Article

Technological Aspects of Blockchain Application for Vehicle-to-Network

Vasiliy Elagin [1], Anastasia Spirkina [1], Mikhail Buinevich [2, 3] and Andrei Vladyko [2, *]

[1] Infocommunication Systems Department, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Prospekt Bolshevikov 22-1, Saint Petersburg 193232, Russia
[2] R&D Department, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Prospekt Bolshevikov 22-1, Saint Petersburg 193232, Russia
[3] Department of Applied Mathematics and IT, Saint-Petersburg University of State Fire Service of Emercom of Russia, Moskovskiy prospekt 149, Saint Petersburg 196105, Russia
* Correspondence: vladyko@sut.ru

Abstract: Over the past decade, wireless communication technologies have developed significantly for intelligent applications in road transport. This paper provides an overview of telecommunications-based intelligent transport systems with a focus on ensuring system safety and resilience. In vehicle-to-everything, these problems are extremely acute due to the specifics of the operation of transport networks, which requires the use of special protection mechanisms. In this regard, it was decided to use blockchain as a system platform to support the needs of transport systems for secure information exchange. This paper describes the technological aspects of implementing blockchain technology in vehicle-to-network; the features of such technology are presented, as well as the features of their interaction.

Keywords: V2X; vehicle-to-network; blockchain; distributed registry; data protection; network; decentralized systems

1. Introduction

Today, due to high urbanization and a steady increase in the number of cars per capita, there are problems associated with the specifics of road networks. Fortunately, new technologies and systems have been developed that can radically change our way of life, and one example is intelligent transport systems. Intelligent transportation systems (ITS) use information and communication technologies to optimize traffic in major cities instead of expanding the physical infrastructure, which saves money, improves living standards, ensures safety, and reduces the environmental impact [1]. One of the most significant features is the tendency to reduce the number of fatalities and injuries in traffic accidents.

The potential of such systems lies in the organization of services for the management of road infrastructure facilities, which is a priority that should help reduce the saturation of the road network. Such systems will significantly improve people’s quality of life and will become a reality in the near future. The modern development of transport networks and their importance for public infrastructure lead to the development of vehicle-to-everything.

There may be different types of vehicle communication networks depending on the participants exchanging data. Networks of mobile nodes, which are strictly moving vehicles communicating with each other, are called vehicle-to-vehicle (V2V). Vehicle-to-infrastructure (V2I) or vehicle-to-pedestrian (V2P) networks are formed when moving vehicles interact with either roadside infrastructure or pedestrians. If a vehicle interacts with IT networks and/or data centers, the network type becomes vehicle-to-network (V2N). The general term that unites all of these types of communications, providing communication of vehicles with various recipients, is called vehicle-to-everything (V2X) [2].

Vehicle-to-everything consists of infocommunication technologies aimed at improving the safety and efficiency of road traffic. This is due to the exchange of information between the objects of the system from a vehicle to any object that can affect the vehicle, and vice versa [3,4].

A feature of such networks is decentralization. V2X networks are characterized by a dynamic topology change due to frequent user changes that form short-term connections.

Vehicle-to-everything networks are used for:

- Assistance for road users (navigation, warning of danger and road conditions, collision avoidance, maneuvering, indication of restrictions, etc.).
- Differentiation of priorities in the movement of transport of various services.

The main objective of such networks is to improve the efficiency of road traffic management and road safety.

However, along with the scale of the networks, the complexity of control over them also grows; the process of administering large heterogeneous networks requires more and more resources for correct management and monitoring of the process.

The main reasons for the problems associated with the information security of transport networks are [5]:

- A lack of means of protecting nodes from intrusions and intruders.
- The ability to listen to channels and replace messages due to the general availability of the transmission medium.
- The need to use complex routing algorithms that take into account the probability of receiving incorrect information from compromised nodes as a result of changes in the network topology.
- The impossibility of implementing a traditional security policy due to the features of the classic vehicle-to-network architecture, such as the absence of a fixed topology and central nodes.

In vehicle-to-network, the problem of ensuring information security is extremely acute due to the specifics of operating automobile networks and the importance of not interfering with third parties in the operation of the system, which requires special security arrangements.

To address these security and reliability issues, blockchain technology can be used to create new forms of distributed architectures. In this network, the components will be able to find agreement on their common state for decentralized and transactional data exchange through a large network of untrusted participants, without relying on a central point [6]. In a broader sense, blockchain is used to define the entire technological ecosystem behind the exchange of digital assets between members of the same network without intermediaries [7].

The practicality of blockchain is undeniable in everything related to data storage and authentication, which will limit all kinds of fraud.

This stage of technological development has the following benefits [8–10]: it is decentralized, so the network participants are equal; the system is reliable, since any attempt to make unauthorized changes will be rejected due to noncompliance with previous copies; data added to the system are verified by other independent participants; it is possible to check any transaction; there are theoretically unlimited records; and confidentiality is assured: with data stored in encrypted form, users can track all transactions, but cannot identify recipients or senders of the information.

The peculiarity of vehicle-to-network is that there are many users who quickly change their location and do not have high capacity. At the same time, blockchain technology may be applicable to solve the assigned tasks within the framework of ensuring security. The use of blockchain technology can qualitatively improve aspects of security in V2N networks.

This paper is structured as follows: Section 2 presents related works. Section 3 summarizes the main technical capabilities of blockchain technology. Section 4 presents the technical characteristics of the implementation of blockchain technology in vehicle-to-network, followed by an analysis of the temporal characteristics of the proposed solution. Finally, Section 5 concludes the paper, presents the findings and results, and defines the background for future work.

2. Related Works

Vehicle-to-everything strives to make the transportation system more intelligent by connecting everything with moving vehicles, but it can be subject to intrusions. A public key infrastructure (PKI)-based authentication protocol provides basic security services for automotive ad hoc networks. However, trust and privacy are still open questions due to the unique characteristics of networks. It is imperative to prevent domestic vehicles from transmitting bogus messages while maintaining the privacy of vehicles from tracking attacks. As a new security technology, blockchain can implement decentralized protection against unauthorized access. A comprehensive overview of the latest blockchain developments for future smart city scenarios along with recent industrial initiatives is discussed in [11–14].

Today, V2X technology can be implemented in various countries to improve transport infrastructure. In this regard, many researchers consider the problems associated with implementing these projects and include various solutions to improve management, as well as describe the importance of using such networks. Thus, in [15], the authors consider an approach to planning vehicles in motion, which uses current data and applies visual sensing methods. In turn, in [16], the authors explain how important vehicle-to-everything is in the management and planning of cities. The authors prove the key points of technology for large-scale vehicle route planning and intelligent traffic planning, and they also propose a multiplayer game theory algorithm for aggregating intra-cluster data by analyzing the competitive and cooperative relationships between sensor nodes. Jing et al., in their study [17], demonstrated the ability to effectively reduce congestion in urban environments to achieve the desired goals using adaptive control of traffic signals.

These works are of great importance in describing the key aspects of technology and the main problems of implementation and use. However, special attention should be given to aspects of security and networking.

Another study [18] analyzed the situation in the field of cybersecurity of wireless automotive networks (vehicular ad hoc network (VANET)) from a systemic point of view. The entire pool of known threats, localized by the objects of attack (vehicles and transport infrastructure, as well as the interface of information and technical interactions between them), are classified on the basis of genetic characteristics. The authors prove that some of the threats are generated by fundamental innovations in the VANET concept, and some are inherited from classic mobile networks.

The same authors, in [19], carried out a comparative assessment of the VANET cybersecurity indicator for three alternative methods of its construction standardized on the basis of IEEE 802.11p and Internet of Vehicles (IoV), where the first component is responsible only for high-speed road transport, and the second for transport infrastructure facilities (“world of things"). An analysis of their results shows the presence of a complex relationship between the degree of centralization of transport network management and the level of cybersecurity of applied information and telecommunication systems.

An analysis of numerous sources describing cybersecurity in VANET/ITS networks allowed the authors of [20] to compile a list of the most “popular” cyberthreats. The article also discusses the application of software-defined networking (SDN) technology to ensure cyber-resilient traffic in ITS.

A number of articles have been devoted to countermeasures against cyberattacks on VANET with a focus on authentication methods. For example, [21,22] provide overviews of threats and attacks that vehicle-to-network is exposed to, and offer solutions to protect car networks from malicious nodes and fake messages using authentication. In [23], the authors describe security and privacy issues that may affect large-scale V2N deployments and suggest solutions through the use of authentication methods. The security issue in the vehicle ad hoc network is also addressed in [24], which provides an end-to-end authentication solution and discusses a hierarchical model that concentrates on fewer message exchanges.

The use of blockchain technology to improve data protection is considered in many studies. For example, in [25], the authors prepared statistics of blockchain research in various aspects in recent years. In [26], blockchain technology is described as a highly reliable system that represents a quantum leap forward in maintaining data security. The authors show that blockchain immutability creates an enabling environment for the combination of blockchain and smart city systems. The authors of [27] considered cloud computing for data storage and computation in V2X. The authors investigate a cloud-based road condition monitoring scenario where the authorities need to monitor road conditions in real time so they can respond in a timely manner to emergency situations. The authors focus on resolving the issues of vehicle authorization, ensuring confidentiality in relation to the cloud server, and checking the source of the report. It can be seen that most of the research has been devoted to protecting information and personal data, as well as improving the quality of network services.

In order to prevent the spread of fake messages in V2I, an algorithm for assessing reputation based on both direct interactions and indirect information about cars is presented in [28]. The study ran a series of experiments to evaluate security, credibility, and performance, and the results showed that blockchain-based anonymous reputation system (BARS) can establish a model of trust with transparency, conditional anonymity, efficiency, and reliability for VANET. A proof of event consensus concept applicable to automotive networks rather than a proof of work or credentials approach is proposed in [29]. Traffic data are collected through roadside blocks, and passing vehicles check for correctness when an event notification is received. How mobility affects the performance of a blockchain system running on a dedicated car network (VANET) is explored in [30].

Nevertheless, despite studies on the topic, at this stage few solutions have been proposed that could provide the necessary level of protection for all objects of the transport infrastructure and at the same time ensure an acceptable quality of service. This study offers an alternative approach to the existing problem to ensure data protection using blockchain technology. Also, our approach determines the network scheme for working with blockchain transactions and the dependence of network characteristics on application characteristics.

3. Technical Aspects of Blockchain Technology

3.1 Introduction to technology

Blockchain protocols, which constitute a promising but still underdeveloped technology, have recently attracted a lot of interest from researchers and industry. Blockchain is a specialized information and communication technology with some specific features. It is a distributed database that consists of an ever-growing list of structured data, in which data storage and processing devices are not connected to a common server [8–10].

Currently, standardization of blockchain technology is in the drawing-board stage. However, the International Organization for Standardization established ISO/TC 307, “Blockchain and distributed ledger technologies,” and ISO/TR 23455:2019, “Blockchain technology and distributed ledgers: Review and relationship between smart contracts in blockchain and distributed ledger systems.” Also, this technology has been considered within the framework of International Telecommunication Union Telecommunications Standardization Sector (ITU-T) sessions, and Technical Report FG DLT D1.3, “Distributed ledger technology standardization landscape,” has been prepared.

Blockchain development can be divided into two main generations. The first generation is an open ledger for monetary transactions with very limited support for programmable transactions. A common application type is cryptocurrency exchange applications. The second generation has become a general programmable infrastructure [6].

3.2 Technical aspects

In blockchain technology, security is ensured through decentralization. A data register is formed, which is managed independently. The network does not rely on any central trusted authority that manages the system, as in centralized systems. Instead, trust is achieved as an emerging property from the interactions between nodes in the network.

The integrity of transactions is organized using cryptographic rules [10,20]. When the nodes of the blockchain network are synchronized, all transaction records are saved and updated on devices.

Once the nodes are loaded, they perform peer-to-peer discovery to communicate with other available nodes using TCP ports.

A node is a device on a blockchain network that allows it to function. A node can be any active electronic device that is connected to the Internet and has an IP address. There are different types of nodes depending on the functionality:

- Full nodes are clients that implement the full blockchain protocol and contain a complete copy of the ledger. Their actions include discovering and communicating with other nodes; sending, receiving, and storing blocks; and verifying transactions. A full node can autonomously validate transactions without an external reference.
- Thin nodes do not store private keys and do not sign transactions themselves. Such nodes only store the titles of blocks in their local storage. They send commands to a remote server for execution. The advantage of thin clients over other types of clients is that users do not need to constantly synchronize the entire registry to their device, and they have easy setup and minimal technical requirements.
- Miners are clients that are not used to send or receive transactions; their only use is to confirm transactions and find solution to puzzles for profit. They can act as full and light knots.
- Tracking nodes (super nodes) are the same full nodes that are public. They communicate with and provide information to any other node that decides to establish a connection with them. Such nodes operate 24/7 and have several established connections transmitting history and transaction data to other nodes around the world. Disadvantages are high processing power and good connection.

All nodes must include routing functionality to validate/propagate messages and maintain connections.

Blocks are containers that aggregate transactions. Each block is identifiable and linked to its previous block in the chain. A block is a kind of container that combines transactions for inclusion in a public ledger. It consists of a header containing metadata and a body from a list of transactions.

A transaction is a signed data structure that expresses the value to be passed. Transactions are state transitions with information about the owner (message), which include new data records and transfers between participants. Transactions were originally transfers of the value of cryptocurrency, but they can be used to transfer any kind of information. Each transaction consists of an input section and an output section that report a list of addresses and associated values, as well as a digital signature.

When a node connects to the network, neighboring blockchain nodes are detected and connected to it. Such nodes are not geographically defined and can be selected at random. The information exchange procedure within the blockchain consists of a number of messages transmitted according to certain rules. The scenario of information exchange between nodes is shown in Figure 1.

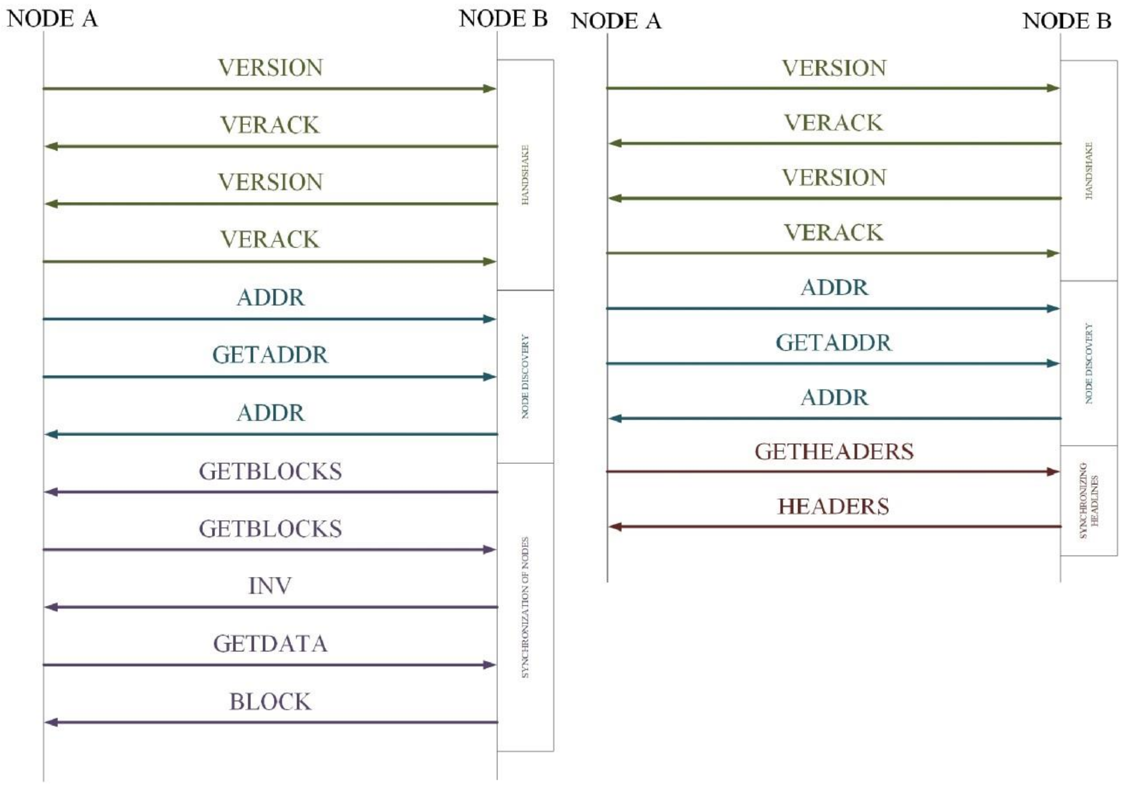

Figure 1. Data exchange scenario between full and light nodes.

The main types of messages used in the data exchange process [31] are as follows: version (to describe the version of a node), verack (to reply to a version message), addr (to provide information about the address of the current node to other known nodes), getaddr (to request information about known active nodes), getblocks (to return inv containing list blocks), inv (to distribute information about objects), getdata (to get the contents of the object), block (to respond with information about the transaction from the hash of the block), getheaders (to request the contents of the header), and headers (information about the contents of the header).

The block propagation mechanism determines how the data are distributed over the network. The main distribution mechanisms are as follows:

- Advertising-based dissemination of information consists in the dissemination of information about the received block (or the block header, depending on the types of nodes), and the nodes will request the block if it is not in their register.
- An unsolicited block advance is applied when the miner is sure that no other node could recognize the block before.
- A hybrid promotion system propagates information from a node to the square root of the number of directly connected peers.
- Intelligent selection of neighbors from a variety of possible neighbors significantly affects overlap, resiliency, and load balancing performance.

Blockchain technology uses cryptographic algorithms to protect user data and ensure system reliability [20]. The cryptographic underpinnings fall into two categories, primary and secondary. The first category is used to provide protection against unauthorized access, public verification, and consensus building (hash and standard digital signatures). The second category is used to enhance the privacy and anonymity of transactions.

Private keys are used by users to sign transactions, while public keys are used to authenticate transactions of other users. Blockchain technology security is ensured through the use of cryptographic primitives and decentralization.

The blockchain data structure is a time-stamped list that records and aggregates data about all transactions that have ever taken place on the blockchain network. Thus, the blockchain provides an immutable data store that only allows transactions to be inserted without updating or deleting any existing transaction on the blockchain to prevent tampering and revision.

Each node contains its own register, and the contents of each register are kept the same using a consensus algorithm. Blockchain consensus algorithms are what keep all the nodes on the network in sync with one another. The key requirement for reaching consensus is the unanimous acceptance of the same data value among nodes in the network, even if some nodes fail or are unreliable. Since blockchain technology does not respond to any trusted entity, consensus mechanisms are used to establish trust between untrusted entities. A number of consensus mechanisms have been proposed and implemented in various blockchain applications:

- Proof-of-work (PoW) is a process that allows network nodes to compete so that their block is next added to the blockchain by solving a computationally expensive puzzle.
- Proof-of-stake (PoS) is an alternative mechanism that allows mining rights to participants in proportion to their ownership of currency on the blockchain network.
- Delegated proof-of-stake (DPoS) is a variation of the PoS algorithm. The owners of the largest balances elect their representatives, each of whom gets the right to sign blocks in the blockchain network. Balance holders have the opportunity to delegate their votes and receive additional income from them.
- Leased proof-of-stake (LPoS) is also a modification of the PoS algorithm, in which any user has the opportunity to transfer his balance to the mining nodes for rent, for additional profit.
- Proof-of-capacity/proof-of-space (PoC) is an algorithm in which each miner calculates a sufficiently large amount of data that is written to the subsystem of the node, while the computing resources are limited by time. Miners compete with each other for the size of the saved data as opposed to the speed of the equipment.
- Proof-of-importance (PoI) is an algorithm in which the importance of a user is determined as the amount of funds available on his balance sheet and the number of transactions performed.
- Proof-of-activity (PoA) is where each miner of the blockchain network tries to generate an empty block header, then it is sent to the network and further verified. Nodes receive this block, make sure it is legal, and add it to the blockchain. The fee is distributed between the miner and the "lucky ones."
- Proof-of-authority (PoAuthority) is how all transactions and blocks are verified through approved accounts.
- Proof-of-burn (PoB) is a process used in the counterparty chain that involves the destruction of tokens. By sending coins to an unspent address, the miner shows a commitment to mining in the system, and therefore receives lifetime mining privileges. The more coins a miner burns, the more he will have the opportunity to mine the next block.

These technical features must be included if the implementation of blockchain technology in V2N is planned.

4. Technical features of the implementation of blockchain technology in V2N, analysis of time characteristics

4.1 Blockchain technology implementation specifications

Vehicle-to-network technology has become an important area of research over the past few years. This type of network is created based on the concept of a car network for a specific need or situation. Today, vehicle-to-network can establish reliable networks that vehicles use to communicate on highways or in urban environments. Such systems support a wide range of applications, from simple transmission of information to neighboring nodes such as mass alert messages, to the distribution of messages with multiple hops over vast distances.

Within the IEEE Communications Society, there is the Vehicular Networks and Telematics Applications (VNTA) Technical Commission, which promotes technical activities in the areas of automotive networking, V2V, V2R and V2I communication, standards, road safety, and real-time vehicle communication [32]. Examples of VANET applications include electronic brake lights that allow the vehicle to respond quickly to emergency situations, the formation of an automobile column, obstacle alerts, acceleration of rescue operations, and distribution of advertising notices. Good vehicle connectivity (V2V), infrastructure (V2I), and vulnerable road users will bring substantial benefits in terms of safety and comfort.

Along with the benefits of vehicle-to-network, many problems can arise. Currently, the telecommunications industry is showing significant progress in its development and offers many modern technologies that can cope with a wide range of tasks. Within vehicle-to-network, one such task is to ensure data security while not degrading the quality of service.

When vehicles communicate with infrastructure facilities, various types of information are transmitted, including vehicle identification data, speed, location, request content, and others. If the confidentiality and integrity of such data are violated, users may be harmed. An intelligent transportation system includes a huge amount of dynamic, critical data in real time, so its security is a major concern. Due to the urgent need to ensure the immutability and integrity of data, the use of special mechanisms that are available in blockchain technology solutions is proposed.

An example vehicle-to-network network is illustrated in Figure 2.

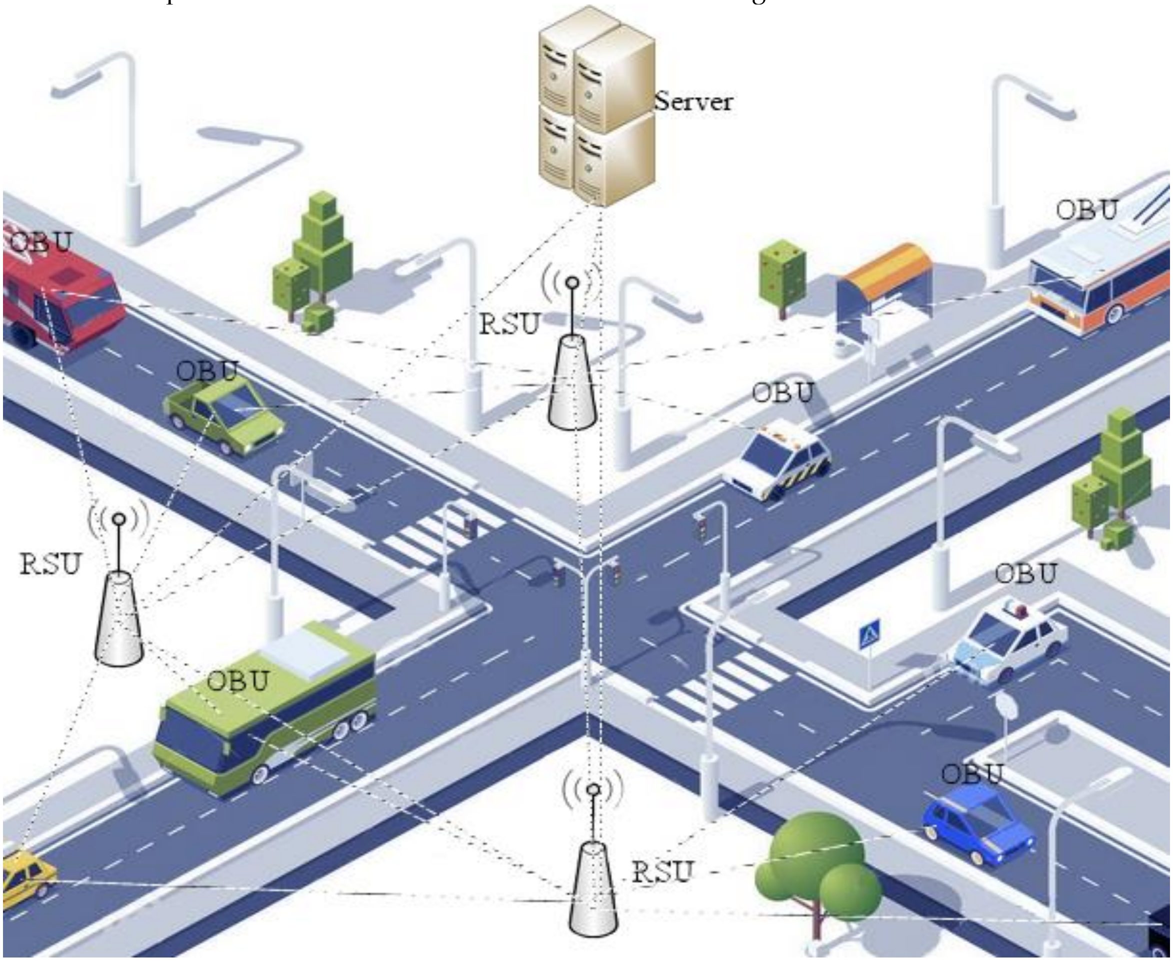

Figure 2. Model vehicle-to-network network.

The critical problems in the implementation of blockchain technology in V2N are low computing resources on vehicles, frequent changes in their location in space, and limited communication resources. Devices located on vehicles are expected to have limited memory and energy.

Since the topology of the vehicle-to-network network must change dynamically in response to the high mobility of the vehicle, it is expedient to use full nodes on road infrastructure facilities (road side units (RSUs)), and light nodes on vehicles (on-board units (OBUs)). In this solution, full nodes verify the correctness of the PoW solution and the transactions contained, and store a complete copy of the ledger. Light nodes take block headers and define a list of events in which they are interested. The architecture of such a network is shown in Figure 3.

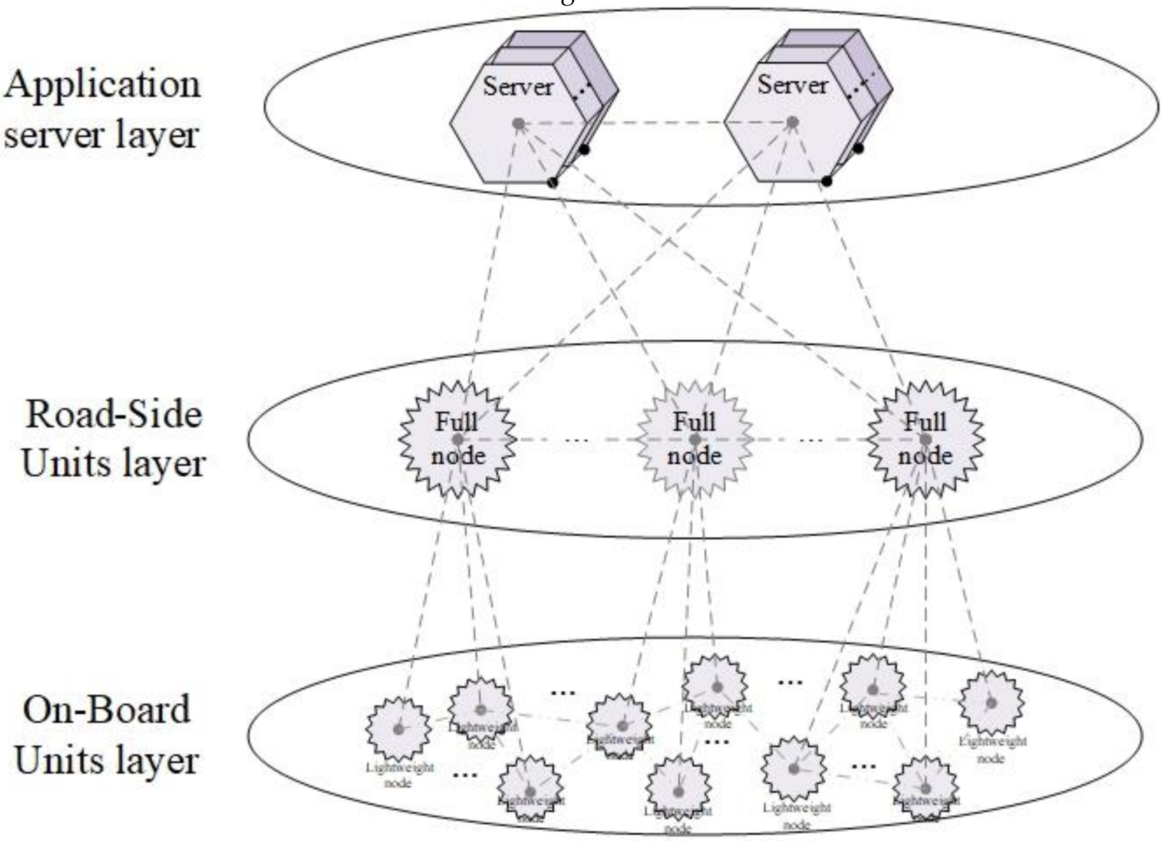

Figure 3. Vehicle-to-everything (V2X) network architecture after blockchain implementation.

However, even if the blockchain technology is used at OBU and RSU facilities, the system will not be completely decentralized, since the transmission, processing, and storage of information on the server will adhere to a centralized nature.

The emergence of blockchain-based applications for V2N prompts research into their communication system requirements and RSU, OBU, and other devices. It is necessary to consider the impact on the system due to the large number of transactions, since during the exchange, the blockchain generates additional traffic to update the registries on all involved nodes, and the increased volume of service traffic that appears during data encryption significantly reduces the share of useful traffic.

Loading of vehicle-to-network will depend on the following:

$$p \sim F(n, \alpha_n, d, m), \qquad (1)$$

where n is the number of nodes in the blockchain network (units), α_n is the rate of formation of transactions (transactions per second), d is the block size (bytes), and m is the interval between blocks.

Blockchain technology is characterized by the transfer of information in sharp bursts. Such spikes occur with synchronization between nodes at primary connections or solutions after a cryptographic problem. An elaborate study of the characteristics of the parameters presented in the dependencies of Equation (1) allows us to assess the impact of each node on the network load and determine the impact on the network characteristics, which is necessary for the high-quality operation of applications [33].

Network latency is defined as the time it takes to confirm a transaction. Blockchain network latency is defined as any delay caused by block propagation on the network. In order to achieve higher scalability, network latency must be low, that is, the time it takes for a protocol to confirm a transaction must be effectively reduced. This is achieved both by using traditional methods of network optimization and by varying the system parameters.

The influence of parameters on system load and scalability are as follows:

- The number of nodes (n) and the intensity of the formation of transactions (αn) in the blockchain network affect the network characteristics in direct proportions. An increase in the number of working nodes or the intensity of the formation of transactions will increase the amount of transmitted and processed information in both the process of validation and the process of synchronizing current registries. The solution to reduce the effect of this parameter is to optimize the number of full and light nodes. With a shorter block interval, the latency at which a transaction is written to the blockchain is reduced, i.e., the transaction is written faster; however, a shorter block interval results in a higher proportion of stale blocks, as more conflicting blocks will be found on the network. Obsolete blocks result in additional costs for validation and distribution across the network.
- Block size (d) and block spacing (s) also affect the network performance in direct proportions. However, there is another task to reduce the processing time of transactions: increasing the size of the block so that miners can include more transactions in one block. If the block size increases, the number of transactions processed per second will increase. This reduces the turn-on time for a transaction, which can reduce system-level latency. To make full use of the network bandwidth and achieve higher throughput and greater efficiency, the interval between blocks should be as small as possible. However, shortening the block generation interval or increasing the block size to increase throughput slows down block sharing on the network and increases the number of lost blocks, compromising security.
- The impact of the amount of the transaction fee on the confirmation time is also taken into consideration. Transaction fees play an important role in determining when transactions are confirmed. For the miner, this is an incentive to mine a specific transaction and include it in a block. The higher the transaction fee, the more likely there will be less time to confirm. However, this does not happen for every transaction; some transactions with higher transaction fees may require longer confirmation times (due to the fact that there may be transactions with the same value in the pool, or algorithms that do not allow complete supplanting of transactions with a smaller amount). This may have little or no impact on overall scalability, as its impact on network latency, latency, and throughput may be negligible.
- The number of miners in the system is also important. Increasing the mining power in the blockchain system will help in evenly distributing energy consumption and with the task of mining blocks throughout the network. It also means faster confirmation times and higher throughput.
- An increase in the number of transactions is in direct proportion to an increase in the confirmation time $C_T \sim n_T$, where C_T is the number of transactions and n_T is confirmation time. An increase in the number of transactions increases the load and latency on the system and network [34].

These parameters describe the inherent impact on load and scalability, but the authors propose considering the impact of allocated and used resources on various network characteristics. When it is possible to describe the model and determine the primary dependencies of blockchain traffic on the characteristics of the network, there is a high probability of providing better-quality service and disposing of network resources on a dedicated area.

A total of 50 virtual clients were created to analyze traffic behavior on a network that can be analogous to V2N. The operating system used in the study was Linux Ubuntu 18.04 LTS.[1]

[1] Geth client data: Version: 1.9.8-stable; Git Commit: d62e9b285777c036c108b89fac0c78f7855ba314; Git Commit Date: 20191126; Architecture: amd64; Protocol Versions: [64 63]; Go Version: go1.13.4; Operating System: linux; GOROOT = / home / travis / .gimme / versions / go1.13.4.linux.amd64; Network complexity: 0x1, private subnet number 57.

The algorithm of the blockchain technology for the nodes participating in the experiment is shown in Figure 4. This algorithm was developed taking into account the knowledge gained, the experiment, and the compilation of data from various sources, including [8–10,31,33].

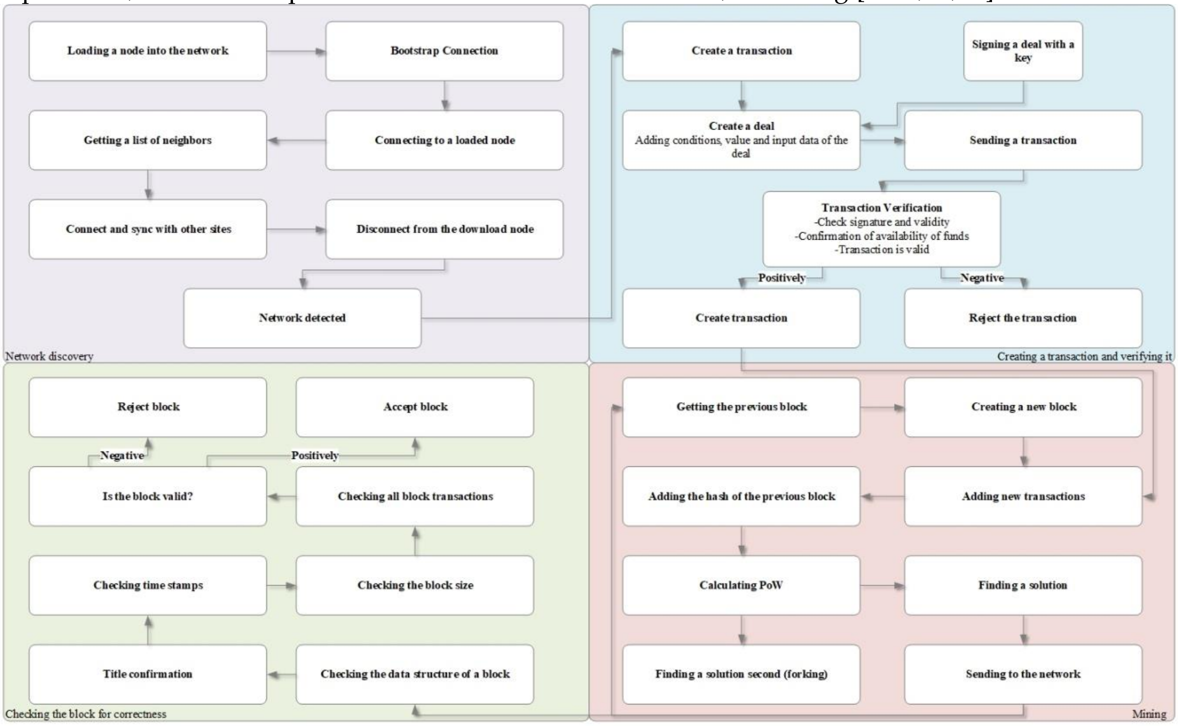
Loading a node into the network
Bootstrap Connection
Getting a list of neighbors
Connecting to a loaded node
Connect and sync with other sites
Disconnect from the download node
Network detected
Network discovery
Create a transaction
Signing a deal with a key
Create a deal
Adding conditions, value and input data of the deal
Sending a transaction
Transaction Verification
-Check signature and validity
-Confirmation of availability of funds
-Transaction is valid
Positively
Negative
Create transaction
Reject the transaction
Creating a transaction and verifying it
Reject block
Accept block
Negative
Positively
Is the block valid?
Checking all block transactions
Checking time stamps
Checking the block size
Title confirmation
Checking the data structure of a block
Checking the block for correctness
Getting the previous block
Creating a new block
Adding the hash of the previous block
Adding new transactions
Calculating PoW
Finding a solution
Finding a solution second (forking)
Sending to the network
Mining

Figure 4. Blockchain algorithm.

When studying an object, it is not always advisable to create a single model covering all of its aspects. It is necessary to know encryption and hashing systems, but it is not necessary to include them in a model that studies system stability. In the presented experiment, it is enough to make some necessary assumptions about the degree of reliability of such ciphers; we will consider them absolutely reliable and operating by default.

In the experiment, virtual clients sent transactions to a similar client at a rate of four transactions per second. As part of the work, four experiments were conducted, each of which generated different amounts of resources, and each experiment was repeated 100 times; the results of statistical treatment are presented. In this case, the nodes represented a complete customer who was at a stationary facility. Obviously, in accordance with Figure 3, these clients were organized on RSUs.

In the analysis of the characteristics of the functional elements, various parameters of the network elements were examined, such as the use of system resources when the technology was loading channels, packet delay between nodes, and delay variation. The results obtained are presented below and divided by experiment.

Experiment 1: In this experiment, 395 GB of read-only memory (ROM) and 31 GB of random-access memory (RAM) (distributed in random order) were allocated to the blockchain nodes.

Table 1. System resource utilization (experiment 1). RAM, random-access memory; ROM, read-only memory.

Node	Actual use		Node performance	
	RAM (GB)	ROM (GB)	RAM (GB)	ROM (GB)
1	0.50 (25.00%)	7 (8.86%)	2	79
2	0.55 (13.75%)	4.7 (5.95%)	4	79
3	0.11 (11.00%)	6.8 (8.61%)	1	79
4	0.60 (7.50%)	5.9 (7.47%)	8	79
5	1.15 (7.19%)	6.4 (8.10%)	16	79

Table 2 shows the values of the channel load between node 5 and other elements of the V2N network during the experiment.

Table 2. Average values of channel bandwidth used (experiment 1).

№ node	During blockchain operation (Gbps)	Before blockchain (Gbps)
1	8.11	10.6
2	5.39	7.44
3	8.30	9.28
4	6.38	9.46

During the experiment to check the network load, graphs of the intensity of packet transmission between different nodes were obtained, presented in Figure 5.

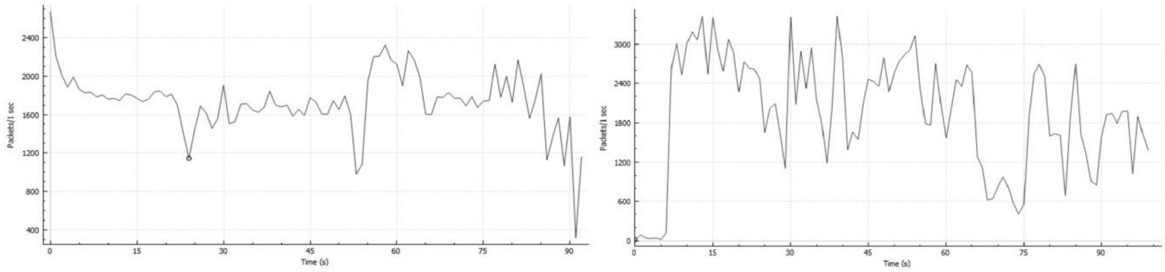

Figure 5. Intensity of loading channels between nodes 1 and 5 (experiment 1): before the blockchain works (left) and during the blockchain operation (right).

When networking with memory, allocation units were operating normally. All devices performed their tasks. When blockchain was running, the channel loading increased by an average of 30%. The latency of packets between nodes during blockchain operation decreased by an average of 88%. At the same time, there was practically no effect on the delay between nodes of another network (4% decrease).

Experiment 2: In this experiment, 395 GB of ROM and 10 GB of RAM (distributed evenly between nodes) were allocated to the blockchain nodes.

Table 3. System resource utilization (experiment 2).

Node	Actual use		Node performance	
	RAM (GB)	ROM (GB)	RAM (GB)	ROM (GB)
1	0.46 (23.00%)	7.7 (9.75%)	2	79
2	0.57 (28.50%)	6.7 (8.48%)	2	79
3	0.48 (24.00%)	6.6 (8.35%)	2	79
4	0.55 (27.50%)	6.8 (8.61%)	2	79
5	0.55 (27.50%)	7.3 (9.24%)	2	79

Table 4 shows the values of the channel load between node 5 and other network elements during the experiment.

Table 4. Average values of channel bandwidth used (experiment 2).

№ node	During blockchain operation (Gbps)	Before blockchain (Gbps)
1	4.98	10.6
2	5.27	12.4
3	4.96	10.8
4	5.59	12.0

When conducting the experiment to check the network load, graphs of the intensity of packet transmission between different nodes were obtained, presented in Figure 6.

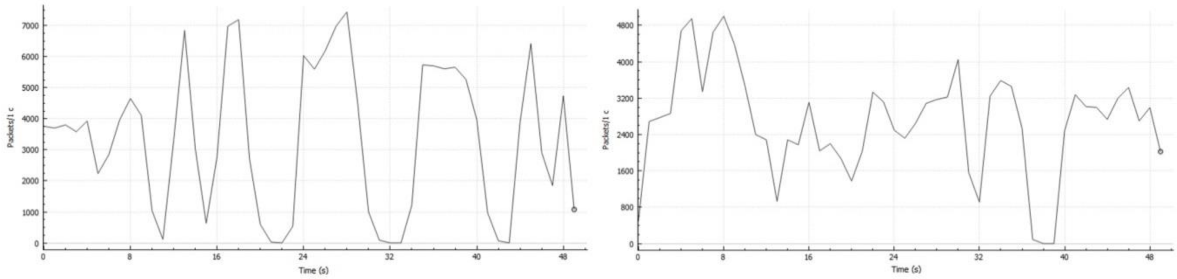

Figure 6. Intensity of loading channels between nodes 1 and 5 (experiment 2): before the blockchain works (left) and during the blockchain operation (right).

When networking with memory allocation, units were operating normally. All devices performed their tasks. When the blockchain was running, the channel load increased by an average of 120%. The latency of packets between nodes during blockchain operation decreased by an average of 49%. At the same time, there was practically no effect on the delay between nodes of another network (1% increase).

Experiment 3: In this experiment, 395 GB of ROM and 5 GB of RAM (distributed evenly between nodes) were allocated to the blockchain nodes.

Table 5. System resource utilization (experiment 3).

Node	Actual use		Node performance	
	RAM (GB)	ROM (GB)	RAM (GB)	ROM (GB)
1	0.38 (38.00%)	9.5 (12.03%)	1	79
2	0.40 (40.00%)	6.7 (8.48%)	1	79
3	0.50 (50.00%)	9.1 (11.52%)	1	79
4	0.57 (57.00%)	9.9 (12.53%)	1	79
5	0.58 (58.00%)	8.5 (10.76%)	1	79

Table 6 shows the values of the channel load between node 5 and other elements of the V2N network during the experiment.

Table 6. Average values of channel bandwidth used (experiment 3).

Node	During blockchain operation (Gbps)	Before blockchain (Gbps)
1	4.68	10.5
2	4.87	10.5
3	4.87	12.6
4	4.53	11.0

When carrying out the experiment to check the network load, graphs of the intensity of packet transmission between different nodes were obtained, presented in Figure 7.

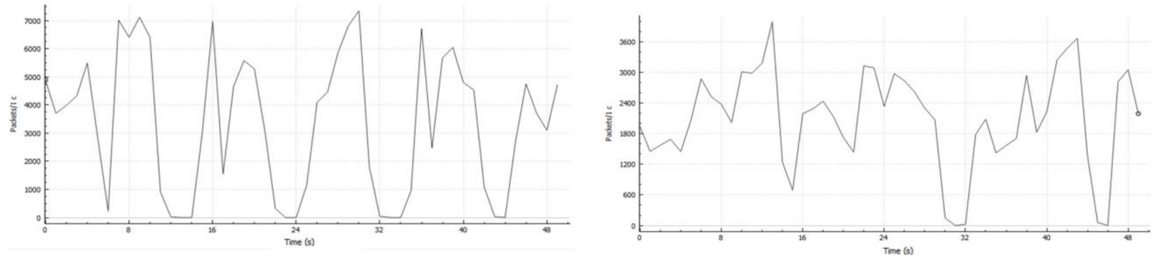

Figure 7. Intensity of loading channels between nodes 1 and 5 (experiment 3): before the blockchain works (left) and during the blockchain operation (right.

When organizing a network with memory allocation, the nodes did not work normally. Synchronization and mining failures partially occurred. When the blockchain was running, the channel load increased by an average of 135%. The latency of packets between nodes during blockchain operation decreased by an average of 53%. At the same time, there was practically no effect on the delay between nodes of another network (1% decrease).

Experiment 4: In this experiment, 395 GB of ROM and 2.5 GB of Random RAM (distributed evenly between nodes) were allocated to the blockchain nodes.

Table 7. System resource utilization (experiment 4).

Node	Actual use		Node performance	
	RAM (GB)	ROM (GB)	RAM (GB)	ROM (GB)
1	0.35 (70.00%)	9.5 (12.03%)	0.5	79
2	0.10 (20.00%)	6.7 (8.48%)	0.5	79
3	0.16 (32.00%)	13 (16.46%)	0.5	79
4	0.16 (32.00%)	13 (16.46%)	0.5	79
5	0.16 (32.00%)	12 (15.19%)	0.5	79

Table 8 shows the values of the channel load between node 5 and other network elements during the experiment.

Table 8. Average values of channel bandwidth used (experiment 4).

№ node	During blockchain operation (Gbps)	Before blockchain (Gbps)
1	2.87	12.6
2	2.67	11.1
3	3.14	10.7
4	2.97	10.3

When conducting the experiment to check the network load, graphs of the intensity of packet transmission between different nodes were obtained, presented in Figure 8.

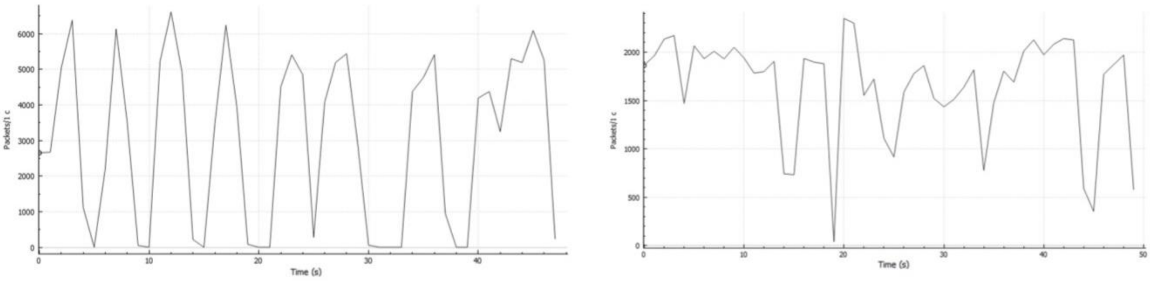

Figure 8. Intensity of loading channels between nodes 1 and 5 (experiment 4): before the blockchain works (left) and during the blockchain operation (right).

When organizing a network with memory allocation, the nodes did not work normally. Nodes did not always complete synchronization successfully. When blockchain was running, the channel load increased by an average of 286%. The latency of packets between nodes during blockchain operation decreased by an average of 51%. At the same time, there was practically no effect on the delay between nodes of another network (1% decrease).

4.2 *Analysis of dependencies of captured characteristics on controlled changes in external factors of the network.*

The experiment showed that for correct operation of the blockchain technology of the type presented here, it was necessary to allocate at least 2 GB of RAM for each node. It can also be seen that with the same provision of allocated resources, the percentage of resources used by the nodes differed. However, the fewer system resources that were allocated, the smaller the channel bandwidth was during the blockchain operation. The experiment showed that the channel bandwidth used depends on the actions of the nodes.

The latency of packets between nodes during blockchain operation decreased significantly (varying from 49% to 88%). At the same time, there was practically no effect on the delay with the nodes of another network. By comparison, delay variation to work the blockchain failed nodes at a time without synchronizing the interaction of mining substantially did not occur between the nodes. However, it can be seen that the variance of the delay variation was significant in all cases.

The data were obtained within the framework of tests, processed using the mathematical apparatus of statistical analysis.

5. Conclusion

The growing number of intelligent vehicles are expected to generate and exchange huge amounts of data, and managed network traffic is expected to be significant. This study provides an overview of intelligent transport systems based on telecommunications with an emphasis on ensuring the safety and resilience of the system. In V2X in general and V2N in particular, the problem of ensuring information security is extremely acute due to the specifics of the operation of transport networks and the importance of not interfering with third parties in the operation of the system. This requires the use of special security mechanisms. To solve such problems, the authors suggest using blockchain technology. The paper defines the scheme of such a system and presents a model and an algorithm. The authors examined various network characteristics and identified the parameters that have a primary impact on the operation of the V2N network. In addition, an experiment was performed showing the numerical characteristics of resource allocation on devices involved in organizing V2N communication. However, the use of blockchain technology cannot be considered an ideal option for V2N, since in addition to the benefits it brings, it is associated with parameters that affect the network, including load and network latency. The attempt made in this study to use the technology translates this issue into the plane of the problem of the optimal (rational) choice of the performance level of nodes and their technical implementation.

As part of further work, it will be necessary to conduct studies to analyze the characteristics of the interaction of devices that are based on stationary (RSU) and mobile (OBU) devices. In this case, it will be necessary to take into account the speed of movement of the nodes, the performance, and the technical devices of the technical equipment.

Author Contributions: All authors contributed equally to this work.

Funding: Vasiliy Elagin and Anastasia Spirkina: This research was funded by RFBR, project number 19-37-90050/19 (Moscow, Russia).

Mikhail Buinevich and Andrei Vladyko: This research was funded by Federal Agency of Communications, contract number П33-1-26/9 (Moscow, Russia).

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

References

1. Meng, Lu (ed.). Evaluation of Intelligent Road Transport Systems: Methods and Results. *Transport* **2016**.
2. Kiela K. et al. Review of V2X–IoT Standards and Frameworks for ITS Applications. *Applied Sciences* **2020,** *10*, 12.

3. Bhover, S. U.; Tugashetti A.; Rashinkar P. V2X communication protocol in VANET for co-operative intelligent transportation system. 2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, 2017, pp. 602-607.
4. Vladyko, A.; Khakimov, A.; Muthanna, A.; Ateya, A.A.; Koucheryavy, A. Distributed Edge Computing to Assist Ultra-Low-Latency VANET Applications. *Future Internet* **2019**, 11, 128.
5. Aliyu, A.; Abdullah, A.H.; Kaiwartya, O.; Cao, Y.; Usman, M.J.; Kumar, S.; Lobiyal, D.K.; Raw, R.S. Cloud Computing in VANETs: Architecture, Taxonomy, and Challenges. *IETE Tech. Rev. 2018*, 35, pp. 523–547.
6. Xu X. et al. The Blockchain as a Software Connector. 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA), Venice, 2016, pp. 182-191.
7. Palmara, P. Tracing and tracking with the blockchain, Tesi di laurea magistrale, Politecnico di Milano, 2018.
8. Mougayar, W. The Business Blockchain; John Wiley & Sons Inc.: Hoboken, NJ, USA, 2016.
9. Goldstein, A.B.; Sokolov, N.A.; Elagin, V.S.; Onufrienko, A.V.; Belozertsev, I.A. Network Characteristics of Blockchain Technology of on Board Communication. In Proceedings of the 2019 Systems of Signals Generating and Processing in the Field of on Board Communications **2019,** pp. 1–5.
10. Elagin, V.; Spirkina, A.; Levakov, A.; Belozertsev, I. Blockchain Behavioral Traffic Model as a Tool to Influence Service IT Security. *Future Internet* **2020**, *12*, 68.
11. Xie, H.Tang; Huang, T.; Yu, F. R.; Xie, R.; Liu, J.; Liu, Y. A survey of blockchain technology applied to smart cities: Research issues and challenges. IEEE Communications Surveys & Tutorials **2019**, 21, 3, pp. 2794–2830.
12. Aujla, G. S.; Singh, M.; Bose, A.; Kumar, N.; Han, G.; Buyya, R. Blocksdn: Blockchain-as-a-service for software defined networking in smart city applications. IEEE Network **2020**, 34, 2, pp. 83–91.
13. Hakak, S.; Khan, W. Z.; Gilkar, G. A.; Imran, M.; Guizani, N.; Securing smart cities through blockchain technology: Architecture, requirements, and challenges. IEEE Network **2020**, 34, 1, pp. 8– 14.
14. Zhang, W.; Wu, Z.; Han, G.; Feng, Y.; Shu, L. Ldc: A lightweight dada consensus algorithm based on the blockchain for the industrial internet of things for smart city applications. F*uture Generation Computer Systems* **2020**.
15. Nellore, K.; Hancke, G.P. Traffic Management for Emergency Vehicle Priority Based on Visual Sensing. *Sensors* **2016**, *16*, 1892.
16. Chen, Y.; Weng, S.; Guo, W.; Xiong, N. A Game Theory Algorithm for Intra-Cluster Data Aggregation in a Vehicular Ad Hoc Network. *Sensors* **2016**, *16*, 245.
17. Jing, P.; Huang, H.; Chen, L. An Adaptive Traffic Signal Control in a Connected Vehicle Environment: A Systematic Review. *Information* **2017**, *8*, 101.
18. Stolyarova, E.S.; Shiryaev, D.M.; Vladyko, A.G.; Buinevich, M.V. VANET/ITS Cybersecurity Threats: Analysis, Categorization and Forecasting. Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, EIConRus-2018, **2018**, pp. 136-141.
19. Buinevich, M.; Izrailov, K.; Stolyarova, E.; Vladyko, A. Combine Method of Forecasting VANET Cybersecurity for Application of High Priority Way. 20th International Conference on Advanced Communication Technology (ICACT). Conference proceedings**. 2018**. pp. 266-271.
20. Buinevich, M.; Vladyko, A. Forecasting Issues of Wireless Communication Networks' Cyber Resilience for An Intelligent Transportation System: An Overview of Cyber Attacks. *Information* **2019**, 10, 27.
21. Sheikh, M.S.; Liang, J.; Wang, W. A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs). *Sensors* **2019**, *19*, 3589.
22. Farooq, S.M.; Hussain, S.M.S.; Kiran, S.; Ustun, T.S. Certificate Based Security Mechanisms in Vehicular Ad-Hoc Networks based on IEC 61850 and IEEE WAVE Standards. *Electronics* **2019**, *8*, 96.
23. Qu, F.; Wu, Z.; Wang, F.; Cho, W. A Security and Privacy Review of VANETs. IEEE Transactions on Intelligent Transportation Systems, 16, 6, pp. 2985-2996.
24. Kumar, G.; Saha, R.; Rai, M.K.; Kim, T. Multidimensional Security Provision for Secure Communication in Vehicular Ad Hoc Networks Using Hierarchical Structure and End-to-End Authentication. IEEE Access, 6, pp. 46558-46567.
25. Muhammad, Shahid; Hahn; Jungpil. A Cross-Disciplinary Review of Blockchain Research Trends and Methodologies: Topic Modeling Approach. 2020. 10.24251/HICSS.2020.495.
26. Sgantzos, K.; Grigg, I. Artificial Intelligence Implementations on the Blockchain. Use Cases and Future Applications. *Future Internet* **2019**, 11, 170.

27. Wang, Y.; Ding, Y.; Wu, Q.; Wei, Y.; Qin, B.; Wang, H. Privacy-Preserving Cloud-Based Road Condition Monitoring With Source Authentication in VANETs. *IEEE Transactions on Information Forensics and Security*, 2019, 14, 7, pp. 1779-1790.
28. Lu, Z.; Liu, W.; Wang, Q.; Qu, G.; Liu, Z. A Privacy-Preserving Trust Model Based on Blockchain for VANETs. *IEEE Access*, 2018, 6, pp. 45655-45664.
29. Yang, Y.; Chou, L.; Tseng, C.; Tseng, F.; Liu, C. Blockchain-Based Traffic Event Validation and Trust Verification for VANETs. *IEEE Access*, 2019, 7, pp. 30868-30877.
30. Kim, S. Impacts of Mobility on Performance of Blockchain in VANET. *IEEE Access*, 2019, 7, pp. 68646-68655.
31. Antonopoulos, A.M. Mastering Bitcoin; O'Reilly Media Inc.: Sebastopol, CA, USA, 2017.
32. Ghori, M.R.; Zamli, K.Z.; Quosthoni, N.; Hisyam M.; Montaser, M. Vehicular ad-hoc network (VANET): Review. 2018 IEEE International Conference on Innovative Research and Development (ICIRD), 2018, pp. 1-6.
33. Vladyko, A.G.; Spirkina, A.V.; Elagin, V.S.; Belozertsev, I.A.; Aptrieva, E.A. Blockchain Models to Improve the Service Security on Board Communications. 2020 Systems of Signals Generating and Processing in the Field of on Board Communications **2020**, pp. 1-5 .
34. Goswami, Sneha. Scalability Analysis of Blockchains Through Blockchain Simulation. UNLV Theses, Dissertations, Professional Papers, and Capstones, 2017, 2976.