City Research Online

City St George's, University of London

Citation: Biswas, S., Yao, Z., Yan, L., Alqhatani, A., Bairagi, A. K., Asiri, F. & Masud, M. (2023). Interoperability Benefits and Challenges in Smart City Services: Blockchain as a Solution. Electronics, 12(4), 1036. doi: 10.3390/electronics12041036

This is the published version of the paper.

This version of the publication may differ from the final published version. To cite this item please consult the publisher's version.

Permanent repository link: https://openaccess.city.ac.uk/id/eprint/32139/

Link to published version: https://doi.org/10.3390/electronics12041036

Copyright and Reuse: Copyright and Moral Rights remain with the author(s) and/or copyright holders. Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge, unless otherwise indicated, provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way. For full details of reuse please refer to City Research Online policy.

City Research Online: http://openaccess.city.ac.uk/ publications@citystgeorges.ac.uk

electronics

MDPI

Article

Interoperability Benefits and Challenges in Smart City Services: Blockchain as a Solution

Sujit Biswas [1,*], Zigang Yao [2,*], Lin Yan [3], Abdulmajeed Alqhatani [4], Anupam Kumar Bairagi [5], Fatima Asiri [6] and Mehedi Masud [7]

[1] School of Architecture, Computing and Engineering, University of East London, London E16 2RD, UK
[2] School of Art Design and Media, East China University of Science and Technology, Shanghai 200237, China
[3] Technical College of ZTE Corporation, Shenzhen 518057, China
[4] Department of Information Systems, College of Computer Science and Information Systems, Najran University, Najran 61441, Saudi Arabia
[5] Computer Science and Engineering Discipline, Khulna University, Khulna 9208, Bangladesh
[6] Information Systems Department, College of Computer Science, King Khaled University, Abha 61421, Saudi Arabia
[7] Department of Computer Science, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia
* Correspondence: s.biswas3@uel.ac.uk (S.B.); zigangyao.cn@outlook.com (Z.Y.)

Abstract: The widespread usage of smart devices with various city-centric services speeds up and improves civic life, in contrast to growing privacy and security concerns. Security issues are exacerbated when e-government service providers trade their services within a centralised framework. Due to security concerns, city-centric centralised services are being converted to blockchain-based systems, which is a very time-consuming and challenging process. The interoperability of these blockchain-based systems is also more challenging due to protocol variances, an excessive amount of local transactions that raise scalability and rapidly occupy memory. In this paper, we have proposed a framework for interoperability across various blockchain-based smart city services. It also summarises how independent service providers might continue self-service choices (i.e., local transactions) without overloading the blockchain network and other organisations. A simulated interoperability network is used to show the network's effectiveness. The experimental outcomes show the scalability and memory optimization of the blockchain network.

Keywords: blockchain; IoT; security and privacy; smart home; distributed ledger technology

check for updates

Citation: Biswas, S.; Yao, Z.; Yan, L.; Alqhatani, A.; Bairagi, A.K.; Asiri, F.; Masud, M. Interoperability Benefits and Challenges in Smart City Services: Blockchain as a Solution. *Electronics* **2023**, *12*, 1036. https://doi.org/10.3390/electronics12041036

Academic Editors: Van Dung Nguyen, Marek Pagáč, Chuan Pham, Huynh Kha Tu, Huu Khoa Tran and Tran Anh Khoa

Received: 4 January 2023
Revised: 8 February 2023
Accepted: 13 February 2023
Published: 19 February 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

With the help of modern technology, consumer electronics, or the Internet of Things (IoT), are evolving into a crucial aspect of daily life. The consumer lifestyle, from home electronics to the workplace (i.e., industry), incorporates IoT in some way that outpaces daily market demand data. The number of IoT devices that are connected globally from 2019 to 2021 is shown as a bar graph in Figure 1, with projections for 2030 provided by [1]. Additionally, it shows the usage and prediction for consumer IoT (CIoT), which largely carries end-user data, from 2019 to 2025. It is predicted that there will be more than 29 billion IoT devices used worldwide by 2030, up from 9.7 billion in 2020. Most of these devices will be used in a city-centric civic society. Furthermore, these ubiquitous city-centric IoT-based services rely on one another in order to provide seamless and quick services that eventually claim interoperability of services [2].

The CIoT used by citizens frequently handles confidential data and is managed independently on a service-specific central server. This is similar to how the majority of industries innovate by incorporating the IoT without making significant changes to their centralised server. However, with these organisations' interoperability, it is possible to leverage the benefits of digitization and rapid communication. For example, modern

industries comprise smart production systems and global value chain networks (supply chain, services, marketing, etc.); such information is crucial for the tax department, bank, insurance, etc. Similarly, e-health inter-system collaboration is vital for patients' data atomicity, insurance claims, and record sharing. Technology that is data-driven, secure, and plan-oriented is crucial for a sustainable environment [3]. For these city-centeric services to work together, it is important to make sure they are safe and fast on any inter-organisational service platform [4,5]. Although an interoperable system can provide enormous benefits, implementing such a large system using existing centralised servers is extremely difficult for access control, dealing with single point of failure and vulnerability issues, data security, and so on [6]. The aforementioned challenging task can be solved using any decentralised service platform, such as Blockchain.

Blockchain (BC), at its core, is a cryptographically secured Distributed Ledger Technology (DLT) that allows for secure data transfer between parties [7]. It provides value exchange (i.e., transactions) without trust authority from a central entity [8]. These transactions are stored in the ledger maintained by a group of connected computers (i.e., peers) distributively, unlike a centralised entity such as a bank database. The BC system performs independent verification (i.e., endorsement) before approving the transaction, which is crucial in ensuring security. Moreover, it allows smart-contract-based inter-organisational transactions as a consortium, which is important for unified intelligent city services. Blockchain as a service platform can enable organisations' existing servers (i.e., centralised servers) to migrate and adapt to a decentralised DLT-based system. These security features and openness inspire the use of this technology in smart cities.

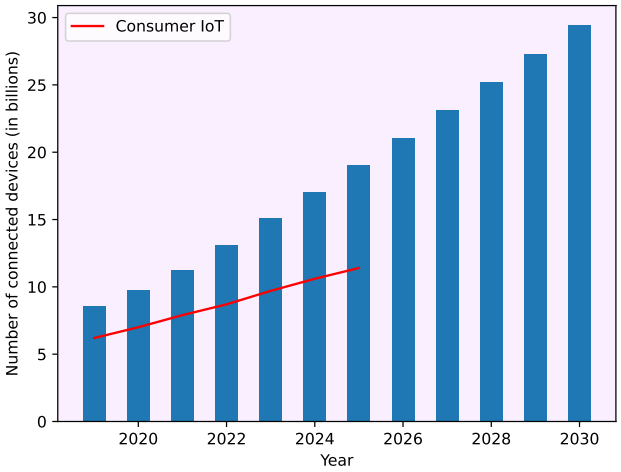

Figure 1. IoT demand statistics.

Recent articles (e.g., [9,10]) have suggested blockchain as an interoperability solution, but migrating typical services to a blockchain-based system is challenging due to differences in the data structure (details in Section 2). Moreover, every local transaction (inter-organisational transactions) is transferred and recorded through the blockchain network. In that case, it will create a massive burden of transactions and require considerable transactions per second (TPS). For a better understanding of the burden and volume of transactions in a smart city, assume there are 50 agencies, each of which has at least 10 peers, each of whom is in charge of 1000 devices or users. As a result, if each user or device makes 10 transactions daily, then there will be 105 transactions from only one agency and a total of 5 million transactions from all agencies. According to our experimental research, a single block with a single transaction would also weigh at least 4.6 kB [11]. If the BC constructs a single block for every 500 transactions, it would use 23 GB of memory each day, or 8.4 TB annually. This issue gets worse with time because ledger data cannot be removed or changed. The difficulty of effective ledger size management and TPS scalability must be resolved in order to profit from the security advantages of BC in the IoT. Due to these

factors, there are two significant challenges with current BC-based smart city solutions, such as ledger storage requirements and transaction per second (TPS) requirements.

This article proposes a blockchain-based interoperable framework for unified smart city services. It enables an organisation to exchange messages (i.e., transactions) locally without overburdening the BC network's interoperability. Additionally, the platform-independent BC platform solely handles intra-organisational transactions, ensuring secure and quick automation, e-governance, lowering intermediary expenses, etc. Moreover, the overall segregation of transactions makes the BC network scalable and optimises the interoperable ledgers. The article also summarises the open research questions and the technical challenges that might be raised in the production environment.

This article contributes

- A novel blockchain-based framework for connecting every independent service provider in smart cities.
- A solution for scalability and over-burden challenges that arise for local transactions of every organisation.
- An encouraging and tested method of preventing memory from filling up quickly in an interoperable BC network.
- A novel method of scaling the TPS in a large, interoperable BC network.

2. Background and Related Works

The idea of a smart city has drawn considerable interest from the research community across a wide range of disciplines, particularly in computer science and information systems [12]. Information sharing between smart city services, such as currency swaps between banks, health information sharing, electric vehicle charging and parking services, tourism applications, and weather information services, is the key to fully electronic governance. A rising number of smart city initiatives have emerged globally in recent years to use this connection and improve the quality of life for citizens. The influence of smart city efforts on the goals outlined in the European Growth Strategy 2020 was examined and published as a report by the European Parliament in 2014 [13]. Moreover, the analysis covered more than 50 smart city projects that were carried out in 37 towns. Most of these services use typical centralised architecture for exchanging information. Although many recent contributions have suggested blockchain interoperability, blockchain-based service interoperability is still in a very early stage [14–17]. The most relevant contributions have been summarised in Table 1.

Table 1. Related contributions summary.

Paper	Contribution	Scalability	Ledger Optimisation
[15]	SQL (typical) and NoSQL (BC-based) system's interoperability	✓	X
[14]	Cross-chain interoperability	X	X
[16]	Scalability solutions	X	X
[18]	Interoperability among protocols	X	X
[17]	Security of medical data exchanges	X	X
[19,20]	Interledger data exchange	X	X
[9]	Interoperability among protocols	X	X

Vitalik Buterin, the architect of the blockchain Ethereum architecture, first thought about the interoperability of the blockchain and presented three options [16]. The first was a notary scheme, in which a reliable group of companies served as mediators and allowed atomic interaction and information sharing across several blockchains. He also introduced a sidechain, which asks for one blockchain to approve the assertions and data of another. Finally, the chosen method was hash-locking, which interlocks several processes

on various blockchains using the hash's original message to guarantee that each interaction refers to the same initial request made by the end user in a way that can be independently verified. Of course, that was a great initiative and introductory concept of interoperability. However, application-centric (e.g., smart cities) interoperability services where multiple actors provide diverse services require very concise guidelines.

The author in [18] proposed interoperability among networks based on a communication protocol that derives trust from the underlying network consensus protocol. Their proposed architecture is adapted for a range of network implementations. They demonstrated a proof-of-concept for trusted data sharing between two independent trade finance and supply-chain networks, each running on Hyperledger Fabric. Blockchain-based interoperability among healthcare organisations has been proposed in [15,17]. They considered a smooth exchange of information between typical relational-database-supported organisations and blockchain-based NoSQL databases. In [19,20], protocol (ILP) was introduced for exchanging information between ledgers, where [20] contributed a payment exchange mechanism among communities and described how web payment Application Programming Interface (APIs) and the power of ILP payments will frequently exchange in the web platform. In [9], the author proposed a secure blockchain interoperability platform for smart city services. They primarily focused on the structural hierarchy of controlling organisations in a smart city. Most of these efforts were for the interoperability of the blockchain protocols (i.e., structural) or the exchange of information between ledgers. To the best of our knowledge, none of the smart city interoperability solutions discussed above is capable of cross-service interoperability. On the contrary, the ultimate approach of this research is the interoperability of blockchain-based services with scalability and ledger optimization.

3. Smart City Use Cases: Challenges and Solutions

The roll-out of smart city infrastructure opens the way for major advances in services for citizens to ensure modern facilities to keep people safe and coordinate events. The range of services depends on the volume of modernization that the authority can ensure. This section presents different use cases (as shown in Figure 2) and their interoperable services in a unified BC network. A summary of some smart city services, such as e-healthcare, vehicular networks, and smart homes, is provided as an example. Finally, they present the requirements and an optimistic, secure way of achieving interoperability.

3.1. E-Healthcare

Intelligent medical devices (i.e., health IoT) are outfitted in modern hospitals, mobile healthcare systems, e-healthcare systems (EHS), and other medical facilities to ensure medical services in a modern city [21]. HIoT used in e-healthcare carries very sophisticated private information about patients [22]. Usually, ubiquitous users (e.g., physicians, nurses, patients, attendants, diagnostics centres, laboratory personnel, administrators, etc.) have to access services. It is very challenging to define "who is accessing whose data". An interoperable system can be more challenging due to the diversity of access. For example, health records are accessed by different authorized organisations, such as insurance companies, research centres, inter-healthcare, etc., for their respective services. Due to heterogeneity, interoperability among these service providers using traditional technology is challenging. The BC-based service provides a-z record encryption and user-specific smart-contract-based access control policies that solve the abovementioned challenges.

3.2. Smart Home

Enormous types of CIoT are part of the smart home (i.e., intelligent freezers, air conditioners, smart fans, etc.), which collect real-life data and require innovative management. As home area information is more private than any other use case, innovative applications may pave the way to disclosing residents' highly privacy-sensitive lifestyles. Traditionally, smart home services in a smart city depend on other services and are controlled through cloud-based services [23]. For example, security messages should be synchronised with

police administration autonomously, utility bills should be merged with banks, electricity with smart grids, etc. [24]. Every service depends on other services, which claim smart interoperability among the city services. Data exchange in a traditional way might be more vulnerable due to centralised cloud-based interoperable networks [11]. Blockchain regulates access control using certificate authorities and smart-contract-based encrypted data exchange for secure interoperability.

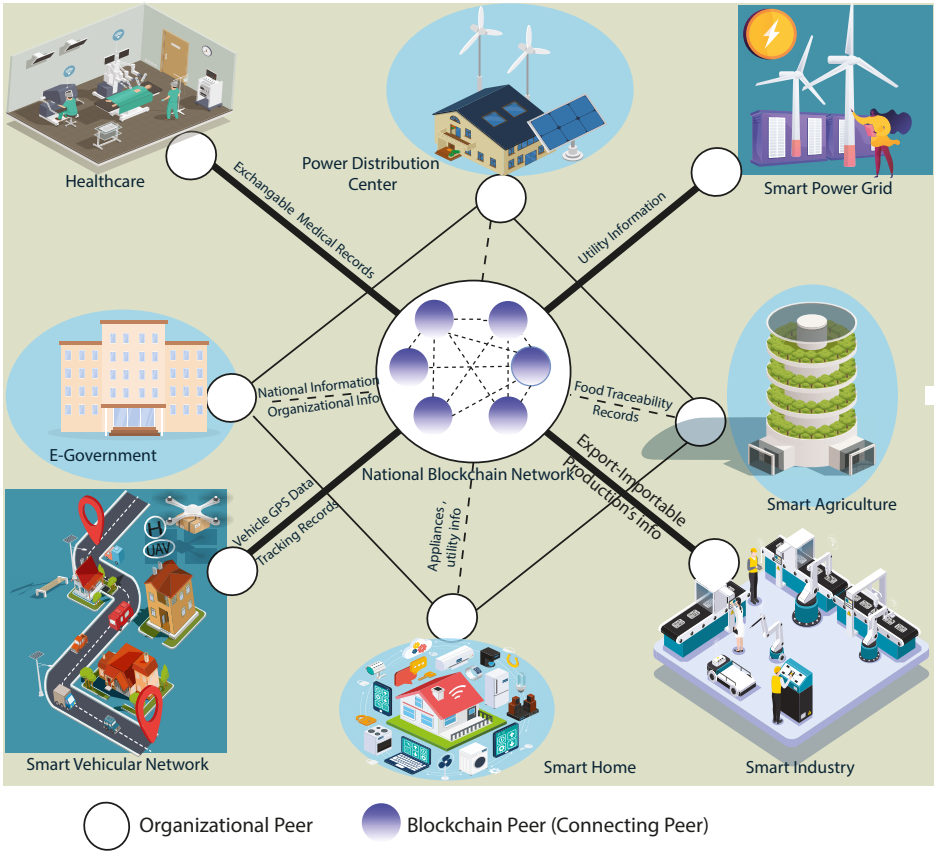

Figure 2. Interoperability of services.

3.3. Vehicular Network

Smart vehicles are integrated with multiple inboard sensors (e.g., headlight range sensor, fuel level sensor, heat sensor, etc.), including GPS, which carries the information of cars and passengers. Vehicular network members (i.e., cars) might be linked directly with the other city services for many reasons, such as product tracking, food preservation conditions monitoring, etc., in the supply chain. Such an information exchange service requires an interoperable and real-time exchange platform. Blockchain can enable secure message dissemination and inter-service communications between vehicles.

3.4. Electronic Government (E-Government)

The e-government system offers great opportunities as an information hub in a smart city. It bridges all existing city-centric services, and a smart administration works in tandem with every service provider in a city that serves as an information center. For example, income tax information for a citizen may be required for administrative purposes. Under an e-government, a relationship between the administrative service providers' server and the income tax server is necessary. Any penetration of an e-government server could result in the release of not only government data but also data from other service providers. The public's confidence in the system has significantly decreased as a result of these issues. A good choice for securing e-government platforms and services is blockchain technology. The management of crucial operations within the organisation could be improved and made

more secure with the help of blockchain-based interoperability among service providers, including administrative services.

4. Generic Challenges: Smart City Use Cases

The various city-centric digital services typically use centralised servers, which creates conventional security issues with additional challenges of interoperable data exchange. Table 2 summarises every smart system's generic challenges and effects.

Table 2. Security and privacy issues in smart systems.

Issues	Challenges	Effects
Data Security	Leakage	Private data might be disclosed
	Tempered	May lose system integrity
	Misplaced	Make system trustless
Communication Security	Authentication	Adversaries may enter the network
	Secure middle-ware	Mobile applications may be compromised and disclose data
	Secure pairing	Wearable IoT may connect with eavesdropper's smartphone
	False data injection	Data integrity can be destroyed
Access Control	Maintain Secrecy	Eavesdropping and data leakage through internal staff
	Integrity	Corruption/interference of data
	Trustworthy control	Lose user confidence, and users can feel uncomfortable
	Policy enforcement	Any kind of control may be lost from the systems.
	Authorization	Wrong privileges of access rights, data might be disclosed.
	Authentication	Can fail to verify who a principal is

- **Communication Security:** Traditional centralised architecture employs standard communication protocols (e.g., WiFi, HTTP, etc.) and security mechanisms (e.g., public-private key) that result in numerous vulnerabilities, such as access control. For example, wiretapping for sniffing packets during the communication process, or man-in-the-middle for intercepting between two legitimate users [25].
- **Single Point of Failure:** In a centralised architecture, all control and data storage are in any central position, which creates a single point of vulnerability. If the primary system fails to provide service in any case, it makes the application's services fail.
- **Message Forgery and Tampering:** Typical network communication is monitored passively, enabling attackers to forge or tamper with messages and re-transmit.
- **Access Control:** Security and privacy mostly depend on the system's access control mechanism, which can be ensured by solving some $'WH'$ questions. For instance, *who* is accessing/sending *what*/*whom* from *where* and *what* is his/her right. It is nearly impossible to maintain access control for diverse users in different use cases in interoperable uniformed digital city services.
- **Heterogeneity of Technologies:** Every independent service provider chooses their own technology, which varies greatly in data structure, logic, communication systems, and so on. It is extremely difficult to bring them together on a single platform.
- **Crowd-Sourced IoT Management:** For public reasons, every square inch of a smart city is somehow monitored by different IoTs, including crowded places. Therefore, it is cumbersome to maintain individual privacy and security from the publicly used IoT. For instance, in IoT-controlled traffic management systems where citizens are allowed to know traffic situations, hijackers may provide the wrong information to citizens due to weak management.

5. Blockchain for Smart City

Starting with the cryptocurrency called Bitcoin, blockchain technology has been introduced as a tremendously secure technology for a public network. The key features such as trustless, anonymous, and a-z encryption make it famous [26]. In this context, private Blockchain (permissioned Blockchain) is introduced, as it is consistent with big

data applications such as smart city use cases. Moreover, it allows the operation of any agreement between parties where transaction structure can vary. Due to outstanding tech features, blockchain technology is being considered for smart city services for some particular goals [27].

5.1. Blockchain for Security Services

The blockchain serves as a service platform for other service providers in a smart city, where the ultimate goal is to ensure security.

- **Architectural Security:** A membership service provider (MSP) ensures the authentication of different organisations, participants, and IoT through certificate authorities. It confirms the reliable intra-organisational infrastructure that is most important for interoperable networks.
- **Transactions Security:** Transactions executed to/from authorised devices and carried through an authorised channel. For communications within the networks, BC components are bound to use those transport layer certificates for inter-component communications. Similarly, users/IoT use their enrollment certificates (ECA) and signature login for forwarding transactions, respectively. These processes ensure secure communications and executions of transactions at every stage.
- **Data Security:** Distributed peers are interconnected and store a ledger. A ledger is a sequence of immutable blocks, and the chain is unbreakable, which protects against data leakage.
- **Validation:** Every transaction executed by valid users is cross-verified through a consensus mechanism. Consensus confirms the validity of the transactions with the consent of at least 51% of authorised peers.

5.2. Blockchain for Interoperability

The mode of organisational integration ensures interoperability, which can be carried out in two ways on blockchain networks. First, all centralised organisations can be upgraded/synchronized with the blockchain system, or access the BC system's interoperability. Second, organisation-specific interoperability nodes are the same BC network infrastructure that enables fast and secure interaction at the local SDK level. Every transaction relayed from one blockchain network will have a hash and Merkel proof of the transaction, proving that the transaction is from a trusted source. An intermediate blockchain network relays transactions and maintains evidence of legitimacy. Application-specific interoperability processes can vary.

- **Structural Interoperability**: Allows the exchange of data, and systems do not need to change the data format, such as for information exchanges between similar organisations (e.g., healthcare, school, etc.)
- **Semantic Interoperability:** Allows the data to be understood by the systems without any modification. This means that the structure and meaning of data are the same. For example, the temperature is stored as an integer but understood as Celsius or Fahrenheit.
- **Process Interoperability:** Incorporates business processes to share a common understanding to enable computer systems. For example, healthcare professionals must standardise business rules to ensure that health information is recorded uniformly and quickly.

6. Blockchain-Based Interoperability Framework

Interoperability opens the possibility of a smooth exchange of transactions among blockchain networks without intermediaries. It is assumed that interoperable city services are compatible with the blockchain network (BCN). Figure 3 presents a blockchain-based interoperable services framework that allows users to interact with different city services where BCN bridges them without spending resources on the translation or experiencing downtime.

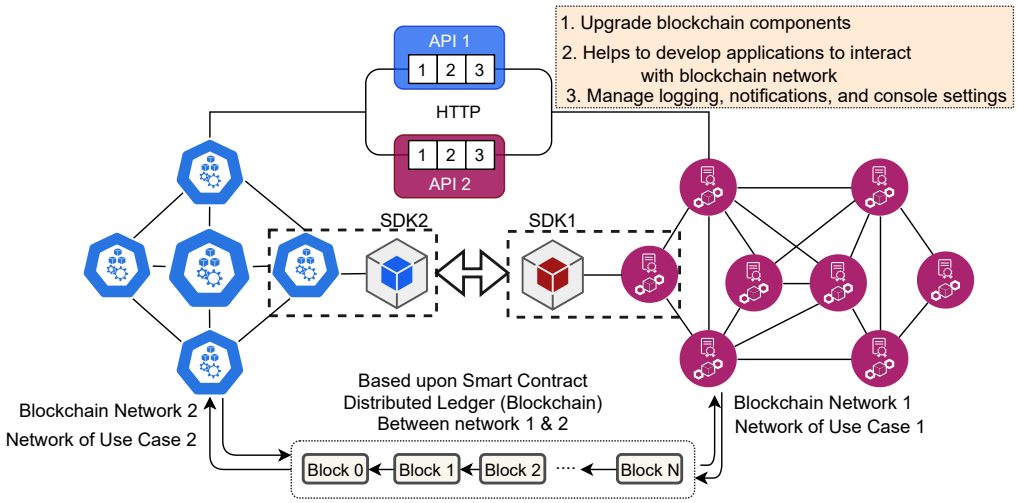

Figure 3. Blockchain-based interoperable framework.

6.1. Overview

The framework recommends open protocols and a system that supports multiple chains [19]. The open protocol allows blockchains to communicate with each other without intermediaries or trust processes. Multiple organisations are connected to a centralised BCN in the architecture, which functions as a core layer of P2P architecture. Every organisation nominates a collaborating peer (P_c) among its local peers that acts as a gateway for bridging with BCN. Ultimately, the core layer of BC forms with the active participation of P_cs. Every organisation handles local transactions by maintaining a local, core, private blockchain network. When an inter-organisational service is required, it sends the request to BCN via P_c. Every organisation maintains its own private ledger, but P_c stores a collaborative ledger. The framework (shown in Figure 3) comprises two independent service providers and their collaborative components as an example.

6.2. Network Architecture

The proposed interoperable blockchain network $IBCN$ is formed with inter-link of multiple BCN- or BC-compatible networks (i.e., $\{BCN_1, BCN_2, BCN_3, \ldots BCN_n\} \in IBCN$). Every independent network has at least one P_c responsible for collaboration with other networks. P_cs forms a P2P network which is introduced as $IBCN$. Every independent network must have a CA that maintains credentials for the components of the organisation. Like collaborative peers, the CA collaborates with a unified (CA^u) while CA^u stores all credentials (i.e., signs, certificates, etc.) of collaborative peers.

6.3. An Independent Network

It is assumed that smart-city-centric services are running on and controlled through an independent BC-compatible network. The independent network can host a small private BC network, or the existing services are BC-compatible in some way. To be a member of the collaborative network, it must run the following functionalities in its network:

- **Certificate Authority:** Every independent network has a Membership Service Provider (MSP) or local Certificate Authority (CA^l), which issues unique certificates, signatures, and public-private keys for every component of the organisation. The credentials are verified during internal transactions in an organisation. In an interoperable network, CA^l-issued certificates are approved through P_c with the proper verification and approval of a unified CA (CA^u).
- **Peers (*P*):** City-centric independent service providers are controlled through a typical private blockchain network with more than three peers. The peers hold their local transactions in a local chain as a ledger. A small organisation with a single server can serve multiple Docker container-based peers to create a P2P network. Such container-

based peers ensure consensus for local transactions, where any container-based peer can play the P_c role [11]. To overcome a single-point failure, a backup server can provide secondary peer services.

- **Collaborator Peer (P_c):** Collaborator Peer, one of the special peers of the P2P network (i.e., $P_c \in P$), is responsible for external collaboration. It only works when required to collaborate with other organisations; otherwise, it functions as a local peer of the organisation. In the absence of P_c, another P is chosen randomly, overcoming a single point of failure. Before going to any transaction, the newly adopted P_c synchronises the interoperable ledger.

6.4. Unified Certificate Authority (CA^u)

CA^u is distinct from local certificate authority (CA^l). It is responsible for credential issuing and maintaining for P_c networks and relevant components. Any expansion or depreciation of the network is subject to the addition or removal of P_c and updates relevant credentials to CA^u. In the proposed network, CA^ls are interlinked with each other through unified CA^u. This interconnection forms a credential exchange network known as a Membership Service Provider (MSP) for an interoperable BC network.

6.5. Transaction Approval

Transaction execution in IBCN is subject to the approval of participating P_c members via consensus, with authentication confirmed via Proof-of-Authority (PoA). Inter-organisation agreements are deployed as smart contracts (a programming script) in P_c, which play endorser roles. Any changes to the smart contract require the approval of the relevant organisation's voting response that is confirmed through PoA. Local transactions were approved within the 51% response of local peers of the organisation.

6.6. SDK and API

Software Development Kit (SDK) provides a way to use a library of APIs, enabling the integration between applications and networks. Applications that leverage this SDK are used to register and enrol members, query the ledger for specific transactions, monitor transaction events, and join other peers to a channel.

6.7. Ledger Maintenance

The framework supports multichain [28], where every independent organisation stores their local transaction record in their private ledger (L_i). Consortium with n organisation maintains $L_1, L_2, \ldots L_n$ ledgers. Inter-organisational transactions are executed in IBCN and store P_c in an interoperable ledger (L^I) separate chain.

7. Evaluations and Analysis

We have simulated the blockchain network by creating individual peers in a Docker container [29]. We used four remote servers to test network connectivity performance, each equipped with an Intel Xeon E7 v3-Core(TM) i7-5960X CPU clocked at 3.00 GHz and 125 GB of RAM.The number of local nodes and connecting peers are initialised in a separate Docker container. Python 3.8 simulates the blockchain network and consensus procedure.

For evaluating the effectiveness of the proposed interoperable framework, we have experimented with increasing the ledger size and the scalability of transactions.

7.1. Scalability Observation

Every service in a smart city uses a huge number of IoT devices, which are increasing daily. Moreover, transaction volume increases exponentially when it is added to an interoperable network. Handling their massive volume of transactions necessitates the use of a scalable blockchain. To minimise the transaction overload on the proposed network, we isolate the organisation-centred local transactions, while interoperability ensures collaborator peers if external collaboration is required.

We have added three organisations with five local peers, including a P_c. For experimental purposes, we assume every P_c represents a smart city service provider under an interoperable network, such as a hospital, insurance company, bank, etc. We assume every transaction is a string without any categorization. We clarify that the ultimate goal is to conduct an experimental evaluation of successful transactions and store them in a BC ledger under an interoperable network.

From our experiments, we observed that credential generation in CA requires 3 ms on average. We fixed the block closing time to 1 s, which means the transaction started but could not execute within the time added to the next block. As shown in the diagram, each device generates five concurrent Tx per second. By generating the source and destination under a local network (e.g., network 1), we evaluated the scalability performance of a private network beyond collaboration. Similarly, interoperability performance is evaluated by sending transactions from one network to another; for example, Tx is generated from network 1, but the destination is network 2. Figure 4 presents the completion time of the transactions (Tx) and fits into a block under a local and interoperable network. Both networks consumed approximately 175 ms until 100 TX, as shown in the figure. For 200 concurrent Tx in the local and interoperable networks, it takes ≈300 ms and 500 ms, respectively. However, time is consumed roughly twice as much in an interoperable network due to consensus time and latency. The execution time is then proportional to the number of Tx in both networks. Although Tx execution time in an interoperable network is higher than the local network, the range is a maximum ≈ 2 s for 500 Tx, which is reasonable. Experimenting with different network parameters, such as consensus algorithm participation, can help scale transactions per second.

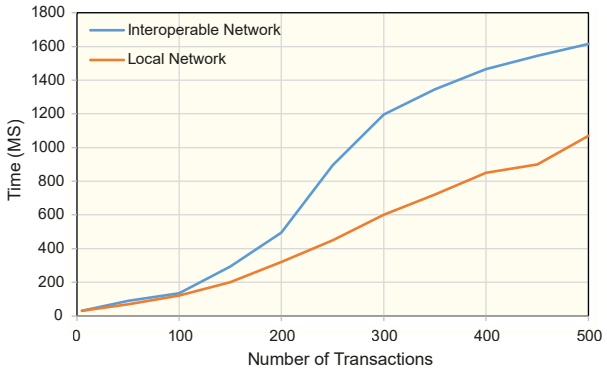

Figure 4. Transaction execution and scalability.

7.2. Ledger Optimization

Blockchains consume memory quickly and scale quickly as the number of Tx increases because they store ledgers in each peer. It is more challenging to store and maintain every local transaction on an interoperable network. Hence, we have used two separate ledgers to store local and interoperable transactions separately. For example, organisation-centric Tx records are kept in regional peers belonging to a service provider, while interoperable Txs are stored in P_cs, a member of an interoperable network.

Figure 5 summarises the ledger growth comparison between private ledgers (local ledger), interoperable ledgers, and typical BC ledgers in a bar graph. The private ledger bar shows the memory's growth with the increase in Tx under an organisation, while the interoperable ledger bar shows the memory's occupancy per block. A typical blockchain ledger bar depicts the scenarios that would occur if every service provider transaction is transferred and executed in an interoperable network. As the figure shows, the block weight grows proportionally as the number of Tx increases in both networks, but not at the same pace as in conventional BC design. The P_c segregates Tx into the private and interoperable ledger based on the parties transacting.

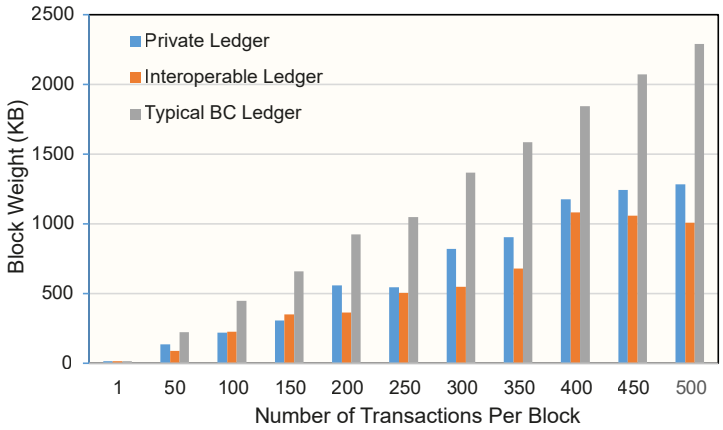

Figure 5. Scalability of transactions.

We used three P_c to form an interoperable network from three service providers, where each service provider has five peers. Every transaction carries some metadata, including participants' signatures, that slightly differ in weight as the number of P_c is less than the number of local peers. This causes differences in weight for the same number of Tx. In conclusion, introducing our proposed framework reduces the overburden of every local Tx from service providers and saves ≈50% more memory in the interoperable network than a typical BC.

8. Challenges and Open Research Issues

The protocol differences in the blockchain network are very challenging for interoperability. Overcoming the differences in the core technical features of protocols (i.e., consensus models, transaction schemes, smart contracts, etc.) is the main barrier to an interoperable network (as shown in Table 3). Several standardisation efforts may be the solution to ensure interoperability.

Table 3. Future research directions.

Challenges	Details
Consensus Algorithm	Protocol-independent consensus algorithm can mitigate the challenges of cross-platform transactions.
Throughput	Scalable framework; is an existing challenge in BC; interoperability can increase one step more.
Public and Private BC linkage	Defines a global standard; can accelerate the interoperability process.
Block Structure	Standard structure; block structures are protocol-specific which is challenging for interoperability.

- Standardise a new blockchain protocol that enforces existing protocols for collaboration. For example, GS1 is an interoperable data standard from IBM and Microsoft for the supply chain.
- Introduce the use of case-specific common and interoperable consensus algorithms in addition to the standard block structure.
- Define any common standard (i.e., block structure, consensus, etc.) for the business blockchain.

9. Conclusions

A blockchain-controlled organisation can leverage security and nonstop service independently. In addition, service providers' secure collaborations can be ensured using blockchain, which is also mandatory for fast citizen services. Our proposed IBCN framework introduces two levels of execution (i.e., local network and interoperable network) that improve scalability and minimise rapid ledger expansion. IBCN allows data and value

sharing among different service providers and facilitates the execution of standard smart contracts within a single blockchain ecosystem. By introducing a collaborating peer, the suggested approach enables the BC ledger to scale across all peers. TPS and ledger weight can be improved significantly, according to the results of the installation testbed. Testbed simulation outcomes show that TPS and ledger weight can be improved significantly. Transactions segregated by collaborating peers save 50% of congestion in an interoperable network, which improves scalability. Similarly, it reduces memory by about 70% compared to a typical blockchain ledger. The overall outcomes prove that blockchain-based interoperability among service providers can make city-centric e-governance faster, more secure, and more effective.

Author Contributions: Conceptualization, S.B. and Z.Y.; methodology, S.B.; software, S.B.; validation, A.K.B., L.Y. and A.A.; formal analysis, S.B.; investigation, S.B.; resources, S.B.; data curation, S.B.; writing—original draft preparation, S.B.; writing—review and editing, A.K.B., M.M. and F.A.; visualization, A.K.B.; supervision, M.M.; funding acquisition, Z.Y. and M.M. All authors have read and agreed to the published version of the manuscript.

Funding: The Research Groups Funding program grant (NU/RG/SERC/12/26), the Deanship of Scientific Research, Najran University, Saudi Arabia. This research is also supported by (1) a Study of the development strategy of the characteristic historical and cultural towns of the Grand Canal Cultural Belt (Lu, Su and Zhe section) 20YJAZH121; (2) Study on the research, collation and conservation of traditional village resources in Taiwan 21&ZD215; (3) Shanghai Summit Discipline in Design.

Acknowledgments: The authors are thankful to the Deanship of Scientific Research at Najran University for funding this work under the Research Groups Funding program grant code (NU/RG/SERC/12/26).

Data Availability Statement: Data is unavailable due to privacy and ethical restrictions.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Vailshery, L.S. IoT Connected Devices Worldwide 2019–2030 | Statista. 2022. Available online: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (accessed on 1 February 2023).
2. Ahlgren, B.; Hidell, M.; Ngai, E.C.H. Internet of Things for Smart Cities: Interoperability and Open Data. *IEEE Internet Comput.* **2016**, *20*, 52–56. [CrossRef]
3. George Lăzăroiu, A.H. Internet of Things Sensing Infrastructures and Data-driven Planning Technologies in Smart Sustainable City Governance and Management. *Geopolit. Hist. Int. Relations* **2021**, *13*, 23.
4. Fernandes, J.; Graciano Neto, V.V.; Santos, R.P.d. An Approach Based on Conceptual Modeling to Understand Factors That Influence Interoperability in Systems-of-Information Systems. In Proceedings of the SBQS '21': XX Brazilian Symposium on Software Quality, Virtual Event, 8–11 November 2021; Association for Computing Machinery: New York, NY, USA, 2021. [CrossRef]
5. d'Aquin, M.; Davies, J.; Motta, E. Smart Cities' Data: Challenges and Opportunities for Semantic Technologies. *IEEE Internet Comput.* **2015**, *19*, 66–70. [CrossRef]
6. Liu, Y.; Shan, G.; Liu, Y.; Alghamdi, A.; Alam, I.; Biswas, S. Blockchain Bridges Critical National Infrastructures: E-Healthcare Data Migration Perspective. *IEEE Access* **2022**, *10*, 28509–28519. [CrossRef]
7. Crowell, B. Blockchain-based Metaverse Platforms: Augmented Analytics Tools, Interconnected Decision-Making Processes, and Computer Vision Algorithms. *Linguist. Philos. Investig.* **2022**, *21*, 121.
8. Biswas, S.; Sharif, K.; Li, F.; Alam, I.; Mohanty, S.P. DAAC: Digital Asset Access Control in a Unified Blockchain Based E-Health System. *IEEE Trans. Big Data* **2022**, *8*, 1273–1287. [CrossRef]
9. Rahman, M.S.; Chamikara, M.; Khalil, I.; Bouras, A. Blockchain-of-blockchains: An interoperable blockchain platform for ensuring IoT data integrity in smart city. *J. Ind. Inf. Integr.* **2022**, *30*, 100408. [CrossRef]
10. Hameed, K.; Barika, M.; Garg, S.; Amin, M.B.; Kang, B. A taxonomy study on securing Blockchain-based Industrial applications: An overview, application perspectives, requirements, attacks, countermeasures, and open issues. *J. Ind. Inf. Integr.* **2022**, *26*, 100312. [CrossRef]
11. Biswas, S.; Sharif, K.; Li, F.; Nour, B.; Wang, Y. A Scalable Blockchain Framework for Secure Transactions in IoT. *IEEE Internet Things J.* **2019**, *6*, 4650–4659. [CrossRef]
12. Gharaibeh, A.; Salahuddin, M.A.; Hussini, S.J.; Khreishah, A.; Khalil, I.; Guizani, M.; Al-Fuqaha, A. Smart cities: A survey on data management, security, and enabling technologies. *IEEE Commun. Surv. Tutorials* **2017**, *19*, 2456–2501. [CrossRef]

13. Focus Group-Smart Sustainable Cities (FG-SSC). *Smart Sustainable Cities: A Guide for City Leaders, Report (05/2015)*; ITU International Telecommunication Union: Geneva, Switzerland, 2017.
14. Pillai, B.; Biswas, K.; Muthukkumarasamy, V. Cross-chain interoperability among blockchain-based systems using transactions. *Knowl. Eng. Rev.* **2020**, *35*, e23. [CrossRef]
15. Biswas, S.; Sharif, K.; Li, F.; Latif, Z.; Kanhere, S.S.; Mohanty, S.P. Interoperability and Synchronization Management of Blockchain-Based Decentralized e-Health Systems. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1363–1376. [CrossRef]
16. Buterin, V. Chain interoperability. *R3 Res. Pap.* **2016**, *9*, 1–24.
17. Biswas, S.; Li, F.; Latif, Z.; Sharif, K.; Bairagi, A.K.; Mohanty, S.P. GlobeChain: An Interoperable Blockchain for Global Sharing of Healthcare Data—A COVID-19 Perspective. *IEEE Consum. Electron. Mag.* **2021**, *10*, 64–69. [CrossRef]
18. Abebe, E.; Behl, D.; Govindarajan, C.; Hu, Y.; Karunamoorthy, D.; Novotny, P.; Pandit, V.; Ramakrishna, V.; Vecchiola, C. Enabling enterprise blockchain interoperability with trusted data transfer (industry track). In Proceedings of the 20th International Middleware Conference Industrial Track, Davis, CA, USA, 9–13 December 2019; pp. 29–35.
19. Neisse, R.; Hernández-Ramos, J.L.; Matheu-García, S.N.; Baldini, G.; Skarmeta, A.; Siris, V.; Lagutin, D.; Nikander, P. An Interledger Blockchain Platform for Cross-Border Management of Cybersecurity Information. *IEEE Internet Comput.* **2020**, *24*, 19–29. [CrossRef]
20. Hope-Bailie, A.; Thomas, S. Interledger: Creating a Standard for Payments. In Proceedings of the 25th International Conference Companion on World Wide Web, Montreal, Canada, 11–15 April 2016; WWW '16 Companion; International World Wide Web Conferences Steering Committee: Geneva, Switzerland, 2016; pp. 281–282. [CrossRef]
21. Nancy Lyons, G.L. Addressing the COVID-19 Crisis by Harnessing Internet of Things Sensors and Machine Learning Algorithms in Data-driven Smart Sustainable Cities. *Geopolit. Hist. Int. Relations* **2020**, *12*, 65.
22. Egala, B.S.; Pradhan, A.K.; Badarla, V.; Mohanty, S.P. Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control. *IEEE Internet Things J.* **2021**, *8*, 11717–11731. [CrossRef]
23. Taylor, P.J.; Dargahi, T.; Dehghantanha, A.; Parizi, R.M.; Choo, K.K.R. A systematic literature review of blockchain cyber security. *Digit. Commun. Netw.* **2020**, *6*, 147–156. [CrossRef]
24. Guo, J.; Ding, X.; Wu, W. A Blockchain-Enabled Ecosystem for Distributed Electricity Trading in Smart City. *IEEE Internet Things J.* **2021**, *8*, 2040–2050. [CrossRef]
25. Lee, J.; Kim, J.; Seo, J. Cyber attack scenarios on smart city and their ripple effects. In Proceedings of the 2019 International Conference on Platform Technology and Service (PlatCon), Jeju, Korea, 28–30 January 2019; pp. 1–5. [CrossRef]
26. Kassab, M.; DeFranco, J.; Malas, T.; Laplante, P.; Destefanis, G.; Neto, V.V.G. Exploring Research in Blockchain for Healthcare and a Roadmap for the Future. *IEEE Trans. Emerg. Top. Comput.* **2021**, *9*, 1835–1852. [CrossRef]
27. Ghazal, T.M.; Kamrul Hasan, M.; Alzoubi, H.M.; Al Hmmadi, M.; Al-Dmour, N.A.; Islam, S.; Kamran, R.; Mago, B. Securing Smart Cities Using Blockchain Technology. In Proceedings of the 2022 1st International Conference on AI in Cybersecurity (ICAIC), Victoria, TX, USA, 24–26 May 2022.
28. Greenspan, D.G. MultiChain Private Blockchain—White Paper. Online. Available online: https://www.multichain.com/white-paper/ (accessed on 1 February 2023).
29. Singh, S.; Singh, N. Containers & Docker: Emerging roles & future of Cloud technology. In Proceedings of the 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Bangalore, India, 21–23 July 2016; pp. 804–807. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.