A Model of Application of Blockchain Technology to Increase Safety in Railway Traffic

Zoran G. Pavlović
College of Railway Engineering
Belgrade Academy of Technical and Art Applied Studies, BATAAS
Belgrade, Republic of Serbia
zoran.pavlovic@vzs.edu.rs, zoran.g.pavlovic@gmail.com

Abstract— **The development of railway traffic also implies the application of advanced computer technologies. Since high-speed trains run on certain routes (Belgrade Center - Novi Sad and back), the management and regulation of such trains is made possible by computers and networks. Humans mainly supervise on the basis of predetermined computer applications and programs. Currently, the railway infrastructure to Subotica is being modernized, the next step includes to Nis, where the prerequisites and the need to improve the safety of road users are being created. This paper analyzes potential attacks as well as the measures that must be taken by the railway company. Blockchain technology is a solution to a potential problem. The paper presents the potential of blockchain, the way of application as well as functioning in order to increase security.**

Keywords-component; blockchain, cryptography, security, rail traffic

I. INTRODUCTION

In accordance with innovative trends in the environment, when it comes to rail passenger transport, the needs of users as well as railway companies must be considered. The first and most important parameter must refer to the safety of all traffic participants (users, employees and third parties) who may be affected by a potential danger [1], [2]. The high-speed train system must provide the necessary parameters based on available advanced Internet technologies [3], [4].

In practice, there are a large number of examples of the application of advanced Internet technologies, which, through their implementation, can improve certain processes [5], [6]. Railway traffic and passenger transport on high-speed lines are using more and more devices that have the task of registering the changes that take place in the process of exploitation. Currently, the ETCS (European Train Control System) is applied on the Belgrade Centar - Nivi Sad route, which includes basic safety measures through:

- KMC (Key Management Center) ,
- PKI (Public Key Infrastructure).

Basically, the primary task of the ETCS system is to control the movement of the train, as well as, if necessary, to protect against speeding. The ETCS system consists of two basic parts, the track part and the locomotive part.

The track equipment of the ETCS level 2 system consists of:

- eurobalise - for the transfer of information between tracks and vehicles, as well as for the transfer of information about the stationing of isolated overlays KM (contact network) and RBC (radio block center) overlays;
- GSM-R (Global Mobile System - Railways) networks - a radio network that performs the function of exchanging information between the RBC and the equipment on the train;
- radio block center (RBC) - which generates a driving permit (MA) based on all the necessary static and dynamic data;
- key management system (KMS) - railway component in charge of managing cryptographic keys on the railway, in order to enable secure radio transmission of ETCS data.

Two-way data exchange between the locomotive and the railway is achieved through a wireless GSM-R network. The RBC generates the driving permit, the axle counters control the occupancy of the station and space sections, and the Eurobalises determine the location of the train.

In the form of maps, RBC contains driving routes, all static data of the railway section (allowed speeds, gradients, track condition, Eurobalise position). Through the direct connection between the RBC and the station signal-safety devices (CBI), the RBC has all the variable information (switch positions, signal display, etc.), with which it calculates the driving permit for each train controlled via ETCS, and can also revoke a previously issued driving license.

When the train passes over the eurobalise, the new position and speed of the train is sent to the RBC, it processes the received data and returns feedback allowing or prohibiting the entry of the train into the next block section, as well as information on the maximum permitted train speed.

For the above reasons, for a train running in the ETCS system, the signal signs of the light signals installed next to the tracks become redundant.

Such an organized train traffic system in ETCS implies a large amount of information that is exchanged in communication between railway and locomotive devices. Every regulated system has its weaknesses and special attention should be paid to the existing protection mechanisms and technologies. The main goal of this paper is to analyze potential attacks and propose a model for increasing security based on blockchain. Cyber security is ensured by blockchain where data privacy is ensured in the railway transport company. Blockchain also represents a large database for storage, use and distribution.

II. ATTACKS ON THE RAILWAY COMPUTER SYSTEM

The basic role of computer systems includes providing information for viewing, processing, storage and transmission. It implies the usual flow of information between interconnected devices in one computer system (eg computer memory with a camera or printer) or between multiple computers that are physically and spatially distant [7][8]. Required information unhindered flow where the enablement is the sharing of resources.

In addition to the mentioned usual flow of information, there may be an attack on the availability of the system where there is an interruption in communication. The easiest form of attack can be the interruption of a communication line, damage to a hardware component, obsolescence of a software program, etc.

Attacks related to integrity (content) involve modifying the message. Then there is a change in the content of the message, which can be a notification, information or even an order. In any case, the recipient of the message does not receive the original message, but a modified one, where the essence of the message and its meaning are changed.

The next type of attack involves learning about the content of the information being transmitted, its secrecy and confidentiality. In this way, an unauthorized person who does not have the right of access, intercepted, gets access to the content of the information. With the help of appropriate software and programs, a third party in the attack can illegally copy the transmitted information. In this case, the requester or the final destination receives the information unchanged, but also without knowing that the attacker also received the same information.

The next type of attack refers to information fabrication, where an unauthorized person creates fake messages within a possible information stream. An example can be identity theft of a specific person and impersonation by sending messages containing wrong information or modifying some messages in the communication of interested parties.

All the listed scenarios of potential attacks can be realized by a malicious person who has the basic idea to disrupt the functioning of railway traffic.

III. RELATED RESEARCH

In the scientific research community, there is a large number of works that have provided electronic business with blockchain technology. The selected examples of researchers show the potential that can be applied in rail transport.

The development of the digital economy is changing the ways of modern business and the exchange of digital information. In the world of digitization, data and information are intensively traded and there is a need to ensure the transmission of transactions over the network. Consistent integrity of data and records in modern distributed information systems can be achieved using blockchain technologies. Blockchain applications are based on distributed ledger, cryptography, consensus, protocols and smart contracts. Blockchain technology and the possibilities of their application in electronic commerce, healthcare, education, agriculture, industry, transportation, telecommunications, administration and other fields [9].

Railways around the world are moving towards digitization to improve their operations. The integration of rail data with data from other modes of transport is becoming a vital part of the next generation of digital transport systems. One of the challenges for further digitization is data integration and security. This situation remains a challenge across organizations and industry boundaries. Blockchain is an emerging technology that could have the potential to act as an enabler for the data integration and security challenge. A moderate review of the literature on the use of blockchain in various industries, especially IoT applications, and in the context of railways is presented. The opportunities and challenges that blockchain technology can offer for the railway industry are outlined. Current and potential rail-related blockchain applications are also discussed. A simple analysis of the technology for the potential adoption rate is also considered. It found that blockchain can offer a number of benefits, including added security and decentralization, but the technology will have a moderate rate of adoption before it reaches a transformative impact [10].

If all vehicles are connected through a wireless communication channel, vehicular ad hoc networks (VANETs) can support a wide range of real-time traffic information services, such as intelligent routing, weather monitoring, emergency calls, etc. However, the accuracy and credibility of messages transmitted between VANETs is of the utmost importance because life may depend on it. A new framework called blockchain-assisted privacy-preserving authentication system (BPAS) is introduced that automatically provides authentication in VANETs while preserving vehicle privacy. This design is very efficient and scalable. It does not require any online registration center (except for system initialization and vehicle registration) and enables conditional tracking and dynamic recall of misbehaving vehicles [11].

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. The existing identity authentication mechanisms in CBTC adopt a single-point fault-sensitive centralized key management system. To improve system security, blockchain is

implemented in CBTC 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. Based on a blockchain-based distributed security scheme, block producer selection and the blockchain client handover decision problem are studied. Aiming to minimize the impact of the key update process on the performance of the CBTC system and to maintain the security of the system at a reasonable level, the block producer selection and block client handover decision problem is formulated using a deep reinforcement learning approach [12].

IV. BASICS OF BLOCKCHAIN APPLICATION

A. *Blockchain Basics*

In recent years, a considerable amount of effort has been invested in protecting computer systems from cyber threats, which is one of the most critical cyber security tasks for individual users and businesses, as even a single attack can result in compromised data and sufficient losses [13].

At the beginning, blockchain technology was applied for bitcoin and cryptocurrencies, while today various application models are being developed and even in traffic. The basic task of blockchain technology is to secure and verify all kinds of data in a pre-decentralized network. A chain of blocks in a blockchain is a series of records, where the next one is added based on the previous one, thus creating a connected chain. Blockchain is immutable because it involves cryptography mechanisms to secure data. This way of applying blockchain technology creates a block containing a time stamp, hash and data. The process implies and includes data that is recorded and verified within one block. Adding a new block implies the content of the previous block, or in other words, it contains the hash of the previous block, which becomes an integral part of the newly created block.

Basically, the application of blockchain technologies can be:

- A public cryptocurrency code where every user is allowed to join online,
- Private where not everyone can access the network, a decentralized system is applied but still controlled by one center and access is limited to a defined network or in other words allowed only to predetermined users or devices,
- The hybrid model implies a combination of public and private models where it is necessary for some data to be publicly available, but at the same time it limits access to secret and sensitive data.

B. *Mechanism of cryptography*

When it comes to the railway company, the participants and devices in the decentralized network are defined in advance, how a new block is created based on received messages, how verification is performed and how the newly created block is added to the block chain. The above can be achieved by applying a cryptographic hash function, or in other words, the process is realized by a mathematical algorithm that maps data of arbitrary length into an output of fixed length.

The cryptographic hash function is a process protection where a fixed-length sequence is taken and calculated on the basic message, which is an addition called a hash (Fig. 1). This means that it is infeasible for a malicious attacker to compute another message and replace it with the underlying message that is protected by the hash function. The algorithm calculates the hash value in a four-step process: the padding step involves adding a one followed by enough zeros, the addition step includes adding a bitwise representation of the message length before padding, an initialization step of the accumulator variable, and a final step with a loop where the message blocks are composed of the bit words that are processed in four cycles [14].

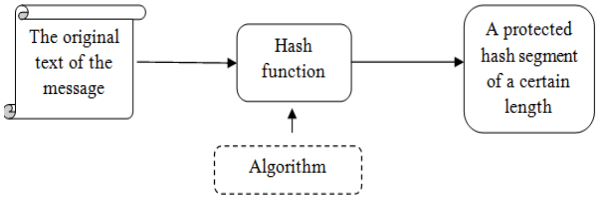

Figure 1. A cryptographic hash function

As already mentioned, blockchain is a technology that is increasingly represented in all areas of electronic business. Today, innovative models based on blockchain are increasingly being implemented in the research community as well as in the economy. Essentially it is a protocol that enables the secure exchange and storage of information that occurs in predetermined processes. This means that the received data is placed in blocks, after which these blocks are cryptographically connected to each other in a chain. This protection mechanism provides a high degree of protection and at the same time the entered data cannot be changed.

In this paper, for the needs of the railway company, a model of increasing safety on high-speed railways using blockchain technology is presented. Currently, the ETCS system is applied on the territory of the railway on about 100 km of track. In the near future, the length of the railway is expected to be 600 km. The modernization of infrastructural capacities obliges the railway company to apply the available mechanisms in order to protect the data of the processes taking place. An attack by a malicious person can cause unimaginable consequences for property and the human factor.

The solution to the eventual problem may be in the blockchain. The ETCS system includes communication and message exchange between devices that are installed on infrastructure facilities as well as on locomotives. All these devices are connected to the hardware on which the software that provides data protection in blockchain technology is installed. In the most unfavorable scenario, when a large number of trains will be running on high-speed tracks, the devices responsible for setting the driving path, balises, transferring information from the locomotive to the devices and

from various devices to the locomotives or the dispatch center, reading occupied transport capacities, issuing tickets and the like there is a possibility of violating the security of the railway system or in other words there is a possibility of violating the integrity of messages exchanged in communication. In this way, there are unwanted consequences that can damage the image of the railway company. Blockchain technology guarantees authenticity and verifies transactions that occur in messaging based on cryptographic algorithms. This means that when the balise placed on the track sends information to the dispatch center or the locomotive, the authenticity must be checked with an algorithm.

The implementation of the functioning of the blockchain in the railway company is shown in fig. 2. 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.

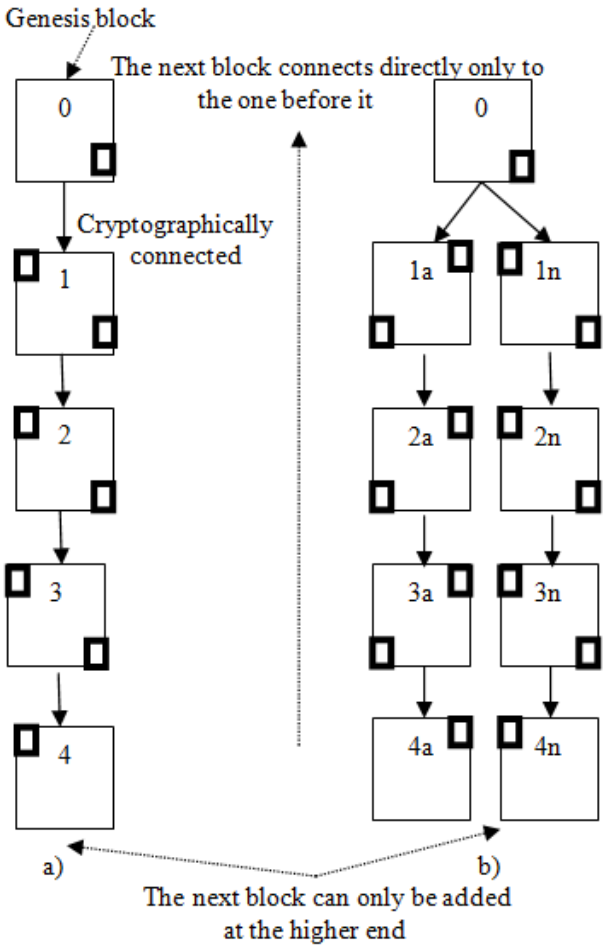

Figure 2. Structure and branching of blockchain application in railways

The first block is always the genesis block. The connection between the blocks is achieved by cryptographic connection. The next block can be connected only after the highest number on which the previous electronic transaction (block) was added. In the same picture under b, the branching of blocks is shown, or in other words, if two or more transactions are started at the same time, the new blocks are connected in parallel with the previous one. When the need for branching ends, the chain of blocks continues linearly. In particular, it should be noted that each subsequent block takes over the addition from the previous block, which is shown in fig. 2 as a small square in the corner.

Each block created in electronic transactions has a defined structure and the most important among them are: magic number, version number, link to the previous block, transaction hash, time stamp, transaction counter and finally the transaction.

All transactions that take place using the blockchain are protected, so that a malicious person cannot violate the integrity of the messages exchanged for the needs of the railway company.

V. CONCLUDING CONSIDERATIONS AND A PROPOSAL FOR FUTURE RESEARCH

This paper presents a model of data protection as well as their storage, distribution and application in a railway company. Every year, the transport company for railway traffic defines a new timetable where malicious people (hackers, terrorists...) can cause unwanted activities. Given that computer technology is becoming more prevalent, it is also important to use innovative protection mechanisms. Cyber security based on blockchain technology today represents the most acceptable solution for large economic entities, for a large number of computer transactions on which the functioning of railway traffic, exchange between infrastructure devices, employees and the like may depend.

The model is described in the most unfavorable possible scenario where electronic transactions of exchange and storage of a large number of messages are performed. The model ensures the integrity of messages as well as their immutability.

Future research must be focused on the implementation of the proposed model. The starting point for the presentation of this model is a unique platform that should be implemented in the railway company. Cyber security encompasses a large number of networked computers and devices that are essentially the basis of the application of blockchain technology.

REFERENCES

[1] 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

[2] Zoran G. Pavlović, Veljko Radičević, Branislav Gavrilović, Marko Bursać, Miloš Milanović; A Sensor Network-Based Model for Increasing Safety on High-Speed Railways, XI Triennial International Conference Heavy Machinery HM 2023 Book of Proceedings, VRNJAČKA BANJA, SERBIA June 21– June 24, 2023, pp B101-B108, https://www.hm.kg.ac.rs/documents/HM2023-Proceedings.pdf

[3] 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

[4] Z. G. Pavlović, "Technologies of electronic business in traffic," *2022 21st International Symposium INFOTEH-JAHORINA (INFOTEH)*, 2022, pp. 1-4, doi: 10.1109/INFOTEH53737.2022.9751297. https://ieeexplore.ieee.org/document/9751297

[5] Pavlović Z, Banjanin M, Vukmirović J, Vukmirović D., (2020,05,04): *Contactless ICT Transaction Model Of The Urban Transport Service*; TRANSPORT, ISSN: 1648-4142 / eISSN: 1648-3480, Vol 35 No 5, pp 500-510. https://doi.org/10.3846/transport.2020.12529

[6] 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

[7] Pavlović, Z. G., Radičević, V., & Nikolić, D. (2021, 10 15). *Tehnologije za zaštitu podataka u digitalnim poslovnim procesima*. (Z. Čekerevac, Ur.) FBIM Transactions, 9(2), 63-70. doi:10.12709/fbim.09.09.02.07 https://www.meste.org/ojs/index.php/fbim/article/view/1202/1311

[8] Nikolić, D., Radičević, V., & Pavlović, Z. G. (2021, 10 15). *Modeliranje arhitekture i infrastrukture inovativnog modela e-poslovanja*. (Z. Čekerevac, Ur.) FBIM Transactions, 9(2), 55-62. doi:10.12709/fbim.09.09.02.06 https://www.meste.org/ojs/index.php/fbim/article/view/1201/1310

[9] Zorica Bogdanović, Božidar Radenković, Marijana Despotović-Zrakić, Dušan Barać, Aleksandra Labus, Tamara Naumović, BLOKCHAIN TECHNOLOGIES: CURRENT STATE AND PERPECTIVES, Book of Proceedings of International Scientific Conference on Digital Economy DIEC, 2/2/2019, Print ISSN**:** 2566-4514 Online-ISSN**:** 2566-4522

[10] F. Naser, "REVIEW : THE POTENTIAL USE OF BLOCKCHAIN TECHNOLOGY IN RAILWAY APPLICATIONS : AN INTRODUCTION OF A MOBILITY AND SPEECH RECOGNITION PROTOTYPE," *2018 IEEE International Conference on Big Data (Big Data)*, Seattle, WA, USA, 2018, pp. 4516-4524, doi: 10.1109/BigData.2018.8622234.

[11] Q. Feng, D. He, S. Zeadally and K. Liang, "BPAS: Blockchain-Assisted Privacy-Preserving Authentication System for Vehicular Ad Hoc Networks," in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4146-4155, June 2020, doi: 10.1109/TII.2019.2948053.

[12] 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. keywords:

[13] "Big Data Analytics and Intelligent Systems for Cyber Threat Intelligence," in *Big Data Analytics and Intelligent Systems for Cyber Threat Intelligence* , River Publishers, 2022, pp.i-xxx.

[14] J.Kurose , K. Ross , Umrežavanje računara, prevod sedmog izdanja , Računarske fakultet, CET, 2018.