14rd International Defense and Homeland Security Simulation Workshop, 008
21st International Multidisciplinary Modeling & Simulation Multiconference

2724-0363 © 2024 The Authors.
doi: 10.46354/i3m.2024.dhss.008

Blockchain for Secure Railway Signal Communication & Protection of Critical Infrastructures

Agostino Bruzzone[1,2,*], Antonio Giovannetti[2], Siddhi Rajendra Gangar[3], Lorenzo Motta[3]

[1]DIME, University of Genoa, Via Opera Pia,15, Genoa, 16145, Italy.
[2]Simulation Team, Via Magliotto,2, Savona, 17100, Italy.
[3]Hitachi Rail STS, Via Paolo Mantovani,5, Genoa, 16151, Italy.

[*]Corresponding author. Email address: agostino,.bruzzone@simulationteam.com

Abstract

Blockchain is transforming the digital world by providing a new perspective on the security, efficiency, and reliability of the system and data. It is a digital public ledger that is decentralized, distributed, and immutable, in which digital data is approved and shared with all participating users. This research study explores the blockchain key concepts and principles. It is currently used in various industries like supply chain, logistics, healthcare, finance, and many more because of its key features. One of the rapidly growing railway industries is the new frontier for blockchain technology, with its groundbreaking use cases having potential for significant impact. This study explores the cybersecurity aspects of blockchain technology and its potential benefits for railway applications and related critical infrastructures. We implemented a basic permissioned blockchain network i.e. Hyperledger Fabric that successfully ensured the integrity, confidentiality, and availability of the signaling data. Finally, the paper concludes by discussing the challenges encountered during the implementation of the disruptive technology and outlines future research directions aimed at gaining more valuable insights into the cybersecurity aspects of blockchain technology.

Keywords: Blockchain, Cybersecurity, Railways, Critical Infrastructures

1. Introduction

In today's rapidly evolving technological advances, blockchain technology disrupts numerous sectors with its potential to revolutionize them. The objective of this research was to explore the potential of blockchain technology to secure railway signal communication and related critical infrastructures. Many people are opting for rail for their daily travel journeys. Rail companies are relying on digital systems to manage ridership and complex infrastructure. As railway operations are becoming increasingly reliant on internet-connected technologies and due to this digitalization, cyberattacks are becoming more frequent. Indeed railways are resulting critical infrastructures and have potential vulnerabilities in terms of cyber-attacks affecting operations, block of transportations for cargo and passengers as well as safety and potential accidents. In railway operations, the most important factor is to ensure the safety, efficiency and security of the railway signaling system.

Railway signaling systems often rely on centralized communication, creating a signal point of failure and are vulnerable to the cyberattacks. A successful cyberattack on this central system could disrupt communication and potentially compromise the integrity of signaling data (Patwardhan et al., 2021). So, leveraging blockchain technology has the potential to address these challenges and enhance the security and efficiency of railway operations. Blockchain technologies known for its distributed, decentralized and tamper-resistant nature, offers the potential solution to these security concerns. Due to decentralization, distributing data across the network nodes and incorporating cryptographic mechanism, blockchain could enhance cybersecurity (Ramachandran, 2024) in terms of integrity, availability, and confidentiality of the data and mitigate the risk of cyberattacks.

2. State of the Art

2.1. Cybersecurity

In cybersecurity, CIA (i.e., Confidentiality, Integrity, and Availability) are the three crucial elements (Veale & Brown, 2020).

- Confidentiality: It means that only the authorized users or systems have access to the data or information or systems.
- Integrity: It assures that the data or information is not altered or tampered with or modified or corrupted.
- Availability: It means having uninterrupted access to the information or data.

In general, when there is cyberattacks these three elements are impacted. They define the security goals of any system and use them as a framework for evaluating and improving the security measures (Cawthra et al., 2020). These elements are fundamental for designing, implementing, and maintaining secure systems (Bruzzone et al., 2013).

2.2. Overview of Blockchain

Blockchain is a decentralized and distributed digital ledgers that records and verifies the transactions across multiple nodes or computers. It provides a secure, transparent, and tamper-resistant way of recording and managing the digital information (Bashir, 2023). The key characteristics of this technology are:

- Decentralization: Each node in the blockchain network maintains a copy of the complete transactions called ledger making it distributed ledger system that records or stores all the transactions, enhancing availability of the data.
- Immutability: It becomes nearly impossible to alter or delete the transactions that are recorded on the blockchain network due to the cryptographic and decentralized nature of the blockchain technology ensuring integrity of the transactions.
- Consensus Mechanism: This mechanism is used in blockchain networks to agree on the validity of the transactions. It maintains the integrity of the ledger by ensuring that all the nodes validate the transactions and reaches consensus on the state of the blockchain.
- Smart Contracts: They are the contract that enforce agreements between the nodes eliminating the need of the intermediators, and they are the automated and self-executing contracts with predefined rules and conditions.

There are two types of the blockchain technology:

- Permissioned blockchain: It is sometimes called as private blockchain where only authorized participants or nodes are able to join the network. They are mostly controlled by an administrator who sets the rules and governs the network (Capocasale et al., 2023). Example: Hyperledger.
- Permissionless blockchain: It is also called a public blockchain, anyone with internet access ccould join and participate in the network. All the transactions are visible to everyone on the network (Capocasale et al., 2023). Example: Bitcoin, Ethereum.

In permissioned blockchain, confidentiality is high due to the restricted access to authorized participants whereas integrity and availability are high in both permissioned as well as permissionless blockchain. Data integrity is ensured through cryptographic nature and consensus mechanism of the blockchain network and decentralized & distributed architecture maintains the availability of the data (Mani, 2017) (Abasi, 2022).

In summary, the Data integrity is maintained because of the blockchain's immutable ledger that ensures that once the data being recorded, it cannot be deleted or altered. Data availability is ensured because of the decentralized and distributed nature of blockchain reduces the risk of single point failure. Data confidentiality is ensured because of the cryptographic nature of the blockchain technology to secure data ensures that only authorized users have access to the data. Hence, the cybersecurity three elements i.e., confidentiality, integrity, and availability of the data is maintained through the key

features of blockchain.

2.3. Industries

Blockchain technology has transformed various industries including banking & finance, supply chain, logistics, healthcare, energy and many more. The key features of this technology make it suitable for a wide range of use cases where trust, security, and transparency are crucial (Crosby et al., 2016).

In this research, we have used Hyperledger Fabric blockchain platform which is an open-source permissioned network that provides solid foundation for developing enterprise grade blockchain networks. Its key features include immutability, decentralization & distributed ledger system, along with its scalability & modular architecture make it suitable for industries like transport. Unlike some other blockchain platforms that use cryptographic mining to secure the network and incentives participants, Hyperledger Fabric does not have a native cryptocurrency. The absence of a native cryptocurrency in Hyperledger Fabric reduces the operational cost of deploying a blockchain network and eliminates the need for expensive mining operations. This makes the platform a cost-effective solution for many businesses and organizations that want to use blockchain technology to improve efficiency, transparency, and security (Hyperledger Fabric, 2020) (Bruzzone et al., 2019).

2.3.1. *Railway Industries*

The digital transformation of the rail industry has the potential to improve the performance, competitiveness, safety, and security of the railway systems. Railway is one of the most intricate and interconnected transportation industry. The entire railway network connects states & cities via a large database, and it is impossible to avoid security problems, improper signaling, safety of passengers, etc. without continuous monitoring and governance. Thus, a piece of any incorrect information could seriously damage the entire railway network. The cyberattack on the railway network could cause significant disruption of the railway operation. One of the railway operations could be railway signaling system. The information threats and vulnerabilities contribute to affect the continuity of railway operation not only causing inconvenience to just train traffic but also financial losses and damages to the reputation of the railway authorities (Meda et al., 2008). In a typical railway signaling system, the wayside controller (WC) communicates its status and relevant information such as signal information, track occupancy information, etc. to the operation command center (OCC). The OCC then processes these data and makes decisions related to the train operations, route assignment, and other activities based on the information received. The OCC then sends the control commands back to the WC (Rail Baltica, 2023). The OCC is a centralized system and cyberattack could potentially damage or fail this centralized system. The cyberattack could impact integrity, availability, and confidentiality of the signaling data which in turns disrupt the railway operations. So, by leveraging and adopting the features of the blockchain technology we could improve cybersecurity of the railway signaling system.

3. Model

The steps that were followed for this model are:

- The network architecture was designed hat includes defining peers, orderer, channels, and other network information.
- After designing the network architecture, Hyperledger fabric network 2.0 was setup.
- Golang programming language was used to write the smart contract.
- JavaScript was used to develop the web interface.
- Nodejs was used for Fabric SDK which basically allows client to interact with the Hyperledger fabric blockchain network.
- An ubuntu VM machine was used for deploying Hyperledger fabric blockchain network and testing this model.

3.1. Architecture

The railway signaling architecture includes three entities i.e., Wayside controller 1 (WC1 or Org1), Wayside Controller 2 (WC2 or Org2), Operation Command Center (OCC) were considered for designing this model. Trackside signals (ID1 and ID2) are associated with the WC1 and WC2 respectively. WC1, WC2, and OCC operates as peers on the blockchain network. Each peers maintains its own ledger on the hyperledger fabric network and this ledger records and updates the signaling data.

The network configuration for this model consists of (Hyperledger Fabric, 2020):

- Peers: They maintain the copy of entire distributed ledger and take participation in the consensus process to validate and endorse the transactions. There are two types of peers: endorsing peers and committing peers. The endorsing peers execute the smart contracts, validate transactions, and provide endorsements whereas committing peers validate and commit the block of the transactions to the ledger. In this model, the data is replicated across multiple peers ensuring the availability of the data even in case of some peers or nodes fail to become available.

- Orderer: It is a node that is responsible for ordering the transactions and delivering the block of transaction to the peers. Here, in this model solo orderer was used as a consensus mechanism to ensure that all then nodes agree on the order of the transaction.
- Channel: Channel is used for secure communication between the participating peers and this channel ensure that only authorized participants are able to access the network i.e., it ensures confidentiality.

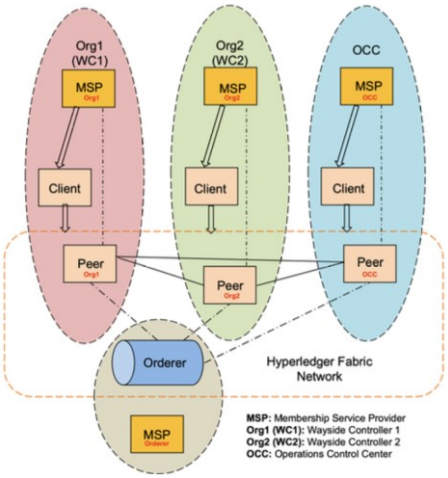

Figure 1. Hyperledger Fabric Network Architecture

- Membership Service Providers (MSP): MSP uses signature-based authentication model for read, write, administer, and endorse transactions and it manages digital identity. In this model, each organization (WC1, WC2, OCC) has its own MSP and each MSP manages its own digital identity which are cryptographic keys (public-private key pair) that are issued by the certificate authorities (CA). Here, when the participating peers interacts within the network, it signs the transaction with its private key. This signature (certificate) is then verified using the organization's public key by the network to ensure integrity of transaction within the network. Thus, MSP enables the network to recognize and trust the identity.

3.2. Hyperledger Fabric blockchain network setup

The process for setting up the hyperledger fabric blockchain network (Hyperledger Fabric, 2020) are as follow:

- Generating cryptographic material such as certificates and keys for the network organization, peers, and orderers.
- Creating the genesis block which defines the initial network configuration; defining the channels which is used for secure communication between the peers; creating peers that participate in the network.
- To build the fabric network that involves starting the peers and orderer docker containers.
- Once the network is up and running, peers join the channel.
- To develop the smart contract that needs to be deployed on the network, install the smart contract on the peers that execute the smart contract; Instantiate the smart contract on the channel created to make it active and ready to process the transactions.

3.3. Smart contract logic

Smart contract also called as chaincode in hyperledger fabric blockchain network (Hyperledger Fabric, 2020) which implement the logic The chaincode logic for this model is as follow:

- The chaincode is deployed and initialized on the fabric network when the "Init" function is called. In this model, no specific tasks are performed during initialization.
- The "Invoke " function used when a transaction is invoked on the chaincode. It determines the specific function i.e., "Generate Command" or "Get signal."
- Generate command: It takes ID and Status of signal as the input parameters, validate this parameter, and generate the corresponding outputs i.e., ID, status, command, response, and timestamp and these outputs are stored on the blockchain network.
- Get signal : Takes ID as the input parameter, read the information corresponding to that ID that was stored on the fabric network and returns the output information i.e., status, command, response, and timestamp.

3.4. Scenario

The web interface written in JavaScript programming language. It runs on a local host where Apache2 is used as a webserver because it is a local development environment. The web interface allows users to see multiple signals. Upon clicking a "Start" icon, the interface initiates a process that automatically changes the signal colors on the display at the defined intervals. This interface provides a function for sending signal IDs, statuses, and timestamps to the chaincode. The Fabric SDK is used for interaction with a hyperledger fabric blockchain network.

The scenario simulates a situation where there are three signals' lights ID1, ID2, and ID3. The signals ID1 and ID2 are considered as legitimate signals while ID3 is considered as an attacker. The signals light sends the

signals that includes ID and status to the fabric network. The output determined based on these ID and status values. For example, if ID1 signals a yellow status, the chaincode logic installed on the peers generates a "caution" command, which is accepted because it originates from valid ID. Conversely, if ID3 signals a yellow status the chaincode logic generates a "caution" command but rejects this ID because it is associated with an invalid ID. Consequently, ID3 is denied access to the fabric network.

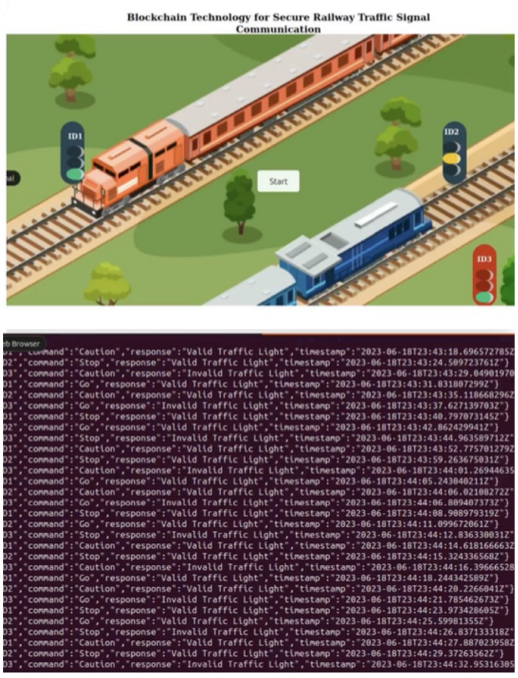

Figure 2. Scenario

4. Conclusions

In conclusion, blockchain technologies for secure railway signal communication provide comprehensive and robust solutions. The model represents that by emphasizing on confidentiality, integrity, and availability, using permissioned blockchain technology (i.e. Hyperledger Fabric), the objective to establish a robust and reliable railway signal communication system could be achieved. During the development of this project, the challenges encountered were during the setup and deployment of the permissioned blockchain network. The documentation and tutorials to set up the fabric network were available but adapting them to the specific requirements was time-consuming and complex. The journey for this research study on blockchain technology provided valuable insights that could provide potentially benefit to rail industry in developing robust, efficient, and secure solution for railway operations.

Due to time and resource limitation, comprehensive testing of permissioned blockchain network (i.e. Hyperledger Fabric network) for secure railway signal communication model on a production environment was not feasible. Therefore, this model was conducted within a development environment.

Some features that need to be implemented and to be carried out in future are as follow:

1. Security Evaluation: To simulate cyberattacks on the fabric network to access the Hyperledger fabric platform's ability to maintain data confidentiality, integrity, and availability. Exploring the private channels configuration in fabric network to restrict data visibility to specific nodes or participants. Also, integration with external CA for identity management and certificate issuance to ensure that the fabric network meets the organization's security requirement and provides a secure and trusted environment.
2. Performance and Network Size: To analyze how the fabric network's performance (i.e. transaction processing speed) is affected by the number of the organizations and peers for each organization participating in the network. This would be carried out by simulating different network sizes and measuring their performance. As the network grows in terms of size, scalability challenges may arise, in terms of data storage and processing the transaction. So, it is necessary to test how well the network handles the increased transactions volume to maintain the network's performance and security.
3. Latency Evaluation: For real time traffic management, analyzing the communication latency between signaling, wayside controllers, and operation control center in the distributed network. It is possible to identify the delay in data transmission by evaluating the latency. Latency plays a vital role for maintaining the efficiency, safety, and security of the railway operations.

In real world railway operations scenarios, conducting the above simulations could provide more valuable insights in terms of security and performance of the Hyperledger fabric network platform. It is possible to access the fabric network's suitability, identify areas for improvement and to make informed decisions related to its deployment in railway operations.

References

Abasi, F. (2022). Blockchain and its impact on information security's CIA-Triad. Forward Security. https://forwardsecurity.com/blockchain-and-its-impact-on-information-securitys-cia-triad/

Bashir, I. (2023). Mastering blockchain: A technical reference guide to the inner workings of Blockchain, from cryptography to DEFi and NTFs (4th ed.). Packt Publishing.

Bruzzone, A., Sinelshchikov, K., & Massei, M. (2019). Application of blockchain in interoperable simulation for strategic decision making. In Proceedings of the 2019 Summer Simulation Conference (SummerSim '19) (pp. 1–9). San Diego, CA, USA; Society for Computer Simulation International. https://dl.acm.org/doi/10.5555/3374138.3374159

Bruzzone, A. G., Merani, D., Massei, M., Tremori, A., Bartolucci, C., & Ferrando, A. (2013). Modeling cyber warfare in heterogeneous networks for protection of infrastructures and operations. Proceedings of I3M2013, Athens, Greece.

Capocasale , V., Gotta, D., & Perboli, G. (2023). Comparative analysis of permissioned blockchain frameworks for industrial applications. Blockchain: Research and Applications, 4(1), 1–13. https://doi.org/doi.org/10.1016/j.bcra.2022.100113

Cawthra, J., Ekstrom, M., Lusty, L., Sweetnam, J., & Townsend, A. (2020). Data integrity: Detecting and Responding to Ransomware and Other Destructive Events. NIST Special Publication 1800-26A. https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html

Crosby, M., Nachiappan, Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). BlockChain Technology: Beyond Bitcoin . Applied Innovation Review, (2), 1–19. https://doi.org/https://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf

Hyperledger Fabric. (2020). A blockchain platform for the enterprise. A Blockchain Platform for the Enterprise - Hyperledger Fabric Docs main documentation. https://hyperledger-fabric.readthedocs.io/en/latest/index.html

Mani, V. (2017). A View of Blockchain Technology From the Information Security Radar. ISACA Journal , 4. https://www.isaca.org/resources/isaca-journal/issues/2017

Meda, E., Picasso, F., Domenico, A. D., Mazzaron, P., Mazzino, N., Motta, L., & Tamponi, A. (2008). In Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems CISIS'08 (pp. 116–122).

Patwardhan, A., Thaduri, A., & Karim, R. (2021). Distributed Ledger for Cybersecurity: Issues and Challenges in Railways. Sustainability, 13(18), 1–19. https://doi.org/10.3390/su131810176.

Ramachandran, K. (2024). Blockchain Technology for enhancing cybersecurity in India. International Journal of Blockchain Technology, 2(1), 9–20.

Rail Baltica. (2023). Railway Control-command signalling system. https://www.railbaltica.org/wp-content/uploads/2023/08/RBDG-MAN-022-0103_RailwayControlCommandSignallingSystem.pdf

Veale, M., & Brown, I. (2020). Cybersecurity. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1533