A Blockchain-based Method Ensuring Integrity of Shared Data in a Distributed-Control Intersection Network

Mohamed El Ghazouani[1], Abdelouafi Ikidid[2], Charafeddine Ait Zaouiat[3],
Aziz Layla[4], Mohamed Lachgar[5], Latifa Er-Rajy[6]

ESIM, Polydisciplinary Faculty of Sidi Bennour, Chouaîb Doukkali University, El Jadida, Morocco[1, 3, 4]
Laboratory of System Analysis, Information Processing and Industrial Management,
EST Salé, Mohammed V University, Salé, Morocco[2]
LTI, National School of Applied Sciences, Chouaîb Doukkali University, El Jadida, Morocco[5]
Computer Science Department, Laboratory of Information Systems Engineering,
Cadi Ayyad University, Marrakesh, Morocco[6]

Abstract—**In modern urban transportation systems, the efficient management of traffic intersections is crucial to ensure smooth traffic flow and reduce congestion. Distributed-control intersection networks, where control decisions are made collaboratively by multiple entities, offer promising solutions. However, maintaining the security and the integrity of shared data among these entities poses significant challenges, including the risk of data tampering and unauthorized modifications. This paper proposes a novel approach that leverages blockchain technology to address these integrity concerns based on intelligent agents. By utilizing the decentralized and transparent nature of blockchain, our method ensures the authenticity and immutability of shared data within the distributed-control intersection network. The paper presents a detailed architecture, highlighting the integration of blockchain into the existing infrastructure, and discusses the benefits of this approach in enhancing data integrity, trust, and overall system reliability. Through a case study and simulation results, the proposed approach demonstrates its effectiveness in maintaining the integrity of shared data, thereby contributing to the advancement of secure and efficient traffic management systems.**

Keywords—Security; data integrity; blockchain; distributed system; congestion; intelligent agent

I. Introduction

In the face of rapidly expanding urban populations, the efficient management of traffic intersections has emerged as a critical aspect of modern urban transportation systems [1]. Traditional traffic control mechanisms, reliant on centralized decision-making, struggle to accommodate the dynamic demands of increasingly congested road networks. This has spurred the development of distributed-control intersection networks, which offer a more adaptive and responsive approach to traffic management. In these networks, control decisions are distributed across multiple entities, allowing real-time adjustments based on traffic conditions, thereby improving overall traffic flow and reducing congestion [2].

The advantages of distributed-control intersection networks are evident, but they bring forth new challenges, particularly concerning the integrity of shared data among the participating entities. The accuracy and authenticity of data exchanged within these networks are pivotal for their successful operation. Compromised or tampered data can lead to erroneous control decisions, potentially resulting in accidents, increased congestion, and even system-wide failures [3]. Hence, the establishment of a robust method to ensure data integrity is crucial.

Blockchain technology continues to evolve, with new consensus mechanisms, scalability solutions, and use cases being developed. Understanding these fundamentals is crucial for grasping the potential impact of blockchain on various industries [4].

This paper introduces a novel approach that leverages blockchain technology to address the integrity concerns in distributed-control intersection networks. Blockchain has emerged as a powerful tool for addressing data integrity concerns in distributed and decentralized systems. Initially introduced as the foundational technology underpinning cryptocurrencies like Bitcoin [5], blockchain has evolved to demonstrate its applicability beyond financial use cases. Its core features, including decentralized data management, immutability, and cryptographic security, make it an ideal candidate for ensuring data integrity in complex systems, such as distributed-control intersection networks.

By presenting a comprehensive analysis of the proposed methodology, backed by a practical case study and simulation results, this paper aims to contribute to the development of robust and trustworthy distributed-control intersection networks that can effectively address the challenges of modern urban transportation. The organization of this paper is as stated below: Section II outlines the related works. The various blockchain fundamentals are discussed in Section III. Section IV describes our proposed methodology. Section V includes the simulation results and discussion. Lastly, a conclusion is outlined in Section VI.

II. Related Works

In recent years, the integration of blockchain technology into various domains has garnered significant attention due to its potential to enhance security, and decentralization. In the context of distributed-control intersection networks, where efficient traffic management is crucial, the utilization of blockchain for ensuring the integrity of shared data has emerged as a promising avenue. Several related works have explored similar themes and provided insights into the application of blockchain in distributed-control systems and intersection networks.

Traditional static control systems may fail to handle emergency situations due to traffic jams. As a solution, Wireless Sensor Networks (WSNs) have gained attention for their ability to detect traffic and mitigate road congestion. K. Nellore and G. P. Hancke [6] have extensively explored traffic management systems that employ WSNs to prevent congestion, prioritize emergency vehicles, and reduce the Average Waiting Time (AWT) at intersections. They offered a comprehensive survey of current urban traffic management strategies, particularly those focused on priority-based signaling, congestion reduction, and improving vehicle AWT. Z. Yang et al. [7] introduced a promising approach to address trust issues in vehicular networks through the use of blockchain and a decentralized trust management system. They introduced a solution to enhance the trustworthiness of messages exchanged among vehicles in vehicular networks, considering the challenging non-trusted environment. A. Daeichian and A. Haghani [8] employed a combination of fuzzy Q-learning (QL) and agent technologies to create a traffic light control framework. Each individual agent engages with neighboring agents, receiving rewards for their decisions. The control choices are determined based on the input of vehicle numbers to schedule the duration of the green traffic light phase. The primary objective is to optimize the reward and minimize the average delay time. A. Ikidid et al. [9] presented a novel approach to address traffic management challenges in Moroccan cities, with a focus on promoting emergency vehicle access and encouraging collective transportation modes. The proposed control system operates at signalized intersections with priority links in urban environments. This system combines multi-agent technology and fuzzy logic to effectively regulate traffic flows.

On the other hand, the significance of data integrity in distributed-control systems has prompted research into various methodologies. T. Rauter [10] emphasized the significance of maintaining the integrity of the entire distributed control system. He categorized specific properties that enable the verification and proof of integrity for various subsystems within the system. Q. Kong et al. [11] introduced a novel, efficient, and location privacy-preserving data sharing scheme with collusion resistance within the Internet of Vehicles (IoV) context. Furthermore, blockchain's decentralized nature has been leveraged for secure data sharing across multiple parties. G. P. Joshi et al. [12] proposed a blockchain-based method for secure and privacy-preserving data sharing in vehicular networks. Although not specific to intersection networks, this work highlights the potential of blockchain in ensuring data integrity and security in vehicular environments. J. Cui et al. [13] proposed an innovative solution utilizing consortium blockchain technology to enable traceable and anonymous vehicle-to-vehicle (V2V) data sharing. It addresses critical issues in current vehicular networks, including data privacy, security, and trust, while also capitalizing on the advantages of emerging technologies such as blockchain and 5G. S. Kudva et al. [14] proposed an innovative approach to selecting miner nodes in vehicular blockchain applications. The proposed method, called the "Proof of Driving" protocol, associates "driving coins" with vehicle features, such as distance traveled, to enhance the randomness in selecting miner nodes. In [15], S. A. Bagloee et al. discussed how a blockchain-based platform can facilitate the deployment of tradable mobility permits (TMP), along with related benefits like dynamic toll pricing, emergency vehicle priority, heavy truck platooning, and connected vehicles. I. M. Varma and N. Kumar introduced the convergence of Internet of Vehicles (IoV) and Software-Defined Networking (SDN), enhanced by blockchain technology, that offers a promising solution to address the complex challenges of vehicular networks, providing improved transportation, security, and network management while also presenting opportunities for further research and development [16]. A set of approaches and protocols have been proposed to determine the feasibility of using blockchain for traffic data security [17] and [18].

While existing related works provide valuable insights into blockchain's potential in distributed-control intersection networks, certain challenges remain unexplored. Integrity of shared data is a crucial factor in real-time traffic management scenarios. Additionally, the interoperability between blockchain and existing traffic infrastructure requires further investigation. The research landscape regarding blockchain's role in ensuring the integrity of shared data in distributed-control intersection networks is steadily growing. By building upon the foundation laid by previous related works, this study aims to contribute to the understanding of how blockchain can effectively enhance data integrity and efficiency in traffic management systems.

III. BLOCKCHAIN FUNDAMENTALS

Blockchain is a revolutionary technology that serves as the foundation for cryptocurrencies like Bitcoin and has far-reaching applications beyond digital currencies. At its core, blockchain is a decentralized and distributed digital ledger that records transactions in a secure, transparent, and immutable manner. Fig. 1 illustrates the benefits that arise from the adoption of blockchain.

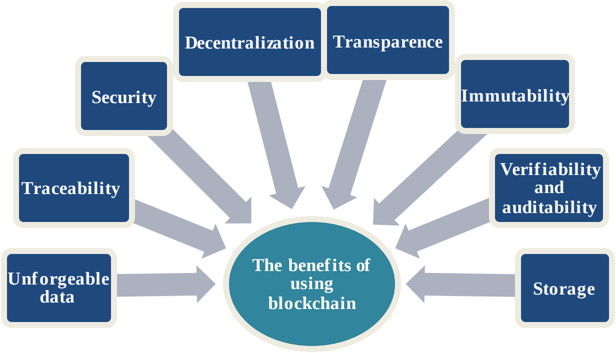

Fig. 1. The benefits of using blockchain.

Blockchain technology has several features that make it highly suitable for ensuring data integrity in a distributed-control intersection network. Here are some key features:

- Decentralization: Blockchain operates on a decentralized network of nodes, where each node stores a copy of the entire blockchain. In a distributed-control intersection network, this decentralization ensures that no single entity has control over the entire system. This feature reduces the risk of a single point of failure and enhances the network's resilience.
- Immutability: Once data is recorded on the blockchain, it is extremely difficult to alter or delete [19]. This immutability ensures that the historical data related to traffic control decisions and intersection activities remain tamper-proof, providing a reliable audit trail.
- Transparency: All participants in the network can view the data recorded on the blockchain [20]. In the context of a distributed-control intersection network, this transparency ensures that all stakeholders, including traffic authorities, city planners, and even the public, can access relevant data, promoting trust and accountability.
- Consensus Mechanisms: Blockchain networks use consensus mechanisms to validate transactions or data entries. This ensures that all nodes in the network agree on the state of the blockchain. Consensus mechanisms such as Proof of Work (PoW) [21] or Proof of Stake (PoS) [22] can be used to ensure that intersection control decisions are agreed upon by the network, minimizing the risk of unauthorized changes.
- Data Integrity: Blockchain can be used to create a secure and tamper-evident record of intersection control decisions, traffic data, and other relevant information. This ensures that the data remains consistent and reliable [23], which is crucial for maintaining the efficiency and safety of the intersection network.
- Smart Contracts: Smart contracts are self-executing contracts with the terms directly written into code [24]. In a distributed-control intersection network, smart contracts could automate and enforce specific rules and conditions, such as prioritizing emergency vehicles or optimizing traffic flow based on predefined criteria.
- Security: Blockchain networks use cryptographic techniques to secure data [25]. This enhances the security of the intersection network, protecting it from unauthorized access, data breaches, and cyberattacks.
- Auditability: Every transaction or data entry on the blockchain is traceable. This auditability ensures that all changes to the intersection network's data can be tracked back to their source, providing accountability and facilitating investigations when necessary.

By leveraging these features, a blockchain-based approach can enhance the integrity of shared data in a distributed-control intersection network, reducing the risk of data manipulation, promoting trust among network participants, and contributing to more secure and efficient traffic management systems.

IV. Proposed Methodology

A. Problem Modeling

A distributed control system (DCS) for light control intersections is a sophisticated networked system designed to manage traffic flow and optimize vehicle and pedestrian movement at intersections. It utilizes advanced technologies and algorithms to efficiently control traffic signals, ensure safety, and minimize congestion. An intersection network consists of multiple intersections that are strategically connected to form a network. These intersections can vary in size and complexity, ranging from simple crossroads to multi-lane junctions. Fig. 2 shows an overview of an intersection network with nine intersections, each intersection has four two-way roads.

The DCS is functionally and spatially distributed. Every intersection is viewed as a network sub-section and controlled by a community named Intersection Control Group (ICG) and consists of a group of autonomous, cooperative, and intelligent agents. Each community acts locally according to its data and communicates with others to coordinate actions. This system promotes flexibility, resilience and efficiency by enabling individual components to contribute to an overall solution without depending on a single central authority. Communication in these distributed systems involves the exchange of information between different interconnected autonomous communities. These communities often communicate via local or wide-area networks, which introduce a security challenge.

The control of each signalized intersection is performed by an ICG, which defines the signal plan. This plan is designed to optimize phase layout while adapting to the constantly changing intersection environment, with control of the entire intersection network being fully distributed and achieved through the collective capacity, communication, and coordination of the ICGs.

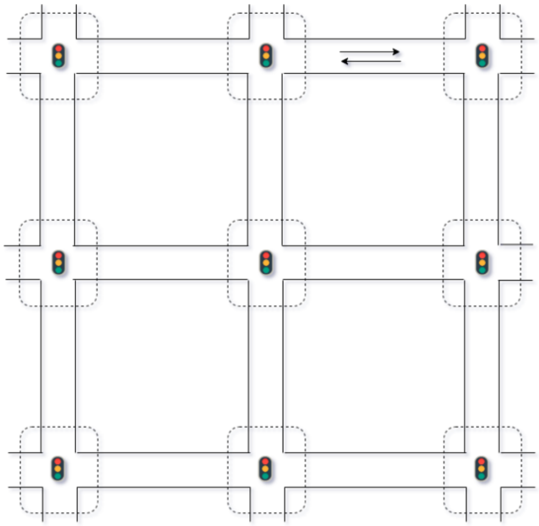

Fig. 2. Signaled intersection network.

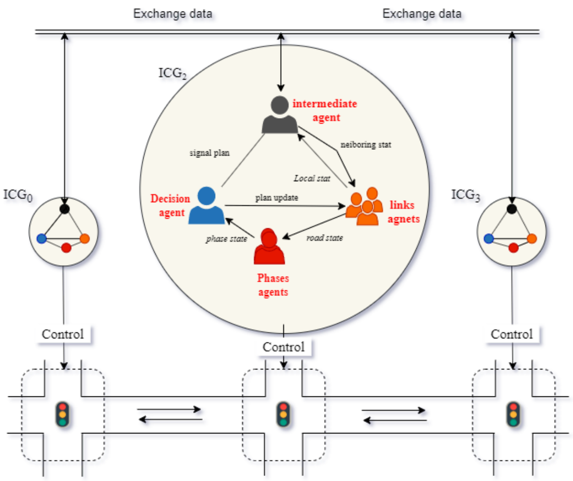

Fig. 3. Overview of distributed-control intersection networks.

Fig. 3 presents an overview of distributed Urban Traffic management System. It generally involves of a set of control groups, each control group consists of:

- Links agents: An agent represents each link, a "link" refers to a specific segment of road that connects two distinct points. An agent link is assigned to supervise each incoming link, with the aim of consistently and promptly monitoring the link state. These specific agents have a limited, local perspective of the environment. In order to maintain system simplicity, no agent is granted a comprehensive overview of the entire network, thereby reducing overall complexity. The goal of this agent is to provide the link state presented by the concentration D. The concentration of a particular road at a given point is the number N of vehicles present between p and p+Δp at an instant t, relative to the length of the section of lane (Eq. 1). The concept of vehicular concentration refers to the density of vehicles occupying a specific section of a road at a given point in time.

$$D_{\Delta t}(p) = D(p, t \to t + \Delta t) = \frac{V}{\Delta t} \qquad (1)$$

- Phase agents: Two distinct agents are employed to oversee phases within an intersection. The Activated Phase Agent handles the active phase, while the Inactive Phase Agent manages phases that are not currently active. The goal of this agent is to provide the phase state.

- Decision agent: The decision agent is the central element of the system architecture, responsible for updating the signal plan according to changes in the environment. This decision-making process is executed collaboratively to prevent isolated optimizations.

- Intermediate agent: The role of the intermediate agent is to establish coordination with the neighboring control group. It acts as a communication interface agent for the intersection control group and mediating external communications. This agent facilitates the exchange of incoming link states with intermediate agents in neighboring control groups.

Ensuring the integrity of communications poses significant challenges in this type of system. As data passes through different nodes and networks to reach the control group, it is susceptible to corruption, interception and unauthorized access

B. Overview of our Proposed System Model

We have seen in our earlier discussions the necessity to apply a new approach that can enhance the integrity of shared data in a distributed-control intersection network, reducing the risk of data manipulation, promoting trust among network participants, and contributing to more secure and efficient traffic management systems. A decentralized network in our model mainly includes several intersections that communicate with each other by sharing information of link state. Hence, design goal of our work is to make the public blockchain usable in the distributed-control intersection networks by storing the local link state of each intersection, which will guarantee the integrity of the data exchanged between the different intersections. Fig. 4 illustrates how different components of our proposal are connected. Detailed descriptions of the proposed system are given in the following:

- Creating blocks: In our model, each intersection system will have an associated blockchain database. All the records of link states are considered as transactions that are validated by the ICG and finally added into immutable blocks of the blockchain. The block contains the link state data, the merkle root, previous block hash, block size and timestamp. Timestamps in the blockchain ensure a chronological record of data.

- Calculating signals plan: Each ICG refers to the neighboring ICG blockchain in order to retrieve their link states that permit to calculate the signals plan of the current intersection.

- ICG: To maintain data integrity of shared link state, each ICG calculates link state then stores it in a new block within a specific blockchain related to the intersection. In case of an intersection system failure, the ICG can then send a data query to ask for historical link state, in a particular moment, from the neighboring ICG's Blockchain.

- ICG Blockchain: each ICG Blockchain maintains the blocks corresponding to the different calculated link states. The blockchain records the history of intersection link states, therefore the use of the blockchain is essential in the event of an intersection system failure, so that the new signals plan of the intersection can be calculated based on the link states previously stored in the blockchain, thereby streamlining the decision-making process in the distributed-control system.

For the intersections, each generation of a link state is treated as a transaction on the blockchain. Every link state data is hashed and added to the blockchain, creating an immutable record. Hashes serve as a fingerprint of the data, making it easy to detect any modifications.

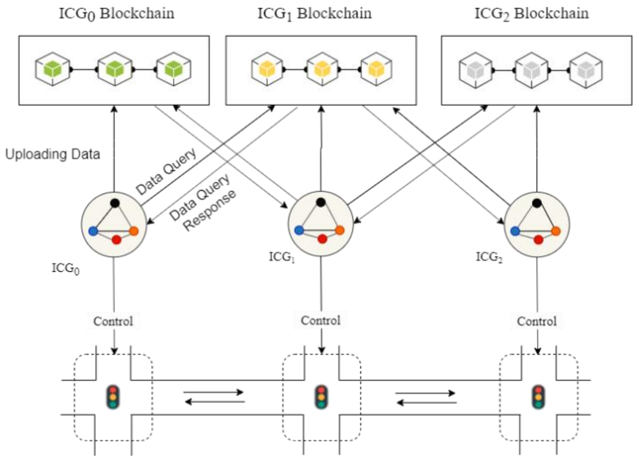

Fig. 4. Overview of blockchain based distributed-control intersection networks.

C. Data Integrity Auditing for Distributed-Control Intersection Networks

Shared data integrity auditing for distributed-control intersection networks using blockchain is a concept that applies the principles of blockchain technology to ensure the accuracy and reliability of data in intersection networks that employ a distributed control approach. In such networks, multiple intersections or traffic management components collaborate to optimize traffic flow and enhance transportation efficiency. Blockchain can play a role in storing the exchanged data and maintaining its integrity among these distributed components.

Auditors (ICGs) can verify the integrity of data by comparing the expected data with the historical records on the blockchain. Automated audits can be performed to constantly monitor and validate data against predefined criteria. All ICGs can independently verify the accuracy of data, promoting trust and transparency within the intersection network.

The provided pseudo-code outlines an algorithm for conducting data integrity auditing according to our proposal. This process ensures the accuracy and consistency of data stored in the blockchain, mitigating potential errors or tampering.

These are the steps of the algorithm:

- The algorithm begins by checking if the target block index is within valid bounds. If not, it returns an error message indicating an invalid index.
- After that, it retrieves the target block from the blockchain using the provided index.
- Then, it calculates the hash of the expected data and compares it with the stored hash of the link state data within the target block. If they do not match, it concludes that the data integrity audit has failed.
- Next, the algorithm iterates through the blockchain starting from the block after the target block. It retrieves each block and its corresponding previous block to verify the chain's integrity. If the PreviousHash of a block does not match the BlockHash of its previous block, the algorithm concludes that the blockchain integrity has been compromised.
- For each block (except the target block), it calculates the hash of the link state data and compares it to the stored hash in the block. If they do not match, the data integrity audit fails.
- If all checks pass, the data integrity audit is successful.

Algorithm: Data Integrity Auditing

```
Input: - Blockchain: The blockchain to be audited
       - Target_Block_Index: The index of the Target_Block to audit
       - Expected_Data: The Expected_Data for the Target_Block
Output: - Audit_Result: Whether the data integrity audit passed or failed

Procedure: PerformDataIntegrityAudit(Blockchain, Target_Block_Index, Expected_Data):
    If Target_Block_Index < 0 or Target_Block_Index >= Length(Blockchain):
        Return "Invalid Target_Block_Index"
    End If

    Target_Block = GetBlockByIndex(Blockchain, Target_Block_Index)

    If HashFunction(Expected_Data) != Target_Block.Link_state Data Hash:
        Return "Data integrity audit failed"
    End If

    For each block in Blockchain from Target_Block_Index + 1 to last block:
        Previous Block = GetBlockByIndex(Blockchain, block.Index - 1)
        If block.PreviousHash != Previous Block.BlockHash:
            Return "Blockchain integrity compromised"
        End If

        If block.Index == Target_Block_Index:
            Continue
        End If

        If HashFunction(block.Link_state Data) != block.Link_state Data Hash:
            Return "Data integrity audit failed"
        End If
    End For
        Return "Data integrity audit passed"
Main:
    Read the Blockchain
    Read Target_Block_Index
    Read Expected_Data
    Audit_Result = PerformDataIntegrityAudit(Blockchain, Target_Block_Index, Expected_Data)
    Print Audit_Result
End Main
```

This algorithm ensures data integrity auditing within a blockchain by verifying the consistency of data in the target block and checking the integrity of the entire blockchain. If any discrepancies are found during this audit process, it indicates potential errors or tampering within the blockchain, thus helping to maintain the reliability and trustworthiness of the data stored in the system.

Implementing data integrity auditing for distributed-control intersection networks using blockchain can offer several benefits:

- Data Consistency: Blockchain's immutability ensures that data remains consistent and trustworthy across all components.

- Enhanced Security: Blockchain's cryptographic mechanisms make data tampering extremely difficult.
- Interoperability: Different components can work together while relying on a common source of truth provided by the blockchain.
- Real-time Auditing: Auditing processes can be automated and performed in real-time, minimizing the risk of errors going undetected.

V. Simulation Results and Discussion

In this section, we provide a detailed overview of the implementation of our proposed blockchain-based method for ensuring the integrity of shared data in a distributed-control intersection network. The implementation was carried out using a combination of software tools, programming languages, and blockchain frameworks.

As shown in Fig. 5, our implementation follows a layered architecture, comprising the following components:

1) Simulation of urban traffic: To simulate various traffic scenarios we use AnyLogic software [26]. AnyLogic is a java-based simulation software used for modeling and analyzing complex systems, including urban traffic.

2) Distributed control system: To develop the distributed control system we use agent-based modeling feature in AnyLogic, which allows to define the agent types, properties, and behaviors.

3) Blockchain network: We utilized the Ethereum blockchain due to its established infrastructure and support for smart contracts. The blockchain network stores transaction data, including link state, network meta-data, and validation mechanisms.

4) Results extraction: The results extraction phase involves collecting data generated from simulation runs. This data is captured at designated points within the model. To evaluate our approach (method-2), we will compare it with a distributed control system without blockchain (method-1).

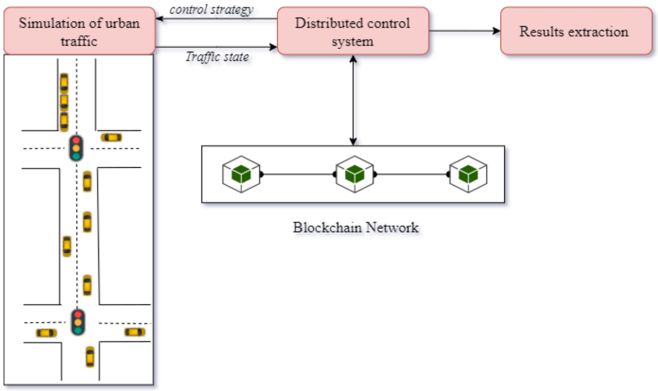

Fig. 5. Process simulation.

We will use four scenarios that collectively help assess the blockchain-based method's effectiveness across varying levels of communication network state and in the face of system failure.

- Scenario 1: Low Network Communication state: In this scenario, the network experiences a situation of low communication bandwidth and high latency. The data exchanges between IGCs, agents, and the blockchain nodes are slow and sporadic. Transactions take longer to propagate through the network, causing delays in data integrity verification and confirmation. This scenario tests the resilience of the blockchain-based method under adverse network conditions and assesses its ability to process and verify transactions with limited bandwidth and high latency. Without a blockchain, a low network communication state might lead to difficulties in transaction verification and data sharing.
- Scenario 2: Medium Network Communication state: Under medium network communication conditions, the network is relatively stable with moderate communication bandwidth and latency. Data exchanges occur at a reasonable pace, allowing transactions to propagate and confirm without significant delays. This scenario aims to evaluate the blockchain's performance under typical operational network conditions, assessing whether the method can efficiently maintain data integrity and transaction consistency. Without blockchain, medium network communication might be more manageable than in a low state, but challenges like data consistency and reliance on intermediaries for verification could arise.
- Scenario 3: High Network Communication state: In a high network communication scenario, the network experiences heavy congestion and high communication demands. Data exchanges between ICG, agents, and blockchain nodes are frequent and rapid. This situation challenges the system's capacity to handle a large volume of transactions without compromising its integrity. The blockchain's ability to handle high transaction throughput and maintain data consistency is assessed, along with its ability to handle potential network bottlenecks. In a high network communication state, non-blockchain systems may struggle to maintain data consistency and handle the influx of real-time transactions.
- Scenario 4: System Failure: In the event of network communication failure, a blockchain system can continue to function locally on ICG. Once communication is restored, the system can automatically synchronize and reconcile the distributed ledger, ensuring data integrity and minimizing the risk of data loss. Network communication failure in a non-blockchain system could lead to data discrepancies, conflicts, and potentially control system failure.

By simulating and analyzing these scenarios involving different network communication state (see Fig. 6) we can gain a comprehensive understanding of how the blockchain-based method performs under various levels of network stability. In summary, blockchain technology offers advantages like decentralization and stability in various network communication scenarios. However, its effectiveness depends on factors such as the specific use case, network conditions, and the degree of decentralization required. Non-blockchain systems might suffice for certain situations.

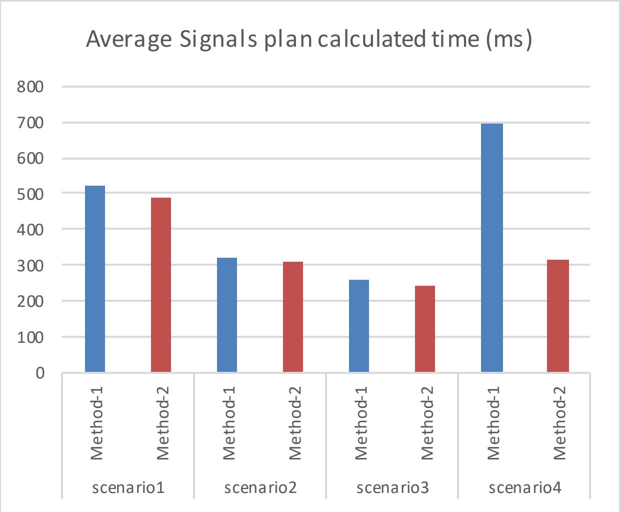

Fig. 6. Average signals plan calculated time.

In the following section, we explore a series of diverse scenarios that cover different urban traffic contexts and situations. These scenarios have been carefully selected to provide relevant examples of concrete traffic situations.

Scenario 1: Low Traffic Condition: In this scenario, the intersection network experiences a period of low traffic. The number of vehicles approaching the intersection is minimal, resulting in infrequent data updates and interactions.

Scenario 2: Medium Traffic Condition: In a medium traffic scenario, the intersection network encounters a moderate volume of vehicles during peak hours.

Scenario 3: High Traffic Condition: During high traffic conditions, the intersection network experiences heavy congestion with a significant influx of vehicles from various directions. This scenario pushes the limits of the system's capacity.

By simulating and analyzing these scenarios, we can gain insights into the system's strengths, weaknesses, and areas for improvement, thereby refining the control of distributed intersection network under a range of conditions.

Fig. 7 presents the average intersection throughput in PVU (Private Vehicle Unit) per hour. The graph shows that the effectiveness of blockchain in ameliorating average intersection throughput depends on congestion levels. While blockchain may not have a direct impact on the low congestion level, it could enhance the average intersection throughput in the medium and high traffic conditions by improving data access speed, collaboration, and coordination among various intersections, potentially contributing to more efficient traffic management and better throughput over time.

As shown in Fig. 8 the response latency of both methods follows a linear trend as the level of congestion increases. The proposed system achieves a latency between 1.22 and 1.83, while the traditional system achieves a latency between 1.32 and 1.95.

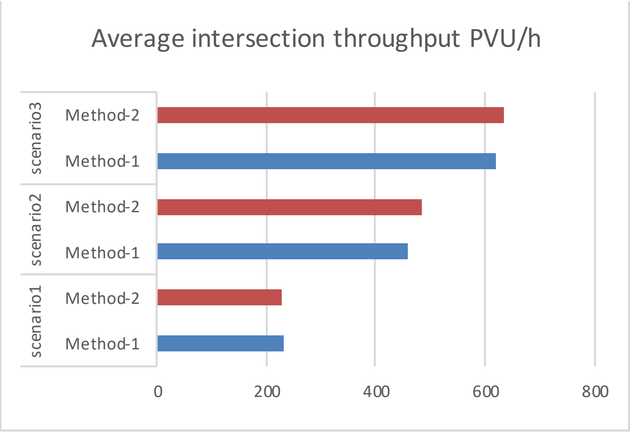

Fig. 7. Average intersection throughput.

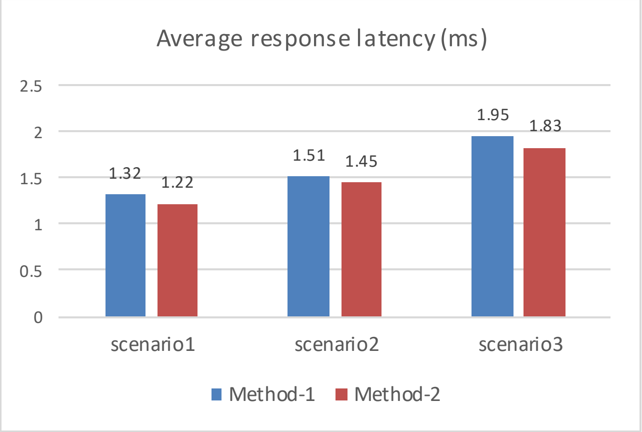

Fig. 8. Average response latency.

Table I shows a comparison of security features between centralized, decentralized and blockchain-based systems:

TABLE I. SECURITY FEATURES COMPARISON BETWEEN CENTRALIZED, DECENTRALIZED AND BLOCKCHAIN-BASED SYSTEM

	Centralized-based system	Decentralized-based system	Blockchain-based system
Decentralization	-	++	++
Traceability	-	-	++
Data integrity	-	+	++
Data availability	-	+	++
Verifiability and auditability	-	+	++
Immutability	-	+	++
Transparency	-	+	++

Centralized systems can compromise data integrity if controlled by a single entity with malicious intent. Decentralized systems mitigate this risk by requiring consensus, and blockchain-based systems, with cryptographic verification and immutability, offer the highest assurance of data integrity. Furthermore, centralized systems' availability hinges on the central entity's stability, which can lead to disruptions. Decentralized systems, sharing data across nodes, increase availability, while blockchain-based systems exhibit resilience, even when ICGs go offline, ensuring continuous data availability.

In summary, centralized systems might compromise security, whereas decentralized and blockchain-based systems enhance security through decentralization, data integrity, availability, auditability, immutability, and transparency. While each approach has its strengths and limitations, blockchain-based systems exhibit comprehensive security features, making them particularly well suited for applications where trust and security are paramount.

VI. Conclusion

In conclusion, the research presented in this paper demonstrates the significant potential of utilizing blockchain technology to enhance the integrity and efficiency of shared data within a distributed-control intersection network. The implementation of a blockchain-based method has been shown to address the challenges associated with data integrity, trust, and transparency in this critical context. By leveraging the decentralized and immutable nature of blockchain, the proposed approach offers a robust solution for ensuring the authenticity and consistency of data exchanged among various intersection nodes.

The results of our experiments indicate that the blockchain-based method not only enhances the overall security posture of the intersection network but also contributes to the efficient management of the road traffic, reducing the risk of unauthorized modifications and data tampering. The blockchain records the history of intersection link states, therefore the use of the blockchain is essential in the event of an intersection system failure, so that the new signals plan of the intersection can be calculated based on the data previously stored in the blokchain, thereby streamlining the decision-making process in the distributed-control system.

It is worth noting that while this paper primarily focuses on the application of blockchain in a distributed-control intersection network, the concepts and insights presented herein have broader implications for other decentralized and data-sensitive systems. Future research could explore scalability and performance optimization, as well as real-world deployment and integration of the proposed solution. As the adoption of blockchain technology continues to expand, the findings of this study contribute to the advancement of secure and trustworthy data sharing in distributed systems, paving the way for safer and more efficient urban traffic management and beyond.

References

[1] M. Obaidat, M. Khodjaeva, J. Holst, and M. Ben Zid, “Security and privacy challenges in vehicular Ad Hoc networks,” Connect. Veh. Internet Things Concepts, Technol. Fram. IoV, pp. 223–251, Jan. 2020, doi: 10.1007/978-3-030-36167-9_9/COVER.

[2] J. A. Guzman, G. Pizarro, and F. Nunez, “A Reinforcement Learning-Based Distributed Control Scheme for Cooperative Intersection Traffic Control,” IEEE Access, vol. 11, pp. 57037–57045, 2023, doi: 10.1109/ACCESS.2023.3283218.

[3] A. Ikidid, M. El Ghazouani, Y. El Khanboubi, C. A. Zaouiat, A. El Fazziki, and M. Sadgal, “A New Approach to Intelligent-Oriented Analysis and Design of Urban Traffic Control: Case of a Traffic Light,” Lect. Notes Networks Syst., vol. 637 LNNS, pp. 217–230, 2023, doi: 10.1007/978-3-031-26384-2_20/COVER.

[4] M. Javaid, A. Haleem, R. Pratap Singh, S. Khan, and R. Suman, “Blockchain technology applications for Industry 4.0: A literature-based review,” Blockchain Res. Appl., vol. 2, no. 4, p. 100027, Dec. 2021, doi: 10.1016/J.BCRA.2021.100027.

[5] N. Satoshi and S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic cash system,” Bitcoin, 2008, doi: 10.1007/s10838-008-9062-0.

[6] K. Nellore and G. P. Hancke, “A survey on urban traffic management system using wireless sensor networks,” Sensors (Switzerland), vol. 16, no. 2, 2016, doi: 10.3390/s16020157.

[7] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, “Blockchain-based decentralized trust management in vehicular networks,” IEEE Internet Things J., vol. 6, no. 2, pp. 1495–1505, 2019, doi: 10.1109/JIOT.2018.2836144.

[8] A. Daeichian and A. Haghani, “Fuzzy Q-Learning-Based Multi-agent System for Intelligent Traffic Control by a Game Theory Approach,” Arab. J. Sci. Eng., vol. 43, no. 6, pp. 3241–3247, Jun. 2018, doi: 10.1007/S13369-017-3018-9/METRICS.

[9] A. Ikidid, A. El Fazziki, and M. Sadgal, “A fuzzy logic supported multi-agent system for urban traffic and priority link control,” J. Univers. Comput. Sci., vol. 27, no. 10, pp. 1026–1045, 2021, doi: 10.3897/jucs.69750.

[10] T. Rauter, “Integrity of Distributed Control Systems,” Student Forum Int. Conf. Dependable Syst. Networks, pp. 1–4, 2016.

[11] Q. Kong, R. Lu, M. Ma, and H. Bao, “A privacy-preserving sensory data sharing scheme in Internet of Vehicles,” Futur. Gener. Comput. Syst., vol. 92, pp. 644–655, 2019, doi: 10.1016/j.future.2017.12.003.

[12] G. P. Joshi, E. Perumal, K. Shankar, U. Tariq, T. Ahmad, and A. Ibrahim, “Toward blockchain-enabled privacy-preserving data transmission in cluster-based vehicular networks,” Electron., vol. 9, no. 9, pp. 1–15, 2020, doi: 10.3390/electronics9091358.

[13] J. Cui, F. Ouyang, Z. Ying, L. Wei, and H. Zhong, “Secure and Efficient Data Sharing Among Vehicles Based on Consortium Blockchain,” IEEE Trans. Intell. Transp. Syst., vol. 23, no. 7, pp. 8857–8867, 2022, doi: 10.1109/TITS.2021.3086976.

[14] S. Kudva, S. Badsha, S. Sengupta, I. Khalil, and A. Zomaya, “Towards secure and practical consensus for blockchain based VANET,” Inf. Sci. (Ny)., vol. 545, pp. 170–187, 2021, doi: 10.1016/j.ins.2020.07.060.

[15] S. Asadi Bagloee, M. Tavana, G. Withers, M. Patriksson, and M. Asadi, “Tradable mobility permit with Bitcoin and Ethereum – A Blockchain application in transportation,” Internet of Things, vol. 8, p. 100103, Dec. 2019, doi: 10.1016/J.IOT.2019.100103.

[16] I. M. Varma and N. Kumar, “A comprehensive survey on SDN and blockchain-based secure vehicular networks,” Veh. Commun., vol. 44, p. 100663, Dec. 2023, doi: 10.1016/J.VEHCOM.2023.100663.

[17] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, “Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles,” IEEE Commun. Mag., vol. 56, no. 10, pp. 50–57, Oct. 2018, doi: 10.1109/MCOM.2018.1800137.

[18] P. M. Dhulavvagol, V. H. Bhajantri, and S. G. Totad, “Blockchain Ethereum Clients Performance Analysis Considering E-Voting Application,” Procedia Comput. Sci., vol. 167, pp. 2506–2515, Jan. 2020, doi: 10.1016/J.PROCS.2020.03.303.

[19] U. Tariq, A. Ibrahim, T. Ahmad, Y. Bouteraa, and A. Elmogy, “Blockchain in internet-of-things: a necessity framework for security, reliability, transparency, immutability and liability,” IET Commun., vol. 13, no. 19, pp. 3187–3192, Dec. 2019, doi: 10.1049/IET-COM.2019.0194.

[20] J. Sedlmeir, J. Lautenschlager, G. Fridgen, and N. Urbach, “The transparency challenge of blockchain in organizations,” Electron. Mark., vol. 32, no. 3, pp. 1779–1794, 2022, doi: 10.1007/s12525-022-00536-0.

[21] C. Schinckus, “Proof-of-work based blockchain technology and Anthropocene: An undermined situation?,” Renew. Sustain. Energy Rev., vol. 152, p. 111682, Dec. 2021, doi: 10.1016/J.RSER.2021.111682.

[22] M. Wendl, M. H. Doan, and R. Sassen, “The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review,” J. Environ. Manage., vol. 326, p. 116530, Jan. 2023, doi: 10.1016/J.JENVMAN.2022.116530.

[23] H. Han, S. Fei, Z. Yan, and X. Zhou, “A survey on blockchain-based integrity auditing for cloud data,” Digit. Commun. Networks, vol. 8, no. 5, pp. 591–603, Oct. 2022, doi: 10.1016/J.DCAN.2022.04.036.

[24] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, “Blockchain smart contracts: Applications, challenges, and future trends,” Peer-to-Peer Netw. Appl., vol. 14, no. 5, pp. 2901–2925, Sep. 2021, doi: 10.1007/S12083-021-01127-0/FIGURES/4.

[25] R. Zhang, R. Xue, and L. Liu, “Security and privacy on blockchain,” ACM Comput. Surv., vol. 52, no. 3, p. 51, Jul. 2019, doi: 10.1145/3316481.

[26] “AnyLogic for Academia – AnyLogic Simulation Software.”