Mechanics Transport Communications

Academic journal http://www.mtc-aj.com

ISSN 1312-3823 (print)
ISSN 2367-6620 (online)
volume 22, issue 3/3, 2024
article № 2587

A MODEL FOR APPLYING BLOCKCHAIN TECHNOLOGY TO INCREASE CYBER SECURITY IN A RAILWAY COMPANY

Zoran G. Pavlović
zoran.pavlovic@vzs.edu.rs

Academy of Technical and Art Applied Studies ATAAS,
Departments School of Railroad Transport, Starine Novaka 24,
REPUBLIC OF SERBIA

Key words: *Information security, cyber security, blockchain technology, rail traffic and transportation*

Abstract: *Cyber security is a big challenge due to the rapid development of computer systems that are used in all companies today. The application of innovative electronic business models requires information security of data that is stored, exchanged and stored in the database. Today, in railway traffic, it is unthinkable to implement a business plan as well as daily processes that are directly related to traffic and transport without the use of computers and their mutual communication in the exchange of messages. Block chain technology is the most secure data protection mechanism in mutual communication between people and computer components. Confidentiality, integrity and availability of data must be ensured by mechanisms and technologies that simultaneously increase the safety of railway processes. This paper presents an innovative model of electronic business based on the application of blockchain technology in railway traffic and transport. The basis and principle of blockchain work are presented, a platform that includes the functioning of blockchain technology on the example of information security in a railway company. The railway company has the appropriate hardware and software infrastructure which in this paper is being extended with blockchain to increase cyber security. The main goal of this work is to secure and protect data in a modern way by applying block chain technology and thereby increase the safety of social property as well as the safety of employees and users who directly or indirectly participate in traffic and transport.*

INTRODUCTION

Today, information security includes the available protection mechanisms related to the protection of data from unauthorized access that enables an unauthorized person to use, modify and, in the worst case, alienate. Information security is the fundamental basis for the functioning of the entire electronic business system in all entities where data is stored, forwarded and stored through hardware and software components as well as computer networks. In order to ensure data security in any organization, enterprise, governmental institutions and non-governmental associations and the like, the following parameters must be implemented and enabled to function:

• Confidentiality – when the protection of data from any unauthorized person is applied, such as the application of certain passwords that are known only to the authorized user or physical access restrictions when computer equipment is in locked rooms.

• Integrity - which refers to the stability and accuracy of the data until the authorized user makes certain changes, as well as that unauthorized persons cannot access the data and at the same time change the data.

• Availability - which refers to the access and application of data at any time and at any time, but only to authorized users.

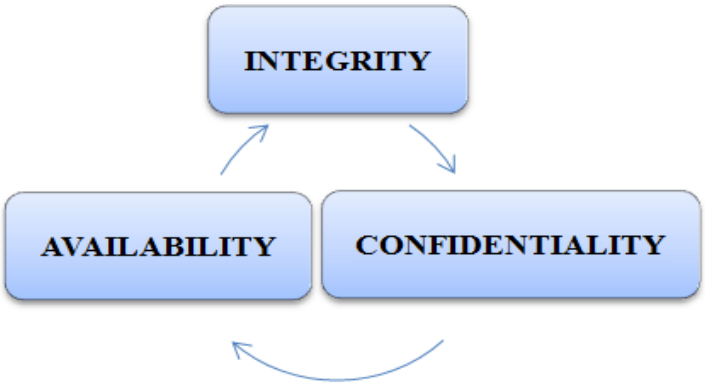

Fig. 1. Parameters of information security

Blockchain is an innovative mechanism for data storage and distribution as well as a technology that provides cyber and information security. In the last decade, for the first time, blockchain technology was developed and applied to operate the cryptocurrency bitcoin in digital banking. Due to its decentralization, high resistance to cyber attacks, today the research and scientific community is trying to insert blockchain technology in all areas of electronic business, or in other words, in every data transaction between people and computers or between different devices that are connected in a computer system. In this paper, a model of application of blockchain technology in railway traffic is presented. There is a special review of the elements and principles that must be respected by interested parties, devices, computers that are connected by the network of all networks through the Internet.

RELATED RESEARCH

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 authors in the paper [1] examine aspects of the cyber security of railway systems taking into account the standards, guidelines, frameworks and technologies used in the industry to assess and mitigate cyber security risks, especially regarding the relationship between the pillars of current security and the security required. Special attention is given to signalling, whose basic reliance on computer and communication technologies allows us to better explore the multifaceted nature of security in modern hyper-connected rail systems.

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. With the introduction of IoT technology in railway systems, they have become vulnerable to cyber attacks. Cyber threats in the author's work [2] will be analyzed through the analysis of the impact of threat groups and attacks where packet congestion is generated in the network of

the railway system. Based on the research, some mitigation techniques are identified to reduce the impact of cyber-attacks on the modern digital railway system.

With the continuous development of the railway business, the architecture of railway application software has become more and more complex, and the security threats it faces are more and more severe. To fix security vulnerabilities exposed in application software, railway companies must passively respond after the software is released and maintained, which increases costs in the software life cycle. Based on the characteristics of railway enterprises, the author's research in the paper [3] designed the structure of the enterprise research and development team, divided the technical tools that support research and development into four domains, standardized the process system that integrates detection and security protection, formed a railway system based on "people-process-technology".

Communication-based train control (CBTC) system ensures high efficiency and orderliness of trains and is widely used in urban rail transit networks. The adoption of wireless communications and networking techniques makes CBTC systems more vulnerable to cyber attacks. Identity verification is an effective approach to improve system security. Existing identity authentication mechanisms in CBTC adopt a single-point fault-sensitive centralized key management system. In order to improve system security, the author's work [4] applies blockchain in systems. The client running the blockchain program not only acts as a block chain of nodes to provide distributed key management for the CBTC system, but also works as a relay node to authenticate communication between train control nodes in the CBTC systems.

Modern railways are powered by traction systems (TPS). There fore, the safety and reliability of TPS is of critical importance for railways, which is a critical infrastructure. TPS, like any other infrastructure, is automated using information and communication technologies (ICT). Similar to smart grids, reactive power compensation and voltage control are important for reliable TPS operation. These compensation systems can be widely controlled or run in two modes. They are either remotely controlled via ICT channels or via a local closed loop system that is monitored remotely. ICT channels are generally vulnerable to cyber attacks. This vulnerability makes the reactive power compensation system/voltage control system vulnerable to cyber attacks. Misuse of the compensation system can interfere with voltage profiles and disrupt TPS operation. Abuse of the compensation system therefore leads to financial losses and unsafe operation of the railway [5].

Compositional architectures enable the reuse of certified (off-the-shelf) components with well-defined delegated responsibility between component developers and system integrators during the design and certification of a cyber-physical system. In the paper [6], the authors show how they used a platform certified according to common criteria for composition design and safety assessments and certificates for safety-critical composite systems in the smart grid, railway and metro domains.

Examples from practice show that achievable secure digital communication [7], that in electronic business processes great attention is paid to the security of digital activities that are realized in transactional steps [8], that cyber security applications and block chain technology can improve the overall organizational and the technological process of work in railway traffic [9],[10],[11], and that the application of available information technology can improve business in railway traffic and transport [12].

BLOCKCHAIN MODEL IN RAILWAY TRAFFIC AND TRANSPORT

Blockchain is basically defined as a distributed and decentralized ledger system where all network transactions are stored. It represents a series of chronological records that are presented in the form of connected blocks that are protected by cryptography. In this way, each block contains a cryptographic hash code, a time stamp and information about the

executed transaction. The basic architecture of the blockchain is shown in Figure 2. The first initial block is also called the genesis block. The connection of blocks is made possible by consensus protocols (Proof of Work - PoW and Proof of Stake - PoS). Each new block contains the hash code of the previous block. In this way, a chain of blocks is created that cannot be interrupted or see the content of the message.

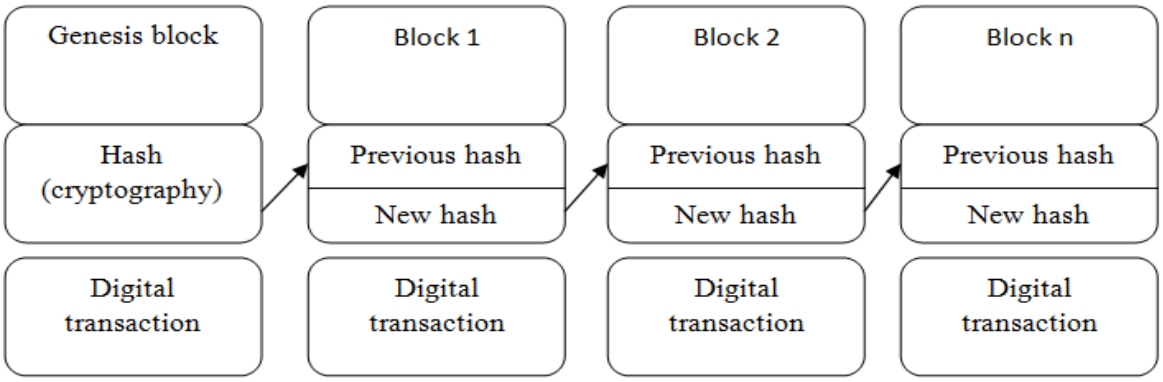

Fig. 2. Blockchain architecture

In this model, a hybrid blockchain network was chosen, which represents a combination of public and private networks. The public network is intended for all interested private and social persons who are not part of the railway system. The public blockchain network is open to all participants and the initiation of transactions where anonymity is guaranteed. The private blockchain network represents the railway's private property, where there are restrictions on accessing and initiating transactions. In this model, the railway uses a private blockchain network to monitor all transactions that are carried out and depend on procedures that are predetermined based on regulations and instructions.

The operation of blockchain to increase cyber security in the railway company involves six steps and is presented in Figure 3.

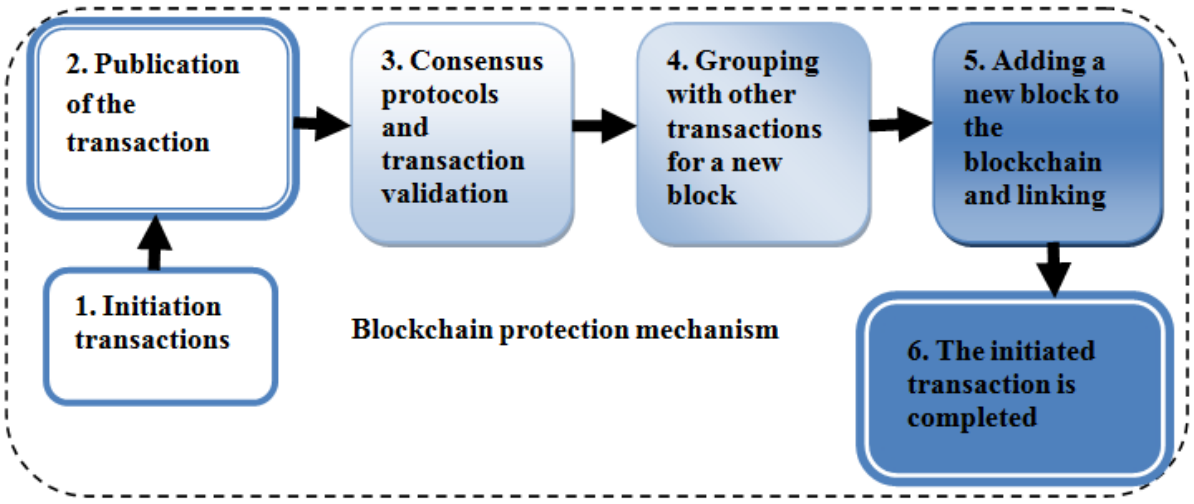

Fig. 3. Steps for the implementation of the blockchain protection mechanism

The first step involves the user or device initiating the transaction. The second step publishes the transaction to the hybrid blockchain network. In the third step, the nodes execute the consensus using the protocol and at the same time the initiated transaction is

validated. In the fourth step after the transaction is validated, the transaction is grouped with other transactions to form a new block in the main ledger. In the fifth step, the new block created is added to the blockchain network and at the same time is connected to the previous block and its hash code. Finally, in the sixth step, the transaction that was initiated was completed.

CONCLUSION

This paper presents a model for increasing cyber security in a railway company using blockchain technology. The railway company represents a complex system that relies on the application of a large number of devices, computers, signaling security and telecommunication facilities, where employees cannot perform their tasks efficiently and safely without the digitization of daily processes. A large number of activities that take place using advanced Internet technologies also require cyber security of the data that is the subject of communication. When taking into account the above and the needs of users who meet their needs through computers, it is necessary to increase the security of all digital activities.

Information security of digital activities must provide availability, confidentiality and integrity of messages exchanged in communication between people, equipment and devices. The solution lies in the application of blockchain technology, which is the strongest protection mechanism using cryptography. By creating a block chain of all transactions in digital messaging, the cyber security of the railway company is increased. A hybrid blockchain network was chosen, which at the same time does not allow access to unauthorized transactions and public access to all interested parties.

REFERENCES:

[1] 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

[2] 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.

[3] Z. Wang, G. Guo, C. Liu and W. Zhu, "Research on Railway DevSecOps System Construction Based on "People-Process-Technology"," *2022 2nd International Signal Processing, Communications and Engineering Management Conference (ISPCEM)*, Montreal, ON, Canada, 2022, pp. 19-23, doi: 10.1109/ISPCEM57418.2022.00010.

[4] L. Zhu, H. Liang, H. Wang, B. Ning and T. Tang, "Joint Security and Train Control Design in Blockchain-Empowered CBTC System," in *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8119-8129, 1 June1, 2022, doi: 10.1109/JIOT.2021.3097156.

[5] S. Chakrabarty and B. Sikdar, "Detection of Cyber Attacks on Railway Autotransformer Traction Power Systems," in *IEEE Transactions on Industry Applications*, vol. 59, no. 6, pp. 7188-7200, Nov.-Dec. 2023, doi: 10.1109/TIA.2023.3307496.

[6] A. Hohenegger *et al.*, "Security Certification of Cyber Physical Systems for Critical Infrastructure based on the Compositional MILS Architecture," *IECON 2021 – 47th Annual Conference of the IEEE Industrial Electronics Society*, Toronto, ON, Canada, 2021, pp. 1-6, doi: 10.1109/IECON48115.2021.9589691.

[7] Pavlović Z, Banjanin M, Vukmirović J, Vukmirović D., (2020,05,04): Contactless ICT Transaction Model Of The Urban Transport Service; Research journal TRANSPORT, ISSN:

1648-4142 / eISSN: 1648-3480, Vol 35 No 5, pp 500-510. https://doi.org/10.3846/transport.2020.12529
[8] 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.
[9] 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
[10] Zoran G. Pavlović, Veljko Radičević, Miloš Stojanović, Vasko Nikolov, Zlatko Belancan; ANALYSIS OF APPLICATION OF MOBILE INTERNET TECHNOLOGIES IN DIGITALIZATION ACTIVITIES, Book of Proceedings, International Multidisciplinary Conference "Challenges of Contemporary Higher Education" - CCHE 2024 Serbia, Kopaonik January 29th - February 2nd 2024 Vol_1, pp564-569 https://drive.google.com/drive/folders/15cMDG0QcNFyAIeeKTUMhqASA1NGZmvzJ
[11] 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
[12] 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