XXI INTERNATIONAL SCIENTIFIC-EXPERT CONFERENCE ON RAILWAYS
RAILCON '24
October 10-11, 2024; Niš, Serbia

Original scientific paper DOI: 10.5937/Railcon24055P

IMPROVING CYBER SECURITY IN RAILWAY TRAFFIC AND TRANSPORT USING BLOCKCHAIN TECHNOLOGY

Zoran PAVLOVIĆ [1] [0000-0001-6076-1811]

Abstract *– Today, the management of railway traffic and transport is mainly based on the application of computer hardware and software components that are installed in the company's official premises. The application of information and communication technologies (ICT) includes all processes that take place in electronic business between employees, citizens, as well as between machines and devices, indirectly or directly. The improvement of business operations of companies with a tendency to grow and the application of digital infrastructure implies the use of protective mechanisms that prevent cyber attacks and threats. Cyber attacks in such complex business processes (the security of traffic regulation from dispatch centers and even to digital money transactions when buying a ticket or paying for the transportation of a shipment) can cause malicious activities from unknown attackers in order to redirect or modify messages. Basically, it is necessary to apply measures to protect connected computer systems, which include signaling, control, mutual communication and the safety of all traffic participants. This paper presents a model of protection, cyber security in the railway company, which implies the application of blockchain technology as today's most powerful mechanism for storing and memorizing data in digital processes.*

Keywords – railway security, ICT, cyber attacks and countermeasures, data protection in digital processes, block chain technology.

1. INTRODUCTION

This paper presents a mechanism for improving cyber security using block chain technology. The basis is a large number of operations that take place in various digital processes, from the exchange of emails between employees to the regulation of traffic from dispatch centers. In addition to the above, service users have the opportunity to satisfy their needs for purchasing and receiving services through the available computer components. The application of innovative technologies is increasingly prevalent both among users and among railway carriers [1],[2]. Block chain is currently one of the safest protection mechanisms [3],[4]. In the following, the available literature will be analyzed where researchers have various approaches in solving problems related to increasing cyber security in railway traffic and transport. The application of information technologies will improve the current protection mechanisms [5]. The paper includes a description and graphic representation of the functioning of block chain technology, which has yet to be implemented in the railway company.

2. RELATED RESEARCH

In practice, there is a large number of works dealing with cyber security in railway traffic. For the purposes of this work, some were selected from which one can see the importance and specificity of the need to protect data that is exchanged in increasingly complex computer systems. The modern development and regulation of railway traffic also implies the application of advanced Internet technologies, which, through a detailed analysis, can have certain disadvantages in addition to great advantages.

Technological advances in the telecommunications industry have brought significant advantages in the management and performance of communications networks. The rail industry is among those that have benefited the most. These interconnected systems, however, have a wide area exposed to cyber attacks. The author's research [6] examines the cyber security aspects of railway systems by considering the standards, guidelines, frameworks and technologies used in the industry to assess and mitigate cyber security risks, particularly in terms of the relationship between security. To do this, special attention is paid

[1] Academy of Technical and Art Applied Studies, Departments School of Railroad Transport, Starine Novaka 24, 11000 Belgrade, Serbia zoran.pavlovic@vzs.edu.rs

to signaling, whose fundamental reliance on computer and communication technologies allows us to better explore the multifaceted nature of safety in modern hyper-connected railway systems. With this in mind, it then moves on to analyze the approaches and tools that practitioners can use to facilitate the cyber security process. In detail, a view of cyber ranges is presented as a technology that enables the modeling and emulation of computer networks and attack defense scenarios, the study of the impact of vulnerabilities, and ultimately the design of countermeasures. It also discusses several possible use cases that are strongly related to the reality of the railway industry.

With the deepening and implementation of China's network power strategy, critical information infrastructure has become increasingly prominent in social development. China's national cyber security strategy proposes protecting critical information infrastructure. In addition, it also declares that nationally critical information infrastructures include information infrastructures related to national security, national welfare and human life. When critical information infrastructure is damaged or partially functional, which may seriously threaten national security and public interests. It is vital to protect critical information infrastructure from damage. Currently, it is necessary to improve the risk assessment system of critical information infrastructure. For critical information infrastructure, there is a lack of a risk assessment method, which is an assessment of the effectiveness of security measures. In order to meet the requirements for ensuring the security of critical information infrastructure, a statistical risk assessment model is set up and a risk assessment method based on the fuzzy analytical infrastructure hierarchy (AHP) process for critical information is proposed. In this paper, the proposed risk price is evaluated in a practical system and the proposed estimation method is also verified [7].

In order to raise the level of automation and information, a large number of common information technologies are applied to railway signaling systems, which leads to an increase in the openness of signaling systems and an increase in security risks. Quantifying the effects of safety risks is an urgent task, which is a major challenge for railway signaling systems due to the lack of safety metrics and an effective assessment approach. In the author's work [8], based on service characteristics and cyber-physical characteristics of railway signaling systems, a resilience-based safety assessment approach is proposed to describe performance changes during different phases of safety events, which can illustrate signaling robustness and recovery capability. systems facing cyber attacks. Considering a typical scenario where malicious jamming attacks are applied to train-ground wireless communications, the proposed security assessment approach shows the security levels of railway signaling systems. Based on the time variation of the resilience indicator, a cognitive control strategy is developed to improve the overall performance and resilience of the signaling system. The simulation results demonstrate the validation and effectiveness of the proposed safety assessment approach.

A simulation of a modern railway system at a cyber range will explore the flexible behavior of cyber-attacks in a modern digital railway system. Modern railway digital simulation architecture will focus on railway signaling system and control command system, which is a classical SCADA system. With the introduction of IoT technology in railway systems, they have become vulnerable to cyber attacks. The simulation is conducted on a cyber range server by simulating STCS. Cyber threats were analyzed through penetration testing using Kali Linux on a simulated STCS at the cyber range. The impact of groups of threat agents is analyzed, especially denial of service (DoS) and key chain attacks that mainly target STCS. A DoS attack generates packet congestion in the railway system network and compromises the SCADA components in the STCS. The quay chain attack compromises the SCADA component, leading to delays in the STCS signaling system. Attack tree analysis helps to understand the behavior of threat agents on STCS. Based on the research, some mitigation techniques have been identified to reduce the impact of cyber attacks on the modern digital railway system [9].

3. DEVELOPMENT OF A MODEL FOR INCREASING CYBER SECURITY IN THE RAILWAY COMPANY

3.1. The basics of cyber security

Since a large number of activities involving the exchange of messages between devices or people take place in the railway company, there is a potential danger of cyber attacks. In practice, network security means protecting the network from potential unauthorized access, where only authorized users can access the network directly, and of course all messages passing through the network are encrypted. Today, there are four types of network security that show good results:

- A firewall that is intended for traffic control between networks AND at the same time protection against connection threats and potential attacks,
- Network segmentation where the network is divided into smaller segments and can increase the security of isolated individual parts,

- Virtual private networks include secure access to the network but only to certain users,
- Email protection, which includes encryption, authentication and at the same time the protection of the software as well as the user.

In contrast to the above, cyber security is a broader concept that includes all aspects and that:

- Training of end users who perform various tasks,
- Ensuring uninterrupted operation when a problem is established or a part of the computer system is damaged,
- Operational security, which includes security in IT operations and digital transactions,
- Information security, which includes information management operations in a secure manner where privacy is guaranteed,
- Security at the application layer where available applications are used,
- Network security where different types of protection are defined in advance.

Solutions to potential problems are in block chain technology, which today is the most reliable mechanism for storing and distributing data in a safe and secure way. The main advantage of block chain is decentralization as well as high resistance to potential attacks.

In the continuation of this work, an innovative model of application of block chain technology in railway traffic is presented.

3.2. Block chain protection mechanism to increase cyber security

Complex computer systems are responsible for a large number of operations that can occur simultaneously. Each digital transaction represents one record. Block chain represents a series of chronologically sorted records that are organized into blocks and linked and protected by cryptography. Each block is formed in the same way and contains a cryptographic hash code, a timestamp and information about the transaction itself. A hash code is the result of a mathematical function of transforming an input of arbitrary length into an encrypted output of fixed length and is a basic tool of modern cryptography. This function is unidirectional or in other words, there is no reverse algorithm by which to get from the hash code to output, received the original input data. Cryptographic hash functions have a large application in applications in the domain of security and digital signing of data, so is their application in block chain platforms one of the bases of security and immutability of transactions. In addition to its own hash, each block also contains a hash code of the previous block, thus guaranteeing the integrity of the data, because any subsequent modification would of data in the block chain required the modification of all previous blocks. In Figure 1 it is given showing the basic architecture of the block chain network.

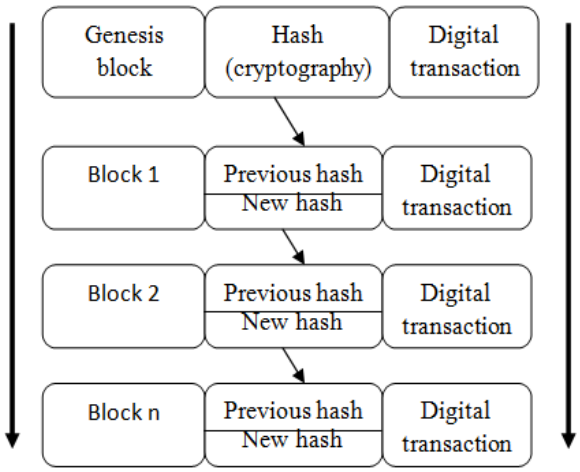

Fig.1. Block chain architecture

An example can be the functioning of the block chain in the railway company shown in Fig. 2.

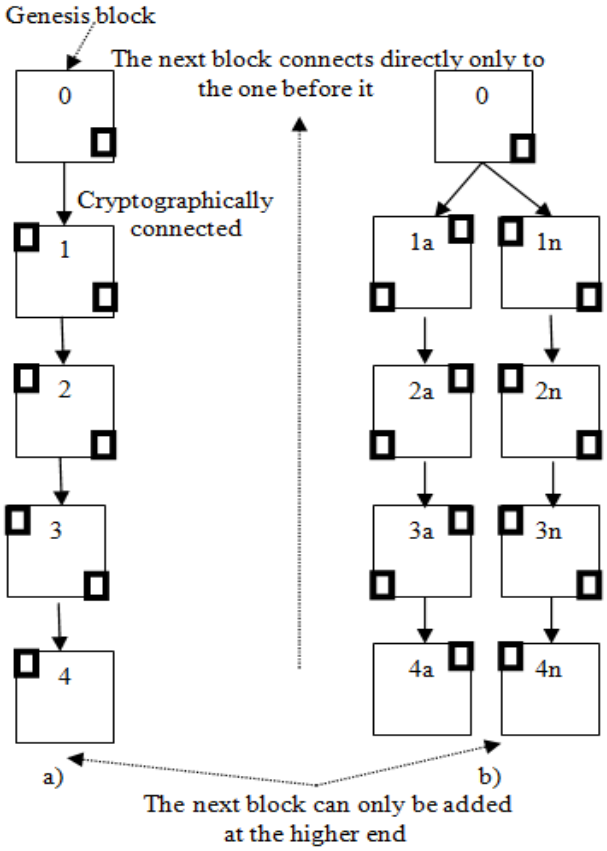

Fig.2. Structure and branching of blocks [3]

All transactions that take place in the network can be linear or branching. In the first case (under a), a linear sequence of blocks containing data on exchanged messages from the departure of the train to the arrival at the destination station is displayed. It can be seen that each block has its predecessor and its successor.

The application of block chain in the manner shown provides storage of a large amount of data related to the exchange of all messages in the form of orders, instructions, notifications, as well as all other processes that take place digitally. Block chain technology secures the mentioned activities from cyber attacks and increases security at the same time. The available hardware and software capacities have the possibility of upgrading in order to improve safety in railway traffic and transport.

There are numerous platforms for the application of block chain, which at the same time enable:

- The speed of the block chain enables a large number of transactions per second,
- Block chain network can be public or private. In this work, a combination of private and public networks is recommended, the private network is used in large companies where only employees and partners who are allowed to participate in transactions can participate. And on the other hand, a public network allows individuals to use block chain technology for their security.
- The security of the block chain is guaranteed by cryptographic techniques and algorithms that require the connection of 50% plus one computer in the world in order to organize a good attack, which is not feasible in practice.

4. CONCLUSION

This paper shows the possibility of implementing the innovative block chain technology, which is based on computer equipment and a network in order to protect digital messages that are exchanged in business processes. With the increase in the use of block chain, the importance of the scalability of that system is gaining importance as well as its application in other companies. Block chain technology can accommodate new applications and a large number of transactions, but this requires changes and the addition of new software technologies to maximize throughput.

In the current and future operations of the railway company, it is understood that operations are based on the management of the protection system where mutual trust is created between interested parties. Block chain technology provides an innovative approach to the remodeling of the railway traffic and transport system and at the same time offers flexibility of data access, security, privacy, decentralized storage, immutability, authentication and the like.

REFERENCES

[1] Pavlović Z, Banjanin M, Vukmirović J, Vukmirović D., (2020): *Contactless ICT Transaction Model Of The Urban Transport Service*; Research journal TRANSPORT, Vol 35 No 5, pp 500-510. https://doi.org/10.3846/transport.2020.12529

[2] Pavlović Zoran; *Model of security of digital processes in electronic railway business*; Mechanics Transport Communications, Academic journal 2023, ISSN1312-3823 (print), ISSN 2367-6620 (online), Volume 21 (Issue 3/1), art. ID: 2409 pp. VI7-VI11

[3] Zoran G. Pavlović : A MODEL OF APPLICATION OF BLOCKCHAIN TECHNOLOGY TO INCREASE SAFETY IN RAILWAY TRAFFIC, *2024, 23nd International Symposium INFOTEH-JAHORINA (INFOTEH)*, East Sarajevo, Bosnia and Herzegovina, 2024, 20-22 March, pp. 342-346, https://infoteh.etf.ues.rs.ba/zbornik/2024/radovi/VRT-6-1.pdf

[4] Z. G. Pavlović, "Innovative Model Of E-Business Increasing Safety On High-Speed Railways," *2023 22nd International Symposium INFOTEH-JAHORINA (INFOTEH)*, East Sarajevo, Bosnia and Herzegovina, 2023, pp. 1-6, doi: 10.1109/INFOTEH57020.2023.10094094. https://ieeexplore.ieee.org/document/10094094

[5] Z. G. Pavlović, Z. Bundalo, M. Bursać and G. Tričković, "Use of information technologies in railway transport," *2021 20th International Symposium INFOTEH-JAHORINA (INFOTEH)*, East Sarajevo, Bosnia and Herzegovina, 2021, pp. 1-4, doi: 10.1109/INFOTEH51037.2021.9400521, https://ieeexplore.ieee.org/document/9400521

[6] S. Soderi, D. Masti and Y. Z. Lun, "Railway Cyber-Security in the Era of Interconnected Systems: A Survey," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 7, pp. 6764-6779, July 2023, doi: 10.1109/TITS.2023.3254442

[7] Z. Guang-jie, Y. Hong-lei and Y. Yi-jie, "Approach of Risk Assessment for Railway Critical Information Infrastructure Based on Fuzzy Analytic Hierarchy Process," *2020 IEEE 5th International Conference on Signal and Image Processing (ICSIP)*, Nanjing, China, 2020, pp. 1015-1020, doi: 10.1109/ICSIP49896.2020.9339457.

[8] H. Wang, M. Ni, S. Gao, F. Bao and H. Tang, "A Resilience-Based Security Assessment Approach for Railway Signalling Systems," *2018 37th Chinese Control Conference (CCC)*, Wuhan, China, 2018, pp. 7724-7729, doi: 10.23919/ChiCC.2018.8483166.

[9] G. Sharma, E. Sherif, M. He and E. Boiten, "Analysis of Cyber-Attacks for Modern Digital Railway System Using Cyber Range," *2022 IEEE Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)*, Gwalior, India, 2022, pp. 1-6, doi: 10.1109/IATMSI56455.2022.10119321.