data analysis and decision-making while ensuring that sensitive information remains secure. To demonstrate the efficacy of this integrated platform, we present a use case in inventory management and sales forecasting for smart city businesses, showcasing its potential to enhance operational efficiency, data privacy, and economic resilience. This synergy of advanced technologies establishes a new standard for secure, adaptable, and collaborative management.

## 1 Introduction

### 1.1 Context and Motivation

The concept of "Smart Cities" has become increasingly significant as an innovative approach to address the challenges of urban growth, enhance citizens' quality of life, and optimize the use of available resources [1]. These cities leverage advanced technologies such as the Internet of Things (IoT), which involves a network of interconnected devices—ranging from smartphones and laptops to vehicles and smartwatches—all equipped with sensing and computing capabilities that enable real-time data collection and analysis to tackle critical issues like traffic management, energy consumption, and public health [2, 3, 4, 5]. In parallel, Foundation Models (FMs), large-scale pre-trained AI models, have permeated various aspects of urban life, becoming integral to numerous smart city processes and applications, from predictive analytics in infrastructure management to personalized citizen services embedded in everyday devices like smartphones and wearables [6].

The widespread deployment of FMs requires them to be fine-tuned and personalized for specific urban contexts, which amplifies the importance of securing these models during training and storage [7]. Traditional approaches relying on centralized data storage and processing have raised significant concerns around data privacy and security, creating potential bottlenecks and increasing risks of privacy breaches [8, 9]. This has driven interest in decentralized techniques such as Federated Learning (FL), which retains data locally on edge devices while allowing for collaborative model training. FL effectively reduces privacy leakage risks during data transmission and alleviates the burden on centralized storage and computation infrastructure [10].

38th Conference on Neural Information Processing Systems (NeurIPS 2024).

However, despite these advances, significant challenges remain, particularly around managing data heterogeneity and ensuring trust in centralized servers [11]. Additionally, as FMs continue to integrate into personal and public devices, the privacy and security of the data and the models themselves become more critical [12]. The need for robust data analysis models that balance high precision and efficiency with rigorous privacy safeguards for citizens is more pressing than ever [13]. These challenges underscore the urgent need for new technological platforms that not only integrate diverse urban data sources but also ensure secure and private storage and handling of model parameters [14].

### 1.2 Contribution of the Paper

This paper proposes an innovative approach that integrates **foundation models**, **federated learning techniques**, and **blockchain technology** to address current challenges in managing data within smart cities. The novelty of this approach lies not in the use of any single technology but in their **strategic combination** to leverage heterogeneous data from various urban infrastructures and information sources. By utilizing these advanced models, the proposal develops predictive capabilities that enhance the accuracy of data analysis and optimize real-time decision-making processes across a range of smart city applications.

At the core of this innovation is the **synergistic use** of federated learning, blockchain, and foundation models. Federated learning enables decentralized model training, allowing data to remain on local devices without needing to be shared, thereby safeguarding both public and private information. This decentralized approach ensures that data privacy is maintained while still enhancing the model's accuracy. The integration of **differential privacy** mechanisms further reinforces data security, preventing the inference of sensitive information from model outputs. Meanwhile, blockchain technology provides a **decentralized infrastructure** and an immutable ledger for all transactions and operations, ensuring integrity, transparency, and fairness throughout the federated learning process. Smart contracts within this blockchain framework establish automated governance rules that promote fair, reliable network operation, while also enabling the implementation of incentives and penalties to encourage appropriate behavior among participants.

To demonstrate the applicability and advantages of this proposal, a specific use case is presented, focusing on **inventory management** and **sales forecasting** for businesses within a smart city. This example illustrates how the combined use of these technologies can provide businesses with advanced tools for inventory control, demand prediction, and real-time optimization of logistics and sales operations, all while ensuring robust data security and privacy. This solution aims not only to improve **operational efficiency** and reduce costs but also to stimulate a more dynamic and resilient economy.

## 2 State of the Art

### 2.1 Review of Current Technologies

In smart cities, the integration of multiple advanced technologies is essential for effective urban data management, improved quality of life, optimized resource use, and predictive event forecasting. At the core of this technological ecosystem are **IoT sensors and networks**, which facilitate continuous data collection from various urban environments by generating real-time data streams from traffic lights, air quality monitors, energy meters, and other sources. These data streams support crucial applications, such as traffic management, environmental monitoring, and resource allocation, enabling dynamic decision-making and enhancing the efficiency of urban services [15, 16].

Building on this foundation, technologies such as **Geographic Information Systems (GIS)** provide sophisticated tools for visualizing, managing, and analyzing spatial data. GIS tools allow cities to map and interpret spatial patterns or design efficient transportation networks, all of which are critical for enhancing urban resilience and sustainability. The integration of GIS with IoT data is further enhanced by **geospatial dashboards**, which enable real-time visualization and analysis, supporting informed decision-making and policy development [17, 18]. Moreover, **Big Data analytics** and predictive

modeling further strengthen this ecosystem by applying advanced machine learning algorithms to detect patterns and trends across the vast datasets generated by smart city systems [19, 20].

To consolidate these technologies into a cohesive framework, **centralized data management** platforms play a crucial role, providing the infrastructure necessary for real-time data analysis and coordinated urban responses. These platforms integrate data from different sources, supported by robust communication networks such as 4G/5G. These networks ensure seamless data transmission and enable adaptive actions in critical areas like traffic control and smart lighting [21, 22].

The integration of these technologies marks significant progress towards a comprehensive framework for smart city management, yet **substantial barriers still need to be addressed** to fully realize this potential. Overcoming these limitations will be crucial for advancing smart city innovations and achieving sustainable, data-driven urban management [23].

### 2.2 Limitations of Current Technologies

While current technologies have enabled significant progress in smart city development, they face **critical limitations** that hinder effective **data management** and **privacy protection**, reflecting broader challenges in integrating diverse systems. One major issue is the lack of data integration and the prevalence of data silos. Centralized platforms, although effective for data collection and analysis, often operate in isolation, resulting in duplicated efforts and preventing a comprehensive view of city operations. The heterogeneity in data formats and quality across different sources complicates integration, limiting decision-making capabilities across various urban domains [24, 25, 26].

Privacy and security concerns are another significant barrier. Centralized data storage increases the **risk of breaches** due to cyberattacks or misuse, and many current solutions lack robust mechanisms to protect sensitive information, especially when data is aggregated from diverse sources.[27, 28]. There is a need for enhanced data governance frameworks to ensure accountable and responsible data sharing, given the power imbalances among stakeholders [29]. Scalability and cost remain critical obstacles. Real-time data processing requires robust and expensive infrastructure, which is often **not scalable or affordable** for larger or rapidly growing cities. The financial burden of maintaining and upgrading centralized systems can be prohibitive [30]. Additionally, limitations in predictive accuracy due to **fragmented data,** lack of continuous model updates, and **inadequate training data** affect the effectiveness of algorithms used to predict urban behavior and needs [31, 32].

These limitations underscore the need for a more integrated, secure, and scalable approach to smart city development, incorporating innovative data governance, advanced security protocols, and flexible, cost-effective infrastructure solutions. Emerging technologies, offer promising pathways to enhance real-time data management, **potentially overcoming some of these barriers** [33, 34, 35].

### 2.3 Proposed Technologies and Combined Solutions

To address the limitations of current smart city technologies, we propose an integrated approach combining Foundation Models, Federated Learning, and Blockchain technology to create a comprehensive solution for challenges such as **data privacy**, **scalability**, and **predictive accuracy**.

**Foundation Models** are large-scale AI models pre-trained on extensive datasets that can be fine-tuned for a wide range of tasks. These models excel in learning from diverse types of data, including text, images, and numerical information, and can be applied across multiple domains within a smart city. By leveraging their ability to understand and interpret complex patterns, foundation models enable more accurate predictions, improve decision-making, and enhance the adaptability of urban systems. Their flexibility allows them to be used in various contexts, and even providing personalized citizen services, all while continuously learning from new data inputs [36, 37].

**Federated Learning** is an approach to machine learning that decentralizes the training process, allowing models to be trained locally on devices rather than requiring data to be centralized on a single server [38]. This method preserves privacy by ensuring that sensitive data never leaves the device, thus reducing risks associated with data breaches and unauthorized access. It also enhances

scalability and cost-efficiency by minimizing the need for large centralized data centers and supporting continuous model improvement across diverse nodes [39].

**Blockchain Technology** adds a layer of security and trust to the system by providing a decentralized and immutable ledger for all transactions and operations within the smart city ecosystem. Each transaction, is recorded transparently, ensuring data integrity and accountability. Blockchain supports smart contracts self-executing programs that automatically enforce rules and agreements. This decentralized governance reduces the reliance on a central authority, thereby preventing single points of failure and ensuring fairness and transparency [40].

The **synergy of these technologies** establishes a robust, flexible, and secure platform that effectively integrates data while enhancing privacy and scalability. This approach overcomes the limitations of traditional centralized systems, fostering a more **dynamic and resilient framework** for managing smart city resources and services, ultimately driving a new era of urban innovation [41].

## 3 Proposed Platform Architecture

### 3.1 Platform Components and Integrated Workflow

The proposed platform addresses smart city data management challenges by integrating Foundation Models, Federated Learning, and Blockchain technology into a unified framework. Foundation models utilize the diverse data capture by the IoT urban sensors to improve predictive analytics across urban domains, with Federated Learning supporting decentralized model training to ensure data privacy. Meanwhile, Blockchain technology secures governance and data integrity through an immutable ledger and automated smart contracts. These components collectively establish a scalable and resilient platform, facilitating efficient smart city management.

The platform's workflow iniciates with the **real-time acquisition** of data from a comprehensive network of IoT sensors strategically deployed across the urban landscape, capturing diverse streams such as traffic patterns, environmental metrics, and energy consumption data. This data is initially managed in decentralized databases on local servers to **preserve privacy** and **reduce centralization risks**. The local servers then perform critical preprocessing tasks, including **data cleansing, anonymization, normalization, and dimensionality reduction**, ensuring data integrity and preparing it for machine learning applications. Federated Learning (FL) enables decentralized model training at these edge nodes, with only the learned model parameters, rather than raw data, transmitted to a central aggregation point or blockchain node. This approach safeguards data privacy while allowing for the integration of locally trained models into a global model, secured by blockchain technology. Blockchain provides an immutable ledger and utilizes consensus mechanisms and smart contracts to validate, aggregate, and govern the integration process, **ensuring data integrity, scalability, and adaptability** within the smart city infrastructure. This seamless integration enhances the platform's capability to manage urban data efficiently and securely, facilitating robust and responsive operations.

### 3.2 Integration and Role of Foundation Models

Foundation models serve as the core of the platform's **predictive analytics capabilities**, drawing upon the **diverse and heterogeneous data streams** collected from various urban components to enhance both the accuracy and depth of urban predictions. These models are trained using a wide array of data sources within the urban environment, such as traffic patterns, energy consumption metrics, mobility behaviors, and citizen activities. The integration of these diverse data types allows foundation models to capture **complex interdependencies** between different urban variables, substantially boosting their predictive performance and applicability across multiple domains.

The inherent flexibility of foundation models in handling heterogeneous data provides a significant advantage over traditional data analysis approaches, which often face challenges when dealing with unstructured data formats, such as free text or raw sensor outputs. By processing large volumes of both structured and unstructured data, these models can perform **more nuanced and comprehensive**

**analyses**, detecting intricate patterns that conventional methods may fail to identify. Furthermore, foundation models are designed to **generalize effectively**, even from limited or incomplete datasets, which is advantageous in urban environments where certain types of data may be sparse or fragmented.

This versatility enables the platform to generate **informed predictions** across a wide range of urban scenarios, from optimizing real-time traffic management to supporting strategic long-term urban planning initiatives. As a result, the use of foundation models contributes to a more **adaptive and responsive smart city infrastructure**, enhancing the capacity to manage and respond to dynamic urban challenges while supporting sustainable growth and improved quality of life for citizens.

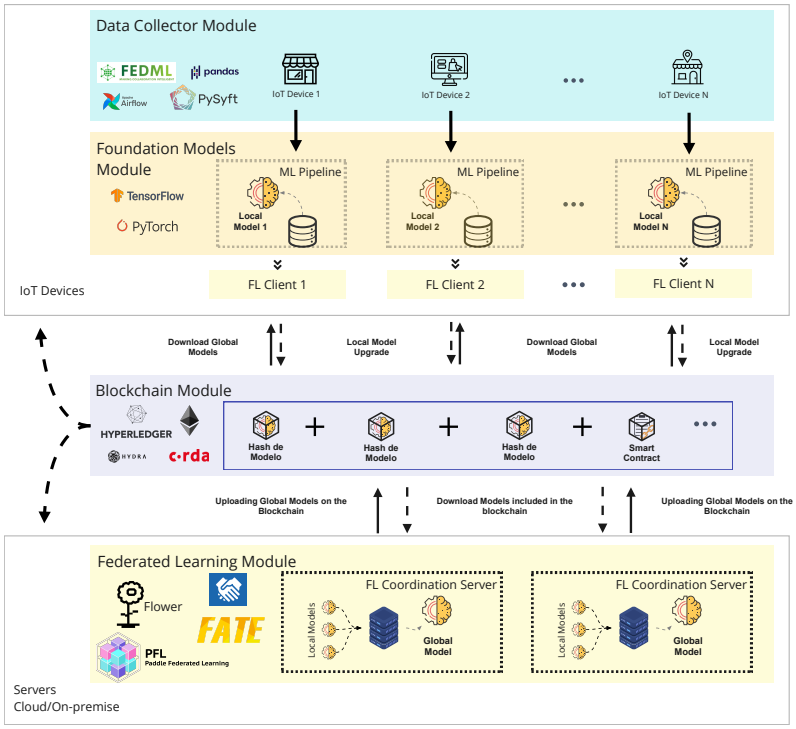


Figure 1: Overview of the Proposed Architecture: Integrating Foundation Models, Federated Learning, and Blockchain Across Multiple Layers.

### 3.3 Federated Learning Approach

The Federated Learning approach within the platform facilitates a decentralized model training process, ensuring data privacy by keeping it local on user devices or at local servers. Instead of consolidating all data in a central server, each local node, such as a server in a smart building or an IoT device, trains its model using its own locally available data. **Only the model parameters**, rather than the raw data, are transmitted to a central server or aggregation node to create a global model. This decentralized training method minimizes the exposure of sensitive data while maintaining high levels of model accuracy and performance.

The aggregation of these local models is managed by a central aggregation server or a blockchain network node, which securely combines the parameters from various local models into an updated global model. This process employs **encryption techniques** and **differential privacy algorithms** to ensure that sensitive information cannot be inferred from the shared parameters. By maintaining a decentralized architecture, the platform enhances its scalability and significantly reduces the risk of sensitive data exposure, while still enabling effective and **privacy-preserving model** training across a wide range of urban applications.

### 3.4 Blockchain Implementation

The implementation of blockchain technology is a critical component of the platform, providing a **secure** and **transparent infrastructure** for network governance, model validation, and data integrity. The blockchain network is architected with **multiple distributed nodes** that participate in consensus processes and manage smart contracts.

To maintain the integrity and reliability of the platform, the blockchain network employs **consensus mechanisms** such as proof-of-stake (PoS) or proof-of-authority (PoA). These mechanisms facilitate agreement among nodes on the state of the blockchain and validate updates to the global model. Voting among nodes is employed to determine which local models are integrated into the global model, using criteria such as performance, data quality, and node reliability. This consensus-driven approach ensures that only the most accurate and reliable models contribute to the **collective intelligence**.

Moreover, blockchain technology safeguards against data manipulation and attacks through its **immutable** and **transparent ledger**. Each time a local model is proposed for integration into the global model, it is recorded on the blockchain, allowing all nodes to verify its validity. Smart contracts automate the governance of this process, including managing rewards for nodes that contribute high-quality models and imposing penalties on those that attempt to manipulate the process with false or erroneous data. This framework not only **enhances security** and **trust** within the network but also ensures a fair and robust environment for continuous learning and adaptation in smart city contexts.

## 4 Privacy and Security: Federated Learning and Blockchain Synergy

### 4.1 Enhanced Privacy Through Differential Privacy

Differential privacy is a foundational methodology for **ensuring the protection of individual-level data** during the training of machine learning models. It enables the extraction of meaningful insights and the construction of robust predictive models while preserving the confidentiality of personal information. This is accomplished through the injection of mathematically controlled noise into the model outputs, which carefully perturbs the results in a manner that **prevents the identification of any specific individual's data** from the aggregate model outputs.

Within the proposed platform for smart city applications, differential privacy acts as a **critical enabler for secure and ethical data usage**, particularly when integrated with FL and Blockchain technologies. Smart cities rely on continuous data collection from various sources and these datasets are inherently heterogeneous, comprising different types of data such as real-time traffic information, environmental parameters, and personal data related to health and behavior. Due to the **sensitive nature** of this information, which often contains granular details about individual behaviors, locations, and preferences, it is essential to implement stringent privacy protections to **maintain public trust and ensure compliance with regulatory standards**.

Moreover, the **combination of differential privacy with Blockchain technology** provides a further layer of protection. Blockchain's secure and transparent management of data flows and model updates ensures that, even if a model update is intercepted, the encrypted and obfuscated nature of the differentially private data makes it nearly impossible to extract meaningful information. This integration creates a robust **privacy-preserving mechanism** that is critical for applications in smart cities, where diverse data from multiple domains are constantly analyzed.

### 4.2 Robust Defense Against Identity-based Attacks

The proposed architecture effectively counters Sybil attacks, a type of security breach where an attacker creates **multiple fake identities to gain disproportionate influence** over a network, by leveraging a combination of blockchain's consensus mechanisms and federated learning's decentralized structure. The integrated approach of this platform addresses these vulnerabilities by using a two-layered defense strategy combining these technologies.

Firstly, blockchain technology introduces robust defense mechanisms through its **consensus rules** and **reputation systems**. Blockchain operates as a decentralized ledger where all transactions and data updates are verified by a network of nodes. To validate model updates or contributions, blockchain employs consensus algorithms, which require nodes to demonstrate their trustworthiness and authority. Only nodes with a proven track record, verified by their historical contributions and the integrity of their actions, are allowed to participate in the model training and aggregation processes. This mechanism effectively **prevents nodes with malicious intent or fake identities** from gaining influence, as any attempt to manipulate the system would require a majority consensus, which is extremely difficult to achieve due to the decentralized nature of blockchain networks.

Secondly, the decentralized nature of FL adds an additional layer of defense. In an FL framework, model training occurs locally on individual nodes—such as servers or devices—using their local data, and only the model updates (rather than the raw data) are shared with the central aggregation point or blockchain node. This structure significantly **limits the potential impact of any single malicious node** because no single node has complete control over the data or the model. The decentralized training approach ensures that even if a Sybil attack is attempted, the malicious nodes cannot significantly skew the overall model's performance or accuracy, as they are just one part of a broader, distributed network of nodes.

### 4.3 Protection Against Data Poisoning

The platform leverages a blockchain-based voting process to **validate local models** generated by each node, ensuring the integrity and quality of the global model. When a node trains a local model using its data, it proposes this model for inclusion in the global model, and the proposal is recorded on the blockchain. This allows other nodes in the network to review and vote on its acceptance. Each node's voting power is proportional to its reputation or stake in the network, depending on the chosen consensus mechanism. Nodes evaluate local models based on several criteria, such as model accuracy, data quality, and consistency with other proposed models. Only those models that receive a majority of positive votes are accepted and integrated into the global model.

To ensure that **only trustworthy nodes participate** in the model validation process, the platform employs a rigorous selection process based on a reputation system. Nodes are continuously evaluated according to their past behavior, the quality of their contributions, and their adherence to network rules. Nodes that demonstrate consistent, reliable behavior gain more weight in the voting process, while those associated with suspicious or low-quality activities are penalized or excluded. The criteria for model acceptance include **minimum thresholds for accuracy** and performance, ensuring that the proposed models are robust and effective. **Data consistency** is another key factor; the data used to train the models must be of high quality, free from significant biases, and representative of real urban conditions. Moreover, all models must comply with **privacy standards**, including differential privacy requirements and the network's data management policies.

## 5 Governance and Regulation with Smart Contracts

### 5.1 Functioning of Smart Contracts

Smart contracts play a pivotal role in automating governance and regulation within the platform by serving as self-executing programs stored on the blockchain. These contracts act as **automatic regulators** of the network, enforcing participation rules, governance protocols, and operational procedures without the need for human intervention. This automation **eliminates the requirement for centralized intermediaries**, reducing the risk of manipulation and ensuring fairness and transparency in all network interactions. Whenever a predefined condition is met, the smart contract triggers automatically to execute the corresponding actions, such as transferring rewards, imposing penalties, or updating the parameters of the global model.

By using smart contracts, the platform establishes a comprehensive framework for **regulating node behavior and maintaining network integrity**. These contracts define the criteria under which nodes

are either rewarded or penalized based on their contributions. Rewards, often in the form of digital tokens, are allocated to nodes that comply with the established standards, such as providing accurate and consistent model updates. These tokens can be used for network services or exchanged for other benefits, fostering positive participation. Smart contracts further enhance the platform's efficiency by automating governance tasks, such as enforcing regular data and model updates from nodes and regulating their participation in key processes like voting. By dynamically adjusting rules based on evolving urban data patterns or city needs, the platform remains adaptable and responsive, ensuring **reliable and secure management of urban data** and decision-making processes in smart cities.

### 5.2 Incentive and Penalty Mechanisms

The platform establishes a **comprehensive system of incentives to encourage positive participation** from network nodes, ensuring their active and constructive contribution to the network's development and maintenance. Nodes that submit **high-quality local models**, which meet the established criteria for accuracy, consistency, and relevance, receive rewards in the form of tokens or credits. This incentivization promotes continuous improvement in data quality and model accuracy. In addition, the platform also incentivizes nodes for **regular participation in governance processes**, such as model validation and voting. Nodes that actively and reliably engage in these activities are granted additional rewards, ensuring sustained commitment to network governance and fostering diverse participation. Furthermore, the platform recognizes nodes that **promote transparency and collaboration**, such as those sharing useful anonymized data or providing technical assistance.

To maintain network integrity, the platform implements automatic **penalties to deter malicious or negligent behavior**. Nodes that attempt to deceive the system by submitting **false, incomplete, or manipulated data** are penalized proportionally to the severity of the misconduct. Penalties can range from the loss of tokens and reduced reputation to temporary or permanent exclusion from the network. In cases of severe malicious activity, such as Sybil **attacks or attempts to manipulate the voting process**, the platform imposes stricter sanctions. Moreover, the platform penalizes nodes that **fail to actively participate in key network governance processes**, such as training local models or voting on model validation. This ensures that all nodes maintain a minimum level of activity and commitment to the network, supporting its continuous operation and development. Together, these governance mechanisms, facilitated by smart contracts, create a balanced framework that promotes fair and efficient platform operation. The incentive structures encourage appropriate behavior while the penalties deter non-compliance, fostering **trust and transparency across the network**.

## 6 Use Case: Federated Token Economy

The core innovation of this proposal lies in the **strategic combination of advanced technologies** to unlock vast potential within the framework of a smart city. This **synergy** aims to demonstrate the transformative possibilities that arise when these technologies are integrated to manage complex urban scenarios. While the proposal's primary focus is on the technological framework, a specific use case is presented to exemplify its practical application, showcasing how these technologies can operate cohesively in a realistic setting.

The proposed use case focuses on a **comprehensive system for managing inventory and forecasting sales**, specifically tailored to assist local businesses in a smart city environment in optimizing operational efficiency and increasing profitability. This system offers a wide range of functionalities, including real-time inventory tracking, reordering alerts and demand and price forecasting.

By leveraging Blockchain and Federated Learning, this use case demonstrates how a **secure and decentralized** communication network can be established between citizens, customers, and local businesses. The proposed architecture uses federated learning, connected to a private blockchain network segmented into two distinct channels, each serving specific roles.

The first channel focuses on **training models for demand prediction and price estimation**, utilizing local models developed from customer data collected by individual businesses. This approach enables

precise and tailored forecasts, enhancing decision-making for local merchants. The integration of federated learning preserves data privacy by keeping the data used for training on local devices or edge servers, without centralizing sensitive information.

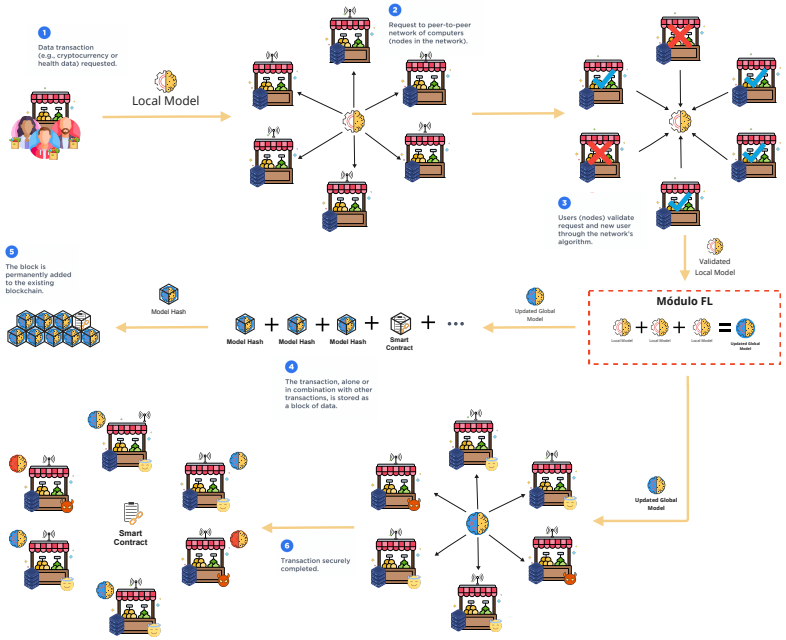


Figure 2: Workflow for Training and Updating the Global Model: Integration of Decentralized Learning and Blockchain.

The global model is updated through a series of stages. Initially, each business gathers customer demand data and trains its predictive model locally. After training, these models are shared across the network via peer-to-peer communication, allowing for cross-evaluation by other businesses. A voting process, regulated by a Smart Contract, determines which models are integrated into the global model. This governance mechanism ensures that only high-quality models are incorporated, maintaining the system's overall integrity and effectiveness. Additionally, Smart Contracts automate the distribution of rewards to businesses that contribute valuable models and impose reward and penalties.

The second blockchain channel is dedicated to **facilitating e-commerce transactions**, allowing for secure payments through tokens or digital currencies. This structure ensures that all transactions are secure and verifiable, building customer trust and enhancing their online shopping experience. The architecture also supports the creation of private channels between businesses and individual users, enabling personalized interactions, such as exclusive discounts that are not visible to other users.

Implementing blockchain within this use case offers multiple benefits, including the creation of an **NFT-based reward system**. These tokens can be used to reward customer loyalty or recognize a business's active participation in the network, thereby fostering stronger customer engagement and loyalty. The issuance and management of these NFTs are governed by Smart Contracts, ensuring transparency and minimizing the potential for misuse. **User authentication** is managed through Wallets or Unique Digital Identification (UID) keys, enabling users to enjoy the benefits of blockchain, fast and secure transactions and participation in network governance.

This case study demonstrates how the proposed technological architecture optimizes local business operations with accurate, personalized predictions while enhancing data security and mitigating privacy risks by avoiding centralized data, establishing a secure and efficient e-commerce infrastructure supported by Smart Contracts and fostering a **collaborative**, **transparent**, and **fair** environment.

## 7 References

## References


[1] Mahmud, R., Kotagiri, R., Buyya, R., Di Martino, B., Li, K., Yang, L., & Esposito, A. (2018) *Internet of Things (Technology, Communications and Computing)*, Springer, Vol. 103, pp. 1–12.

[2] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015) *Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications*, IEEE Communications Surveys & Tutorials, 17(4), pp. 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

[3] Li, T., Zhao, M., & Wong, K. K. L. (2020) *Machine learning based code dissemination by selection of reliability mobile vehicles in 5G networks*, Computer Communications, 152(2), pp. 109–118. https://doi.org/10.1016/j.comcom.2020.01.034

[4] Rath, M., & Pattanayak, B. (2019) *Technological improvement in modern health care applications using internet of things (IoT) and proposal of novel health care approach*, International Journal of Human Rights in Healthcare, 12(2), pp. 148–162. https://doi.org/10.1108/IJHRH-01-2018-0007

[5] Qiu, J., Du, L., Zhang, D., Su, S., & Tian, Z. (2019) *Nei-TTE: Intelligent traffic time estimation based on fine-grained time derivation of road segments for smart city*, IEEE Transactions on Industrial Informatics, 16(4), pp. 2659–2666. https://doi.org/10.1109/TII.9424

[6] Zhang, W., Han, J., Xu, Z., Ni, H., Liu, H., & Xiong, H. (2024). *Towards Urban General Intelligence: A Review and Outlook of Urban Foundation Models*. arXiv preprint arXiv:2402.01749.

[7] Hu, S., Chen, X., Ni, W., Hossain, E., & Wang, X. (2021) *Distributed Machine Learning for Wireless Communication Networks: Techniques, Architectures, and Applications*, IEEE Communications Surveys & Tutorials, 23(3), pp. 1458–1493. https://doi.org/10.1109/COMST.2021.3064646

[8] Guan, Z., Si, G., Zhang, X., Wu, L., Guizani, N., Du, X., & Ma, Y. (2018) *Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities*, IEEE Communications Magazine, 56(7), pp. 82–88. https://doi.org/10.1109/MCOM.2018.1700401

[9] Zhou, L., Wu, D., Chen, J., & Dong, Z. (2017) *Greening the smart cities: Energy-efficient massive content delivery via D2D communications*, IEEE Transactions on Industrial Informatics, 14(4), pp. 1626–1634. https://doi.org/10.1109/TII.9424

[10] Nguyen, D. C., Ding, M., Pathirana, P. N., & Seneviratne, A. (2021) *Federated Learning Meets Blockchain in Edge Computing: Opportunities and Challenges*, IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2021.3063261

[11] Jiang, J., Cao, J., Saxena, D., Jiang, S., & Ferradi, H. (2023). *Blockchain-empowered Federated Learning: Challenges, Solutions, and Future Directions*. Computers Surveys, 55(11), pp. 1-31. https://doi.org/10.1145/3574383

[12] Khan, L. U., Tran, N. H., Pandey, S. R., Saad, W., Han, Z., Nguyen, M. N., & Hong, C. S. (2019) *Federated learning for edge networks: Resource optimization and incentive mechanism*, Preprint, arXiv:1911.05642.

[13] Zhu, J., Cao, J., Saxena, D., Jiang, S., & Ferradi, H. (2023) *Blockchain-empowered Federated Learning: Challenges, Solutions, and Future Directions*, Computers Surveys, 55(11), pp. 1-31. https://doi.org/10.1145/3574383

[14] McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017) *Communication-efficient Learning of Deep Networks from Decentralized Data*, In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, AISTATS 2017, pp. 1273–1282. Fort Lauderdale, FL, USA.

[15] Ullah, A., Anwar, S.M., Li, J. et al. (2024). *Smart cities: the role of Internet of Things and machine learning in realizing a data-centric smart environment*. Complex Intell. Syst. 10, 1607–1637. https://doi.org/10.1007/s40747-023-01175-4

[16] Esfandi, S., Tayebi, S., Byrne, J., Taminiau, J., Giyahchi, G., & Alavi, S. (2024). *Smart Cities and Urban Energy Planning: An Advanced Review of Promises and Challenges*. Smart Cities, 7, pp. 414-444. https://doi.org/10.3390/smartcities7010016

[17] Bazargani, J. S., Sadeghi-Niaraki, A., & Choi, S. M. (2021). *A Survey of GIS and IoT Integration: Applications and Architecture*. Applied Sciences, 11(21), 10365. https://doi.org/10.3390/app112110365

[18] Jing, C., Du, M., Li, S., & Liu, S. (2019). *Geospatial Dashboards for Monitoring Smart City Performance*. Sustainability, 11(20), 5648. https://doi.org/10.3390/su11205648

[19] Khang, A., Gupta, S. K., Rani, S., & Karras, D. A. (Eds.). (2023). *Smart Cities: IoT Technologies, big data solutions, cloud platforms, and cybersecurity techniques*. CRC Press.

[20] Bellini, P., & Pantaleo, G. (2023). *Special Issue on the Internet of Things (IoT) in Smart Cities*. Applied Sciences, 13(7), 4392. https://doi.org/10.3390/app13074392

[21] Sharma, H., Haque, A., & Blaabjerg, F. (2021). *Machine Learning in Wireless Sensor Networks for Smart Cities: A Survey*. Electronics, 10(9), 1012. https://doi.org/10.3390/electronics10091012

[22] Wolniak, R., & Stecuła, K. (2024). *Artificial Intelligence in Smart Cities—Applications, Barriers, and Future Directions: A Review*. Smart Cities, 7(3), 1346-1389. https://doi.org/10.3390/smartcities7030057

[23] Syed, A. S., Sierra-Sosa, D., Kumar, A., & Elmaghraby, A. (2021). *IoT in Smart Cities: A Survey of Technologies, Practices and Challenges*. Smart Cities, 4(2), 429-475. https://doi.org/10.3390/smartcities4020024

[24] Khawaja, S., & Javidroozi, V. (2023). *Blockchain technology as an enabler for cross-sectoral systems integration for developing smart sustainable cities*. IET Smart Cities.

[25] Pandya, S., Srivastava, G., Jhaveri, R., Babu, M. R., Bhattacharya, S., Maddikunta, P. K. R., ... & Gadekallu, T. R. (2023). *Federated learning for smart cities: A comprehensive survey*. Sustainable Energy Technologies and Assessments, 55, 102987.

[26] Nepal, J. P., Yuangyai, N., Gyawali, S., & Yuangyai, C. (2022). *Blockchain-based smart renewable energy: Review of operational and transactional challenges*. Energies.

[27] Kvalvik, P., Sánchez-Gordón, M., & Colomo-Palacios, R. (2023). *Beyond technology in smart cities: A multivocal literature review on data governance*. Aslib Journal of Information Management.

[28] Hakak, S., Khan, W. Z., Gilkar, G. A., Imran, M., & Guizani, N. (2020). *Securing smart cities through blockchain technology: Architecture, requirements, and challenges*. IEEE Network.

[29] Parenti, C., Noori, N., & Janssen, M. (2022). *A smart governance diffusion model for blockchain as an anti-corruption tool*. Journal of Network and Computer Applications.

[30] Jafari, T., Watson, J., & Mellor, K. (2023). *Infrastructure elements of digital twins in smart cities: storage, computation, and network components*. Artificial Intelligence Review.

[31] Liu, T., Sabrina, F., Jang-Jaccard, J., Xu, W., & Wei, Y. (2022). *Artificial intelligence-enabled DDoS detection for blockchain-based smart transport systems*. Sensors.

[32] Hasan, M. K., Akhtaruzzaman, Md., Kabir, S. R., Gadekallu, T., Islam, S., Magalingam, P., Hassan, R., Alazab, M., & Alazab, M. (2022). *Evolution of Industry and Blockchain Era: Monitoring Price Hike and Corruption Using BIoT for Smart Government and Industry 4.0*. IEEE Transactions on Industrial Informatics, 18, 1-1. https://doi.org/10.1109/TII.2022.3164066.

[33] Loss, S., Singh, H. P., Cacho, N., & Lopes, F. (2022). *Using FIWARE and blockchain in smart cities solutions*. Cluster Computing.

[34] El-Agamy, R.F., Sayed, H.A., AL Akhatatneh, A.M. et al. (2024). *Comprehensive analysis of digital twins in smart cities: a 4200-paper bibliometric study*. Artif Intell Rev 57, 154. https://doi.org/10.1007/s10462-024-10781-8

[35] Weil, R. (2023). *Infrastructure elements of digital twins in smart cities: storage, computation, and network components*. Artificial Intelligence Review.

[36] Ullah, A., et al. (2024). *The Role of LLMs in Sustainable Smart Cities: Applications, Challenges, and Future Directions*. arXiv. https://doi.org/10.48550/arXiv.2402.14596.

[37] Luo, et al. (2024). *Federated TrustChain: Blockchain-Enhanced LLM Training and Unlearning*. arXiv. https://doi.org/10.48550/arXiv.2406.04076.

[38] Yang, Q., et al. (2019). *Federated machine learning: Concept and applications*. ACM Transactions on Intelligent Systems and Technology (TIST), 10(2), 1–19.

[39] Wang, Z., & Hu, Q. (2021). *Blockchain-based federated learning: A comprehensive survey*. arXiv. https://doi.org/10.48550/arXiv.2110.02182.

[40] Esposito, C., et al. (2021). *Blockchain-based authentication and authorization for smart city applications*. Information Processing and Management, 58(2), 102468. https://doi.org/10.1016/j.ipm.2021.102468.

[41] Nguyen, T. M., et al. (2021). *Blockchain for Smart City: A Review and Directions*. IEEE Internet of Things Journal.

## NeurIPS Paper Checklist

1. **Claims**

   Question: Do the main claims made in the abstract and introduction accurately reflect the paper's contributions and scope?

   Answer: [Yes]

   **Justification**: The abstract and introduction clearly state the paper's contributions, including the integration of advanced technologies like Foundation Models, Federated Learning, and Blockchain, and accurately reflect the scope of the work as presented throughout the paper.

   Guidelines:

   - The answer NA means that the abstract and introduction do not include the claims made in the paper.
   - The abstract and/or introduction should clearly state the claims made, including the contributions made in the paper and important assumptions and limitations. A No or NA answer to this question will not be perceived well by the reviewers.
   - The claims made should match theoretical and experimental results, and reflect how much the results can be expected to generalize to other settings.
   - It is fine to include aspirational goals as motivation as long as it is clear that these goals are not attained by the paper.

2. **Limitations**

   Question: Does the paper discuss the limitations of the work performed by the authors?

   Answer: [No]

   **Justification**: The paper does not include a specific section discussing the limitations of the proposed approach, nor does it explicitly address assumptions or potential drawbacks within the current content.

   Guidelines:

   - The answer NA means that the paper has no limitation while the answer No means that the paper has limitations, but those are not discussed in the paper.
   - The authors are encouraged to create a separate "Limitations" section in their paper.
   - The paper should point out any strong assumptions and how robust the results are to violations of these assumptions (e.g., independence assumptions, noiseless settings, model well-specification, asymptotic approximations only holding locally). The authors should reflect on how these assumptions might be violated in practice and what the implications would be.
   - The authors should reflect on the scope of the claims made, e.g., if the approach was only tested on a few datasets or with a few runs. In general, empirical results often depend on implicit assumptions, which should be articulated.
   - The authors should reflect on the factors that influence the performance of the approach. For example, a facial recognition algorithm may perform poorly when image resolution is low or images are taken in low lighting. Or a speech-to-text system might not be used reliably to provide closed captions for online lectures because it fails to handle technical jargon.
   - The authors should discuss the computational efficiency of the proposed algorithms and how they scale with dataset size.
   - If applicable, the authors should discuss possible limitations of their approach to address problems of privacy and fairness.
   - While the authors might fear that complete honesty about limitations might be used by reviewers as grounds for rejection, a worse outcome might be that reviewers discover limitations that aren't acknowledged in the paper. The authors should use their best

judgment and recognize that individual actions in favor of transparency play an important role in developing norms that preserve the integrity of the community. Reviewers will be specifically instructed to not penalize honesty concerning limitations.

3. **Theory Assumptions and Proofs**

   Question: For each theoretical result, does the paper provide the full set of assumptions and a complete (and correct) proof?

   Answer: [NA]

   **Justification**: The paper does not include any theoretical results that require formal assumptions.

   Guidelines:

   - The answer NA means that the paper does not include theoretical results.
   - All the theorems, formulas, and proofs in the paper should be numbered and cross-referenced.
   - All assumptions should be clearly stated or referenced in the statement of any theorems.
   - The proofs can either appear in the main paper or the supplemental material, but if they appear in the supplemental material, the authors are encouraged to provide a short proof sketch to provide intuition.
   - Inversely, any informal proof provided in the core of the paper should be complemented by formal proofs provided in appendix or supplemental material.
   - Theorems and Lemmas that the proof relies upon should be properly referenced.

4. **Experimental Result Reproducibility**

   Question: Does the paper fully disclose all the information needed to reproduce the main experimental results of the paper to the extent that it affects the main claims and/or conclusions of the paper (regardless of whether the code and data are provided or not)?

   Answer: [Yes]

   **Justification**: The contribution is primarily a new model architecture, and the paper describes the architecture clearly and fully, including all necessary components such model layers, and the overall workflow, to ensure reproducibility.

   Guidelines:

   - The answer NA means that the paper does not include experiments.
   - If the paper includes experiments, a No answer to this question will not be perceived well by the reviewers: Making the paper reproducible is important, regardless of whether the code and data are provided or not.
   - If the contribution is a dataset and/or model, the authors should describe the steps taken to make their results reproducible or verifiable.
   - Depending on the contribution, reproducibility can be accomplished in various ways. For example, if the contribution is a novel architecture, describing the architecture fully might suffice, or if the contribution is a specific model and empirical evaluation, it may be necessary to either make it possible for others to replicate the model with the same dataset, or provide access to the model. In general. releasing code and data is often one good way to accomplish this, but reproducibility can also be provided via detailed instructions for how to replicate the results, access to a hosted model (e.g., in the case of a large language model), releasing of a model checkpoint, or other means that are appropriate to the research performed.
   - While NeurIPS does not require releasing code, the conference does require all submissions to provide some reasonable avenue for reproducibility, which may depend on the nature of the contribution. For example
     (a) If the contribution is primarily a new algorithm, the paper should make it clear how to reproduce that algorithm.

(b) If the contribution is primarily a new model architecture, the paper should describe the architecture clearly and fully.

(c) If the contribution is a new model (e.g., a large language model), then there should either be a way to access this model for reproducing the results or a way to reproduce the model (e.g., with an open-source dataset or instructions for how to construct the dataset).

(d) We recognize that reproducibility may be tricky in some cases, in which case authors are welcome to describe the particular way they provide for reproducibility. In the case of closed-source models, it may be that access to the model is limited in some way (e.g., to registered users), but it should be possible for other researchers to have some path to reproducing or verifying the results.

5. **Open access to data and code**

   Question: Does the paper provide open access to the data and code, with sufficient instructions to faithfully reproduce the main experimental results, as described in supplemental material?

   Answer: [No]

   **Justification**: The paper does not provide open access to the data and code required to reproduce the experimental results due to confidentiality agreements and proprietary data restrictions. However, the paper provides detailed descriptions of the methodologies and sufficient information about the experimental setup to facilitate reproduction by other researchers.

   Guidelines:

   - The answer NA means that paper does not include experiments requiring code.
   - Please see the NeurIPS code and data submission guidelines (`https://nips.cc/public/guides/CodeSubmissionPolicy`) for more details.
   - While we encourage the release of code and data, we understand that this might not be possible, so "No" is an acceptable answer. Papers cannot be rejected simply for not including code, unless this is central to the contribution (e.g., for a new open-source benchmark).
   - The instructions should contain the exact command and environment needed to run to reproduce the results. See the NeurIPS code and data submission guidelines (`https://nips.cc/public/guides/CodeSubmissionPolicy`) for more details.
   - The authors should provide instructions on data access and preparation, including how to access the raw data, preprocessed data, intermediate data, and generated data, etc.
   - The authors should provide scripts to reproduce all experimental results for the new proposed method and baselines. If only a subset of experiments are reproducible, they should state which ones are omitted from the script and why.
   - At submission time, to preserve anonymity, the authors should release anonymized versions (if applicable).
   - Providing as much information as possible in supplemental material (appended to the paper) is recommended, but including URLs to data and code is permitted.

6. **Experimental Setting/Details**

   Question: Does the paper specify all the training and test details (e.g., data splits, hyperparameters, how they were chosen, type of optimizer, etc.) necessary to understand the results?

   Answer: [NA]

   **Justification**: The paper does not include experiments that require specification of training or test details, such as data splits, hyperparameters, or optimizer types, as it primarily focuses on proposing a new architectural framework rather than conducting model training or evaluation experiments.

Guidelines:

- The answer NA means that the paper does not include experiments.
- The experimental setting should be presented in the core of the paper to a level of detail that is necessary to appreciate the results and make sense of them.
- The full details can be provided either with the code, in appendix, or as supplemental material.

7. **Experiment Statistical Significance**

   Question: Does the paper report error bars suitably and correctly defined or other appropriate information about the statistical significance of the experiments?

   Answer: [NA]

   **Justification**: The paper does not include experiments; hence, there are no reported error bars, confidence intervals, or statistical significance tests related to experimental results

   Guidelines:

   - The answer NA means that the paper does not include experiments.
   - The authors should answer "Yes" if the results are accompanied by error bars, confidence intervals, or statistical significance tests, at least for the experiments that support the main claims of the paper.
   - The factors of variability that the error bars are capturing should be clearly stated (for example, train/test split, initialization, random drawing of some parameter, or overall run with given experimental conditions).
   - The method for calculating the error bars should be explained (closed form formula, call to a library function, bootstrap, etc.)
   - The assumptions made should be given (e.g., Normally distributed errors).
   - It should be clear whether the error bar is the standard deviation or the standard error of the mean.
   - It is OK to report 1-sigma error bars, but one should state it. The authors should preferably report a 2-sigma error bar than state that they have a 96% CI, if the hypothesis of Normality of errors is not verified.
   - For asymmetric distributions, the authors should be careful not to show in tables or figures symmetric error bars that would yield results that are out of range (e.g. negative error rates).
   - If error bars are reported in tables or plots, The authors should explain in the text how they were calculated and reference the corresponding figures or tables in the text.

8. **Experiments Compute Resources**

   Question: For each experiment, does the paper provide sufficient information on the computer resources (type of compute workers, memory, time of execution) needed to reproduce the experiments?

   Answer: [NA]

   **Justification**: The paper does not include experiments; therefore, no information about compute resources, such as type of compute workers, memory, or execution time, is necessary.

   Guidelines:

   - The answer NA means that the paper does not include experiments.
   - The paper should indicate the type of compute workers CPU or GPU, internal cluster, or cloud provider, including relevant memory and storage.
   - The paper should provide the amount of compute required for each of the individual experimental runs as well as estimate the total compute.
   - The paper should disclose whether the full research project required more compute than the experiments reported in the paper (e.g., preliminary or failed experiments that didn't make it into the paper).

9. **Code Of Ethics**

   Question: Does the research conducted in the paper conform, in every respect, with the NeurIPS Code of Ethics `https://neurips.cc/public/EthicsGuidelines`?

   Answer: [Yes]

   **Justification**: The research aligns with the NeurIPS Code of Ethics, adhering to all guidelines related to transparency, privacy, data integrity, fairness, and social responsibility.

   Guidelines:

   - The answer NA means that the authors have not reviewed the NeurIPS Code of Ethics.
   - If the authors answer No, they should explain the special circumstances that require a deviation from the Code of Ethics.
   - The authors should make sure to preserve anonymity (e.g., if there is a special consideration due to laws or regulations in their jurisdiction).

10. **Broader Impacts**

    Question: Does the paper discuss both potential positive societal impacts and negative societal impacts of the work performed?

    Answer: [Yes]

    **Justification**: The paper does not dedicate a specific section to discussing broader societal impacts; however, it evaluates these impacts throughout the proposal. The primary aim of the paper is to create a positive impact on smart cities and enhance the lives of their citizens by addressing data privacy, security, and scalability challenges in urban environments.

    Guidelines:

    - The answer NA means that there is no societal impact of the work performed.
    - If the authors answer NA or No, they should explain why their work has no societal impact or why the paper does not address societal impact.
    - Examples of negative societal impacts include potential malicious or unintended uses (e.g., disinformation, generating fake profiles, surveillance), fairness considerations (e.g., deployment of technologies that could make decisions that unfairly impact specific groups), privacy considerations, and security considerations.
    - The conference expects that many papers will be foundational research and not tied to particular applications, let alone deployments. However, if there is a direct path to any negative applications, the authors should point it out. For example, it is legitimate to point out that an improvement in the quality of generative models could be used to generate deepfakes for disinformation. On the other hand, it is not needed to point out that a generic algorithm for optimizing neural networks could enable people to train models that generate Deepfakes faster.
    - The authors should consider possible harms that could arise when the technology is being used as intended and functioning correctly, harms that could arise when the technology is being used as intended but gives incorrect results, and harms following from (intentional or unintentional) misuse of the technology.
    - If there are negative societal impacts, the authors could also discuss possible mitigation strategies (e.g., gated release of models, providing defenses in addition to attacks, mechanisms for monitoring misuse, mechanisms to monitor how a system learns from feedback over time, improving the efficiency and accessibility of ML).

11. **Safeguards**

    Question: Does the paper describe safeguards that have been put in place for responsible release of data or models that have a high risk for misuse (e.g., pretrained language models, image generators, or scraped datasets)?

    Answer: [NA]

**Justification**: The paper does not involve the release of data or models with a high risk of misuse, such as pretrained language models, image generators, or scraped datasets. The proposed framework focuses on integrating existing technologies in smart city contexts and does not necessitate safeguards for data or models that could be misused.

Guidelines:

- The answer NA means that the paper poses no such risks.
- Released models that have a high risk for misuse or dual-use should be released with necessary safeguards to allow for controlled use of the model, for example by requiring that users adhere to usage guidelines or restrictions to access the model or implementing safety filters.
- Datasets that have been scraped from the Internet could pose safety risks. The authors should describe how they avoided releasing unsafe images.
- We recognize that providing effective safeguards is challenging, and many papers do not require this, but we encourage authors to take this into account and make a best faith effort.

12. **Licenses for existing assets**

Question: Are the creators or original owners of assets (e.g., code, data, models), used in the paper, properly credited and are the license and terms of use explicitly mentioned and properly respected?

Answer: [NA]

**Justification**: The paper does not use any existing assets such as code, data, or models created by other parties that require specific licensing or terms of use. The proposed framework is an original contribution, and all references to existing technologies or concepts are properly cited in accordance with academic standards.

Guidelines:

- The answer NA means that the paper does not use existing assets.
- The authors should cite the original paper that produced the code package or dataset.
- The authors should state which version of the asset is used and, if possible, include a URL.
- The name of the license (e.g., CC-BY 4.0) should be included for each asset.
- For scraped data from a particular source (e.g., website), the copyright and terms of service of that source should be provided.
- If assets are released, the license, copyright information, and terms of use in the package should be provided. For popular datasets, `paperswithcode.com/datasets` has curated licenses for some datasets. Their licensing guide can help determine the license of a dataset.
- For existing datasets that are re-packaged, both the original license and the license of the derived asset (if it has changed) should be provided.
- If this information is not available online, the authors are encouraged to reach out to the asset's creators.

13. **New Assets**

Question: Are new assets introduced in the paper well documented and is the documentation provided alongside the assets?

Answer: [NA]

**Justification**: The paper does not introduce any new assets such as datasets, code, or models. The focus is on presenting a conceptual framework and architecture for smart city technologies, and no new digital assets are released as part of this work.

Guidelines:

- The answer NA means that the paper does not release new assets.
- Researchers should communicate the details of the dataset/code/model as part of their submissions via structured templates. This includes details about training, license, limitations, etc.
- The paper should discuss whether and how consent was obtained from people whose asset is used.
- At submission time, remember to anonymize your assets (if applicable). You can either create an anonymized URL or include an anonymized zip file.

14. **Crowdsourcing and Research with Human Subjects**

    Question: For crowdsourcing experiments and research with human subjects, does the paper include the full text of instructions given to participants and screenshots, if applicable, as well as details about compensation (if any)?

    Answer: [NA]

    **Justification**: The paper does not involve any crowdsourcing experiments or research involving human subjects. It focuses solely on the technical aspects of a proposed framework for smart city technologies, without the need for human participants or related experiments.

    Guidelines:

    - The answer NA means that the paper does not involve crowdsourcing nor research with human subjects.
    - Including this information in the supplemental material is fine, but if the main contribution of the paper involves human subjects, then as much detail as possible should be included in the main paper.
    - According to the NeurIPS Code of Ethics, workers involved in data collection, curation, or other labor should be paid at least the minimum wage in the country of the data collector.

15. **Institutional Review Board (IRB) Approvals or Equivalent for Research with Human Subjects**

    Question: Does the paper describe potential risks incurred by study participants, whether such risks were disclosed to the subjects, and whether Institutional Review Board (IRB) approvals (or an equivalent approval/review based on the requirements of your country or institution) were obtained?

    Answer: [NA]

    **Justification**: The paper does not involve any research with human subjects, and therefore, there is no need for Institutional Review Board (IRB) approvals or equivalent ethical reviews. The research is focused on a technological framework and does not involve human participants or related risks.

    Guidelines:

    - The answer NA means that the paper does not involve crowdsourcing nor research with human subjects.
    - Depending on the country in which research is conducted, IRB approval (or equivalent) may be required for any human subjects research. If you obtained IRB approval, you should clearly state this in the paper.
    - We recognize that the procedures for this may vary significantly between institutions and locations, and we expect authors to adhere to the NeurIPS Code of Ethics and the guidelines for their institution.
    - For initial submissions, do not include any information that would break anonymity (if applicable), such as the institution conducting the review.