Distributed Ledger for Cybersecurity: Issues and Challenges in Railways

Amit Patwardhan *, Adithya Thaduri and Ramin Karim

Abstract: The railway is a complex technical system of systems in a multi-stakeholder environment. The implementation of digital technologies is essential for achieving operational excellence and addressing stakeholders’ needs and requirements in relation to the railways. Digitalization is highly dependent on an appropriate digital infrastructure provided through proper information logistics, whereas cybersecurity is critical for the overall security and safety of the railway systems. However, it is important to understand the various issues and challenges presented by governance, business, and technical requirements. Hence, this paper is the first link in the chain to explore, understand, and address such requirements. The purpose of this paper is to identify aspects of distributed ledgers and to provide a taxonomy of issues and challenges to develop a secure and resilient data sharing framework for railway stakeholders.

Keywords: railways; cybersecurity; blockchain; distributed ledger

1. Introduction

The railways are a critical part of the infrastructure in any country. The operations of freight as well as passenger services have strict requirements of reliability, availability, maintainability, and safety. The consistency of railway transport in terms of schedules and availability is affected by various factors related to the operation and maintenance of the overall infrastructure and the support of various railway stakeholders. The current segregation and structure of the railways has its roots in the deregulation of the railways, which started in Europe in the 1980s with the intention of ensuring the best use of public funds and to create a sustainable environment within economic and legal requirements [1]. Reducing the state monopoly allowed private actors to come into the domain and improve efficiency through competition, investment through entrepreneurship, and lack of government constraints with innovative practices to provide a better quality of service and comfort to the passengers with a lower cost to society [2]. Deregulation over a period helped to bring in a common European market for services, material, equipment, and standardization in the railways to set railways as the preferred mode of transport [3]. Different countries worldwide have followed different models in the deregulation process to simplify the process of bringing in private operators [4–7].

The functionality of railway systems depends on various factors including people, policies, processes, software applications, information, infrastructure, etc. Vertical separation was created to segregate the infrastructure and operations to ease the process of entry for new operators. The vertical segregation of the overall operations and services resulting from deregulation has created an array of stakeholders who are responsible for different aspects of the system while working within the regulations to fulfil the requirements. Stakeholders support different parts of the system; some of the stakeholders in railways are regulators, infrastructure managers, manufacturers of high-value equipment, manufacturers of rolling stock, rail-set owners, rail-set operators, maintenance service providers, etc. Operators compete through a tendering process to gain the rights to operate in a certain...
region or route; however, to reduce the cost of operations, the operators do not own the rail-sets, which they acquire on lease from the rail-set owners. In the Swedish context, rail-set (locomotive with passenger coaches and freight wagons) owners and operators are separate entities. This creates a condition where different operators may use the same equipment at different points in time. The segregation of stakeholders and the necessity of the equipment being shared in space and time increases the complexity of data sharing and requires various governance, business, and technology-related issues to be resolved.

Regular use and exposure to the elements leads to the deterioration and the eventual failure of components, equipment, and infrastructure. Failure of equipment in a connected and dependent railway infrastructure affects multiple stakeholders and disturbs the overall operations. Smooth and secure railway operations require a constant maintenance effort on infrastructure and the rolling stock. The steps of inspection, detection and prediction, maintenance planning, scheduling, and process are indispensable to maintain high availability. The development of tools and techniques in conditions-based maintenance has led to an improvement in the overall utilization of the equipment. These maintenance methods are in turn dependent on the fusion of a large amount of sensor data, inspection reports, maintenance processes, etc., and eventually domain knowledge. The collection, storage, communication, processing, and management of data, processing models, and results represents the linchpin to deliver the future expected by the end-users considering data-driven decision making.

The increasing requirements of railways in terms of data collection, transmission, storage, processing, and overall data management has increased the need for digitalization. The internet, the digital expressway connecting the edge devices, and the cloud infrastructure simplify the creation and maintenance of scalable communication and computing infrastructure to support the requirements in the digital domain. However, the digital domain is plagued by issues of cybersecurity and cyber threats. With their expansion, railways have an ever-increasing need for communication and computation resources and in turn, their dependence on digitalization creates exposure to cyber threats [8,9].

Data storage and sharing have traditionally followed a centralised architecture. However, cyber threats engender a single point of failure. Additionally, data integrity is questionable since a malicious agency can not only access the data but also can modify the stored contents to represent false conditions. Complexity, lack of resources, and issues pertaining to cybersecurity create a reluctance towards data sharing and large amounts of collected data are not used within the organization or shared among the stakeholders [10].

In a multi-stakeholder environment, confidence in the security of any individual organization is difficult due to the secrecy maintained about the cybersecurity practices. During a data transfer, the source and destination require authentication for each transaction, while the communication and sharing of the credentials themselves can be insecure. The data or the models exchanged do not provide any assurance of integrity and lack metadata, ownership, and lineage. Consequently, a low level of Expected-Level-of-Trust (ELoT) requires a higher level of cybersecurity. In this work, the cybersecurity architecture is assumed to be on the lowest level of ELoT, also called Zero-Trust, which is the most challenging scenario. Enabling the cybersecurity for the Zero-Trust scenario in relation to the railways can be achieved based on different approaches. One of these approaches is through a decentralized consensus-based governance model, implemented through the concept of distributed ledgers.

Distributed ledgers provide data security through open algorithms with well-evaluated resilient security practices and usage guidelines. All the participants apply the practices following the same set of guidelines, setting the same and known level of security decreasing the level of ELoT.

Distributed data storage for a multi-stakeholder environment such as the railways requires support for maintaining data integrity and data security. Maintaining integrity, authenticity, and consensus for the stored data has limitations when implemented through centralised data storage. In recent years, developments in distributed consensus algorithms
have provided the base for distributed ledgers. Distributed ledgers provide a robust data storage layer with a strong resistance to cyber threats [11]. Distributed ledgers have been applied in the context of the railways for solving technical issues involving ticketing, customs clearance, data collection, etc. [12–14]. Technological issues represent only one aspect required for the application of technology. A unified environment for sharing data among the railway’s stakeholders in a security-conscious manner creates the foundation for such an environment. Dynamic ownership transfer based on time, location, and equipment is a domain requirement for railways. A mechanism to share data, models, information, and the introduction of partners with data processing expertise is required for advancing the data-driven decision-making process.

Taking the example of a route with a train shuttling between two towns, considering only the maintenance point of view and the requirements and interdependency of various stakeholders can be explored. The data collected by onboard sensors about the train operations will be of interest and are required for improvement for the stakeholders such as the locomotive manufacturer, the railcar manufacturer, the rail-set owner, the operator, the infrastructure owner, and the maintenance provider. Similarly, the data collected by the wayside detectors or light detection and ranging (Lidar) equipment is under the ownership of the infrastructure owner but are useful to the locomotive manufacturer, the railcar manufacturer, the rail-set owner, the operator, the maintenance provider, and the infrastructure owners themselves [15,16]. The locomotive and the railcars may be exchanged between operators due to replacement or maintenance requirements. Further, it is of interest to share the data with data processing experts to facilitate improved data analytics and the generated information with the correct stakeholders. The data collected over a period even from a single route may have different ownership and many interested parties [17].

The literature study shows that distributed ledgers have been used in railways to provide immutability in scenarios such as ticketing, customs, maintenance data collection, etc. However, some of the cases utilise a single copy of the ledger within a single organization, and hence may not be utilising the distributed ledger technology to its full potential [13,18]. Moreover, studies have addressed and utilized the distributed ledger for and from the technical perspective only. A multistakeholder environment such as the railway has a requirement of democratization and disintermediation. However, as per the authors’ knowledge, an encompassing perspective related to addressing and adapting issues and challenges from different layers of the organization has not been sufficiently explored, creating data and knowledge silos. Hence, a holistic view addressing the governance, business, and technology aspects among the stakeholders is required for vertical and horizontal integration.

This work addresses the research question “What are the aspects that need to be addressed in a multi-stakeholder environment to develop secure and resilient data and model sharing framework in railways?” The paper is structured as follows, Section 2 provides the research methodology, Section 3 discusses the theoretical framework of distributed ledgers and smart contracts. Section 4 presents the result in two parts: (i) properties that have been identified to be of consequence for the use of distributed ledgers to create a secure, distributed data sharing environment for railway stakeholders, (ii) a taxonomy of the issues and challenges to be addressed for the creation of a data-sharing environment for railway stakeholders. Section 5 is the discussion and finally, Section 6 is the conclusion and describes the future scope of work based on the overall study.

2. Research Methodology

The research methodology, flow, and methods for this research are shown in Figure 1 and the description is as follows. In order to obtain the issues and challenges faced by the railway organizations, a literature study was performed by conducting a web-based search of articles on the deregulation of the railways and the issues in multistakeholder environments. Similarly, a literature study on the use of distributed ledgers and blockchain
in the railways was performed. This provided the scenarios in which distributed ledgers have been used in railways. The online databases used were Google scholar, Science Direct, and the Institute of Electrical and Electronic Engineers (IEEE) Xplore Digital Library. An analysis of the collected issues was performed and the issues were combined based on similarities.

![Research Methodology](image)

**Figure 1.** Research Methodology flow and methods.

Multiple semi-structured interviews with personnel from IT, security, and related areas of railway organizations representing domains such as the infrastructure provider, the system integrators, the equipment providers, the rail-set owners, operations, maintenance service providers, etc., were conducted. More than 40 personnel from various organizations participated in this activity and the analysis from this stage resulted in the classification of the issues into the three categories as well as the addition of new issues into the taxonomy.

A survey was designed and conducted with individuals from different railway organizations. The aim of the survey was to validate the issues faced on a day-to-day basis, while operating at different layers of the organization. The analysis of the survey highlighted the governance-based issues and a high level of awareness about cybersecurity. A final taxonomy based on this analysis was developed; however, some of the issues were found to overlap in more than one category. In such cases, the most relevant category as per high level system integration was given priority. Finally, an issue of awareness was added to all the categories, since this is vital for the decision-making process for all the categories.

3. Technical Framework

3.1. Cybersecurity in Railways

Railways have been categorised as “large technical systems” where the system is described as a “coherent structure comprised of interacting, interconnected components” [19,20]. Various aspects of the railways have been explored and discussed in the literature to analyze and understand the requirements for the design, development, operation, and maintenance for fulfilling the varied requirements of the stakeholders and business operations today and in the future [21–26].

Various technical challenges impact railway operations and the adaption of technology in the railway domain. The network of railway resources through the internet has exposed the railways’ infrastructure to various indirect and direct threats. Cybersecurity aims to protect equipment, data, people, and operations from malicious and non-malicious actors through the implementation of measures to regulate control access [27]. A cyberattack is an attempt to destroy, expose, alter, disable, steal, gain unauthorized access to, or make unauthorized use of an asset [28]. Railways have been exposed to and targeted by various cyber-attacks and their impact has been discussed in the literature [29–31].

3.2. Distributed Ledgers

Large technical systems such as railways with various layers of horizontal and vertical separation have overall operations that are dependent on the availability, integrity, and
authenticity of data, and in turn, a consensus about the overall state of the system. Building up consensus among multiple entities in a distributed system with the possibility of entities giving different answers to the same question at different times is described as the Byzantine Generals problem [31].

Distributed ledgers are a mechanism to create consensus among the participants in an untrusted environment. Distributed ledgers can be implemented through various mechanisms such as Blockchain [32] and directed acyclic graphs [33]. In 2008, Nakamoto [32] described Blockchain and the later release of Bitcoin, its prototype for financial domain cryptocurrency, as setting the example for the use of the distributed ledger in an untrusted environment.

Blockchain works by collecting transactions [34] together in blocks and creates a chain by using the hash of the previous block within the newly created block. This connection between the parent and the child has a one-to-one relationship. As more transactions come in, new blocks are created. Since this is an untrusted environment, each participant stores the entire chain of blocks locally and can check the authenticity of any new transaction request.

The creation of a new block is called “mining” and is performed by miners who are the participants competing to find a block with a hash value numerically less than the global set value. The hash calculated for a block uses the hash of all the included transactions, time, and a random value called a nonce (number used only once), where the miner (the entity performing the job of mining) checks through all the possible values for the nonce. This is the work performed by the miner, and if a legal value is found the miner shares the cryptographically signed block with all the neighbours who check its correctness. If it is found to be legal, they include it as the latest block. Finding a legal block requires a large number of calculations repeatedly for different nonce values and block creation rights are awarded to the miner first to report the block. This process requires massive amounts of processing power and in turn, time and energy. Anyone interested in joining a Blockchain network may join without any requirement of authentication or need to declare their identity.

This mechanism of acknowledging the authority of an unknown entity in a permissionless blockchain based on its ability to solve time-consuming mathematical problems and associating the work performed to a unique user through cryptography is called “Proof-of-Work” [32]. Blockchain creates a distributed ledger shared by all the participants and any new block consisting of many transactions made by participants can be verified for authenticity by all the other participants before appending it to their copy of the chain. If a malicious agent wants to revert a transaction, it must convince or control more than 50% of the miners to join and generate all the legal blocks after the modified block.

Blockchain can be classified as a public consortium and a private blockchain based on anonymity and trust among the participants. A public blockchain provides complete anonymity and operates in an untrusted environment with all the participants responsible for the authentication of transactions. In the case of consortium and private blockchains, participants may not be responsible for the authentication of transactions all the time as discussed by the authors of [35]. The use of consortium and private blockchains based on “Proof-of-Stake” and “Proof-of-Authority” are capable of a significantly higher throughput compared to Proof-of-Work [36]. Many industries which require data sharing among known partners operating in a closed environment trying to integrate distributed ledgers and smart contracts for improving secure data transactions do not require the stringent security of a public blockchain. In such a case, “Proof-of-Work” and the associated computation is not required; rather, Proof-of-Stake [37] or Proof-of-Authority [38] can be used.

The use of blockchain has been explored in various domains such as healthcare data management [39,40] to provide patient data protection regulation while opening new opportunities for data management and the convenience of data sharing. Blockchain has also been used in the industrial internet of things to provide product traceability, smart diagnostics, maintenance, product certification, machine to machine transactions, supplier identity,
reputation tracking, and a registry of assets and an inventory \cite{41,42}. Blockchain is used in the case of vehicular networks to provide user privacy, information security, remote track and trace, regulatory compliance, and remote software updates \cite{43,44}. In a supply chain scenario, blockchain is used to connect the chain from the provider, producer, processor, distributor, retailer, and the consumer while optimizing transparency and traceability \cite{45–47}. In relation to the integrity and authentication of property, blockchain has been used for land records management, its process redesign, technology readiness, and socio-political requirements. The state of development and the aspects impacting the overall adaption to land record management for two similar projects have been explored \cite{48}. There is a need for a broader prospective with governance from a technology-driven to a need-driven approach with changes in technology and administrative processes to bring information integrity \cite{49}. In railways, blockchain has been tried in different scenarios such as ticketing with data access and competition preservation, transit, and customs, operations system monitoring, control, and maintenance \cite{14,17,50–52}. Ongoing developments to fulfil business requirements through an advancement in technology, improving understanding, and support for the implementation of such requirements has come through many ongoing projects \cite{53–58}.

3.3. Smart Contracts

A smart contract is a software code that can record, evaluate, or execute legally relevant events according to the terms of the contract. It can be embedded in the hardware and software in such a way as to make a breach of contract expensive \cite{54,59}. In the case of Blockchain, a smart contract is a piece of code implemented and stored on the blockchain by one of the participants to allow others to access the smart contract if supported by the required credentials to perform the encoded action \cite{50,53–55}. Smart contracts allow the creation of execution rules based on who, when, how, and what, can define data access mechanisms as read, and can evaluate and append from the blockchain. This allows the translation of legal contracts as event-driven code to automate the execution of the contracts. There are various states of the lifetime of the smart contract: (i) Creation: when the smart contract is coded, (ii) consensus: when the smart contract is distributed in bytecode format to all the nodes, (iii) activation: when parties activate a contract, (iv) execution: when the required trigger is met, the contract is executed and values are updated on the blockchain. The triggers can be on-chain as a transaction and off-chain as a data oracle, (v) settlement: finalization of transaction on-chain or off-chain, (vi) audit: transactions are stored on the blockchain, and a complete chain of transactions is auditable. Various stages of smart contract processing are shown in Figure 2.

Figure 2. States of Smart Contract.

4. Results

To investigate the properties of the distributed ledger and to categorise the issues and challenges in the creation of a secure and distributed digital environment for railways stakeholders, the first step is to collect the data. The results are based on the data collected and
analyzed through the literature surveys, workshops, and discussions, and questionnaires with various industry partners representing different aspects of railways stakeholders such as the regulating agency, the manufacturers, the operators, and the service providers. The results are comprised of two sections: (i) properties that have been identified to be of consequence for the use of a distributed ledger to create a secure, distributed data sharing environment, (ii) issues and challenges to be addressed for creation of a data-sharing environment.

4.1. Properties of Distributed Ledgers

Distributed ledgers not only store data in a distributed manner, but they also provide additional inherent properties to create a secure digital environment.

Decentralization: Each participant can keep a complete copy of the distributed ledger, authenticate the ongoing transactions, and update the local copy. The transactions are propagated through the network and are visible to all the participants. Since each participant authenticates any transaction to be appended to its chain, there is no need for a central authority. The loss of distributed ledger data at a single stakeholder does not result in a loss of data and downtime for dependent stakeholders.

Data integrity: Data integrity is crucial for the validity of data over its lifetime. Data stored on a distributed ledger becomes a part of the hash value generated and used in the next block. If a malicious party wishes to modify stored data it must change the hash value generated for the block and recompute all the subsequent blocks. Such a modification will be reflected in the local ledger, but it will not be accepted by the rest of the participants. Changes made locally to older transactions that are already a part of the blockchain will not be accepted by the network, hence providing data integrity. To control a distributed ledger, more than half of the participants will have to join; this is termed a 51% attack in blockchain terminology.

Authenticity: The transactions on the distributed ledger are signed through asymmetric cryptography, and users maintain a pair of keys. The creation of a new contract involves the digital signature of the initiating participant. When a new transaction is received, participants check the digital signature to authenticate the operation from a legitimate source before including it in its local copy. This digital signature maintains and ensures the authenticity of the data when accessed by other stakeholders.

Data transparency: Distributed ledgers store the data as time-stamped transactions that are digitally signed with the data owner’s key, and any user can authenticate the ownership of the data. This authenticity of the data is verifiable by all the participants in the ledger. A large amount of data is shared through storage services such as the interplanetary file system (IPFS) and the hash key of the data is shared on the distributed ledger. The data security of sensitive data is maintained by asymmetric cryptography by the owner before storage.

Disintermediation: When two or more parties wish to perform a transaction on the distributed ledger there is no intermediary required to authenticate the transaction. Pre-defined smart contracts are executed based on the status of values in the distributed ledger or the external values registered by trusted oracles. Smart contracts append new data to the distributed ledger or generate events consumable outside the distributed ledger to trigger further actions. All the active participants will authenticate, accept, and store the transaction. This removes the cost of trust payable to the intermediary third party and reduces the time required to validate the transactions.

Democratization: All the participants on the distributed ledger have the same and equal rights to initiate, receive, and authenticate a transaction. There is no central authority to authenticate the transactions or to remain in sole control of the data. This can allow for the inclusion of new participants providing data processing services.

Irreversible: Blockchain is an append-only data structure. Transactions once performed on the distributed ledger become a part of a block and the hash value of the block is used to generate the child block. Hence, once a transaction is made it becomes a permanent part of the distributed ledger and cannot be removed or modified.
**Consensus:** A copy of the distributed ledger is maintained by each of the participants and updated when new transactions are reported, and then they are locally authenticated and stored. This mechanism leads to a consensus about the contents of the ledger in the case of the Proof-of-Work scenario. In the case of Proof-of-Stake or Proof-of-Authority, a smaller number of participants authenticate the operation which the rest of the participants accept. In all the cases a local copy is maintained which is identical for all the participants. Consensus removes the dependence for data access on a single source.

**Provenance:** All the transactions recorded in the distributed ledger are digitally signed by the owner of the transaction. Further, any updates can be linked to previous transactions. This provides standalone irrefutable evidence about the ownership and the change of ownership as a chain of transactions. Provenance is valuable since it establishes the lineage of data during the long life of an asset.

**Immutability:** Transactions once stored in a block on the distributed ledger are not standalone entities; rather, they are linked as a part of a chain where a subsequent block depends on the value of its parent block. Any attempted modification to a block will break the chain between the parent and the child in the local chain and will be rejected by the rest of the network. The immutability of the data ascertains the availability of data representing the stages of the data source through its lifetime.

**Non-repudiation:** This is the assurance that a party cannot successfully dispute the authenticity of the transaction created by them. Transactions must be signed with a secret private key and can be authenticated with a public key. A transaction without the knowledge of the owner is only possible if the key is acquired by a malicious agent. Non-repudiation is responsible for creating trust in stored data and ensures a binding link between the participant and the transaction on the distributed ledger.

**Auditable:** Each transaction made on the distributed ledger is stored with all the nodes connected to the network and is digitally signed by the transaction owner. Any node on the network can audit an individual transaction or a sequence of transactions without any external dependency. Auditability of the chain of transactions is required to trace the provenance and authenticity in a decentralised digital environment. Auditability along with the other properties of a distributed ledger such as the provenance, authenticity, and democratization of the data help establish a chronological record of events through the lifetime of the system.

### 4.2. Taxonomy

The railway’s infrastructure is operated, managed, and maintained by an interdependent group of stakeholders. A safe and secure environment for sharing data and computational models while enabling the storage, access, and processing of data over the long lifetime of the equipment while supporting clear ownership and access credentials will allow better decision support tools to be developed. Initial steps for the creation of such an environment will begin with an analysis of the requirements of the railway’s stakeholders, interdependencies, operations, maintenance structure, etc.

The taxonomy of issues and challenges developed during this study through workshops, presentations, questionnaires, and discussions with stakeholders handling different aspects of railways has been divided into three categories, namely, governance, business, and technology. Some of the issues cover a broad area and can be placed under more than one category. In such cases, the most relevant category as per high level system integration was selected and is shown in Table 1.
Table 1. Taxonomy of the issues and challenges related to cybersecurity in railways.

| Governance | Aspects related to overall governance of the system |
|-----------|--------------------------------------------------|
| Regulation | Defining the rules of operations for data management |
| Democratisation | Brings in equality of rights, opportunities and rules for data access |
| Legislative aspects | Legal contracts defining data access, and interpretation of such contracts |
| Safety | Safety related to data collection, processing, analysis, exchange etc. |
| Confidentiality | Duty of the organization to maintain secrecy of data |
| Privacy | Right of individual to maintain secrecy of personal data |
| Fairness | Fair share of information, risk and returns to all stakeholders |
| Transparency | Assurance of source and openness about collection, use and sharing of data |
| Authentication and authorisation | Open standardized methods of authentication and authorization for cyber and physical systems |
| Ownership | Ownership establishment, lease and transfer with auditable records |
| Integrity | Secure data and metadata, transfer and storage, authenticated source, auditable record and ownership |
| Proprietary systems | Indispensable due to organization requirements, incompatible between stakeholders |
| Organizational requirements | Requirements to fulfil organizations interests and future plans |
| Standards | Essential for interoperability, economics of scale and to add momentum to research |
| Upgradability | Secure, resilient, robust mechanism to perform unsupervised software upgrade |
| Awareness | Awareness of short- and long-term goals, plans and activities |
| Business | Aspects related to business operations |
| Relative advantage | Advantages of new technology as compared to current practices, which may not only be in technical domain |
| Compatibility | Compatibility and improvement from current processes, not just digitalization of the current process |
| Complexity | Complexity in terms of technology adaptation, resource availability, cost of transition |
| Trialability | Evaluate and apply solutions to well understood problems to access usability |
| Observability | Clear and measurable benefits, through adaptation of new technology |
| Awareness Technology | Awareness of core requirements of business operations procedures |
| Cybersecurity | Managing and maintaining secure systems |
| Cost trade-off | Design time decisions can impact in the long run and can be difficult to anticipate |
| Data Volume | Acquiring, transmission, storage and processing issues due to large amount of data |
| Data Silos | Impacts efficiency of decision-making process due to limitations of data availability |
| Backward compatibility | Backward compatibility is required to maintain system access and data exchange |
| Data formats | Incompatible data storage and exchange formats, lock-in with selected data formats |
| Technical constraints | Incompatible technology stacks, data processing models and domain requirements between partners |
| Technical risk | Risk due to lack of understanding of system complexity, limitations of technology |
| Awareness | Awareness of available technology, solved problems and technical issues |
• Governance

Deregulation in the railways, unlike domains such as power distribution, gas, and telecommunication requires a linkage between the horizontally and vertically separated entities due to the overlapping requirements of space, equipment, and schedules. Governance plays a significant role by setting up the responsibilities, rules, and requirements for various stakeholders. However, many factors require a high ELoT among the stakeholders and hence they have to be bound by rules, regulations, and legal contracts.

**Regulation:** The availability, safety, and security of railway operations is governed by policies and regulations. This not only controls the overall operations, but also the data flow and data sharing, defining when to share, with whom, how to share, and what to share. The security of implementation and its verifiability, the security based on the data category, and the requirements of the environment need to be defined and bound by regulations. Such regulations can be defined and applied by the consortium of railway stakeholders creating a data-sharing environment.

**Democratization:** The need for democratization in a data-sharing environment bring rights, opportunities, and responsibilities among the stakeholders to create trust, and facilitate the growth of the environment by defining requirements, principles, and quality; hence, clarifying the roles and expectations. Democratization of the system will also allow new players to be brought into the domain for tasks related to data processing, analysis, and decision support, which in turn results in better facilities being made available to the railways’ stakeholders.

**Legislative aspects:** Interoperability among the stakeholders of railways is governed by legal contracts which establish the terms of access. Organizations entering the legal contracts may define the nature of data to be shared and can set up the gateways for sharing. This involves facilitating the availability of data, its quality, latency, period of availability, mechanism of availability, access rights, usage restrictions, etc. Such systems need to be implemented and maintained as per the legal contract. The implementation of such systems separately for each organization is time-consuming, error-prone, non-uniform, and costly.

**Safety:** Railways operate under safety by design. The safety of operations, personnel, and equipment is an important aspect of railway systems. Defining a safety strategy and adapting a regulatory safety framework for the improvement of safety related to data collection, quality, processing, analysis, and exchange is needed to maintain the overall safety of transport systems.

**Confidentiality:** Confidentiality in terms of the duty of an organization to maintain secrecy regarding data of personnel, processes, equipment, locations, operations, system design, their interfaces, etc. is a requirement to maintain the security of railways system. Data may be used directly and indirectly to extract information and hence the process of data gathering, handling, management, usage, and sharing requires control of what is shared, with whom, when, and how. The standardization and automation of such processes are required to adhere to the requirements.

**Privacy:** Railways handle large amounts of data such as personal, financial, transit, passenger data, transported goods, communications, etc., with the requirement of maintaining the privacy of personal information. Different methods such as expunging data, anonymization, data masking, and perturbation are required to maintain privacy on various aspects when such data is to be shared between railway stakeholders. Standardized methods that are implemented, made available and automated as per the requirements and followed by all involved participants are required for maintaining the privacy of data.

**Fairness:** Co-ordination mechanisms to maintain a fair share of information, risks, and returns are required when the integration of technology is to be performed among different users of the same infrastructure to ensure overall efficiency. The apportion of risks and revenues for all the stakeholders is possible through governance and brings in the incentive to integrate competing parties.
Transparency: Transparency is the assurance of sources and the correctness of data with ease of access and work irrespective of data generation methods. Similarly, at the user end, there is a need for openness about the way data is collected, used, and shared. Transparency among the related stakeholders is another important requirement for the establishment of trust. Metadata in terms of administration, rights, structural, description, technical, etc. is important to maintain transparency.

Authentication and Authorization: The creation and maintenance of a unique secure identity for stakeholders, assets, infrastructure, etc. throughout the domain in a unified and extendable categorical manner is needed. The security mechanism should be proven to be secure against possible cyberthreats and include security protocols for physical and digital systems. The authentication of data providers and receivers to ascertain their identity and authorization to provide privileges and maintain indisputable proof and record of ownership, access, update, and transfer of data are essential for maintaining the security of a system. Open and standardized authentication and authorization methods, built on proven security layers, create a secure by design environment.

Ownership: The establishment of static ownership of physical or digital assets is a well-understood and used process. However, in railways, physical assets can be leased to a user by the owner for a period, hence creating a dynamic leased ownership. The data for the given period generated through that asset needs to be shared with the user of the asset, the owner of the infrastructure where the assets interact, and the stakeholders responsible for performing the maintenance on all interacting assets. Systems with leased data ownership for third-party data analytics experts with access control, access logging, and assuring fair use are required to extend the possibility of data-driven decision-making. The identification of a permanent, dynamic, and temporary ownership of the asset and the associated infrastructure is necessary to be able to handle data sharing with appropriate stakeholders for the proper duration. The creation of ownership handling mechanisms in terms of automatic ownership establishment, transfer, lease, etc., and generation and maintenance of auditable records are required to maintain fair use and encourage data sharing.

Integrity: The process of decision-making and the generation of knowledge depends on data processing. It is important to be able to trust the data in terms of the source, content, and metadata in the long term to create data-driven systems. Data from resources with a long lifetime and frequently changing ownership as in the case of high-value components in the railways must store sufficient metadata along with the raw data to define the history, current condition, updates in system configuration, ownership, ownership transfer, etc. Suitable methods are required to store the raw data, associated metadata, and methods of ownership transfer with the assurance of integrity. Secure data transmission and storage, from authenticated sources, with an auditable record, while maintaining ownership, etc. are required to maintain the overall integrity of the data.

Proprietary systems: Proprietary systems are developed due to organizations working in the same domain while developing technology. Due to varied requirements, the focus and outlook end up with highly different architectures, structures, and terminology for similar physical world scenarios. Even when following the same standards, the details of design and development vary to a large degree, effectively creating formats and systems incapable of communicating and sharing data even with organizations working in the same domain.

Proprietary systems are designed and implemented to fulfill the organization’s requirements. Details that are hidden and known only to one owning party limit the trust when multiple parties need to contribute data to create data integration for information extraction. While such proprietary systems are indispensable, open and structured data access mechanisms and shared information about the contributed data, its availability, terms of use, and access to extracted information are required to create data flow among the stakeholders.
Organizational requirements: Ongoing development, up-gradation plans, and future requirements analysis must be aligned for the fulfilment of the organization’s interests. Ideas and development at early stages cannot be exposed due to frequent changes, updates to the systems, and data confidentiality. Moreover, in the case of competing interests, it may not be in the best interest of the organization to share data related to its intellectual property. A data-sharing environment should provide safety of data while providing fine-grained control over the access rights and control over the transfer of data while providing programmable methods to control data access rights.

Standards: Uncertainty regarding data collection, ownership, and a lack of common nomenclature to describe different types of data affects the flow from data to the decision when crossing organization boundaries and is addressed through standardization. Systems requiring coordination and collaboration among various railway stakeholders require a mechanism of transfer of data and information and require interoperability issues at various levels of organizational structure to be solved.

Maintaining open standards allows seamless operations across boundaries, improves the interoperability of products, applications, and services, and discourages vendor lock-in. Standardization brings in benefits from economics of scale to researchers, regulators, and the end-user, and ensures the security and privacy of data while adding momentum to research and development. Standardization supports the interoperation beyond systems, protocols, data semantics, harmonizes the technology development process, and provides compliance which is required for defining and describing critical infrastructure such as railways.

The standardization of nomenclature, data formats, and the data sharing environment is a requirement for a multi-stakeholder environment for the onboarding process and integration effort. The creation of data sharing standards, proliferation, timely updates, and finally obsolescence management are essential for a data-sharing environment. Standards and recommendations impacting different aspects of railways are available from various railways and other agencies. However, the lack of available standards for new domains such as a distributed ledger due to high activity in the core domain and the variety of available technology stacks retards the process of integration.

Upgradability: Railway systems can be categorized as civil, mechanical, electrical, electronics, computing, and software systems in increasing order of agility during the design, development, operations, maintenance, and upgrade lifecycle. Upgradeability is a necessary and useful feature concerning software systems. Software systems, data collection methods, data formats, processing algorithms, transmission technologies, etc., are required to be upgraded over time. This may happen due to changes in or an improved understanding of requirements, underlying systems, security, maintainability, availability of better technology, etc. The cybersecurity of systems needs upgrades as well as this is dependent on the technology, system architecture, software development practices, detection of vulnerabilities at different layers of the technology stack, etc. A lack of upgradeability adds cost to the system in terms of the replacement of systems, lags in technology, and vulnerabilities in the system.

Upgradability in software systems connected to a network or accessible physically is less error-prone; however, large numbers of computing systems under the category of embedded systems with a limited amount of storage, memory, processing power, communication bandwidth, and up-gradation support in the firmware are used as the edge computing devices and at times they are difficult to access due to the large numbers and they are dangerous and difficult or in a distant location, making them difficult to reach. The integration of such systems with proper authentication, authorization, and secure communication is required for maintenance and upgradability.

Awareness: The awareness of requirements of various stakeholders for authorities is needed to create suitable regulations and awareness of regulations to be adhered to for:
• Business

The stakeholders in deregulated railways are separate entities with different business models. To best utilise new technology, the evaluation of its challenges for business application in terms of growth opportunity, financial, and operational factors must be evaluated.

**Relative advantage:** It compares the differences and advantages of new technology as compared to current practice in terms of its architecture, security, ease of use, automation, ability to describe complex systems, etc. Solutions addressing well-understood problems with low criticality allow ease of integration of new technology. Long-term projects with well analyzed use cases and deliverables with evaluation and feedback throughout the lifetime of the project will allow integration to critical projects; however, in railways, scenario projects will be highly dependent on the governance, legal, and security aspects.

**Compatibility:** It can be used in terms of similarity, ease of integration, and the use of the new technology being evaluated and the solutions already in place. Maintaining the CIA triad of confidentiality, integrity, and availability is a core requirement for the smooth functioning of railways. Confidentiality, integrity, and availability are currently achieved through a centralized structure and data sharing happens through webpages, the application program interface (API), file transfers, etc., but are plagued by various cybersecurity issues. The decentralized structure of distributed ledgers is the stark opposite, and although it provides excellent CIA support, it creates compatibility issues requiring the reorganization at various levels of the workflow. The design, development, and maintenance with blockchain technology is dissimilar to current web/cloud-based development practices and hence will require recruiting/retraining of technical teams.

**Complexity:** Integration of distributed ledger technology into regular use is due to the lack of maturity and stability attributed to the exploration of new ideas and a high rate of development. However, various projects catering to business requirements are under development and address generic applicable issues. A lack of available expertise and domain integration experience due to the high focus of experts on the financial domain also creates complexity from a business integration point of view.

Blockchain technology is young with development efforts distributed over various parallel stacks that are experimenting with different ideas and architectures. The standardization of nomenclature, technology, applicability, etc., is a requirement for ease of integration of technology from a governance and business point of view. A lack of standardization adds a layer of complexity while describing, defining, and developing solutions.

**Trialability:** It refers to the availability of tested scenarios, case studies, demonstrators, code libraries, etc., for ease of development of proof-of-concept solutions. Blockchain has had a maximum focus towards financial domains and hence maximum development and demonstrators are available for financial systems. Interest towards the wider application of the technology has started research and led to the development of applications for blockchain in other domains. However, the development of technology utilization has not reached the maturity to be able to provide case studies for the easy evaluation and technical stacks for quick integration for applicability and trialability.

**Observability:** Clear and visible benefits in terms of data confidentiality, integrity, availability, etc. are helpful for the integration of technology. Well-established technology stacks have clear benefits, while modern technology stacks lag in adaption. However, in the case of blockchain, it provides clear benefits in terms of data confidentiality, integrity, and availability. Moreover, the distributed architecture of blockchain provides the promise of secure accessibility. However, although the inherent properties of blockchain create a secure and stable environment, a lack of observability in terms of demonstrators and case studies limits adaptability in business scenarios.

Clear and visible benefits are important for the integration of technology, established technologies, or technologies with similar architecture are easier to integrate due to easier visibility of use case scenarios, available resources, the safety of decisions, etc.

**Awareness:** An awareness of current and future requirements, actual processes in use, methods to evaluate process outcome, etc. is required to define, evaluate, and implement
the business process for true digitalization instead of presenting data on a screen. An awareness of business processes is important to be able to understand the requirements to be fulfilled and to redefine processes in a digital native format.

• Technology

Cybersecurity: Security is an ever-changing landscape in the cyber world. The effect of security lapses, its short- and long-term effects and implications, and the lifetime of the exposed data can be difficult to conceive. Cybersecurity is seen as the preservation of the confidentiality, integrity, and availability of information in cyberspace. Cybersecurity covers all kinds of digital operations, networking, data transmission, control, and storage of data.

Various kinds of cyber-attacks are possible which may compromise or deteriorate digital or physical infrastructure with varying degrees of damage from operations and equipment to loss of life. Cybersecurity is an ongoing process; the security team must plug every hole that may be used while the perpetrators must only find a few weaknesses. A proper security cover requires various areas of system design to be covered and depends on updating technical as well as human factor requirements with constant monitoring and up-gradation of the cover.

Various layers of security are required to provide overall security for the collaboration of information sharing among the railway’s partners to achieve confidentiality, integrity, and availability, and to harmonize the goals of the collaborator’s security of access control, information transmission, and data storage must be ascertained. The integration of all the security requirements should be under a unified information security system defining security procedures and requirements.

Cybersecurity is a moving target with new vulnerabilities detected very often in the software in use for a very long term. In addition to supporting the requirements of availability, integrity, and safety, cybersecurity adds another requirement to the list. The environment for data exchange should support the protection, detection, identification, response, and recovery to handle cyber threats at different stages and threat levels.

A critical factor in cybersecurity is the human factor and targeted attacks focused on people, their roles, and access to data are soft targets as compared to infrastructure. However, the technical, procedural, or functional vulnerabilities of the system are targeted by exploiting the human psyche. Proper cyber hygiene is required in the form of a continuous upgrade of cybersecurity education, awareness, training, and experience in addition to upgrading and maintaining digital infrastructure.

Cost trade-off: In the initial stages of the lifetime of the system, the cost in terms of storage, transmission, processing, etc., may appear extravagant and hence the cost acts as a deterrent to applying the best possible long-term approaches resulting in technical debt. Although the visibility of the threat and its implications may not be well understood initially and may be justifiable at the design stage due to cost savings or technology limitations, their constraints and impact in the long run may require larger corrective action as in the case of the millennium bug and the year 2038 problem. These issues become important when the lifetime of the system is long, spanning decades, and future technology developments, and requirements cannot be easily anticipated.

Data volume: Railways generate large amounts of data e.g., condition monitoring of a considerable number of systems, collecting data for multiple attributes, and the high data acquisition rate generates large volumes of data. Data-driven models depend on long-term operational data for learning and predicting the system condition. Recent data collection schemes such as point cloud data and drone-based videos are being explored and used in certain scenarios. These systems can generate a large amount of data per scan and multiple repeat scans are required to observe the deterioration phenomena. This large volume of data needs to be securely transmitted, stored, processed, analyzed, and archived. The generation of knowledge from data may require the sharing of data with external experts. The sharing of results requires additional metadata to share processing models for deduction of sound inference and configuration data to ascertain the system state.
Data Silos: A lack of interoperability leads to the creation of data silos where the data is present and available to an organization or a group within the organization while others are unaware, unable to access, or able to access with restrictions. The cost of data silos is in the form of an inability to make decisions due to lack of data and leads to a reduction in operational efficiency.

Backward compatibility: As organizations improve their understanding of systems, requirements while updating and upgrading the technology, and changes in data storage formats and structures become requirements as legacy systems are enhanced or replaced. The requirement of maintaining backward compatibility means that the dependency of other organizations as defined in interoperability terms must be fulfilled. This creates an overhead of data structure, conversion, and representation to maintain access in case of equipment and system upgrades.

Data formats: Data sampled from a substantial number of sensors, at a high data rate for an extended period can generate massive amounts of data. The storage of these data is possible in a substantial number of incompatible formats, depending upon the availability and the selection during the design phase. Over time, the system capability, sensor range, sampling rate, sampling systems resolution, etc., change, and hence data storage formats need to be upgraded. Systems dependent upon and consuming such data need to be upgraded as per the data format update.

In a multistakeholder system such as railways, dependency creates a lock-in for the data vendor and consumer; moreover, there is more than one data consumer for maintenance-related data. Any planned upgrade in the data format triggers requirement changes for all data consumers.

Technical constraints: Organizations as per work and technical culture may use different technology stacks. This leads to incompatibility of data storage, access mechanisms, technology deployment, etc. Data exchange formats can be standardized, and data access channels can be created; however, data processing models, visualizations, interfaces, and terminology can be completely different and need a deeper integration of various stakeholders to simplify and maximize the interoperability.

Technical risk: Catering to the requirements of various stakeholders with varied systems poses a technical risk due to individual system complexity, system requirements, the limitations of technology due to a lack of available skilled personnel, frequent changes in the technology stack, etc. Technical risks need to be addressed through a proper study of the requirements supported by human resources with technical and project management skills alongside tools and technologies.

Awareness: An awareness of the available technologies, solved problems, and the risks and rewards of modern technology are key to designing the architecture and implementing the technical solutions.

5. Discussion

Railway systems are created with a “safety by design” mindset. Similarly, the architecture of the digital environment for railways needs a “security by design” mindset. Addressing various challenges is required to overcome the issues and represents a step towards creating a secure, robust, and extendable data-sharing environment. The core values in the railways of safety, availability, reliability, etc., and the involvement of various stakeholders with different requirements at separate layers of operations makes it important to cumulate challenges to be able to address and fulfill the requirements of data sharing environment.

Cybersecurity architecture for data and model exchange for railway stakeholders has to minimise ELoT to improve its robustness. This is possible by utilising standardised, well-tested, and resilient security mechanisms to be used by all the stakeholders. Such architecture becomes increasingly important since data, model, metadata, ownership, access control, provenance etc. are important for maintaining data relevance throughout the multi-decade lifetime of the equipment.
Distributed ledgers provide security, integrity, and authentication along with ownership resolution. Blockchains implement distributed ledgers with various approaches and functionalities. A private blockchain with “Proof-of-Stake” provides a secure environment for the users with sustainable computation and energy requirements. The properties of distributed ledgers such as data integrity, provenance, and auditability create a dependable information logistics system. Non-repudiation and consensus create an environment where the information is available and can be trusted to be correct as per the source of origin. Disintermediation creates a path for the easier setup of transactions among the railway stakeholders and such transactions can be executed very fast once the legal contracts are established. Smart contracts allow for the creation of self-executing code with the ability to read, evaluate, and append data to the blockchain. This can simplify the creation of a large number of simple data exchange contracts while being able to filter data based on source, permanent ownership, limited time ownership, etc.

The design, implementation, and integration of technology for multi-stakeholder environments such as railways requires a large number of challenges to be addressed, where technology issues form only a part of the overall scenario. The issues and challenges identified in the study have been categorised in a taxonomy under various categories, namely, governance, business, and technology. Governance issues address the requirements of overall regulation and rules to support and benefit the stakeholders. Business challenges address the methods of evaluation and process of integration in a financially sustainable way. Finally, technology issues address the various issues in the current methods and bottlenecks in the adaption of new technology. Some of the issues identified may be categorised under more than one category; however, the current categorization has been chosen to address the most relevant category as per high level system integration. The factor of awareness has been maintained under all the categories due to its importance in creating an understanding and the knowledge of requirements suitable for all the categories.

6. Conclusions

It can be concluded from the findings from this research that digital ledgers along with the smart contracts have the technical prowess to address the requirements of a secure and resilient data and model sharing architecture in a multi-stakeholder environment such as railways.

Secondly, as per the data collected from semi-structured interviews, it can be concluded that the issues and challenges posed by governance aspects such as digital asset ownership (provenance, transfer, lease), legislative aspects (legal contract and smart contract interoperability) etc., with a secure foundation, are the most important challenges to be addressed.

One of the additional conclusions is that data extraction and assimilation are as important as data security. Allowing the users to access the data along with its metadata is important for the long-term usability of the data itself. The availability of the metadata along with the data is also crucial for understanding the railway asset itself during its long operational period.

Finally, the research community can benefit from the generated taxonomy by using it for evaluating the issues and challenges of technology integration, and industry can utilise the developed taxonomy for developing future roadmaps.

Our research team will work on addressing some of the challenges in our future work by exploring and implementing use cases to best address the requirements of the railway stakeholders.

Author Contributions: Conceptualization, A.P. and R.K.; methodology, A.P., A.T. and R.K.; writing—original draft preparation, A.P.; writing—review and editing, A.P., A.T. and R.K.; visualization, A.P.; supervision, A.T. and R.K.; project administration and funding acquisition, R.K. All authors have read and agreed to the published version of the manuscript.
Funding: This research is a part of AI Factory for Railways (AIFR) project at Luleå University of Technology (Diarienr: 2019-05140) (www.ltu.se/research/subjects/Drift-och-underhall/Forskningsprojekt/aifr?l=en, accessed on 9 August 2020).

Data Availability Statement: Data collected during the duration of this research is available at LTU digital archives.

Acknowledgments: The authors would like to thank the Swedish Innovation Agency Vinnova, JVTC, Trafikverket, INFRANORD, and Norrtåg, etc., for their financial support to carry out this work within the framework of AIFR project (www.ltu.se/aifr, accessed on 9 August 2020).

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References
1. Alexandersson, G.; Hultén, S. The Swedish Railway Deregulation Path. Rev. Netw. Econ. 2009, 7, 18–36. [CrossRef]
2. Asteris, M. Rail Privatisation: A Platform for Success. Econ. Aff. 1994, 14, 19–23. [CrossRef]
3. Alexandersson, G.; Hultén, S.; Nilsson, J.-E.; Pydoko, R. The Liberalization of Railway Passenger Transport in Sweden: Outstanding Regulatory Challenges; Working Papers Transport Economics 2012:5; Centre for Transport Studies Stockholm: Stockholm, Sweden, 2012.
4. Wellings, R. The Privatisation of the UK Railway Industry: An Experiment in Railway Structure. Econ. Aff. 2014, 34, 255–266. [CrossRef]
5. Saito, T. Japanese private railway companies and their business diversification. Jpn. Railw. Transp. Rev. 1997, 10, 2–9.
6. Taylor, Z.; Ciechanowski, A. Deregulation in Polish rail transport. Transp. Rev. 2006, 26, 305–324. [CrossRef]
7. Hilmola, O.-P.; Leino, J. Deregulation and privatization process in Finnish railways. In Second Research Meeting Held at Moscow—Strategic Role of Logistics and Supply Chain Management; Research Report Vol. 177; Lappeenranta University of Technology, Department of Industrial Engineering and Management: Lappeenranta, Finland, 2006; pp. 81–96.
8. Thaduri, A.; Aljumaili, M.; Kour, R.; Karim, R. Cybersecurity for eMaintenance in railway infrastructure: Risks and consequences. Int. J. Syst. Assur. Eng. Manag. 2019, 10, 149–159. [CrossRef]
9. Kour, R.; Aljumaili, M.; Karim, R.; Treten, P. eMaintenance in railways: Issues and challenges in cybersecurity. Proc. Inst. Mech. Eng. Part F J. Rail Rapid Transit 2019, 233, 1012–1022. [CrossRef]
10. Asplund, M. Wayside Condition Monitoring System for Railway Wheel Profiles: Applications and Performance Assessment. Ph.D. Thesis, Luleå University of Technology, Lulea, Sweden, 2016; p. 162.
11. Wang, H.; Wang, Y.; Cao, Z.; Li, Z.; Xiong, G. An overview of blockchain security analysis. In Communications in Computer and Information Science; Springer: Berlin, Germany, 2019; Volume 970, pp. 55–72. [CrossRef]
12. Sturmans, A.; Hudenko, J.; Juruss, M. The Application of Blockchain Technologies for Rail Transit Customs Procedures; Springer: Cham, Switzerland, 2020; Volume 117. [CrossRef]
13. Abbas, Y.; Martinetti, A.; Moerman, J.J.; Hamberg, T.; van Dongen, L.A. Do you have confidence in how your rolling stock has been maintained? A blockchain-led knowledge-sharing platform for building trust between stakeholders. Int. J. Inf. Manag. 2020, 55, 102228. [CrossRef]
14. Preece, J.D.; Easton, J.M. Blockchain Technology as a Mechanism for Digital Railway Ticketing. In Proceedings of the 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 9–12 December 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 3599–3606. [CrossRef]
15. Palo, M.; Galar, D.; Nordmark, T.; Asplund, M.; Larsson, D. Condition monitoring at the wheel/rail interface for decision-making support. Proc. Inst. Mech. Eng. Part F J. Rail Rapid Transit 2014, 228, 705–715. [CrossRef]
16. Artyachandra, M.R.M.F.; Brilakis, I. Understanding the challenge of digitally twinning the geometry of existing rail infrastructure. In Proceedings of the 12th FARU International Research Conference, Homagama, Colombo, Sri Lanka, 3–4 December 2019; pp. 25–32. [CrossRef]
17. Lohr, M.; Hund, J.; Jurjens, J.; Staab, S. Ensuring genuineness for selectively disclosed confidential data using distributed ledgers: Applications to rail wayside monitoring. In Proceedings of the 2019 2nd IEEE International Conference on Blockchain (Blockchain 2019), Atlanta, GA, USA, 14–17 July 2019; pp. 477–482. [CrossRef]
18. Naser, F. Review: The Potential Use of Blockchain Technology in Railway Applications. In Proceedings of the 2018 IEEE International Conference on Big Data, Seattle, WA, USA, 10–13 December 2018; pp. 4516–4524.
19. Cohen, E.A.; Hughes, T.P. Rescuing Prometheus; Vintage: New York, NY, USA, 1998; Volume 77. [CrossRef]
20. Peirone, D. The Governance of Complex Systems: The Case of British Railways. Econ. ePolit. Ind. 2007, 34, 47–70.
21. Khatri, V.; Brown, C.V. Designing data governance. Commun. ACM 2010, 53, 148–152. [CrossRef]
22. Commission, E. Roadmap to a Single European Transport Area: Towards a Competitive and Resource Efficient Transport System: White Paper; Publications Office of the European Union: Luxembourg, 2011.
23. Jägare, V.; Juntti, U.; Karim, R. Governance of digital data sharing in a cross-organisational railway maintenance context. In Proceedings of the 5th International Workshop and Congress on eMaintenance, Stockholm, Sweden, 14–15 May 2019; Luleå University of Technology: Luleå, Sweden, 2019; pp. 1–8.

24. Juntti, U.; Larsson, L.; Karim, R. Implementation of eMaintenance concept within the Swedish railway. In Proceedings of the COMADEM 2014, Brisbane, Australia, 16–18 September 2014.

25. Lotfi, Z.; Mukhtar, M.; Sahran, S.; Zadeh, A.T. Information Sharing in Supply Chain Management. Procedia Technol. 2013, 11, 298–304. [CrossRef]

26. Linton, J. Diffusion of Innovations; Simon and Schuster: New York, NY, USA, 1998; Volume 9. [CrossRef]

27. ISO. ISO/IEC 27032:2012. Information Technology—Security Techniques—Guidelines for Identification Collection Acquisition and Preservation of Digital Evidence; ISO: Geneva, Switzerland, 2012.

28. Disterer, G. ISO/IEC 27000, 27001 and 27002 for Information Security Management. J. Inf. Secur. 2013, 4, 92–100. [CrossRef]

29. Pita, A.M. Real-World Cyber Security Challenges in Rail Systems. Available online: https://railsystemsaustralia.com.au/wp-content/uploads/2020/02/Real-World%20Cyber%20Security%20Challenges%20in%20Rail%20Systems_final.pdf (accessed on 1 November 2020).

30. Kour, R.; Karim, R. Cybersecurity workforce in railway: Its maturity and awareness. J. Qual. Maint. Eng. 2020, 27, 453–464. [CrossRef]

31. Lamport, L.; Shostak, R.; Pease, M. The Byzantine Generals Problem. In ACM Transactions on Programming Languages and Systems (TOPLAS); Association for Computing Machinery: New York, NY, USA, 1982; Volume 4, pp. 382–401. [CrossRef]

32. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. SSRN Electron. J. 2008. [CrossRef]

33. Benˇ ci´c, F.M.; Žarko, I.P. Distributed ledger technology: Blockchain compared to directed acyclic graph. In Proceedings of the 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), Vienna, Austria, 2–6 July 2018; IEEE: Piscataway, NJ, USA, 2018; Volume 2018, pp. 1569–1570. [CrossRef]

34. Antonopoulos, A.M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies; O’Reilly Media, Inc.: Newton, MA, USA, 2014; ISBN 978-1-449-37404-4.

35. Monrat, A.A.; Schelen, O.; Andersson, K. A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access 2019, 7, 117134–117151. [CrossRef]

36. Monrat, A.A.; Schelen, O.; Andersson, K. Performance Evaluation of Permissioned Blockchain Platforms. In Proceedings of the 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), Gold Coast, Australia, 16–18 December 2020. [CrossRef]

37. Dinh, T.T.A.; Wang, J.; Chen, G.; Liu, R.; Ooi, B.C.; Tan, K.L. BLOCKBENCH: A framework for analyzing private blockchains. In Proceedings of the 2017 ACM International Conference on Management of Data, Chicago, IL, USA, 14–19 May 2017; Part F1277. Association for Computing Machinery: Chicago, IL, USA, 2017; pp. 1085–1100. [CrossRef]

38. De Angelis, S.; AIELLO, L.; Baldoni, R.; Lombardi, F.; Margheri, A.; Sassone, V. PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain. CELIR Workshop Proc. 2018, 2058, 1–11.

39. Khatooon, A. A blockchain-based smart contract system for healthcare management. Electronics 2020, 9, 94. [CrossRef]

40. Kuo, T.T.; Kim, H.E.; Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health care applications. J. Am. Med. Inform. Assoc. 2017, 24, 1211–1220. [CrossRef]

41. Bahga, A.; Madisetti, V.K. Blockchain Platform for Industrial Internet of Things. J. Softw. Eng. Appl. 2016, 9, 533–546. [CrossRef]

42. Brody, P.; Puresswaran, V. Device democracy: vFabricing the future of the internet of things. IBM Sept. 2014, 7, 15.

43. Dorri, A.; Steger, M.; Kanhere, S.S.; Jurdak, R. Blockchain: A Distributed Solution to Automotive Security and Privacy. IEEE Commun. Mag. 2017, 55, 119–125. [CrossRef]

44. Astarita, V.; Giorfè, V.P.; Mirabelli, G.; Solina, V. A Review of Blockchain-Based Systems in Transportation. Information 2020, 11, 21. [CrossRef]

45. Astarita, V.; Giorfè, V.P.; Mirabelli, G.; Solina, V. A Review of Blockchain-Based Systems in Transportation. Information 2020, 11, 21. [CrossRef]

46. Francesc, K.; Swanson, D. The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency. Logistics 2018, 2, 2. [CrossRef]

47. Dobrovnik, M.; Herold, D.; Fürst, E.; Kummer, S. Blockchain for and in Logistics: What to Adopt and Where to Start. Logistics 2018, 2, 18. [CrossRef]

48. Benbunan-Fich, R.; Castellanos, A. Digitalization of land records: From paper to blockchain. In Proceedings of the 2017 ACM International Conference on Management of Data, Chicago, IL, USA, 14–19 May 2017; Part F1277. Association for Computing Machinery: Chicago, IL, USA, 2017; pp. 1085–1100. [CrossRef]

49. Zhao, L.; Huang, Y.; Jiang, T. High-speed railway environmental monitoring data identity authentication scheme based on consortium blockchain. In Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications, Xi’an China, 9–11 December 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 7–13. [CrossRef]

50. Kuperberg, M.; Kindler, D.; Jeschke, S. Are Smart Contracts and Blockchains Suitable for Decentralized Railway Control? arXiv 2019, 5, 36–61. [CrossRef]
52. Preece, J.; Easton, J.; Preece, J.D.; Easton, J.M. A Review of Prospective Applications of Blockchain Technology in the Railway Industry. *Int. J. Railw. Technol.* 2019, preprint. [CrossRef]

53. Buterin, V. Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform. Ethereum, 2014. Available online: https://ethereum.org/en/whitepaper/ (accessed on 1 November 2019).

54. Wood, G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. (Yellow Paper). Available online: http://gavwood.com/paper.pdf (accessed on 1 July 2020).

55. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26 April 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 1–15. [CrossRef]

56. JP Morgan Chase Quorum Whitepaper; New York JP Morgan Chase. 2016. Available online: https://github.com/ConsenSys/quorum/blob/master/docs/Quorum%20Whitepaper%20v0.2.pdf (accessed on 1 June 2020).

57. Hearn, M. Corda: A Distributed Ledger; Whitepaper. 2016. Available online: https://www.r3.com/wp-content/uploads/2017/06/corda_nontechnical_R3.pdf (accessed on 1 July 2020).

58. Iansiti, M.; Lakhani, K.R. The truth about blockchain. *Harv. Bus. Rev.* 2017, 2017, 119–127.

59. Szabo, N. Smart Contracts: Building Blocks for Digital Markets. *EXTROPY J. Transhum. Thought* 1996, 18, 50–53.