Using Blockchain in Privacy-Oriented Networking

Preet Chodavadia
Fisher College of Science and Mathematics
Towson University
Towson, United States
pchodav1@students.towson.edu

Legendre Cooper
Fisher College of Science and Mathematics
Towson University
Towson, United States
lcoope16@students.towson.edu

Nathan Ketterlinus
Fisher College of Science and Mathematics
Towson University
Towson, United States
nketter1@students.towson.edu

Owen Segala
Fisher College of Science and Mathematics
Towson University
Towson, United States
Osegala1@students.towson.edu

Kevin Yomba
Fisher College of Science and Mathematics
Towson University
Towson, United States
kyomba1@students.towson.edu

***Abstract*—Blockchain technology is widely known for its use in cryptocurrencies like Bitcoin and Ethereum. At its core, it is a distributed ledger, appended to by a consensus mechanism agreed upon by members of a network. Content on a blockchain is effectively immutable, and transparent to all members of the network, while maintaining the privacy of members involved in any particular transaction. This paper investigates the application of blockchain technology in the wider context of data networking. Of interest are blockchain applications in the Internet of Things (IoT) and in vehicle automation. While investigating these domains, interest is paid to how blockchain solves traditional issues of data integrity and security, privacy preservation, and authentication mechanisms. To accomplish this, we consider how the blockchain can be leveraged to offer secure data exchange in the IoT, peer-to-peer (P2P) Networking, and distributed data storage. As a conclusion, we establish that blockchain technology has significant promise in the future of networking as a robust, secure paradigm for communication.**

Keywords—Blockchain, consensus mechanism, IoT, data integrity, privacy, 5G, P2P, networking

I. Introduction

Many modern networking problems are closely related to issues of data integrity, privacy preservation, and user authentication. The technology behind the same blockchain that powers cryptocurrencies like Bitcoin and Ethereum can be leveraged to solve a lot of these key issues in novel ways that do not significantly sacrifice performance. This is critically important in scenarios where real-time communication is important. This paper examines how blockchain can be used in networking to address the problems listed above. It begins by defining what a blockchain is as well as discussing various strengths that the framework has to offer as a form of P2P communication. This is followed by examining its applications in IoT scenarios, as well as in vehicular networks, both in car-to-car communication and on an infrastructural level by examining blockchain enabled "smart" intersections. By the end of the paper, the reader should have a comprehensive understanding of how blockchain technology can be used in these scenarios, and how the inherent properties of blockchain can apply to a more general set of networking problems.

II. Background - What is a Blockchain?

The term Blockchain likely conjures images of cryptocurrencies like Bitcoin, as well as massive arrays of GPUs being used to "mine" them in an obfuscated process that seems to accomplish nothing but use enormous amounts of electricity and drive the price of consumer-grade GPUs through the roof. While this may be the unfortunate reputation that the blockchain has, the technology that drives it is built in such a way that is fundamentally better equipped to solve many modern networking problems than many traditional solutions. This section serves as a primer to these networking discussions by defining what a blockchain is and how it works.

A. Taxonomy of a Blockchain

At its core, a blockchain is simply a publicly available ledger. The ledger records every transaction between members of the blockchain (or network) and distributes this transactional information to all other members of the network in units called blocks, as shown in Fig. 1.

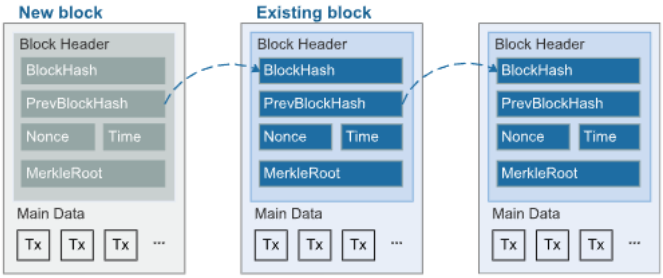

Fig. 1. Illustration of a chain of blocks. Tx stands for transaction [1].

The biggest selling point of this model is its decentralization, with no one authority auditing transactions or tampering with the chain. Instead, new nodes can only be appended to the end of a blockchain (like a linked list), and consensus on what to add is achieved by all members of the network through one of several consensus mechanisms, the most well-known being Proof-of-Work (PoW) and Proof-of-Stake (PoS). With this core idea of decentralization and consensus in mind, benefits of the blockchain become readily apparent, such as:

- Decentralization: transaction records are stored in a P2P network. Since there is no central controller, there is

also no bottleneck on the network from said central controller.

- Transparency: Every node has access to the blockchain's complete ledger. This gives the blockchain credibility as an accurate source of current transactions.
- Immutability: All blocks on the chain are irreversible and immutable unless one person controls >50% of voters. As networks get larger, attacks like this quickly become improbable.
- Security: Each transaction is broadcast, checked, validated, and linked by nodes across the network. Any tampering is easily detected, and thus strongly discouraged.
- Auditability: Any network member can iterate through the entire transaction history with timestamps associated with each transaction. This becomes incredibly relevant when proofreading a blockchain for tampering and following resources through a chain.
- Autonomy: Each node sends and receives transactions independently through consensus mechanisms and public/private key pairs. This eliminates the need for human interaction and third-party auditors (like a central controller). It also necessarily prevents conflicting or double records in the blockchain.
- Pseudonymity: Network nodes are typically given a pseudonym address to avoid identity exposure. This allows blockchain technology to be used in spaces that demand high privacy.

These benefits are described in much more detail in [1], although the descriptions provided here are adequate for the forthcoming conversations. Blockchains have clear advantages in networking. Decentralization allows for enormous performance gains over traditional designs when implemented properly. Immutability and pseudonymity are also cornerstones of data and user security in any network setting.

However, the main drawback of conventional blockchains is the energy used in the consensus mechanism. PoW consensus has nodes calculating (mining) potential hash values for each new transaction until a hash equal to or smaller than a given target is found [1]. Two big issues with this should be obvious: Firstly, as target hash values get smaller, computation time quickly becomes infeasible for real time communication, and associated electricity use dramatically increases. Secondly, nodes in this system must be incentivized to mine in some way. Bitcoin awards the miner that discovers the correct hash with currency, but this structure may not translate to other use cases as well. This example highlights flaws with PoW, but every consensus mechanism has problems. There have been strides in recent years in developing more mature mechanisms, and the issue is now one of selecting the right mechanism for the job.

For the sake of completeness, one last aspect of blockchains must be addressed before investigating their operation. Blockchains exist as one of three categories: public, private, or consortium. Differences between the three are covered in Table I, as defined in [1].

A complete visualization of a typical blockchain's architecture is shown in Fig. 2.

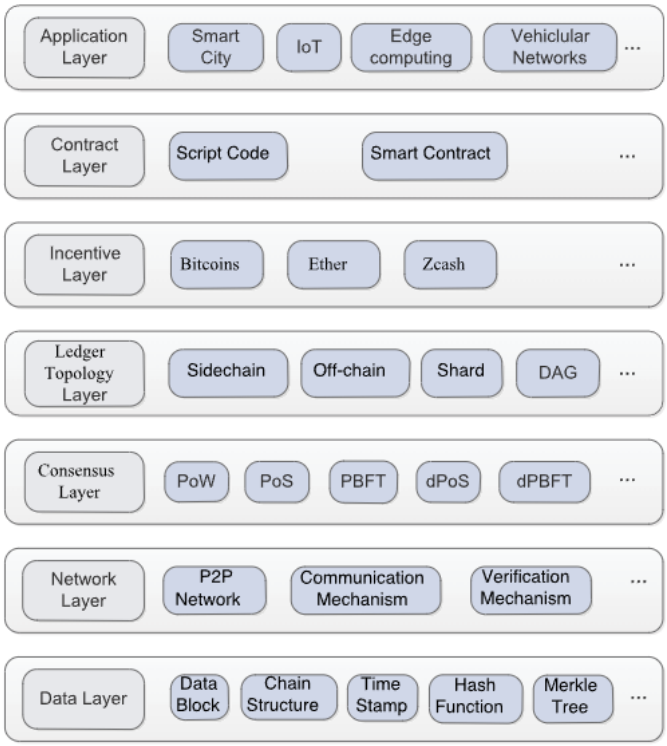

Fig. 2. A general architecture of blockchain [1].

B. *Function of a Blockchain*

With such an extensive definition of what a blockchain is, we now describe the process by which a blockchain operates. A lot of the details were mentioned in the previous section, so the discussion here is abridged.

Every time two members of the blockchain network want to transact, that transaction is broadcasted to every other node in a P2P fashion. The nodes validate the transaction with the selected consensus mechanism. Once verified, the completed block is then added to the blockchain, and every node's local copy of the ledger is updated. This process is visualized in Fig. 3.

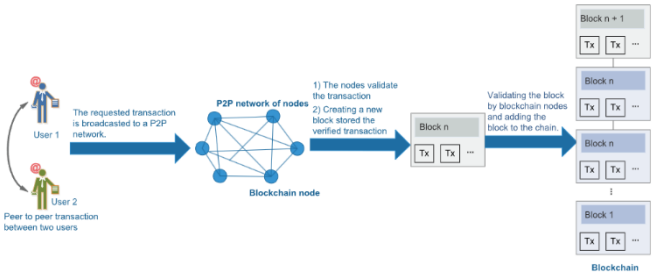

Fig. 3. A typical processing procedure of blockchain network [1]

III. Applications in IoT

Blockchain technology has the potential to revolutionize how devices interact within the IoT ecosystem. It is able to provide pragmatic solutions to problems like data integrity, privacy, and security. Due to the decentralized nature of the blockchain itself, it assures that no single point of failure exists like in traditional methods, like cloud computing, while its

immutable ledger securely records interactions between devices to prevent unauthorized tampering of data throughout the IoT [2].

A. Data Integrity and Authentication

Data integrity is one of the prime concerns in IoT networks, where millions of devices generate and communicate data across large-scale networks. Blockchain provides a secure framework for maintaining data integrity by recording all transactions and communications on a distributed ledger. Liu et al. proposed a framework where the immutability of the blockchain could be utilized to ensure verification against IoT data modifications or unauthorized changes [1]. This method is useful when the IoT devices are in an environment that is susceptible to, for example, replay and man-in-the-middle attacks.

B. Data Collection and Exhange in 5G-Enabled IoT

Karim et al. proposes a blockchain-based secure Data Collection and Exchange scheme, namely BSDCE-IoV, in 5G IoT environments. In this model, the IoT devices can securely communicate by encrypting data before transmission and verifying each exchange via the consensus mechanism of the blockchain [3]. This BSDCE-IoV scheme also allows support for privacy preservation by anonymizing device identities. This ensures that even when the data is publicly accessible, the device's identities remain secure.

C. Integration of Edge Computing

With the integration of the blockchain into IoT, we can see edge computing take place, which is where data processing occurs near the source, reducing latency and enhancing real time decision-making. Liu et al. suggests that edge devices can serve as nodes in a blockchain network, participating in consensus and maintaining a copy of the ledger. Such a configuration allows IoT networks to handle a large volume of transactions without the risk of data overload into central servers [1].

IV. Applications in Vechicular Networks

Modern day road systems provide a great analog for examining various aspects of networking. Specifically, many concepts in one domain extend to the other through graph theory. With this critical concept in mind, we now examine two ways in which the blockchain is being implemented in road networks: in vehicle-to-vehicle communication (i.e., P2P), as well as in developing "smart" intersections, which dynamically adapt to the needs of the road.

A. Vehicle-to-Vehicle communication

In real world scenarios, vehicle-to-vehicle (V2V) communication seems like an insurmountable problem. How should a network go about handling such a dynamic system where nodes are joining and leaving the network at such a rapid rate? How does one define where one network ends and another network starts? Is there a mechanism that lets all cars communicate and receive what they need in real time? These questions are critical to answer because the stakes in such an environment are so high. A slight mistake can have disastrous consequences, such as collisions and increased traffic, data discrepancies, conflicts, and potentially control system failure in traditional smart systems [3].

In this section, we examine a blockchain based solution proposed in [3] to these problems. It builds upon existing work to construct a paradigm where cars can communicate with the blockchain center through trusted roadside units (RSUs), which communicate with each other. These RSUs can then communicate with control rooms (CRs), who interact with a central registration authority (RA). CRs and the RA work together to register vehicles currently on the network, as well as those attempting to join it. This relationship is diagrammed in Fig. 4. Note that the RA is critical to data integrity and user privacy, as it ensures all members using the network are registered and held accountable for their transactions.

TABLE I.

COMPARISONS AMONG PUBLIC BLOCKCHAIN, PRIVATE BLOCKCHAIN, AND CONSORTIUM BLOCKCHAIN [1]

Property	Public blockchain	Private blockchain	Consortium blockchain
Participants	Free Anonymous, could be malicious	Permissioned Identified and trusted	Permissioned Identified and trusted
Consensus determination	All miners	One organization	Selected set of nodes
Read permission	Public	Public or restricted	Public or restricted
Immutability	Yes	Partial	Partial
Efficiency	Low	High	High
Centralized	No	Yes	Partial
Consensus process	Permissionless	Permissioned	Permissioned

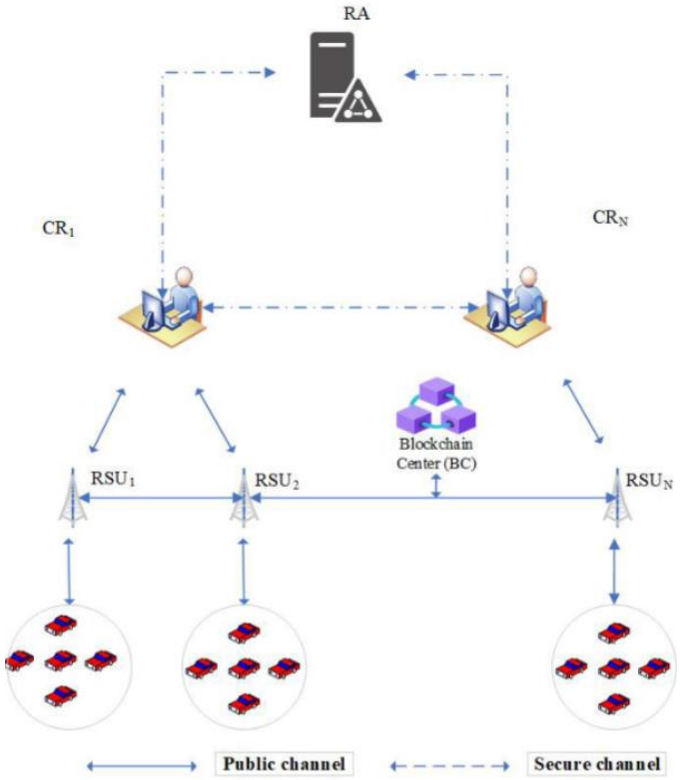

Fig. 4. IoV component registration [3].

Because access to the Blockchain is delegated through RSUs, the system is made secure by nature of being a private blockchain. For someone to attack the network, they would have to interfere directly with an unfeasible amount of RSUs simultaneously. Furthermore, the system is resilient to several types of cyber-attacks, such as: replay attacks, Man-in-the-Middle attacks, vehicle impersonation attacks, impersonation attack of RSU, Sybil attacks, and GPS attacks [3].

As for time complexity, the advent and widespread adoption of 5G technology, as well as a continual increase in available computing power makes this framework one that could function fast enough to be considered real-time. [3] reports this framework achieving round-trip communication between vehicles and RSUs in as little as 16.484 ms, with each block able to contain 3 messages with an average total cost of just 2240 bits. With such low overhead, this model highlights how blockchain technology can be leveraged to provide real time communication in such demanding environments, while maintaining data integrity and user privacy in a P2P setting.

B. Blockchain Enabled Intersections

After analyzing blockchain's applications on the vehicular level, we now pivot to examine its uses in the higher level of intersections of traffic networks. With a well-coordinated network of intersections, the possibility of more efficient traffic flow and faster commutes opens. The biggest challenges with such a system, however, are again related to data security and integrity. If one bad actor could modify the data that the network was accessing, congestion could rapidly become catastrophic, and accidents could occur. By leveraging blockchain's strengths of transparency, autonomy, and immutability, [4] proposes a framework for a blockchain-enabled network of intersections that significantly improves data security, while providing comparable performance to traditional smart intersections. A visual summary of this implementation is provided in Fig. 5.

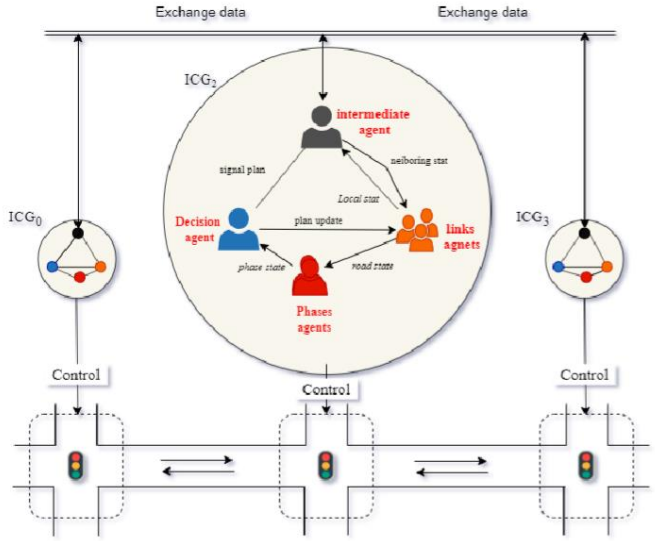

Fig. 5. Overview of distributed-control intersection network [4].

The key points are that local intersections can query their copy of the blockchain to gather the state of their part of the road network. Once this state is gathered, the intersection control group (ICG) for that intersection can determine how to control itself. This data is then codified into a block with a timestamp and a hash, and then added to the blockchain. A not-so-obvious advantage of this system is that in the unlikely event of a node failure, the ICG can simply recover its state by querying recent events in the blockchain, and resume operation as normal. Additionally, included hases ensure that the sytem can detect any tampering with blocks, and course correct around them. As for latency, [4] finds that this system can operate with an average response time of less than 2 ms.

V. Discussion

After examining applications of blockchain in secure, real-time communication scenarios, we now examine how it differs from traditional networking solutions. Holistically, the biggest difference is blockchain's decentralization. Consider a messaging application that uses a traditional centralized server to allow clients to communicate with each other. Companies that provide such servers are burdened with protecting their user's data. Clearly, there is an inherent risk of data theft, scraping, brokerage or leakage by the central server, and unauthorized, possibly malicious actors outside the network may be able to view logged messages stored on the server if they attack it properly. With an analogous application that uses the blockchain to send, receive, and store messages between users, many of these issues quickly disappear. With no centralized server storing messages, there is no third to scrape, steal, or broker a user's data in the first place. The blockchain's core properties of transparency, immutability, and auditability make tampering with messages infeasible for a malicious actor in the network. As addressed earlier, blockchain networks are resistant to tactics like replay attacks, Man-in-the-Middle attacks, Sybil attacks, and others, by design, especially on

larger networks. For these reasons blockchain has significant merit for a mode of communication between privacy-oriented individuals. Note that on private blockchains, for an external attacker to gain access to data stored on the blockchain, they would have to either join the network or steal a physical device that is a member. While this is possible, it is also an example of a social engineering attack common to all communication systems. Additionally, blockchain's core feature of pseudonymity adds another layer of identity security, so that even if data is leaked, people's identities can still be hidden should they desire.

Comparing blockchain networking to traditional peer-to-peer networking reaches a similar conclusion as when compared to a server-based architecture. While the benefits of decentralization are common to both P2P and blockchain networks, blockchain provides extra security with minimal overhead, assuming an appropriate consensus mechanism is selected. To reiterate, decentralization removes the "weakest link" of a centralized server, transparency, immutability, and auditability ensures exchanged messages are tamper-proof and exactly what is intended to be received, and security and pseudonymity ensures shared data and information is seen only by those authorized to see it.

VI. Conclusion

This paper highlights the potential of blockchain technology as a robust solution to longstanding challenges in data networking, particularly in IoT scenarios and in vehicular networks. By leveraging blockchain's strengths, like decentralization, immutability, security, and pseudonymity, solutions are offered to address issues related to data integrity, privacy, and authentication. Through the examples of IoT and vehicle-to-vehicle communication, as well as blockchain-enabled traffic intersections, we observe how blockchain can enhance network efficiency and security in both individual and larger-scale applications. Although challenges remain, such as consensus mechanism inefficiencies, blockchain's versatility suggests promising pathways to integrate it with next-generation networking technologies like 5G. These findings highlight the transformative potential of blockchain beyond cryptocurrency, positioning it as a valuable tool for secure, efficient, and scalable data communication and management across varied networked environments.

References

[1] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. Leung, "Blockchain and machine learning for communications and Networking Systems," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1392–1431, 2020. doi:10.1109/comst.2020.2975911

[2] S. M. Karim, A. Habbal, S. A. Chaudhry, and A. Irshad, "BSDCE-Iov: Blockchain-based Secure Data Collection and Exchange Scheme for Iov in 5G environment," *IEEE Access*, vol. 11, pp. 36158–36175, 2023. doi:10.1109/access.2023.3265959

[3] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based Data Integrity Service Framework for IOT data," *2017 IEEE International Conference on Web Services (ICWS)*, Jun. 2017. doi:10.1109/icws.2017.54

[4] M. E. Ghazouani *et al.*, "A blockchain-based method ensuring integrity of shared data in a distributed-control intersection network," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 10, 2023. doi:10.14569/ijacsa.2023.014105