A Cross-Chain Interoperability Architecture for Smart City Environments

Matthieu Amet*§, Darshan M*‡, Gautam Srivastava*†, Jorge Crichigno¶
*Department of Computer Science, Lakehead University, Thunder Bay, ON, P7B 5E1,Canada
{gsrivast,dmanoj1,mjamet}@lakeheadu.ca
†Department of Mathematics and Computer Science, Brandon University, Brandon, MB, R7A 6A9, Canada
srivastavag@brandonu.ca
‡Department of Computer Science and Engineering, Amrita School of Engineering, Coimbatore, India
cb.en.u4cse19126@cb.students.amrita.edu
§Department of Computer Science, Université de Lorraine, Nancy, France
matthieu.amet3@etu.univ-lorraine.fr
¶College of Engineering and Computing, University of South Carolina, Columbia, USA
jcrichigno@cec.sc.edu

***Abstract*—Blockchains have become quintessential for cutting-edge technology demands in the world. This trend will only continue to increase in the future. Looking at all modern technologies that seem to move towards decentralized architecture, blockchain and distributed ledger technology fit perfectly. In times of conventional database-orientated systems, modern frameworks made huge developments when application programming interfaces (APIs) and data were used cross-platform between centralized entities. A natural evolution for blockchain technology would be to enable communication and data exchange between blockchains (ie. both private and public). This could help not only digitize but could also set in a revolution for digital record-keeping that can be used for automation in the future. Our research work enables and tests interoperability between blockchains in different real-world scenarios. The research work also tries to understand various elements of a smart city environment and a few use-cases are discussed and experimented on.**

***Index Terms*—Interoperability, Blockchain, Multiple chains, Networking, Smart cities, Cross-chain.**

I. Introduction

In our information society, data exchange has become more than life-essential. These data exchanges taking part between two entities allow a lot of new possibilities that require being flawless and completely trustworthy. We must know who sent the data, when the data was sent, keep the data private if it is sensitive and most of all, the data must be immutable. This is why, in this domain, the benefits of the blockchain are no longer to be proven. Indeed, the blockchain respects the principle of immutability, integrity, disponibility, authentication and non-repudiation. A private blockchain might as well contains confidential information. Furthermore, the Internet seems to subside from a social web 2.0 to a brand new decentralized web3 [1] less reliant on states and private companies but more reliant on services. That is why it is important to link those services to answer users' needs. Indeed, we recently saw a rise of service providers that acts as third parties between people, companies such as Uber Eats, Kayak, Fiverr, etc. Blockchain might replace these third parties [2] to get back to a P2P trustless application to connect offerers and applicants. This web3 could revolutionize these needs by reducing or even removing third parties. A lot of private enterprises are moving towards blockchains or are interested in blockchain technology to handle their data. These blockchains are mostly private so that only the needs of the enterprise are satisfied. This also removes the possibility of a single point of failure. At present, many scholars are mainly focusing on the use of a unique blockchain for smart cities. Nevertheless, cities are by nature heterogeneous environments, so smart cities might as well be diversified. The model of a smart city by Giffinger [3] shows well the challenge to resolve in smart cities in Figure 1.

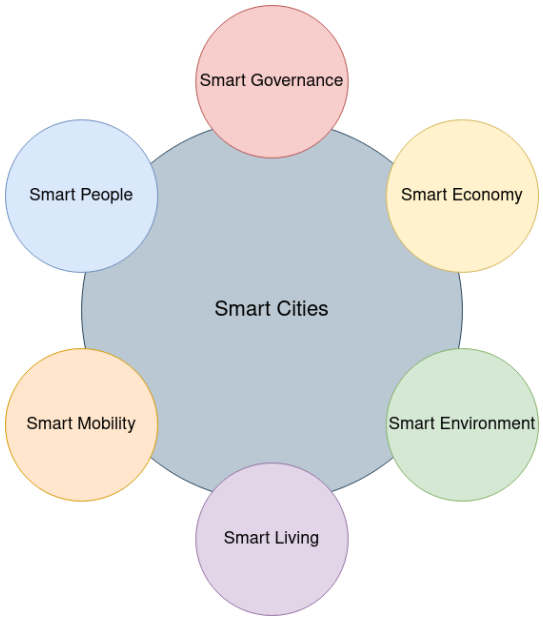

Figure 1. Model of a smart city by Giffingers [3].

978-1-6654-5975-4/22 © 2022 IEEE

A singular blockchain might not respond to the needs of smart cities. For example, a unique blockchain for the use of the government, healthcare, shops, and private enterprises might not be accurate in the use cases and needs of entities. If we wanted this blockchain to adapt to entities it would require a lot of work which seems undoable. Furthermore, having a lot of intermediaries on a single blockchain might lead to network congestion. Hence, having only one blockchain does not seem like a viable solution to answer all the needs of a smart city. That is why this paper aims to introduce the idea of a Main chain that links already existing blockchains and users in a peer-to-peer (P2P) relationship. This blockchain would include the guarantee of immutability and confidentiality if needed. This chain would allow multiple private or public entities connected to the network to exchange data freely and trustlessly. These entities, if they want to, can use their blockchain to link it to the network to send and receive data from other entities in the whole city. For example, if health insurance needs information from a patient in a hospital, the health insurance can request data via its blockchain, and the hospital can send the data trustlessly via its blockchain. The Main blockchain would also provide its services by connecting people to private entities, (e.g a potential client to a hotel), or even connecting people to other people (e.g a user who needs a driver, a user who wants his food delivered).
In summary, this research work contributes to the following methodologies and frameworks.

- Insights of existing blockchain operations and communication channels.
- Preliminary knowledge of blockchain and its ecosystem.
- Meticulous Understanding of real-world use cases for blockchain-based interoperability.
- Mixed Nodes architecture for blockchain-based interoperability.
- Implementation of the entire proposed architecture using C++.
- Rigorous testing using unbiased advanced methods that simulate a real-world scenario.
- Comparison of different scenarios and detailed results with visualization.

The paper is organized as follows. In Section II, we cover some related works about blockchains and cross-chains. Section III reviews some background knowledge to have to fully understand the paper. Section IV presents our architecture for an interoperable smart city environment. Section V discusses the implementation of our solution. Section VI focuses on the results and tests of the implementation. Finally, Section VII concludes the paper and Section VIII addresses future works.

II. Related Works

A. Blockchain in Smart Cities

This subsection focuses on papers trying to solve a particular category of a smart city via a single blockchain.
Cheema *et al.* [4] presented work the helps to understand the necessity for a secure and reliable vehicular system in the growing complexity of traffic and congestion. The authors proposed a way of having a vehicular backhaul network using a private blockchain via drones and RoadSide Units (RSUs) with a Trusted Authority (TA) authenticating the drones. The model presents a tree structure for the same blockchain and can send data to and from using the concept of "mixed nodes". This mixed node infrastructure contributes a major part to the interoperability between blockchains.

Petersen *et al.* [5] propose conventional governance tasks on blockchain such that it is highly visible and transparent. It also tries to adopt a permission level blockchain where only after user authentication the task could be performed. This enables it to maintain security and user authentication which is much required in an organization. The scope of this research work limits itself to automating governance tasks. It does not consider private blockchains. The proposed solution is inspired by this as the "mixed nodes" need to authenticate and then pass on the block information to the other "non-mixed nodes" in the chain.

Zhao *et al.* [6] resort to a 3-layer blockchain with a rating scheme for the authentication of malicious vehicles in a vehicular network. The proposed network works with RSUs, a Certificate Authority (CA) and a database. It tries to reduce the consensus time by adopting a joint Proof of Stake-modified Practical Byzantine Fault Tolerance (PoS-mPBFT) algorithm which also enhances security. This work acts as a catalyst for the proposed solution since a mixture of private blockchains working on different consensus algorithms is used to compare the latency and throughput. The authentication of malicious vehicles concept is expanded to nodes in the private entity blockchain so that security and transparency of the transactions are maintained.

Liu *et al.* [7] propose a solution that embraces the "sharing mechanisms" of data sharing for smart city environments. The authors suggested a smart city blockchain with local data sent to nodes of a blockchain to have public data. The Lightweight and Trusted Sharing Mechanism (LTSM) is based on federated learning and blockchain which makes it secure for data transfer. The node selection algorithm helps in understanding the behaviour of some nodes as malicious or not. The proposed solution acquires its message transfer properties from this research work in multiple cross-link chains.

B. CrossChain for Smart Cities

This subsection is centered on papers trying to solve challenges with several blockchains.

Chang *et al.* [8] propose a way to link private blockchains via the main chain relaying data using smart contracts. This helps the proposed solution to understand the pitfalls of such a system since smart contracts are immutable. Moreover, cross-application data are independent in different blockchain ecosystems which makes it impossible to directly transfer data on the multichain. Lack of control over the data administration protocols leads to unsafe data sharing. The existing research work does not provide user safety despite successful data transfer.

Alkhodair *et al.* [9] implement a chain for vehicles and edges using a Secure Unique Identification List (SUIL) and a Dynamic Block List (DBL) exchanging data to a Tangle blockchain, a network can be inferred. The proposed solution improves latency with the help of a new consensus algorithm termed "Multi-Chain Proof of Rapid Authentication". The proposed solution references this algorithm for validating nodes in the blockchain. Though the solution provides necessary use-case applications, it does not maintain a full-fledged ledger to authenticate blocks.

He *et al.* [10] investigate an architecture of 3 chains for 3 different tasks is understood. The three blockchains are named quality chain, censorship chain and rating chains. Their goal is to produce a score through the different steps of deploying services in a smart city environment. To ensure cross-chain security calculation, Cosi protocol and multi-sign encryption algorithms are used to transmit public and private information on the cross-chain respectively. The proposed solution infers some of the techniques for the transmission of data in the multi-chain environment.

Yunhua *et al.* [11] implement three different chains. The first blockchain would be responsible for storing the digital certificates and related operations such as the creation and revocation of electric vehicles and charging piles to "remove" a CA. The second blockchain would store charging information and finally, the third blockchain would store evaluation information. To ensure the mutual exclusion of information, the solution employs an algorithm that utilizes hash mutexes to lock block resources but it still uses a smart contract to relay the information in a cross-chain environment. The proposed solution is inspired by this research work as a lock-based resource block helps in securely transferring the data across multiple chains.

Polkadot and Cosmos [12], [13] are two papers about blockchains with the same goal of bringing interoperability to the multitude of blockchains that already exists using Polkadot's Relay Chain and Cosmos's Hub.

Košt'ál *et al.* [14] discover a double blockchain coloured network where one is public and contains regular transactions and the second is private to store information about the real coverage of the assets from the first blockchain is proposed. This methodology is useful in the case of large dataset scenarios.

Mercan *et al.* [15] discuss that data regarding boat rentals is stored on three different blockchains namely EOS, Stellar and Ethereum. Three different blockchains are used to reduce the cost of storing data. The proposed solution would also have large chunks of data when used in the smart city environment.

Biswas *et al.* [16] present the safekeeping medical records on the blockchain are inferred. The solution helps in building an interoperable blockchain-based data sharing procedure. Instead of conventional "centralized" data sharing mechanisms that have a single point of failure, data leakage and access control issues, the research work diverges into blockchain-based data storing and sharing mechanisms which help in countering all these issues. The proposed solution uses this sort of mechanism to branch into different sectors of real-world scenarios where blockchain-based interoperability would help in solving problems for the better.

III. Preliminary

Blockchain is a distributed ledger that stores information about transactions in a distributed manner in the form of blocks. For readers novice to the blockchain, here are the fundamentals that one must know about to thoroughly understand the research work.

A. Understanding a basic block

A block acts like a simple data storage unit which contains the data in an encrypted format to ensure security. It also has a hash associated with it that helps in the identification of the block. Adding to this, it also stores the hash of the previous block as shown in Figure 2.

B. Hash

Hash is a function that is required for the encryption standards of blockchain computation. After passing an arbitrary length string to the hashing algorithm (SHA256 in this case) hashes of fixed length are produced as the output. Also, the same data will always produce the same hashed value. This is also known as cryptographic hashing.

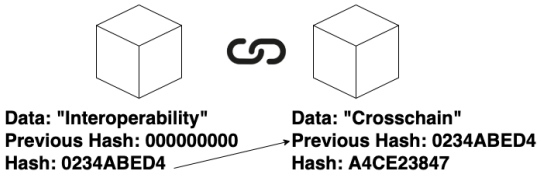

Figure 2. Blockchain visualization using hash values.

C. Transaction

The decision to add a transaction to the chain on a public blockchain is decided by consensus. This means that the transaction must be accepted by the majority of "nodes" (or computers in the network). The people who own the machines in the network are rewarded for confirming transactions.

D. Consensus Algorithm

A consensus algorithm is a method through which all peers in a Blockchain network reach a consensus on the current state of the distributed ledger. Consensus algorithms achieve blockchain network resilience and create trust amongst unknown peers in a distributed computing environment in this way. In essence, the consensus protocol ensures that every new block added to the Blockchain is the only version of the truth that all nodes in the Blockchain agree on.

E. Properties of Distributed Ledger Technology

- **Distributed**: Data on the blockchain is replicated, shared and synchronized among parties involved on a distributed ledger without the need for a central administrator. Unlike traditional database-oriented systems, blockchain provides an independent data-sharing platform.
- **Immutability**: Once data is entered on the blockchain, it cannot be deleted. Changes can be made only by appending new or updated information. With blockchain users have a permanent record or audit trail of all data entered.
- **Digital**: With automation taking over most of the mundane tasks away, digital record keeping would help in this regard. Once the data is permanently stored and is immutable sharing private information would be easy since users do not have to worry about changes made to the data. For private enterprises, this would mean higher throughput since tasks can be automated with good security.

F. Real-Life Blockchain applications

This subsection would help the readers understand some real-life use cases where blockchain is used and how its properties are leveraged. The following are divided into different sectors of industry.

- Aviation: For decades, aerospace industries and their customers have been suffocated by inefficient paperwork and storage systems. Honeywell (NYSE: HON) is addressing these issues by incorporating aircraft record generation into its digital blockchain ledger. This gives Honeywell's customers a straightforward user interface for searching and retrieving scattered data, resulting in a degree of speed and efficiency never seen before in the aerospace sector.
- Healthcare: Blockchain technology has the potential to improve health care by putting the patient at the centre of the system and improving health data security, privacy, and interoperability. By making electronic medical records more efficient, disintermediated, and secure, this technology could create a new model for health information exchanges (HIE). While this new, fast-expanding discipline is not a panacea, it does provide fertile ground for experimentation, investment, and proof-of-concept testing.
- Education: Students have authority over their academic identities thanks to blockchain, which gives them ownership of their records. This makes it much easier for graduates who are job looking, for example, to prove the veracity of the credentials on their Curriculum Vitae and offers them more control over what an employer can access.

IV. Proposed Architecture

The proposed solution's architecture aims to link several independent blockchains using the main chain to help a consensus between a diversity of entities. This way multiple entities can share data on the blockchain with utmost security.

A. Motivation

With the heterogeneity of smart cities, multiple use cases can be inspired by using interoperability between multiple blockchain entities. To answer the question, of why we are building this, the following are a few real-world examples where our solution can be used effectively for both digital record keeping and automation.

1) Healthcare and Insurance Firms: Healthcare entities and Insurance firms need to exchange data and monetary value securely. This can only happen if both entities are validated and verified on the network. By doing so, automating the insurance reimbursement through the network turns into a very convenient task.

2) Private Company and its Customers/Employees: A private company that uses a blockchain can directly keep track of its customers/employees. Messages can be parsed through different networks and direct business value can be propelled further.

3) Gig Economy: A user might want to request a paid service from another user, such as getting groceries delivered. This user can then send a request to the main chain acting like a third party. Another user can accept this request and complete the task to get his/her payment. As the blockchain acts as the third party, the cost of the delivery is reduced for the offer maker and the payment that the delivery guy gets is increased.

B. Network Architecture

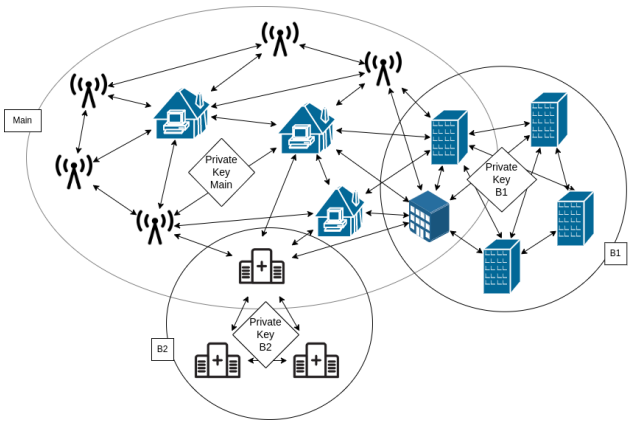

Figure 3. Network Interoperability Architecture.

In Figure 3, we have three networks based on blockchain. There is the B1 network that needs to send data to B2. The proposed solution achieves this by relaying the data over the main network. To understand this, the sequence diagram is presented in Figure 4.

Table I below can be used to understand the notations used in the sequence diagram.

Alice wants to send a message M to Bob from B1 to B2. M is encrypted with K^{+}_{Bob}. H^{M}_{Bob} is encrypted with

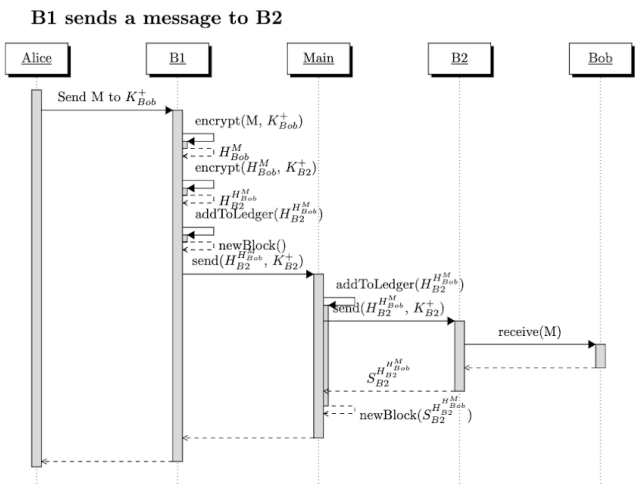

Figure 4. Sequence diagram for interoperability.

Table I
NOTATIONS USED IN THE SEQUENCE DIAGRAM.

Character	*Description*
K^+_A	Public key of A
K^-_A	Private key of A
H^M_A	Encryption of M with the public key of A
S^M_A	Signature of M using the private key of A

K^+_{B2}. $H^{H^M_{Bob}}_{B2}$ is added to the B1 ledger with K^+_{B2} as the blockchain of destination. The block containing the transaction is created, added and finalized via X1 consensus to the B1 blockchain. Mixed nodes of B1 send the new transaction to the main blockchain. The Main blockchain records a pending transaction through their blockchain and forwards this transaction to the destination blockchain (B2). Mixed nodes of B2 receive the transaction and forward it to B2 nodes The block containing the transaction is created, added and finalized via X2 consensus to the B2 blockchain. This information, signed by B2 is forwarded to Main, Main puts the transaction as successful, if B1 wants to check the status of the transaction it can ask the network as the data on main is public. B2 gets H^M_{Bob} in clear using K^-_{B2}. Bob gets M in clear using K^-_{Bob}.

C. Design Goals

For the solution to ensure security goals and beyond, we have used simple yet sophisticated concepts. The dictionary data structure is used to store all the public keys for all blockchains. Then there is the mixed node which acts as a node for both B_i ($i = 1, 2, \ldots$) and the main chain. This helps in the actual transaction between the main network and subnetworks. To attain confidentiality, the solution uses the RSA encryption algorithm at the node level. Hashing Algorithm is used (SHA256 in this case) for the transaction to take place. A consensus algorithm is also provided so that only verified users can add the blocks.
With this in mind, we have designed the solution such that users and businesses can use this methodology with utmost security and reliability.

V. IMPLEMENTATION

Simulating an entirely new ecosystem that enables interoperability between blockchains has always been a tough task. Even with advanced machines, tools and computing power, exchanging data on the blockchain has never been possible efficiently, until now. To bring interoperability most securely the solution uses various tools and frameworks. To address the technical gaps concerning blockchain, the proposed solution is implemented using C++. Even though most developers use either Solidity or Rust for their blockchain-based work, the solution had been implemented using C++ due to its long list of advantages. To list a few, C++ offers primitive control over memory, advanced multi-threading, and other object-oriented features like function overloading, runtime polymorphism, etc. These merits come in handy for the implementation of the computing nodes as each node is a single thread. Hence, to simulate the entire test environment multiple threads are executed concurrently. For RSA-related cryptography, the crypto++ library is used. SHA-256 function is employed for encryption which can be found on Zedwood[1]. During a critical transaction (ie. message passing) locks over the shared resources are implemented using mutex and synchronization is done using semaphores. The ledger records all the transactions between multiple chains which also helps in avoiding invalid memory access.

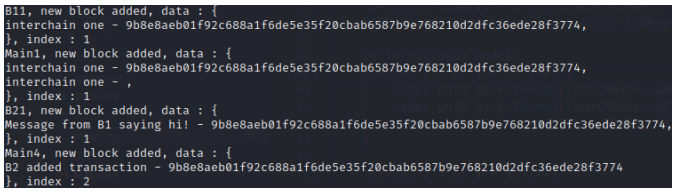

Figure 5. Successful transaction of the message.

In Figure 5, we can infer that data can be exchanged between blockchains based on the proposed methodology.

VI. TESTS

A. Test Environment

- Tests were done using a Linux 5.17.0 machine with 8 GB RAM and Intel Core i5 9th gen
- Parameters were the number of transactions in a block, consensus, number of nodes / mixed nodes, with or without cross-chain transactions. Difficulty could also be a parameter but it was not changed because it wasn't relevant enough for the PoS blockchains and too simple or too complicated to find a block for PoW blockchains.
- Blocks were created using the number of transactions 512, 1024, 2048, 4096, 8192 for single blockchains and 512, 1024 and 2048 for cross-chain blockchains. Adding more transactions to a block created a segfault of recursion for Merkle trees this size.

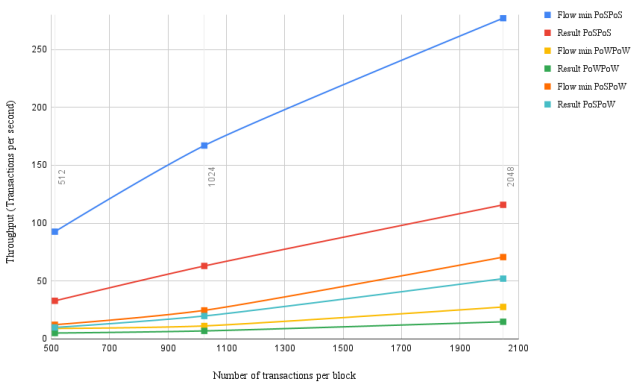

Figure 6. Result visualization.

The graph is taken from the optimized results of all cross-chain combinations and the results depict that the PoS-PoS cross-chain is the most efficient method and the PoW-PoW cross-chain is the least efficient method to transfer data and messages on the blockchain. The PoS-PoW cross-chain falls right in the middle of the PoS-PoS and PoW-PoW cross-chain which also depicts the enhanced results of the mixed nodes algorithm.

VII. Conclusion

Blockchain interoperability has always been an untapped research sector. With this research work, we hope that Interoperability is studied in greater depth. The results obtained with this research work are fundamentals for blockchain interoperability. After careful study of the real-world scenarios where interoperability can be wisely used, this research work would prove to be the foundation of any sort of data exchange between blockchain networks. With the future heading towards peer-to-peer networking and decentralized technology, this research work would act like APIs and data exchange platforms in the blockchain environment. From understanding the real-world scenario to developing the code from scratch and performing test runs, we have concluded that blockchain interoperability is quite possible and implementable without losing data and computational power. By adding interoperability to the blockchain of private entities, we enable them to communicate and exchange data securely. With the results obtained, we can conclude that compute power is not lost while using this framework. The graph obtained after gruesome testing provided us with vivid conclusions of how a combination of blockchains would perform in real-world use cases.

VIII. Future Work

The future of blockchain interoperability is quite exciting. This would enable blockchain owners and maintainers to collaborate. The potential they would unlock is potentially limitless. All the methodologies used in this research work such as analyzing real-world use cases, performing tests etc. can be studied further and expanded with intelligent techniques. We would like to expand this research work to make it powerful enough to enable smart contract deployment on a blockchain with a trigger argument coming from another blockchain. This would enable boundless automation while storing and using the data securely.

[1]http://www.zedwood.com/

Acknowledgment

This work is funded by the Globalink Research Internship (GRI) program of Mathematics of Information Technology and Complex Systems (MITACS). Both Darshan M. and Matthieu Amet were interns through this program of Dr. Gautam Srivastava.

References

[1] J. Bambacht and J. Pouwelse, "Web3: A decentralized societal infrastructure for identity, trust, money, and data," *arXiv preprint arXiv:2203.00398*, 2022.

[2] M. Mut-Puigserver, M. A. Cabot-Nadal, and M. M. Payeras-Capellà, "Removing the trusted third party in a confidential multiparty registered edelivery protocol using blockchain," *IEEE Access*, vol. 8, pp. 106 855–106 871, 2020.

[3] R. Giffinger, "Smart city concepts: Chances and risks of energy efficient urban development," in *Smart Cities, Green Technologies, and Intelligent Transport Systems*. Springer, 2015, pp. 3–16.

[4] M. A. Cheema, M. K. Shehzad, H. K. Qureshi, S. A. Hassan, and H. Jung, "A drone-aided blockchain-based smart vehicular network," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4160–4170, 2020.

[5] D. Petersen, "Automating governance: Blockchain delivered governance for business networks," *Industrial Marketing Management*, vol. 102, pp. 177–189, 2022.

[6] N. Zhao, H. Wu, and X. Zhao, "Consortium blockchain-based secure software defined vehicular network," *Mobile Networks and Applications*, vol. 25, no. 1, pp. 314–327, 2020.

[7] C. Liu, S. Guo, S. Guo, Y. Yan, X. Qiu, and S. Zhang, "Ltsm: Lightweight and trusted sharing mechanism of iot data in smart city," *IEEE Internet of Things Journal*, vol. 9, no. 7, pp. 5080–5093, 2021.

[8] J. Chang, J. Ni, J. Xiao, X. Dai, and H. Jin, "Synergychain: A multichain-based data sharing framework with hierarchical access control," *IEEE Internet of Things Journal*, 2021.

[9] A. Alkhodair, S. Mohanty, E. Kougianos, and D. Puthal, "Mcpora: A multi-chain proof of rapid authentication for post-blockchain based security in large scale complex cyber-physical systems," in *2020 IEEE computer society annual symposium on VLSI (ISVLSI)*. IEEE, 2020, pp. 446–451.

[10] Y. He, C. Zhang, B. Wu, Y. Yang, K. Xiao, and H. Li, "Cross-chain trusted service quality computing scheme for multi-chain model-based 5g network slicing sla," *IEEE Internet of Things Journal*, 2021.

[11] ——, "A cross-chain trusted reputation scheme for a shared charging platform based on blockchain," *IEEE Internet of Things Journal*, 2021.

[12] G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework," *White Paper*, vol. 21, pp. 2327–4662, 2016.

[13] J. Kwon and E. Buchman, "Cosmos: A network of distributed ledgers," *URL https://cosmos. network/whitepaper*, 2016.

[14] K. Košťál, "Multi-chain architecture for blockchain networks," *Information Sciences & Technologies: Bulletin of the ACM Slovakia*, vol. 12, no. 2, pp. 8–14, 2020.

[15] S. Mercan, M. Cebe, E. Tekiner, K. Akkaya, M. Chang, and S. Uluagac, "A cost-efficient iot forensics framework with blockchain," in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2020, pp. 1–5.

[16] S. Biswas, K. Sharif, F. Li, A. K. Bairagi, Z. Latif, and S. P. Mohanty, "Globechain: An interoperable blockchain for global sharing of healthcare data—a covid-19 perspective," *IEEE Consumer Electronics Magazine*, vol. 10, no. 5, pp. 64–69, 2021.