BLOCKCHAINS FOR CONDITION MONITORING

B4CM

Project title:	Blockchains for Condition Monitoring
Starting date:	1st December 2018
Duration in months:	48
Call identifier:	H2020-S2RJU-OC-2018
Topic:	S2R-OC-IPX-03-2018
Grant agreement number:	826156

Deliverable D2.1

B4CM commercial arrangements: Technical report detailing how business-specific requirements / arrangements can be captured in smart contracts and deployed within the framework

Due date of deliverable:	31st August 2021
Actual submission date:	31st August 2021 (revised 12th January 2022)
Lead contractor for deliverable:	University of Birmingham (UoB)
Dissemination level:	Public
Revision:	Final

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826156.

Shift2Rail

Authors

Author(s)	**University of Birmingham (UoB)** Rahma Alzahrani
Contributors(s)	John Easton (UoB)
	Simon Herko (IB)

Document History

Date	Description
31st August 2021	Draft for approval.
12th January 2022	Updated draft including changes in line with reviewer comments: • More detail on the implications of working with highly dynamic datasets within the framework • Updates to background survey and additional commentary around small transactions (e.g. data from IoT monitoring devices) and micropayments • Flowcharts and additional explanatory text associated with the scenarios presented under “Accounting Model” • Minor restructuring to give additional context to reader by bringing forward section on demonstrator use cases (to be used in future work packages)

Disclaimer

Executive Summary

The pursuit of higher quality services in the railway sector is a continuous process, and the availability in recent years of affordable, reliable, digitally enabled additions to traditionally mechanical-based infrastructure systems has provided a fruitful avenue for advancement. Remote Condition Monitoring (RCM) systems are one example of a tool that has been widely deployed to improve the standards of maintenance, reliability, and safety across the rail network. Such systems offer particular benefits at the traditional boundaries of responsibility within the industry (e.g. the interface between the infrastructure and rolling stock) where complex physical interactions may make the cause to defects difficult to determine. Although this type of cross-interface monitoring of assets may be the most technically practical solution to many industry-wide problems, commercially they can prove complex as the business paying to install, maintain, and operate the sensing device is not the party benefitting from the data collected. As a result, it can be hard to generate business cases for the purchase, installation and operation of cross-interface monitoring systems that would have recognised industry-wide benefits.

The aim of this deliverable is to outline the processes by which business / contractual exchanges may be captured and translated into smart contracts for use within the B4CM software framework, and to link these to the use of micropayment models for remuneration.

The document begins with an overview of the background to the area, before moving into a more detailed discussion of arrangements for commercial access to data via the framework, and the accounting model to be applied. It concludes by introducing two industry Use Cases, which will be developed in Work Package 3.

Abbreviations and Acronyms

Abbreviation / Acronym	Definition
B4CM	Blockchains for Condition Monitoring
DLT	Distributed Ledger Technology
GB	Great Britain
IET	Institution of Engineering and Technology
IM	Infrastructure Manager
IPR	Intellectual Property Rights
MQTT	Message Queuing Telemetry Transport
NR	Network Rail
QoS	Quality of Service
RailBAM	Rail Bearing Acoustic Monitoring
RCM	Remote Condition Monitoring
RSSB	Rail Safety and Standards Board
SC	Smart Contract
TTP	Trusted Third Party
UOMS	Unattended Overhead Monitoring System
VT	Virgin Trains
XIRCM	Cross (X) Industry Remote Condition Monitoring

Table of Contents

1. Background to the B4CM Project

Over the past decade there has been a significant level of investment throughout Europe in the digitalisation of the rail network. This includes the installation of sensors on the infrastructure and vehicles, the deployment of next generation traffic management systems that allow real-time management of the system, and the provision of mobile applications for passengers and staff. Despite the wealth of new data provided by these systems, the railways are still struggling in their aspiration to be an information-led industry due to a lack of traceability of information usage, and the commercial barriers between stakeholders.

Blockchains are a disruptive technology that have the potential to accelerate the development of rail as the primary medium-distance carrier within the wider multi-modal transportation system. Directly funded by the rail industry via the EU Shift2Rail Joint Undertaking, the B4CM project will identify key use cases for the technology within the railways, deliver a blockchain-based testbed that enables the benefits of the technology to be formally evaluated, and demonstrate the value of blockchains in the attribution of data costs across organisational boundaries within the European rail sector.

The overall aim of the B4CM project is to develop and deliver a blockchain-based testbed for the attribution of data costs across organisational boundaries, and to demonstrate the operation of the framework and in the context of the European Rail Industry, enabling future developers to extend the tools produced based on a known working configuration.

B4CM has the following research and training objectives:

Objective 1: To identify and develop use cases that support the application of blockchain in the railway sector;

Objective 2: To develop an implementable blockchain framework for the attribution of data costs in systems crossing organisational boundaries;

Objective 3: To evaluate mechanisms for the incorporation of the developed blockchain framework into the financial processes of the European rail sector;

Objective 4: To develop a testbed, demonstrating the operation of the framework in the context of rail sector, enabling future developers to extend the tools produced based on a known working configuration;

Objective 5: To disseminate the findings of the project and the lessons learned to influence best practice in innovation and technology uptake in a key and evolving field within the European rail sector;

Objective 6: To support the development of a researcher in gaining a PhD and thus generating a skilled specialist valuable to the European rail sector.

This document, reporting the B4CM arrangements around commercial processes, is written primarily in response to Objectives 1 and 3 of the B4CM project.

2. Objective / Aim of Deliverable

As outlined in the description of work this deliverable will outline the processes by which business / contractual exchanges may be captured and translated into smart contracts for use within the framework, along with the proposals for the use of micropayment models for remuneration.

3. Background

The pursuit of higher quality services in the railway sector is a continuous process, and the availability in recent years of affordable, reliable, digitally enabled additions to traditionally mechanical-based infrastructure systems has provided a fruitful avenue for advancement. Remote Condition Monitoring (RCM) systems are one example of a tool that has been widely deployed to improve the standards of maintenance, reliability, and safety across the rail network. The advanced warnings of incipient faults provided by RCM data enable preventative maintenance to be performed before service-impacting failures arise, leading to reduced costs of disruption and increased passenger satisfaction. The perceived benefits of RCM have led the industry to install sensors on an ever-higher proportion of its assets, with a corresponding increase in the volume of data generated. In general, and according to [1], railway RCM operations can be divided into four major divisions (quadrants), which are defined by the location of the monitoring sensors and the assets being monitored; train monitoring train, infrastructure monitoring infrastructure, train monitoring infrastructure, and infrastructure monitoring train. In countries such as the UK, where the vast majority of the mainline rail infrastructure is maintained by a single Infrastructure Manager (IM), sensors that are mounted on assets belonging to one stakeholder but are being used to monitor assets related to another will, by definition, fall into the train monitoring infrastructure or infrastructure monitoring train quadrants; an example of this would be sensors mounted on the tracks that are used to detect wheel flats on the rolling stock [2]. Although this type of cross-interface monitoring of assets may be the most technically practical solution to many industry-wide problems, commercially they can prove complex as the business paying to install, maintain, and operate the sensing device is not the party benefitting from the data collected. As a result, it can be hard to generate business cases for the purchase, installation and operation of cross-interface monitoring systems that would have recognised industry-wide benefits.

In order to address this issue, it is widely recognised within GB rail that either closer collaborations must be established between stakeholders to enable more effective cross-interface business cases to be developed, or there must be a trusted audit process that can enable costs of data collection to be fairly attributed based on business benefits accrued by individual stakeholders. To investigate these issues the Rail Safety and Standards Board (RSSB) set up a Cross-Industry RCM (XIRCM) research program, who in turn acted as sponsor to the T1010 research project [3] from 2013 onwards. The stated aim of T1010 was to overcome the barriers for rail companies to use remote condition monitoring (RCM) systems across company boundaries, with the first round of findings presented by RSSB and Network Rail at the IET RCM conference in 2014 [4].

A key component of business case generation for cross-interface RCM is the assignment of value to the data generated by one party but used by another. In order to address the cost issue, it was suggested in Project T1010 that commercial agreements could be established between all the actors in a new condition monitoring workflow before installation of the system began [5]. However, there are issues with this approach; commercial agreements do not remove the need for a trusted third party (arbiter) to ensure compliance with the terms of the agreement, and they do not inherently include any ongoing audit mechanism that

would act as evidence should issues arise. In combination, these two issues act as a barrier to the full exploitation of XIRCM data and cost sharing between stakeholders.

Distributed Ledger Technologies (DLTs) have several features which can be leveraged to address the issues outlined. The benefits offered to the industry through improved system-wide asset information and decision support are clear, but for those benefits to be realised in a privatised rail system where the separation of business functions is the main architectural driver, the commercial implications of the operation of cross-industry systems for each actor must be clear. Further to this, existing investments in specific RCM systems made by the industry are currently only in their mid-life stages, meaning a method to deliver the clear understanding of operational costs must be cognizant of, and compatible with, the methods of operation of these existing assets. DLTs are one possible solution to these issues, offering the potential for traceability of data flows between industry actors with minimum restructuring of the current systems. By understanding the flows of data between actors, and the ultimate costs / benefits accrued by the installation and use of the system (for which mechanisms are already in place), it will be possible to accurately assign costs to the relevant parties, to cut down on the operational inefficiencies associated with manual attribution and Trusted Third Parties, and to enable improved understanding of data provenance via the decentralized and immutable record in the ledger.

Blockchains are a specific type of DLT constructed from structured sequences of blocks connected via cryptographic hashes, providing a tamper-proof ledger that leads to a traceable and auditable log of all activities between stakeholders. In industrial environments, the implementation of this technology facilities greater integration of business processes and stakeholder data, with the blockchain delivering three major protocols: decentralization, cryptography and consensus [6]. Due to the censorship-resistant and tamper-proof digital networks of distributed trust created by this revolutionary technology, blockchain-driven technologies help to enhance transactions and make them more reliable and safer. Industrial deployments of the blockchain are still in the early stages of development, and further work is required to establish the full extent of the value the technology offers. However, substantial efforts have been made to investigate its applicability and future penetration in numerous industries, including the industrial sector, as the new technology continues to mature [7], [8]. The transformative potential of Blockchain technology in industry settings has already been established in the literature [9], and in the rail industry specifically Blockchain-based applications for ticket sales, invoicing and freight distribution, among others, have also been investigated [10].

Large volumes of data are generated daily by RCM systems installed on the GB rail network. While this data is already utilised to improve performance within the context for which the system was initially specified, in many cases opportunities exist for the realisation of additional benefits by sharing this data between stakeholders and across system boundaries, enabling it to be used in problems that cross traditional industry interfaces (primarily the separation between the infrastructure and vehicles). The continuous improvement of system performance through RCM-informed operations and maintenance is a field of intensive research and many projects focusing on this area have been initiated [11]. At present, the industry is still on an upward performance trend in this area, and localised sensor systems used in isolation are still providing operational benefits. However, moving forwards the industry is expecting these systems to coalesce into fewer, multi-party

and sensor environments, essentially evolving the network's current RCM capability into an "Internet of Railway Things" [12] requiring new ways of managing, processing, and accounting for data. This amalgamation of state-of-the-art IT, cloud computing and big data, presented as an IoT paradigm will ultimately lead to a viable "smart railway" fit for the next century [13].

Depending on the nature of the sensors deployed the data produced by RCM systems takes many forms, including audio, video, pictorial, continuous analogue measurements, and digital signals. In order for the raw datastreams to have operational value, they must first be processed, cleaned and aligned to the point where they can be reliably used as the basis for analytics. There are six recognised levels of data analysis in condition monitoring [14], ranging from raw data collection (at the lowest levels), through the generation of alarms in response to defined alert criteria, to a full diagnostic function that involves sending prognostic information to the operations and maintenance team to instruct them to repair a particular asset before it fails. The data used as the input to each level of the stack (or indeed the analytics process itself) may originate from multiple stakeholders, and as the level of data processing increases, the inherent value of data becomes higher as a result of the additional knowledge associated with it. According to [5], unless specific contractual provisions say otherwise, it is typical for the Intellectual Property Rights (IPR) to data recorded by RCM systems to be held by the party that collected it, while the IPR for derived data (data the results from a processing chain and is considered "enhanced") belongs to the party who performed the processing.

As is the case in any trading environment, successful RCM deployments require that both the providers and the consumers of the data gathered comply with any contractual arrangements made around the system, and particularly when ensuring the quality and reliability of the data and advisory information produced. To this end, it is desirable for a traceable mechanism to exist within the system that monitors the provenance of the RCM data; this provenance information provides evidence that directly affects payment, compensation, or refund processing. In current RCM deployments, a Trustworthy Third Party (TTP) such as a bank, third escrow mediator, or conflict board may be a requirement to manage these needs.

DLTs, in the form of blockchains and smart contracts, have the potential to offer great value to industry in this context enabling operators of RCM systems to dispense with the need for a TTP and inherently prevent the RCM data generated from being falsified, altered or corrupted without the changes being evident. Further to this, in order to both quantitatively and qualitatively monitor and manage the flows of data between providers and consumers, Smart Contracts (SC) may be deployed on the blockchain. Deployed SC are essentially distributed executable scripts running in the blockchain [15], and this combination of traceability (as provided by the chain itself) and transformation / transaction of data (as provided by the SC) provides an environment in which the whole value chain around items of data may be audited and understood. As pointed out by Christidis and Devetsikiotis [16], in a traditional relational database management system, a SC would essentially be used as a stored process, but by using SC within the underlying execution framework offered by the blockchain, a wide range of applications can be created.

Within the literature, a range of examples of the use of blockchains in partial solutions to the problems seen in cross-industry RCM may be found. Existing studies on the use of micropayments between stakeholders linked to IoT data exchange, for example, have suggested that SC-based frameworks would form an appropriate basis for that use case. In the Saranyu system [17], Nayak et al created a cloud tenant and service management system using Quorum (a private blockchain network) as a platform, but ultimately failed to capture appropriate information on charging tenants. A subscription-based model for trading data on cloud platforms was also introduced by Al-Zahrani [18]. In the proposed model, the ledger tracked all subscriptions and orders, and this included those on which the request has not been concluded and finalized, providing potentially useful information to forensic investigators should problems occur. A blockchain-based solution using Ethereum was launched in [19] which regulated both payments to, and access by, the owners of data generating IoT devices. When subscribing to a particular IoT device and before accessing the data processed in the MQTT broker, which represented a single point of failure within the system, data owners paid a deposit in ether (the “currency” of the chain).

With the exception of [17], none of the work identified provided a mechanism for the suspension or revocation of malicious actors / account subscriptions, other than the removal of the associated data from the cloud platform used. Typically, the authors assumed that data providers acted honestly in all the systems surveyed and did not address the issues raised by the presence of falsified or garbage data that may have been deliberately inserted into the platform to deceive customers. The payment companies BitPay [20], BitHalo [21], and DCSP [22] have considered the issue of dishonest actors, and all have previously proposed the use of double deposit escrow. In all three proposals, both the buyer and the supplier use SC to create an escrow for the deposited values, but the actual transfer of assets is made off-chain. Both parties must acknowledge the SC that the transaction is successfully made in order to unlock the escrow. Should confirmation not be given, both forfeit their deposits. A dual-deposit escrow mechanism identical to the previous three schemes was suggested by Asgaonkar and Krishnamachari [23] but offered a subsequent dispute resolution stage (potentially preventing deposit loss) and involving the main payment transaction. However, this system was only suitable for one-time usage scenarios, and the buyer was required to review every transaction and provide a reply to open the escrow and process the payment. The seller received no compensation if the customer did not respond (regardless of the presence or absence of malicious intent) and would forfeit their deposit and right to payment. A different data sharing mechanism is proposed in [24], in which data hash values are encrypted with a symmetrical key and deposited in a secure location off-chain by the data provider before the transaction is actioned. In the cloud, all providers are able to promote their data services and public keys. To enable consumers to gain one-time access to the appropriate records, SC were generated on the fly and the activity logged on the chain to be used in the resolution of any potential disputes.

In the B4CM project, the framework proposed will build on the escrow proposals discussed above but will additionally include litigation solutions that ensure escrow locking or payment/compensation loss do not take place.

Recently methodologies for connecting IoT devices to the blockchain in order to establish secure machine-to-machine data transactions have been proposed in a number of research

papers. In [31], Iftekhar et al presented an Attribute-Based Access Control framework that leveraged the Hyperledger blockchain in the management of trustworthy access control between the IoT devices. In order to separate people and IoT devices, the system utilizes Hyperledger Fabric configurations, allowing the access rights to smart contracts to be regulated and controlled by predefined rules and, within the smart contracts themselves, access management to be controlled programmatically.

In dynamic IoT environments, Putra et al in [32] introduced a blockchain-based TRS (Trust and Reputation System) for monitoring and controlling access to the chain from the IoT, which consecutively assesses and measures the IoT node trust and reputation levels in a self-adapting and reliable manner. An attribute-based access control policy was proposed that would enable the establishment of trust based on reputation; within the system nodes would therefore dynamically gain different access rights based on past behaviour, reenforcing positive actions within the network.

Zhang et al Presented a smart contract-based scheme composed of several Access Control Contracts (ACCs), a Judge Contract and a Register Contract to enable distributed, trustworthy access control in IoT ecosystem. For each access control contract, one access control mechanism is offered to a subject-object pair, and each access control contract evaluates the behaviour of the subject to implement both predetermined access rights and dynamic access rights validation [33].

Truong et al. proposed Sash, an architecture for trading IoT data using the blockchain, in which data owners could be remunerated by selling their data [34]. The proposal is based around automated updates to the access control list (ACL) for resources by the blockchain without the involvement of the data owner, with the changes being triggered once the data consumer has paid for the off-chain encrypted data. Although promising the work contains no mention of how cryptographic keys are distributed to decrypt the captured data, which may be delegated to a separate authority or provided by the data owner. Utilizing a cryptographic key distributor authority makes the network more centralized and reliant on authority, which weakens the blockchain's decentralization property and by extension the whole rationale for the proposed architecture over one of the better established, more traditional alternatives.

The B4CM platform is incorporating ideas from [31] as part of its core offering, building on the proposed mechanisms for trading data between IoT devices in railway.

Section 4 will now provide further context by presenting two case studies that illustrate the challenges around cross-interface management of data in the rail industry.

4. Cross-Interface Data Sharing in GB Rail

The management of data at industry interfaces is a well-recognise challenge in many sectors, including rail. What is perhaps less well understood, is why data exchange is not simply an engineering problem. In this section the B4CM team introduce two case studies of cross-interface data exchanges of the type commonly encountered within the industry, these will be used as test cases in the later stages of the project. The first case study will be the Unattended Overhead Line Equipment Monitoring System (UOMS). The second will be the Rail Bearing Acoustic Monitoring system (RailBAM). A brief description of each use case is discussed in the following subsections.

Train-based system monitoring infrastructure: Overhead Line Equipment Monitoring System (UOMS)

Overhead wire is used for the transmission of electrical energy to electrified trains. The Pantograph, an apparatus mounted to the train, slides along the wire capturing the electricity required to operate the train. Both overhead wire and pantograph may have defects that may cause costly damage. The overhead wires are subject to deterioration and abrasion by the time as a result of wear and tear [25]. This abrasion and irregularity in overhead wire is causing the carbon blocks on the pantograph head to be damaged in addition to the friction impact [26].

As a result, this may cause significant impact on passengers with a high level of delay when the service is down.

The damage to the pantograph's head which may shorten the lifetime of the head will lead to off-site maintenance or replacement in depots. In contrast, fixing the overhead wire must be held on-site within a short period during the traffic closure which might be very difficult to achieve in most cases without costly consequences.

So, knowing the location of the defects on the wire at an early stage is very important for the railway operator leading to effective maintenance to avoid severe and costly damages. To accomplish this, a proposal by Virgin Trains a previous train operating company in UK was introduced to attach Unattended Overhead Line Monitoring System (UOMS) equipment to a class 390 train. This device will measure the longitudinal force on pantograph whilst in service. Any exceedance for a pre-determined threshold, then, the force value, the date and time, and location will be recorded. Next, the recorded data should be downloaded off the train and sent to Network Rail for further analysis and interpretation and also sent to Virgin Trains.

Current Business Case

Obviously, Virgin Trains and Network Rail were the direct beneficiaries from the collected data. According to project T1010, Virgin Trains paid a third party (Lloyds Register Rail) to manually collect raw data off the trains and send it by email to both Virgin Trains and Network Rail which leaves uncertainty in referring the ownership of the data [27]. Conducting the analysis of the collected raw data was then handled by Network Rail, noticing that, the cost of this procedure has not been included in any agreement before. Thus, any party other than VT and NR who may have interest to access this data would find some extent of complexity and ambiguity regarding whom he should contact.

Infrastructure-based system monitoring Train: Acoustic axle bearing monitoring system (RailBAM)

Axle journal bearing, upon which the wheel is rotating, is one of the most important parts for the train. Primarily, any degradation or failure in this part will cause major and costly impact when the train is taken out of service for expensive repair. At the worst case, the impact might be greater if the failure leads to derail and causes dangerous accident. Therefore, rail operators pay considerable attention in maintaining and monitoring this part as safety precaution [28]. One of the most recent technologies used to help in providing predictive maintenance is RailBAM (Rail Bearing Acoustic Monitoring). This technology is developed by Track IQ, a Wabtec company, and now Siemens has an exclusive international agency agreement to sell and supply this product [29].

Basically, this technology depends on the emitted noise produced from bearings when wheels are rotating while passing the track. This emission will vary according to the condition level of these bearings and used later in assessing their state and checking for defects. In case the emitted noise indicates a presence of defect, rolling stock maintainers will be alerted to plan a maintenance visit for fixing the defect without impacting the train service. By this predictive way, defects will be monitored a long time before arriving at failure stage that might cause additional costs or early wheelsets damage.

RailBAM technology composites of two main acoustic cabinets mounted on either side of the mainline, and continuously record the acoustic emissions come out from journal bearings on both sides of the passing axle of each rolling stock. A third cabinet which houses all communication and power equipment needed for system operation, is also installed away from the track. The third enclosure enables the collected data to be processed on-site and transmitted via secure VPN connection to web server for real time access. Each rolling stock maintainers will be allowed through web-based server to access the data of their own fleet. Identifying the train is achieved by supplied RFID tags fitted to each rolling stock (Radio Frequency Identification) which will be associated with the acoustic files generated by the trackside reader as the train passes.

Principally, the operation begins when a train passes the acoustic sensors which capture and store the sound profile emitted from each axle journal bearing. Then, system links the acoustic file to the train tags and associates the pass-by date and time. The system analyses the acoustic data for known distress frequencies. These very small amplitude sounds can be identified giving the train maintainer up to 9 months (100,000 miles) notice of a failure [27]. To keep the data updated, repeated pass-by will be also recorded to observe any worsening in the condition of any axle journal bearing. In the event that an axle journal bearing is flagged as carrying a defect, then corrective maintenance for the unit can be scheduled for the next exam. In some cases, as long as the system is not showing any defect that requires immediate attention, axle journal bearing can stay in service even beyond its maintenance interval.

The first RailBAM system in UK was supplied by Siemens in 2009 and was targeting only passenger rolling stocks. Noting the result, additional two more trackside unites have been installed later and more train units have been equipped with tags to gain benefits from this system. In fact, the number of flagged assets which are monitored by the three RailBAM installations is increasing as more fleets are being tagged as franchises are renewed [30].

Current Business Case

There are several parties in rail industry interested in the data generated by RailBAM system such as Network Rail, TOCs, FOCs, and other train manufacturers and maintainers. In project T1010, template contracts were created that can be used when negotiating the commercial arrangements for cross-industry RCM systems [5]. The commercial agreements take place between Siemens and those parties under which Siemens provides them with limited access to their data through the web portal FleetONE and protects the confidentiality of others data. The data ownership is vested to the organization that procures the RailBAM equipment, hence, an agreement with that organization is sought in terms of data distribution. There are no details around the payment policy, and there is a major concern about the pivotal relationship between Network Rail and the train operator which doesn't reflect who pays for the XIRCM project and who receives the major benefit from the project. In the bid to solve the aforementioned problems and organize the process of data sharing between stakeholders in UOMS and RailBAM use cases, the developed framework provides fair distribution of costs and guarantees concise agreements building between involved partis. Leveraging the inherited characteristics of blockchain, it will be possible to track all the orders and payments transactions that are shared and accessed only by permissioned members on an immutable ledger.

The funding of equipment installation, purchasing, and maintaining will not be included as this is maintained differently according to each stakeholder. We only concern about processing the agreement and finding the cost attribution of sharing the captured and processed data between data providers and interested consumers.

Implications of case studies on industry data sharing

As can be seen from the case studies, far from being a technical problem (which could largely be solved with COTS software solutions), data sharing within the rail industry is a complex socio-economic issue that includes aspects not only of technology, but also commercial practice, governance, and trust between actors. To compete effectively with other transport modes, the railways must realise the economic and performance benefits that can be realised through the sharing of datasets. However, in a competitive industry we must also accept that certain forms of data may have huge commercial value, and the costs of managing and maintaining data of high quality must be recoupable by the organisations generating and sharing them. The need for monetization of data generates requirements for secure, traceable access by known actors, but with the prospect of large financial gains, we must also consider the possibility that not all actors within the system will necessarily act in a way that maximises the benefit to their consumers or the wider rail industry; examples of this could include introducing undisclosed delays into the release of time-sensitive data to maintain a competitive advantage, or the issuing of low accuracy or falsified data. With that in mind, Section 5 will now describe how trust handled within the B4CM framework.

5. Proposed Framework

In project Deliverable D1.1, the authors present their proposed framework for the audit of RCM data in industrial systems. The framework replaces the TTP typically involved in these systems with a permissioned blockchain architecture, leaving data producers / data owners (providers), data users (consumers), and smart contracts as the key actors in the system. Figure 1 illustrates this change; Figure 1 (a) shows a typical trust arrangement that would apply in a none DLT-based RCM network, in this case all parties must trust that the other producing / consuming parties will honour their obligations under the agreement defining the distribution of system costs, the TTP reviews local financial cost assessments provided by the other actors in order to confirm adherence to the applicable terms. This process will henceforth be referred to as "local cost monitoring". As the local cost monitoring of both providers and consumers is dependent on the data they report, even with the TTP in place there is no guarantee of strict adherence to the terms of the contractual agreements between the parties.

As an example of the requirement for trust, consider Quality of Service (QoS) criteria place on a data provider. Honest providers could choose to comply with the terms of the signed agreement and offer the requested level of service that they initially advertised; this would result in an estimated cost calculation for the data as delivered and an associated attribution of the cost to the consumer. The consumer, on the other hand, will have their own interpretation of the quality of the service they have received; this may tally with that of the provider, or may be impacted by external factors such as network latency resulting in a different view of the fair attribution of the cost from the consumer's side. To reinforce their point of view, both parties will provide evidence, but as there is no confidence between them, there will be no trust in the correctness of their evidence. The presence of the TTP goes some way to mediating these issues, but still requires that the evidence as presented by the provider and consumer is fundamentally accurate, or that the TTP can identify when that evidence is incorrect, and (ideally) who is in error. By comparison, the relationships and trust between actors required in the proposed framework is shown in Figure 1 (b). A trust relationship between the provider and the customer is no longer necessary, although both sides do need to trust the DLT and the SCs that implement the accounting logic, data access / delivery agreements, and cost allocations. Sections 6 and 7 will explain these procedures in detail.

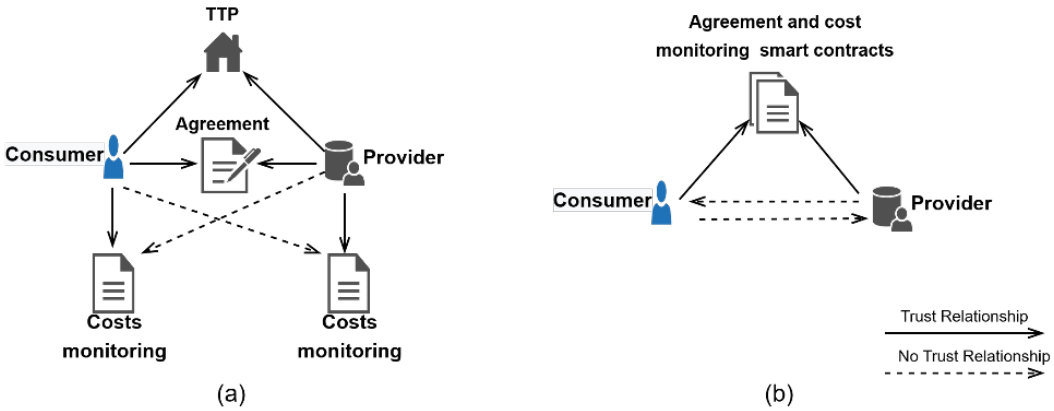

Figure 1: Trust relationship between actors.

6. Access Agreement Model

The commercial agreements originally outlined in project T1010 [5] have driven the definition of the components used in the SC for the access agreement and cost estimation process between provider and consumer as shown in Figure 2. Two new records, "DataAgreement" and "Escrow", will be automatically generated by SC and appended to the ledger each time a new data access request is made by a consumer to a producer. The DataAgreement will hold information on the new agreement between the data consumer and data provider, including the data offered by the provider, the unit price, and the period of validity. The Escrow record will form the basis for enforcement of access to the data and exchange of payment on release, and as such is primarily suited to the management of transfers of static or semi-static datasets (historical corpuses of monitoring data, reference data on the infrastructure, asset information etc.).
In real-time monitoring, when highly dynamic data exchanges take place for very short periods in (near) real time between IoT devices or cloud data lakes, a full Escrow process may not be practical or applicable (as the dynamic relationships are formed for very short periods, and human "agreement" and validation is not achieveable); in these cases data requests will be processed subtlety differently, using predefined access control lists that permit access to the chain / trading facility by legitimate devices only. *DataProvider* and *DataConsumer* attributes in the *OfferRequests* records will then represent IoT device / cloud platform IDs. Access control will be implemented within the deployed smart contract to grants access restrictions as per specifications in the network. Exchanges would be limited in size and value, making payments very small and frequent; although this scenario would not be practical in the general case (as there would be a huge overhead for larger datasets), it would apply well in this scenario and would require minimal changes to the Escrow based mechanism already defined.

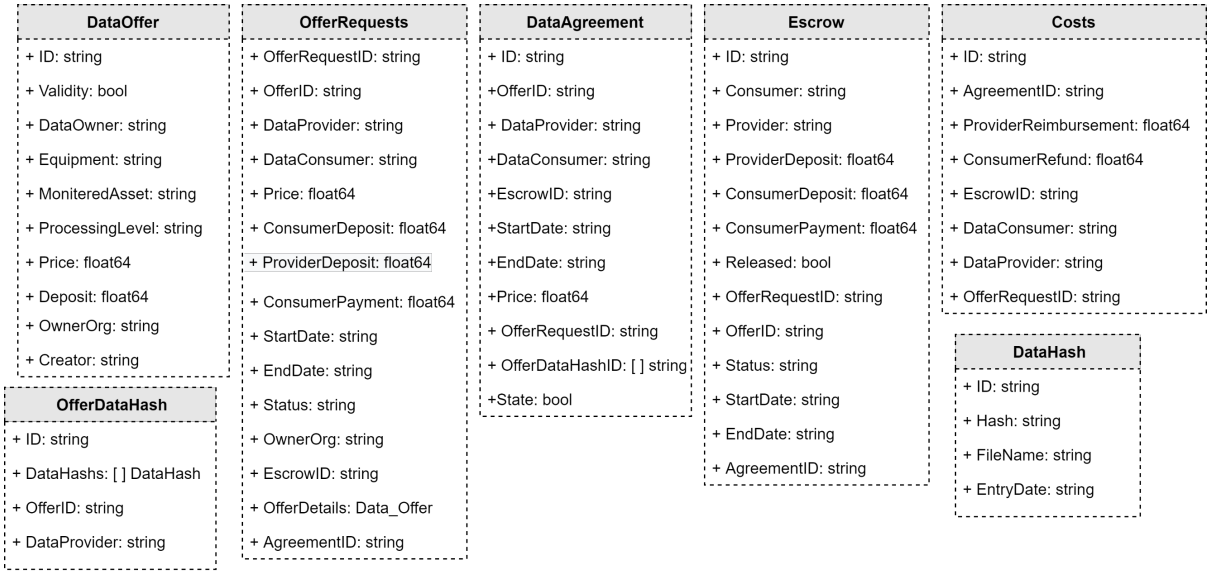

Figure 2: Data structure for commercial agreements.

Recall that the IPR for the RCM data belongs to the provider, thus, no other party in the system will be able to advertise an offer for exactly the same data (although they may be able to advertise derivative forms) and this mechanism is protected by hash values. Both

data providers and data consumers must be registered with the trustworthy authority (in this case the permissioned blockchain) in the set-up process of the system and must have their IDs and public/private key pairs before participating.
The overall flow of the access agreement process is as follows:

1. The customer will submit a request to the SC in which they will specify the offer they are interested in, along with the subscription duration and all payments.
2. The authenticity of the submitted request will be tested by the SC. If it is not legitimate, so the request will be denied. A payment mechanism is triggered if the offer is still available; this process is addressed in depth in Section 7.
3. After completing the payment process, the SC will automatically create a new agreement between the provider and consumer in addition to building an escrow to hold the payment. Both provider and consumer will be informed of establishment of the agreement.
4. Prior to uploading the original data onto the external storage, the provider's private key and the consumer's public key will be used to sign and encrypt data respectively as follows: consumerPublicKey(providerPrivateKey(D)).
5. The consumer will decrypt the data they gain access to on the off-chain storage and compare its hash with the hash value provided in the on-chain record to validate its integrity.

In this proposed model two types of malicious behaviour on the part of the data provider can be proven by the consumer:

a. Sending falsified or incomplete data;
b. Undue delay in uploading evidential hash values to the on-chain record.

If the QoS by either party is found to violate the terms of the agreement, both provider and consumer can revoke the agreement before the stated expiry date. This action is permanent, i.e. the agreement cannot be revived once revoked; instead, a new agreement must be entered into from the beginning. Figure 3 shows the sequence of creating the data access agreement while in Figure 4 additional steps are needed when involving IoT devices in the proposed framework. To prepare the participated IoT devices to output the hash digest on the blockchain or establishing a new agreement to acquire data, the owner of the device will be responsible for the management of deposited budget which will be used in processing the micropayment when interacting with the blockchain. In addition, the data provider will maintain Access Control List (ACL) to the deployed smart contract to specify which device will be legitimate to send request to the provider device in order to gain access to the offered data.

7. Accounting Model

Payments on any trading site may be realised using post-paid or pre-paid models. The post-paid model requires the provider to place trust in the consumer (buyer) that the payment will be made as agreed after the data is delivered. The pre-paid model requires that the consumer places trust in the provider that the data will be delivered once the payment has been made as agreed. Neither model guarantees both consumer and provider satisfaction, and both bear some risk if the other party breaches the terms of the agreement. There is also a requirement for a TTP to provide both the provider and the consumer with an escrow service.

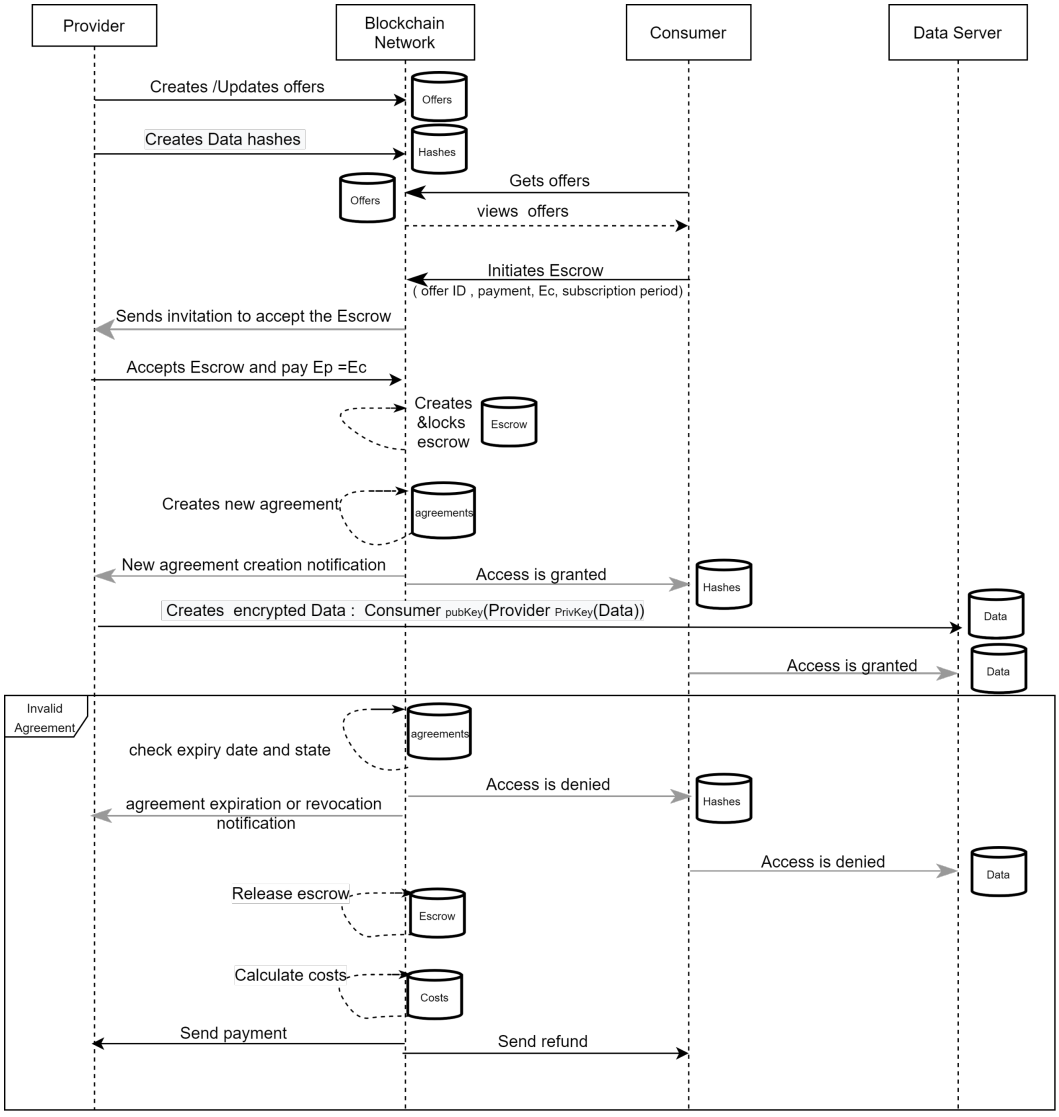

Figure 3:Data access agreement sequence model.

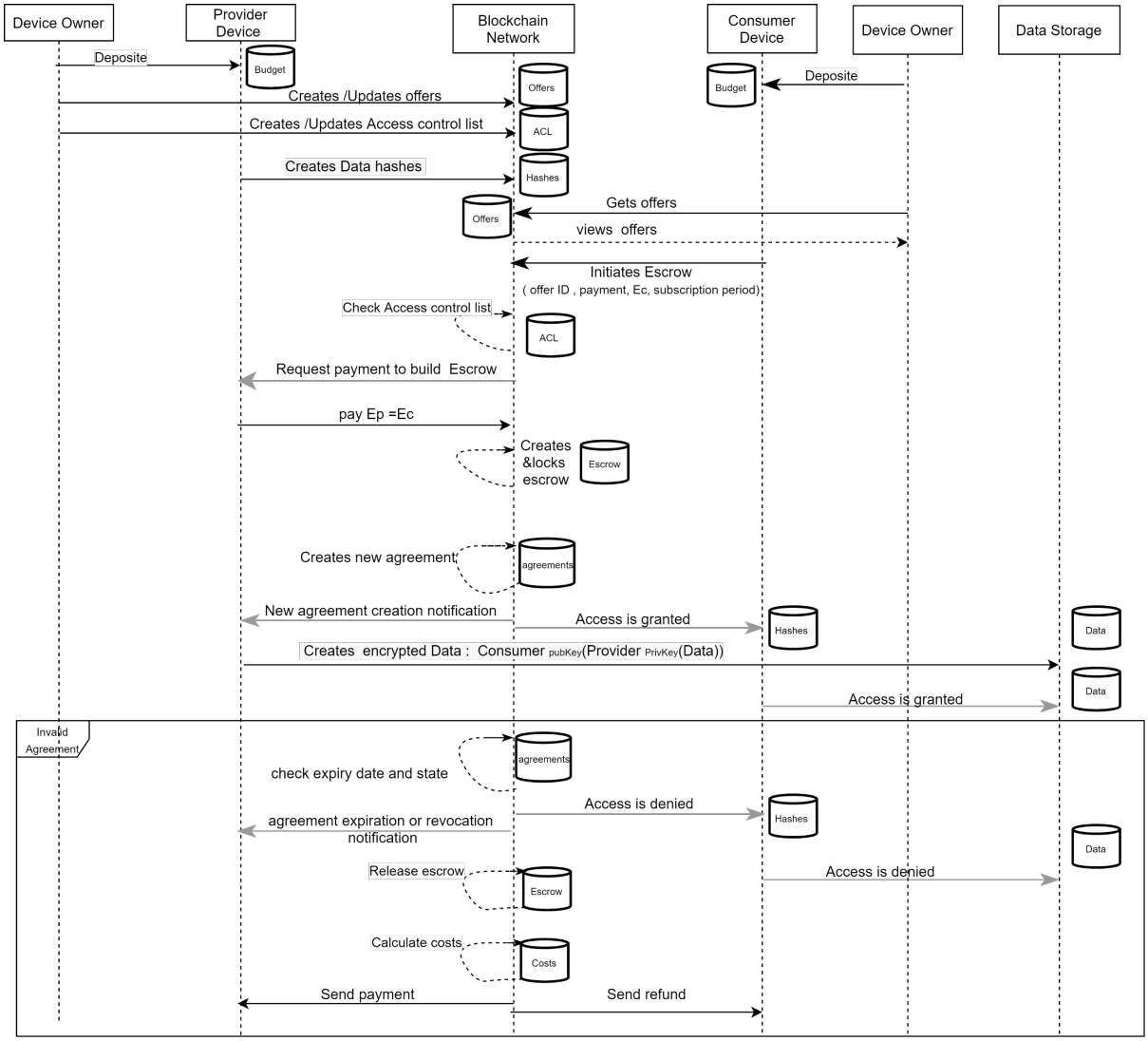

Figure 4: IoT Data access agreement sequence model.

In the proposed framework, SC will be used to provide escrow, removing the need for a TTP and ensuring the payment is released the provider after the data is delivered and the consumer agrees that it meets the stipulations of the agreement / assuming a revocation request in not made. The escrow SC is also responsible for managing any penalty payments required by the agreement, and these would be charged in advance of any data exchanging process by both provider and client.

The provider is expected to deploy the following attributes and values with the offer they are advertising as shown in Figure 2:

D_{price}: Denotes the data price of certain offer in a specified period.

E: Denotes the deposit both consumer (E_{cns}) and provider (E_{prd}) should pay to build an escrow. The deposit will act as the penalty in case of any breach of the terms, and therefore must be set at a level that acts as a deterrent for both parties.

h(D): Denotes the hash value of the shared data.

The flow of the payment process is as follows:

1. An escrow SC will be initiated once the consumer responds to a published offer. The escrow details the offer being responded to, and triggers payment of the corresponding charge and deposit by the consumer. On receipt, the SC will then direct the request to the provider.
2. On receiving the request, the provider will check if the payment and deposit detailed in the escrow are matched with their offer. Then, in order to lock up the escrow, the provider must pay their deposit, which may not be less than the deposit of the consumer. If the provider determines that the size of the payment or the deposit does not match with the terms of their offer, the provider can reject the request and the consumer will get back their payment.
3. The process of locking the escrow will trigger a SC to initiate an agreement, in which the period over which the consumer has access to the provider's data is specified.
4. The cost of data consumption will be monitored via the SC when the escrow is released. The escrow will be released automatically if either of the two states below are realised:
    a. The agreement's expiry date is reached; or
    b. The agreement is revoked.

In both cases, if there is a claim of inappropriate activity from either side it should be evaluated before calculating the final cost attribution. The deposits that have been charged would then be used in settling any penalties due if maleficence has been proven on either side. Figure 5 summarises all the possible outcomes of an investigation into QoS breaches between a provider and consumer. Costs are calculated based on each scenario, which are outlined in equations 1-4. The terminology below is used in the equations:

$Cns_{Payment}$: Denotes the payment that consumer should pay when initiating the offer request. It represents the total of D_{price} and E_{cns}.

$Act_{Payment}$: Denotes the actual payment of the consumed data based on the period of use; this value should be less than or equal to $Cns_{Payment}$.

$Prd_{Reimbursement}$: Denotes the final cost that will be transferred to the provider based on the status of the agreement and the raised claims.

Cns_{Refund}: Denotes the refunds that will be transferred to the consumer based on the status of the agreement and the raised claims.

To calculate the ActPayment three different dates will be considered:

Rvc_{Date}: Denotes the revocation date.

$Start_{Date}$: Denotes the beginning of the agreement, as declared in the agreement.

Exp_{Date}: Denotes the end date of the agreement, as declared in the agreement.

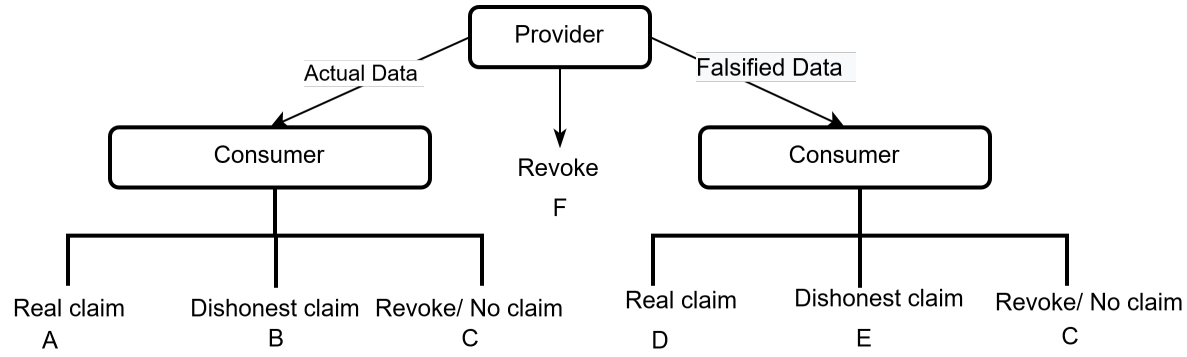

Figure 5: Outcomes of all possible trading scenarios.

Scenario A: The consumer receives the requested data as agreed but raises a genuine complaint about the latency in providing the appropriate hashes to the network. As illustrated in Figure 6, the deployed SC will evaluate this claim by checking the time of appended hash values on the chain, using the block's timestamp. As the consumer's claim is genuine, the agreement will then be revoked, triggering the calculation of costs as illustrated in equation 1. In equation 1 the delta between the start time of the agreement and the revocation time (Rvc_{Date}) is used as a factor to calculate the actual payment to be due to the provider. The consumer then will be refunded any money remaining from their initial payment (made on instantiation of the agreement), and in compensation awarded the deposit payments of both parties.

$$Act_{Payment} = D_p * (Rvc_{Date} - Start_{Date})$$

$$Prd_{Reimbursement} = Act_{Payment} \quad (1)$$

$$Cns_{Refund} = (Cns_{Payment} - Act_{Payment}) + E_{prd} + E_{cns}$$

Scenario B: The consumer falsely claims the data is corrupted or incomplete, or that the hash values are not appended to the chain in a timely fashion. In this case, the cost SC will evaluate both cases to validate the claim. The former is evaluated in the same way as a claim against the accuracy of the provided data; the SC requests the received data, which is signed using the provider's private key enabling verification of the data source, and then applies a hashing process to the data, enabling it to be compared with the hashed value that is stored on-chain (see Figure 9 for the full process). The latency in appending hash values will be validated as mentioned before in scenario A, and illustrated in Figure 6. In this scenario, the consumer's claim will be found to be false by the SC, and as a result the agreement will be revoked and the cost will be calculated as outlined in equation 2. In a similar way to equation 1, the actual payment will be calculated by using the revocation time, and the calculated payment will be credited to the provider. The provider will be further compensated by the two deposits. Should any of the initial payment remain at this stage, then the consumer will be refunded by the remainder of his payment.

$$Act_{Payment} = D_p * (Rvc_{Date} - Start_{Date})$$

$$Prd_{Reimbursement} = Act_{Payment} + E_{prd} + E_{cns} \quad (2)$$

$$Cns_{Refund} = Cns_{Payment} - Act_{Payment}$$

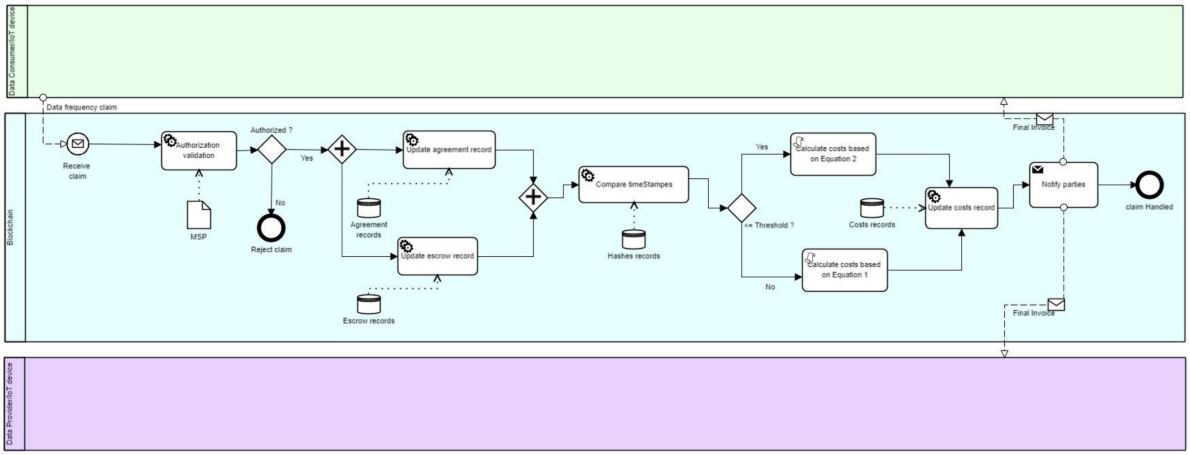

Figure 6: Revoking an agreement due to frequency claim.

Scenario C: As shown in Figure 7, the consumer revokes the agreement without raising any claim. In this case the agreement will be revoked and the cost will be calculated as outlined in equation 3. In this scenario the revocation time is again used to calculate the actual payment due to the provider, who is also credited with the return of his deposit. Once payment to the provider is made, the consumer will be refunded the remainder of his initial payment along (as this is a "no fault" claim) with the return of his deposit.

$$Act_{Payment} = D_p * (Rvc_{Date} - Start_{Date})$$

$$Prd_{Reimbursement} = Act_{Payment} + E_{prd} \quad (3)$$

$$Cns_{Refund} = Cns_{Payment} - Act_{Payment} + E_{cns}$$

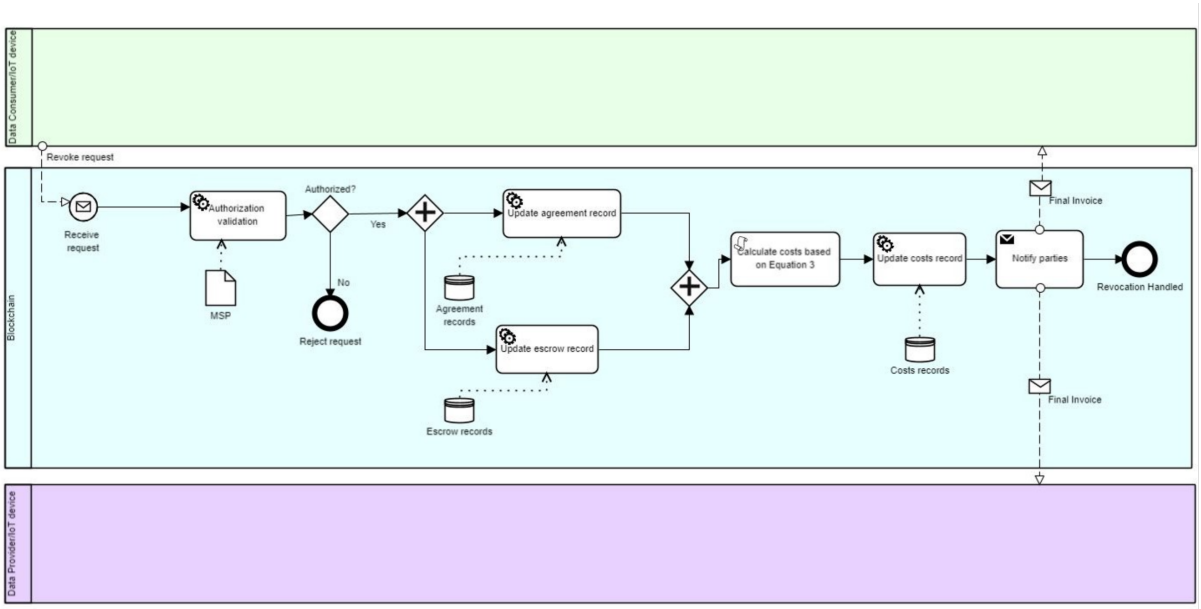

Figure 7: Revoking an agreement without claim.

A similar process illustrated in Figure 8 will be triggered when the agreement reaches the pre-agreed expiry date without any revocation or complains from the consumer's side. Equation 4 differs from equation 3 in that the expiry time of the agreement is used instead of the revocation time to calculate the actual payment, but otherwise they are identical.

$$Act_{Payment} = D_p * (Exp_{Date} - Start_{Date})$$

$$Prd_{Reimbursement} = Act_{Payment} + E_{prd} \quad (4)$$

$$Cns_{Refund} = Cns_{Payment} - Act_{Payment} + E_{cns}$$

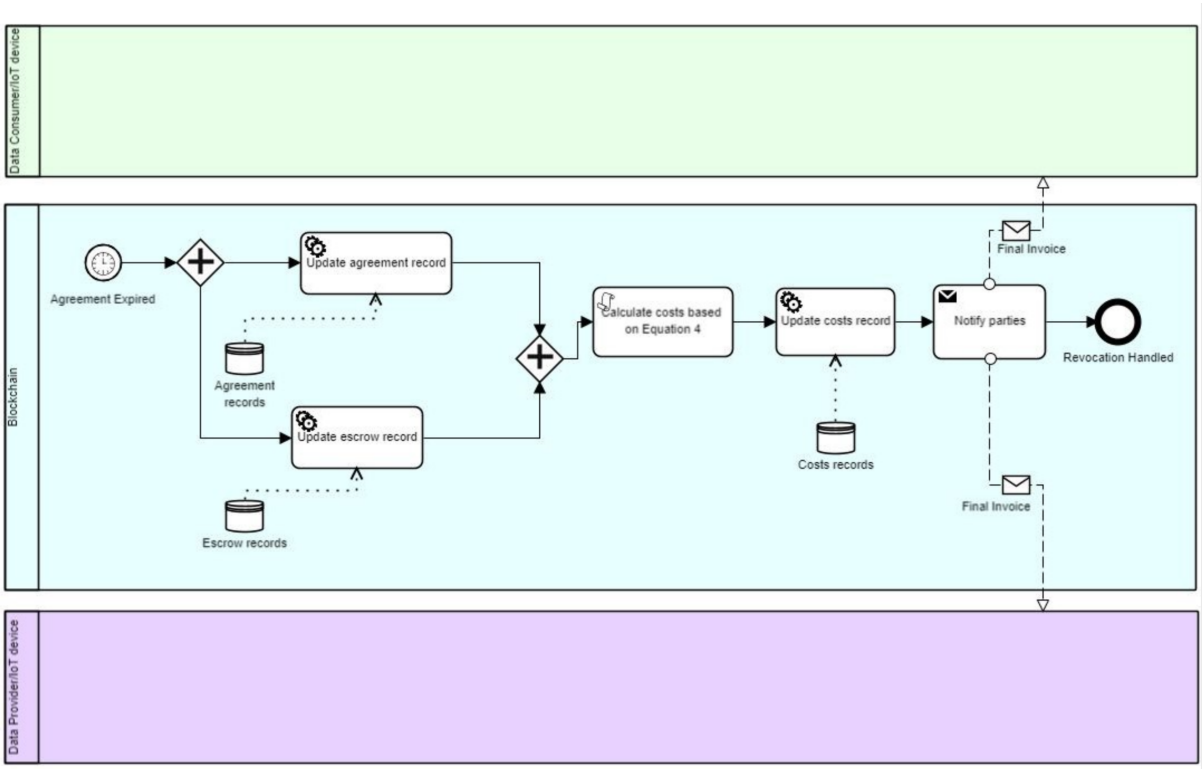

Figure 8: Expiry of an agreement.

Scenario D: The provider sends falsified/incorrect data to the consumer, which the consumer detects. In this case, the consumer raises a claim to the SC, which will request the original raw data to hash and compare the result to the hash value stored on the chain. As a result of the provider's actions the agreement will be revoked, triggering the calculation of costs according to equation 1; the process is illustrated in Figure 9.

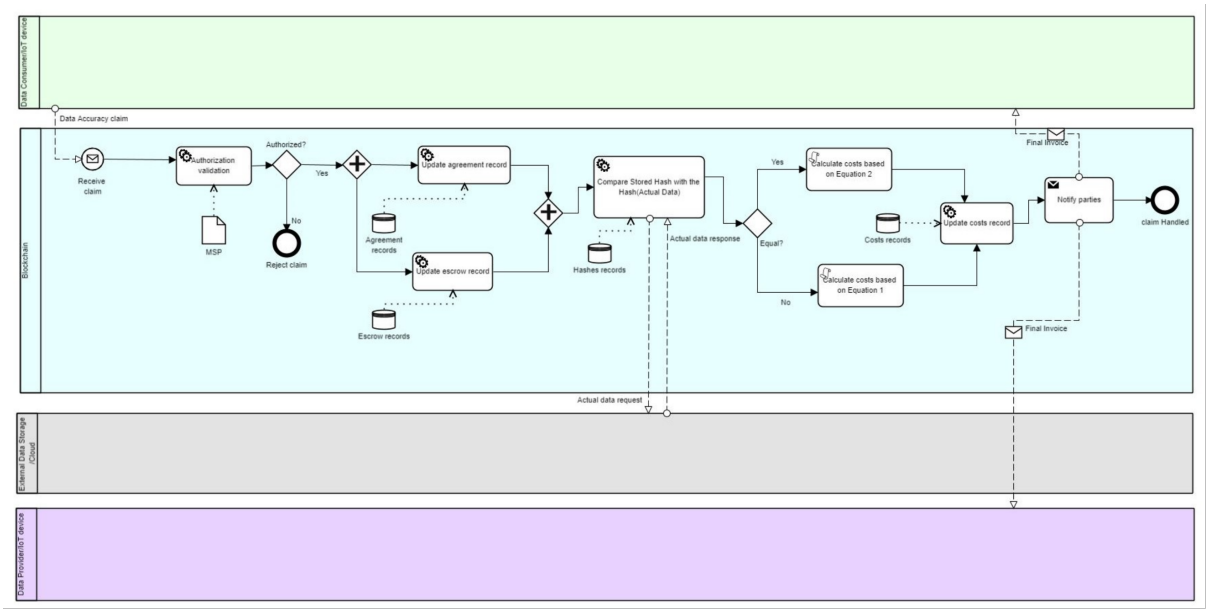

Figure 9: Revoking an agreement due to claim of accuracy issues.

Scenario E: The consumer raises a genuine claim against the provider but attaches the wrong evidence leading the SC to evaluate the claim as false. Such a situation may occur if, for example, the provider uploaded the right hash values to the network at the right time but sent the wrong data to the consumer on the external storage. When the consumer identifies the mismatch between the hash values, there is a risk of raising a latency claim rather than an accuracy claim resulting from the mismatched hash. Were the consumer to raise a latency claim in this situation then the SC would prove the claim false and process the cost according to equation (2). In this scenario resolution and reimbursement of the consumer would be possible if the consumer provided the signed original data to a dispute board. The provider won't be able to show the hash value that match with the provided singed data that has uploaded to the network on the same date. This would of course require such a board to be in place and may reduce the overall financial benefit of the blockchain implementation.

Scenario F: The provider chooses to revoke the request as they can no longer provide the data as advertised, or they are unwilling to provide the data for another reason. In this case costs will be calculated according to equation 1, with the process illustrated in Figure 10. Such a scenario could arise if the consumer was suspected of data reselling, against the terms of the agreement with a provider. Proof of data reselling would be achieved by comparing hash values uploaded to the chain as part of a data offer. Such a case would require the intervention of the dispute board and may lead to legal action.

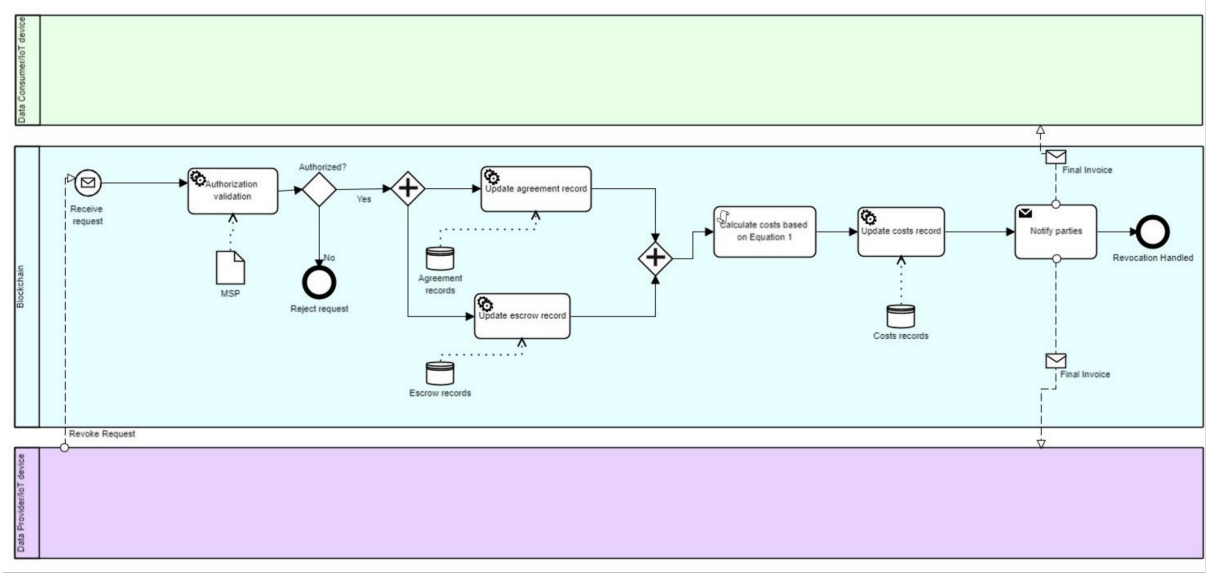

Figure 10: Revoking an agreement from the provider side.

8. Management of Data in Real Time

Rail assets have long service lives and are typically slow to fail, meaning that in many cases even monitoring data does not necessarily need to be exchanged between actors in real or near real time. In many cases, time delays of a few minutes or even hours will often not make a huge difference to the operational decision-making process, as remedial work can only be carried out when vehicles return to depots, or, in the case of major infrastructure work, at specific times of the day when the route is quiet. Despite this, as the rail industry adopts an increasingly data-driven approach to planning, true real-time applications of monitoring data are being identified and it is interesting to consider how these might fit within the proposed framework.

When considering the addition of small, dynamic interactions between data producers and consumers there are three key elements of the framework that would need to be considered: first, arrangements would need to be in place for devices / services to be able to initialise new data exchanges independently of any human supervision, secondly, automation would need to be in place to manage quality / proof of receipt checking such that transactions could be completed, and finally, consideration would need to be given to the impact of large numbers of small transactions on the blockchain itself, including factors such as the computational load of the hashing operations, potential delays to logging of transactions, and the impacts of grouping transactions together within blocks on validity checks. These are briefly commented on below.

Authority to Initiate Agreements

By far the largest hurdle to the management of dynamic data agreements within the framework as it currently stands, lies with the commercial “authority” to act in the name of a particular industry stakeholder. By establishing a new data exchange agreement, even if the expected payment is to be very small, monitoring devices would essentially be acting with the financial authority of their owner/operator companies, but not under the direct supervision of an employee of that company. This would certainly raise interesting legal questions in the event of a problem. As seen from the literature introduced in Section 3, a number of attempts have already been made in the literature to address this type of issue; Iftekhar et al [31] made use of lists of pre-authorised devices, which would at least allow companies some degree of control of which devices and services can initiate transactions on their behalf, and adoption of a policy of this type would allow this type of transaction to be managed within the B4CM framework as currently proposed.

Resolution of Conflicts

In the Escrow based framework being developed by the project team, the risk of delivery of data different to that which was being purchased can be managed by validating the hash of the delivered data against the hash associated with the offer. In several of the other Scenarios however, some element of human intervention is involved in the conflict resolution process, and that is infeasible in situations where large numbers of small transactions are taking place. Furthermore, the protection offered by the data hashes on small payloads is much reduced, meaning that, in practice additional measures would need to be in place to manage conflicts with data exchanges at this scale.

The inclusion of automated data validation checks to the framework would go some way to resolving this issue, and a range of commercial tools are available to assist with precisely this problem. As a starting point for asset data at scale for example, it would be sensible to look for distributions of the data that matched historical norms for the asset type in question, although of course that assumption fails where assets in non-standard failure modes are considered. Regardless of the technical solution employed, should truly dynamic access to the framework for short periods be required as part of an industry use case, some kind of automated validity checking would be required in order to trigger resolutions as appropriate.

Performance Implications

It has been shown in the literature [35], that in configurations with larger blocksizes overall transaction latency increases with higher arrival rates. If you assume that dynamic data delivery from IoT type devices will be at high rates (due to the need to capture high resolution asset data for current waveforms etc.) and from large numbers of devices, then it follows that the arrival rate at the blockchain would indeed be higher on average than in more static use cases (as envisaged in the current framework).

This is certainly an issue that would need to be address in commercial implementations of the framework, and would traditionally involve some buffering of data at the sending device in order to bundle information into fewer, larger payloads (traditionally what the industry would do with waveforms represeneting the current through a point machine motor for example, where the whole swing is transmitted having been gathered and down sampled at the machine, rather than individual datapoints being transmitted in their raw form). Depending on the application area, this might be a suitable compromise, but the sacrifice of timely data in favour of ease of technological implementation is a difficult question, and further work in this area would be needed to develop the currently framework further towards that particular usage scenario.

9. Conclusions

RCM is a critical technology in the evolution of the smart railway, enabling improved reliability at reduced cost. As sensors attached to fixed and mobile assets are increasingly used to inform the operational decision making of the industry, it is becoming critical that the business processes that distribute the costs and benefits of such systems across stakeholders within the industry are aligned in a way that is fair to all parties. The ability to trade in RCM data offers a net market advantage to the industry, as this enables easy access to data by any party that believes they have a use case, whilst also ensuring data providers are adequately reimbursed.

Traditional approaches to the management of costs associated with cross-stakeholder RCM deployments in rail have relied on specific business-to-business commercial agreements and predefined costs. These lack the flexibility required to fully exploit the data generated in the "big data" age, where automated model development often requires access to a wide range of data resources from across an industry. Furthermore, the specific use cases being investigated are unlikely to have been foreseen at the time the RCM systems were procured, meaning the initial agreements would need to be modified to support new usage scenarios, an expensive and time-consuming process. Some legacy collaboration arrangements are not wholly defined or explicit and are thus open to misinterpretation or may not be enforceable.

The B4CM project aims to provide the rail industry with an alternative to the traditional model for attribution of RCM costs. This paper has introduced a new architecture based on blockchain technology which ensures the rights to data are allocated to the data provider as long as they supply the blockchain network with evidential hash values. The architecture simplifies the mechanism for coordination between a data provider and data users, while also allowing automation of the underlying business agreements and cost distribution. A service quality agreement between provider and consumer is established enabling both actors to prove some violating behaviours; for example, a consumer may claim low service quality, prove their claim, and be paid for; otherwise, for making dishonest claims, the consumer would be fined. Fundamentally, the proposed system allows all stakeholders to contribute, and realise revenue from, their data while enabling cross-industry use cases that are currently not easily realised.

References

[1] C. P. Ward et al, “Condition monitoring opportunities using vehicle-based sensors,” Proceedings of the Institution of Mechanical Engineers. Part F, Journal of Rail and Rapid Transit, vol. 225, (2), pp. 202-218, 2011.

[2] A. Alemi, F. Corman, and G. Lodewijks, “Condition monitoring approaches for the detection of railway wheel defects,” Proceedings of the Institution of Mechanical Engineers. Part F, Journal of Rail and Rapid Transit, vol. 231, (8), pp. 961-981, 2017.

[3] Sparkrail, Cross-industry remote condition monitoring (T1010). [Online]. Available: http://www.sparkrail.org/Lists/Records/DispForm.aspx? ID=8096.

[4] G. J. Tucker and A. Hall, “Breaking down the barriers to more cross-industry Remote Condition Monitoring (RCM),” in 6th IET Conference on Railway Condition Monitoring (RCM 2014), Birmingham, UK, September 2014, pp. 1-6.

[5] Sparkrail, Cross-industry remote condition monitoring, Commercial, Final report Appendix E Standard Form (Template) (T1010 Report Appendix).

[6] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain technology: Beyond bitcoin,” Applied Innovation, vol. 2, pp. 6-10, 2016.

[7] M. Friedlmaier, A. Tumasjan, and I. M. Welpe, “Disrupting industries with blockchain: The industry, venture capital funding, and regional distribution of blockchain ventures,” in Proceedings of the 51st Hawaii International Conference on System Sciences, 2016.

[8] M. Risius and K. Spohrer, “A blockchain research framework,” Business & Information Systems Engineering, vol. 59, (6), pp. 385-409, 2017.

[9] B. Biswas and R. Gupta, “Analysis of barriers to implement blockchain in industry and service sectors,” Computers & Industrial Engineering, vol. 136, pp. 225-241, 2019.

[10] P. Mcmahon, T. Zhang, and R. Dwight, “Requirements for big data adoption for railway asset management," IEEE Access, vol. 8, pp. 15543-15564, 2020.

[11] D. Galar, D. Seneviratne, and U. Kumar, “Big data in railway O&M: A dependability approach,” in S. Kohli, A. V. Senthil Kumar, J. M. Easton, and C. Roberts (Eds.), Innovative applications of big data in the railway industry. IGI Global, Hershey, PA, pp. 1-26, 2017.

[12] J. M. Easton. “Blockchains: A distributed data ledger for the rail industry,” in S. Kohli, A. V. Senthil Kumar, J. M. Easton, and C. Roberts (Eds.), Innovative applications of big data in the railway industry. IGI Global, Hershey, PA, pp. 27-39, 2017.

[13] Q. Y. Li et al, “Chapter 14 - Smart railway based on the Internet of Things,” in H.-H. Hsu, C.-Y. Chang, and C.-H. Hsu (Eds.), Big data analytics for sensor-network collected intelligence. Elsevier Inc., pp. 280-297, 2017.

[14] ISO13374-2: “Condition monitoring and diagnostics of machines – Data processing, communication and presentation – Part 2: Data processing”, 2007.

[15] M. Alharby, A. Aldweesh, and A. V. Moorsel, “Blockchain-based smart contracts: A systematic mapping study of academic research,” in International Conference on Cloud Computing, Big Data and Blockchain (ICCBB), Fuzhou, China, 2018, pp. 1-6.

[16] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292-2303, 2016.

[17] S. Nayak, N. C. Narendra, A. Shukla, and J. Kempf, “Saranyu: Using smart contracts and blockchain for cloud tenant management,” in 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2018, pp. 857-861.

[18] F. A. Al-Zahrani, “Subscription-based data-sharing model using blockchain and data as a service,” IEEE Access, vol. 8, pp. 115966-115981, 2020.

[19] A. Suliman, Z. Husain, M. Abououf, M. Alblooshi, and K. Salah, “Monetization of IoT data using smart contracts,” IET Networks, vol. 8, pp. 32-37, January 2019.

[20] Bit-Bay, Double deposit escrow. [Online]. Available: https://bitbay.market/double-deposit-escrow

[21] D. Zimbeck, Two party double deposit trustless escrow in cryptographic networks and bitcoin. [Online], 2014. Available: https://bithalo.org/whitepaper_twosided.pdf

[22] G. Bigi, A. Bracciali, G. Meacci, and E. Tuosto, “Validation of decentralised smart contracts through game theory and formal methods,” in C. Bodei, G. Ferrari, and C. Priami (Eds.), Programming languages with applications to biology and security. Springer, pp. 142-161, 2015.

[23] A. Asgaonkar and B. Krishnamachari, “Solving the buyer and seller’s dilemma: A dual-deposit escrow smart contract for provably cheat-proof delivery and payment for a digital good without a trusted mediator,” in 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea (South), 2019, pp. 262-267.

[24] H. Desai, K. Liu, M. Kantarcioglu, and L. Kagal, “Adjudicating violations in data sharing agreements using smart contracts,” in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 1553-1560.

[25] R. K. Aggarwal, A. T. Johns, J. A. S. B. Jayasinghe, and W. Su, “An overview of the condition monitoring of overhead lines,” Electr. Power Syst. Res., vol. 53, no. 1, pp. 15-22, Jan. 2000, doi: 10.1016/S0378-7796(99)00037-1.

[26] E. Karakose, M. T. Gencoglu, M. Karakose, I. Aydin, and E. Akin, “A New Experimental Approach Using Image Processing-Based Tracking for an Efficient Fault Diagnosis in Pantograph-Catenary Systems,” IEEE Trans. Ind. Inform., vol. 13, no. 2, pp. 635-643, Apr. 2017, doi: 10.1109/TII.2016.2628042.

[27] “Cross-industry remote condition monitoring and data sharing - a templated approach to commercial implementation.” Mar. 2015. [Online]. Available: http://www.sparkrail.org/Lists/Records/DispForm.aspx? ID=22276

[28] A. Amini, M. Entezami, Z. Huang, H. Rowshandel, and M. Papaelias, “Wayside detection of faults in railway axle bearings using time spectral kurtosis analysis on high-frequency acoustic emission signals,” Adv. Mech. Eng., vol. 8, no. 11, p.1687814016676000, Nov. 2016, doi: 10.1177/1687814016676000.

[29] “RailBAM | Bearing Acoustic Monitor.” https://www.trackiq.net/RailBAM.html (accessed Jul. 28, 2021).

[30] C. Kessell, “Bearing Up for Reliability - Rail Engineer.” https://www.railengineer.co.uk/bearing-up-for-reliability/ (accessed Jul. 28, 2021).

[31] A. Iftekhar, X. Cui, Q. Tao, and C. Zheng, “Hyperledger Fabric Access Control System for Internet of Things Layer in Blockchain-Based Applications,” *Entropy*, vol. 23, no. 8, Art. no. 8, Aug. 2021, doi: 10.3390/e23081054.

[32] G. D. Putra, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, “Trust Management in Decentralized IoT Access Control System,” *arXiv:1912.10247 [cs]*, Mar. 2020, Accessed: Nov. 05, 2021. [Online]. Available: http://arxiv.org/abs/1912.10247

[33] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, “Smart Contract-Based Access Control for the Internet of Things,” *arXiv:1802.04410 [cs]*, Feb. 2018, Accessed: Nov. 04, 2021. [Online]. Available: http://arxiv.org/abs/1802.04410

[34] H. T. T. Truong, M. Almeida, G. Karame, and C. Soriente, “Towards Secure and Decentralized Sharing of IoT Data,” in *2019 IEEE International Conference on Blockchain (Blockchain)*, Jul. 2019, pp. 176–183. doi: 10.1109/Blockchain.2019.00031.

[35] X. Xu, G. Sun, L. Luo, H. Cao, H. Yu and A. V. Vasilakos, “Latency performance modeling and analysis for hyperledger fabric blockchain network,” Information Processing & Management, vol. 58, no. 1, Jan. 2021, doi: 10.1016/j.ipm.2020.102436.