IN2DREAMS

Contract No. 777596

INtelligent solutions 2ward the Development of Railway Energy and Asset Management Systems in Europe

D4.1 The Data Transactions model in railways ecosystems

DUE DATE OF DELIVERABLE: 28/02/2018

ACTUAL SUBMISSION DATE: 14/03/2018

Leader/Responsible of this Deliverable: CEFRIEL
Reviewed: Y

Document status		
Revision	Date	Description
0.1	22/12/2017	ToC and first draft contributes on DLTs
0.2	11/01/2018	Received comments and revisions by T4.1 partners
0.3	30/01/2018	Added a revised version of the AS-IS and scenario analysis
0.4	01/02/2018	Added an introduction to legal aspects of DLT
0.5	02/02/2018	Received comments and revisions on AS-IS and scenario analysis
0.9	05/02/2018	Draft ready for peer review
1	19/02/2018	Addressed comments from TMT
2	14/03/2018	Final version after TMT approval and Quality Check

Project funded from the European Union's Horizon 2020 research and innovation programme		
Dissemination Level		
PU	Public	X
CO	Confidential, restricted under conditions set out in Model Grant Agreement	
CI	Classified, information as referred to in Commission Decision 2001/844/EC	

Start date of project: 01/09/2017 Duration: 24 Months

Executive Summary

Task 4.1 is focused on the analysis of the activities and currently employs workflows related to the railway assets management, with the goal of identifying the most promising ones that can greatly benefits from the adoption of Distributed Ledger Technologies (DLTs).

DLTs are becoming an interesting alternative to traditional information systems nowadays, even if they are not yet fully mature, because of their nature of decentralised systems where no single user has full control on all the information. The key features of DLTs indeed are:

- Immutability of the recorded data
- Governance is decentralised, reaching the point of “public governance” (each node count as one) in case of public DLT systems
- No central infrastructure needed
- Complete transparency of the system

These key aspects make DLTs suitable to use in ecosystems where participants do not fully trust each other. A DLT would indeed act as the technological base of a transparent and tamper-proof information system, that could be audited by each participant giving them the assurance that everything is working as expected. Moreover, a DLT system could implement “programmable logics” called “smart contracts”, to automatise the execution of workflows and transactions while keeping all the key features listed previously.

However, not all the scenarios and use cases are suitable for the employment of a DLT. Some requirements, explained better in the Chapter 2, must be satisfied to speculate that a DLT would be beneficial to a selected use case. To summarise, it is important that a selected use case presents multiple actors that do not fully trust each other.

Analysing the *As-Is* of asset management in the railway ecosystem (Chapter 3), four use cases have been identified:

- Asset Maintenance
- Public Procurement
- Data Monetisation
- Train Path Allocation

Each of them has been analysed (Chapter 5) to better identify what would be the benefits and drawbacks related to the employment of a DLT in their specific case, also considering some preliminary legal considerations on the employment of DLTs and Smart Contracts (Chapter4)

RFI, an Infrastructure Manager (IM), being the main actor in the railways ecosystem, weighted the pros and cons of each use case and decided that the Asset Maintenance one is the most promising at this time (Chapter 6). In the following tasks of WP4, a working prototype will be developed and deployed in the asset maintenance scenario.

Abbreviations and Acronyms

Abbreviation	Description
EU	European Union
GA	Grant Agreement
H2020	Horizon 2020 framework programme
JU	Shift2Rail Joint Undertaking
DLT	Distributed Ledger Technology
IM	Infrastructure Manager
RU	Railway Undertaking
RNE	RailNetEurope

TABLE OF CONTENTS

List of Figures

List of Tables

1 Introduction

The present document is the output of Task 4.1.

T4.1 had to deal with the identification and definition of data exchange scenarios in the railways asset management and related use cases, selecting the most suitable one that will be used to drive the requirements of the whole blockchain and smart contract architecture (the development of which will be the goal of the following tasks of WP4). The scope of this task is the broadest and as general as possible, taking into account currently existing processes and data exchange scenarios between the different parties involved, but also trying to include future scenarios derived by vision and future directions of the whole ecosystem. To accomplish this task at the widest level possible, T4.1 acted in collaboration with other Shift2RAIL relevant recipients (IN2RAIL, In2SMART and In2STEMPO).

This document's objectives are:

- To identify the advantages and benefits of DLT/smart contracts for operational efficiency, processes and relationship management of actors involved in the data exchange;
- To define the specific business scenarios for railways ecosystem, emerging as relevant for the application of DLT and smart contracts.

To achieve them, the document follows a structure that aims at explaining to the reader firstly what a blockchain and its related technologies are, and what are the relevant processes inside the railways assets management.

After a brief background overview, Chapter 2 explains at a high level the technological nature of blockchains and Distributed Ledger Technologies (DLTs), listing and justifying the possible benefits that could derive from their use.

The Chapter 3 will define the railways asset management procedures with relative actors and their roles.

Chapter 4 introduces the topic of what legal consequences could have the application of blockchain and smart contracts inside the railways ecosystem (topic that will be deeply covered in Task and reported in D)

Finally, in Chapter 5 the identified use cases are described, explicating how the employment of a blockchain may bring benefits to them.

The main results of this deliverable are: the identification of a set of use cases of potential interest for the application of DLTs to the asset management in the railways ecosystem; and the selection of the use case for the pilot implementation.

Regarding this last output, it is important to note that the final selection of the use case has been performed by RFI (the Infrastructure Manager or IM) according to its internal business requirements.

1.1 Background

Distributed ledger and blockchain technology are rising as one of the most interesting field of research and application in the field of Computer Science. They are recognised to have the potential to bring the “paradigm” of “trust” for the Web, since their promise to cut off the “central authority” with a decentralised distributed ledger [1].

This means in theory that in an ecosystem of many actors, that even do not know or trust each other, there is no need any more for a central “authority” for exchanging “value” like money or assets properties. Moreover, the fact that there is not a central authority, leads the “ecosystem” to be more resilient to potential security attacks, since it is really inconvenient to “tamper” the ledger. Finally, the cost for maintaining the “ecosystem” is spread among all nodes.

The potential applications are in almost any field of human activities, from private to public, from industrial application to government, touching any kind of digital aspects of life. There are great expectations on their potential to improve the efficiency, sustainability and automation of complex ecosystems like railways. Nevertheless, there is presently a total lack for standards and the technology is still immature. The maturity is not expected to be reached before 10 years [1] . Some of the most interesting fields of enterprise applications are transport and supply chain. Since blockchain approaches have a strong impact on relationship and management of the system, the technology maturity should be accompanied also with advances and clarification in regulations and norms, especially about the compliances and liability.

In the following paragraphs the main aspects of DLT will be recalled, and the basics definitions of elements, such as distributed ledger, blockchain, private and public blockchain, and smart contracts, will be given in order to have a common reference for the scope of In2DREAMS. An exhaustive study material can be retrieved in references [2] [3] [4].

2 Distributed Ledger Technology/Blockchain Landscape

2.1 Overview

The distributed ledger technology landscape is composed by two families, i) the "public" one, like Bitcoin, used when there is no permission required to take part to the network or ii) the "private" one when such a permission is required. DLT main feature is to be able to cut off third parties in the exchange of trusted data or assets. Moreover, if combined with smart contracts they can also execute logics in a distributed rather than centralised way, giving to all the participants the possibility to audit the logic executions, making its manipulation virtually impossible.

2.2 Blockchain and DLT

In Figure 1 the distinctions between the two families of DLT is shown, together with examples of real implementations.

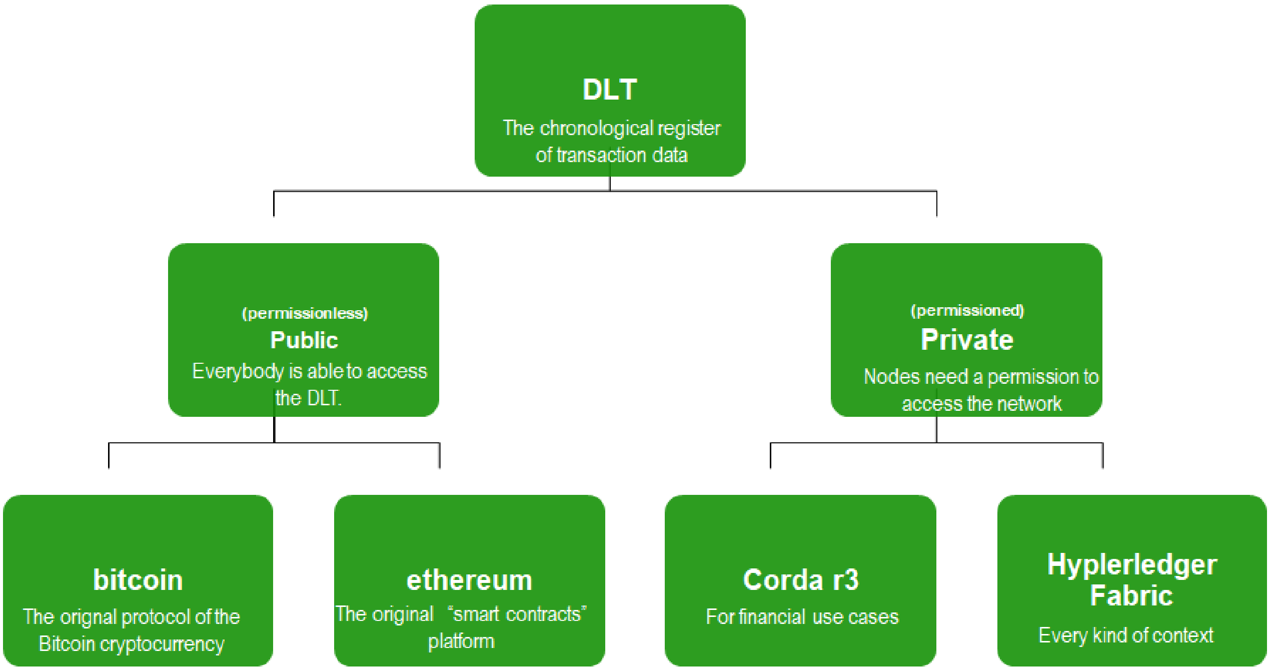

DLT
The chronological register of transaction data
(permissionless)
Public
Everybody is able to access the DLT.
(permissioned)
Private
Nodes need a permission to access the network
bitcoin
The orignal protocol of the Bitcoin cryptocurrency
ethereum
The original "smart contracts" platform
Corda r3
For financial use cases
Hyplerledger Fabric
Every kind of context

Figure 1: This figure shows a possible classification of DLT and some examples

The term blockchain refers to the linked chain of all the transactions that happened since that particular blockchain system is up and running. It can be seen as a kind of database.

In the first examples of blockchain based systems, this database is a chronologically ordered chain of blocks in which each block is back-linked to the previous one. Blocks are data structures that contain a certain number of verified transactions. It maintains a continuously growing list of transaction data records, cryptographically secured from tampering:

- Transactions have to be validated by the nodes to be included in the "block", the validation time is the timestamp;

- On public blockchain systems, the database is replicated and maintained synchronised by design on each full node of a network where all nodes are equal. Each full node thus have an identical copy of the same ledger; on private blockchain systems instead not all the network nodes have a copy of the ledger to preserve confidentiality, still ensuring that the database is replicated on more than a node;
- The database is immutable since once the block is written, it is not possible to modify it;
- The database can be inspected by all peers in the network;
- The rules for approving and maintaining the ledger may differ. The “consensus layer” defines the rulesets of a specific blockchain protocol, thus impacting the main features of a blockchain.

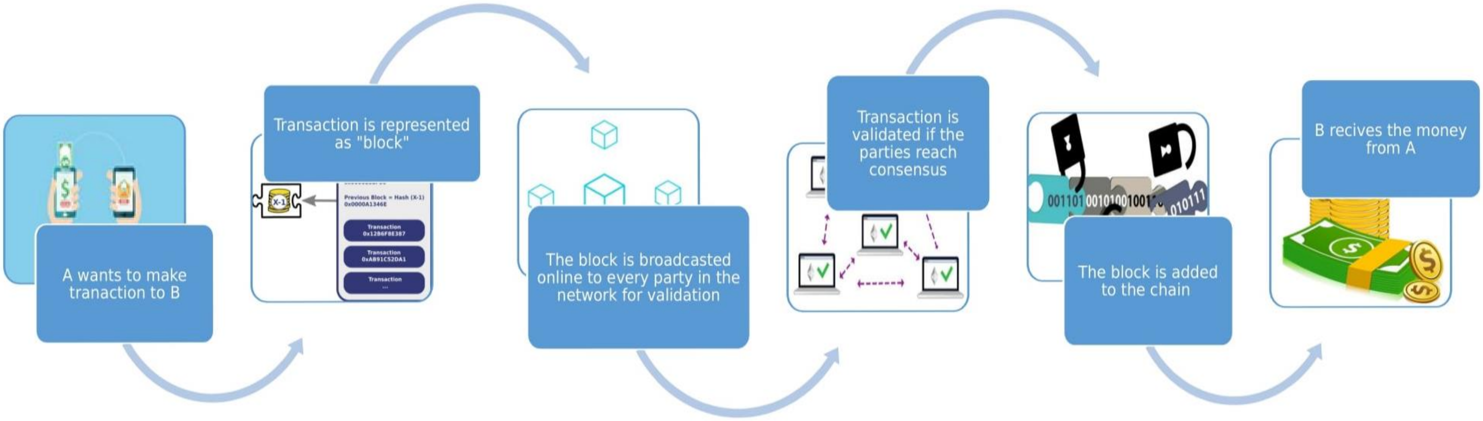

A wants to make tranaction to B
Transaction is represented as "block"
The block is broadcasted online to every party in the network for validation
Transaction is validated if the parties reach consensus
The block is added to the chain
B recives the money from A

Figure 2: Steps involved in transaction validation

Comparing traditional databases, based on RDBMS, with distributed ledgers, it is possible to spot some keys differences listed in the following table:

RDBMS	DLT
Storage of data in central database	Storage of data in multiple instances; replicated across a network of peers
Single point of failure	Maintenance is synchronised in the multiple instances
Based on authentication, authorisation and auditing; no guarantee of tampering resistance.	A consensus mechanism is needed to guarantee fault tolerance; system cryptographically secured from tampering
The data is stored in collection of tables	The data are stored in a chronological manner as a growing append-only list in which each element points to the previous one.

Table 1: Differences between RDMS and DLT

The key benefits of DLTs are:

- To achieve tamperproof and trust between participants;
- Resilience to system failures;
- To have multiple copies kept synchronised “by design” by the blockchain protocol;
- To have a Consensus mechanism that replaces third parties and solves the Byzantine problem [3].

There are different consensus algorithms with distinct characteristics; in every one of them every peer has to process the transactions, to verify that transactions are valid according to some established criteria and to assess the validity of blocks containing the transactions.

The consensus algorithm is a key component of a blockchain/DLT network. It sets the rules and the incentive schemes that allow reaching consistency between copies of the blockchain held by every participating node. There are algorithms based on the selection of a random leader that assembles blocks and validating peers that digitally sign it; other algorithms, like *proof of work,* require computational power to solve a cryptographic puzzle in order to commit transactions to a valid block.

2.3 Smart Contracts

The first preliminary ideas, that later evolved in the Smart contracts concept, originated in late '90s, when blockchains did not exist yet. It was only with their debut that the first working implementation of a Smart Contract based systemin 2015 - the Ethereum project – was visible. The idea behind smart contract is the decoupling of the contract layer from the blockchain layer, where the ledger itself is used by smart contracts to automatically trigger transactions when certain pre-defined conditions are met.

By decoupling the smart contract layer from the blockchain layer, blockchains like Ethereum aim at providing a more flexible development environment than the Bitcoin blockchain.

These smart contracts are not "legal contracts ". They may have properties of contractual agreements, in case they technologically implement commercial agreements, but should not be confused with legal contracts. They are pieces of code running on top of a blockchain network, able to execute "***if-then-else logics***" to enable the execution of "rules" (that may be derived from legal contracts obligations) to exchange digital assets. (An introduction to this topic is presented in Chapter 4).

If and when the conditions pre-defined in the smart contract are fulfilled, the smart contract will auto execute a transaction according to the defined arbitrary rules. Smart contracts aim at providing a technological way to automatically enforce traditional contract law.

Let’s take a couple of examples to clarify what a smart contract is and how it works: a Smart contract could be used to execute the term of a purchase contract between a supplier and a buyer to regulate the procedures for the execution of the contract. The smart contract may contain a formal rule like “If buyer receives product X by Time Y, then pay supplier 1000 OR if the product is not on time, then pay 800”. The formal rules may easily represent the fees and the penalties of a contract.

Another example is a smart contract that allows to use the DLT as an ownership register: The smart contract acts like a notary that in one direction register the "ownership" into the DLT and on the other way allows anybody, in case of public blockchain, to read the DLT and check if such an ownership exists.

The smart contract can be also programmed with a formal rule that the ownership may be transferred by a subject A to B under certain conditions. In this case the smart contract may act as a "notary".

Furthermore, smart contracts can be used for more complex transactions like governing a group of people that share the same interests and goals in a decentralised manner.

With blockchains and smart contracts it is predictable a future in which contracts are embedded in digital code and stored in transparent, shared databases, where they are protected from deletion and tampering.

In an ideal implementation, smart contracts would have the following features (at the current maturity level of the existing implementations not all of these desiderata are completely met):

- **Speed**– smart contracts are basically software code to automate tasks while standard contracts are time-consuming and costly
- **Safety**- at least in theory its practically impossible to hack the smart contract. Encryption keeps the documents safe
- **Trust**- all of the transactions are encrypted and saved on the ledger, the possibility of losing data is impossible
- **Autonomy**- there is no intermediaries to confirm or to rely on them, user can make his own contract since execution is managed automatically by the network
- **Savings**- smart contracts can save money since the intermediaries are eliminated by design.

2.4 Public Blockchain

In a public blockchain network, the blockchain is a trusted and public ledger of transactions, that everyone can audit but no single user controls. Everyone can join the network at any time and participate to consensus without authorisation. The algorithms and mechanisms at the base of a public blockchain network can be seen as a whole as a protocol that operates on top of the Internet, like the HTTP or the E-Mail.

The network typically has an incentive scheme to encourage more participants to join it. Nowadays, Bitcoin is the largest among public blockchain networks. It was designed to securely cut out the third parties in any exchange of asset scenario. It is a peer-to-peer network where nodes communicate exchanging messages in the form of transactions and blocks. Each transaction is verified and synced with every node that maintains a local copy of the blockchain. every single node updates it with the messages received by its peers that are independently validated [4].

Unless this has occurred, the next transaction cannot move forward. Anyone with a computer and internet connection can set up a node and synchronise the entire blockchain history by downloading it and verifying it independently. While this redundancy makes public blockchain virtually impossible to control by single entities, it also makes it slow and wasteful.

As it is decentralised and relies on cryptographic proofs for value transfer, a public blockchain is also very hard to hack: in such a system a hacker should be faster than the whole network and overtake the network hashrate, thus making a hacking extremely expensive if not impossible to achieve, considering also that the value of hacked coins could drop to zero if a hack is discovered.

One of the drawbacks of a public blockchain is the substantial amount of computational power that is necessary to maintain a distributed ledger at a large scale; this is due to the proof-of-work consensus algorithm, the most used within the public blockchains projects. Within this consensus algorithm, each network node is competing with each other for building the next block of the blockchain: a really complex and resource intensive cryptographic problem must be solved to link the block created by the node to the blockchain. The first node that is able to solve the problem sends the newly created block to its peers for their verification. Each peer, once has correctly verified the block, adds it to its local copy of the blockchain, thus spreading the knowledge of the new block to all the network. The process of block creation, in a proof-of-work based blockchain, is very time and resource intensive; and this has two consequences: the confirmation time of the single transaction is not instantaneous and is directly correlated to the whole number of pending transactions in the network; and the user has to pay a fee to remunerate the nodes work. The fee amount is related to the number of pending transactions in the network and the block size: since block space is limited, users that are willing to pay higher fees can obtain a faster confirmation (i.e. in the following block).

Another disadvantage, present in some of the public blockchains available, is the openness of public blockchain, which implies no privacy for transactions even if it is difficult to correlate a transaction to a real person. This issue, present in Bitcoin and Ethereum and many others, has been addressed in other public blockchains thanks to different cryptographic protocols focused on privacy (e.g. zero knowledge proofs).

2.4.1 Proof-Of-Work and Proof-Of-Stake for the public blockchains

Proof-of-Work (PoW) is one of the most used consensus algorithms in public blockchains (e.g. Bitcoin) to verify and write transactions on the blockchain.

In order to agree on a certain state of the blockchain, consensus needs to be established by applying a predefined set of rules that all honest nodes will enforce on their own ledger replica. In the context of PoW based blockchains, mining is another name for the process of finding blocks of transactions that are compliant with the consensus rules and contain a valid PoW. In simple terms, finding a valid PoW means giving a cryptographic proof that to find a certain block parameter, usually the block header cryptographic hash, a great amount of resources have been consumed.

Each node, also called miner, needs to provide a proof that he solved this specific cryptographic puzzle in order to add a block to the blockchain [3] . Each time the challenge is solved a new block is added to the blockchain and the node (or miner) who solved it is rewarded with some cryptocurrency units. This proof is very difficult to produce but it is very easy to validate thus this make the blockchain network hard to manipulate. The required cryptographic proof is time and resource consuming, and this ensures that no maliciously crafted transactions are added to the blockchain since the malicious node would have to compete and beat the entire computational power of the rest of the network to be the one who solves the puzzle first.

Proof-of-Stake (PoS) [5] is another consensus algorithm that works differently from PoW trying to address its issues. In this algorithm, validators take turns by proposing and voting on the next block where the importance of the validators vote depends on the stake he has in the network in terms of cryptocurrency units. PoS is surely less time and resource consuming than PoW but is more susceptible to manipulations by validators which owns the majority of the crypto tokens of the network.

2.5 Private Blockchain

When the DLT is accessible only under permission, it may be called "private blockchain network". The main aspects of private blockchains regard the governance of the network and the sustainability model due to the lack of native cryptocurrency; only public blockchains are capable of govern and economically support themselves thanks to the incentive schemes consisting in crypto tokens rewards.

To take part in the network, an actor requires an invitation and must be validated either by the network starter or by a set of rules put in place by the network starter. The private blockchain is the way through which private organisations are trying to respond to compelling questions about blockchains. From the point of view of a private organisation, indeed, there are some needs that a public blockchain cannot satisfy for its intrinsic nature.

- The ledger cannot be public since it might contain data relevant for the business that cannot be shared to other participants;
- The system should be able to work without cryptocurrency as the network does not need to economically support itself since it is backed by a private organisation.
- Network scalability should be possible at an affordable cost
- The time needed for transactions confirmation should be short.

The most representative frameworks for private blockchains are Hyperledger Fabric and R3; the specific technical aspects of the two will be discussed in D4.2.

The main characteristics of private blockchains are:

- Ability to define the governance model;
- Ability to combine the DLT with traditional payment systems;
- Ability to define the consensus mechanism so that to be more scalable in term of timing;
- Ability to guarantee confidentiality of the transactions and also of the smart contracts.

In the following table, a preliminary comparison between the different DLTs technologies, both public and private, is provided. A deeper comparison between selected DLTs, with the goal of selected the one that will be used for the prototype implementation, will be the focus of T4.2.

	Open Source	Currency	Public	Description of platform	Consensus	Governance	Smart contracts
Ethereum	Yes	-Ether -Tokens via smart contracts	-Yes -(Permission less, public or private)	Generic blockchain platform	-Mining based on proof-of-work(PoW) -Ledger level	Ethereum developers	-Yes -Smart contract code(Solidity)
Hyperledger Fabric	Yes	-None -Possibility for currency and tokens via chain code	-No -Private (Permissioned)	Modular blockchain platform	-Freedom of choose between more types of consensus -Transaction level	Linux Foundation	-Yes -Smart contract code(Go,Java)
R3 Corda	Yes	-None	-No -Private (Permissioned)	Specialised distributed ledger platform for financial industry (and possible broad use)	-Freedom of choose between more types of consensus -Transaction level	R3	-Yes -Smart contract code(Kotlin,Java) -Smart legal contract(legal prose)
Bitcoin	Yes	-Bitcoin	-Yes	Generic blockchain platform	-Mining based on proof-of-work(PoW) -Ledger level	Bitcoin developers	-No
Stellar	Yes	-Lumens	-Yes	Distributed payment infrastructure, micropayments	-Stellar consensus protocol(SCP)	Stellar developers	-Yes

Table 2: Comparison between different blockchain platforms and their characteristics

2.6 Guidelines for adoption of DLT Technologies

When a specific use case is chosen, a fundamental question must be answered: Is a a blockchain needed? And in case of a positive answer, is a public or a private blockchain needed?

As already said in the previous sections, blockchains, both public and private, make possible to have a system that is *by design* super partes and in which participants of a digital ecosystem may place their trust.Through it, the blockchainsmake connections with all the other participants without the need of knowing and trust them. This sure advantage already underlines an important aspect that a use case should have: the presence of an ecosystem where different actors participate.

Making sure that indeed an ecosystem is present, it is then possible to appreciate what such a family of technology may bring as advantages: a tamper-proof record of all the transactions happening between the ecosystem's participants. Also, here another question arises: is there a member of the ecosystem that everybody can or want to trust? In case of positive answer, should it be considered if a traditional database can actually do the job it is needed, as using a blockchain may actually not bring useful features that it is really needed?

If, after these two questions, the conclusion is that a blockchain might be needed for the chosen use case, it is important to understand if a public blockchain could do the job, or if a private one is better.

The fundamental aspects to analyse here are two: governance and confidentiality. A public blockchain has the advantage to give an already set up and maintained infrastructure that can used with a *pay as you go* policy (the transaction fees, that can be seen as pure OPEX); but this comes at the cost of confidentiality (in same cases) and loss of control over the governance of the network. If it is needed to control who has access to the network and who has or has not the rights to see a specific block written on the blockchain, a private blockchain network (also known as a permissioned blockchain) is needed. This of course means that the infrastructure will have to be built and maintained together by all the participants of the ecosystem, thus increasing the CAPEX.

In Figure 3, what has just been said is described in a useful flow chart.

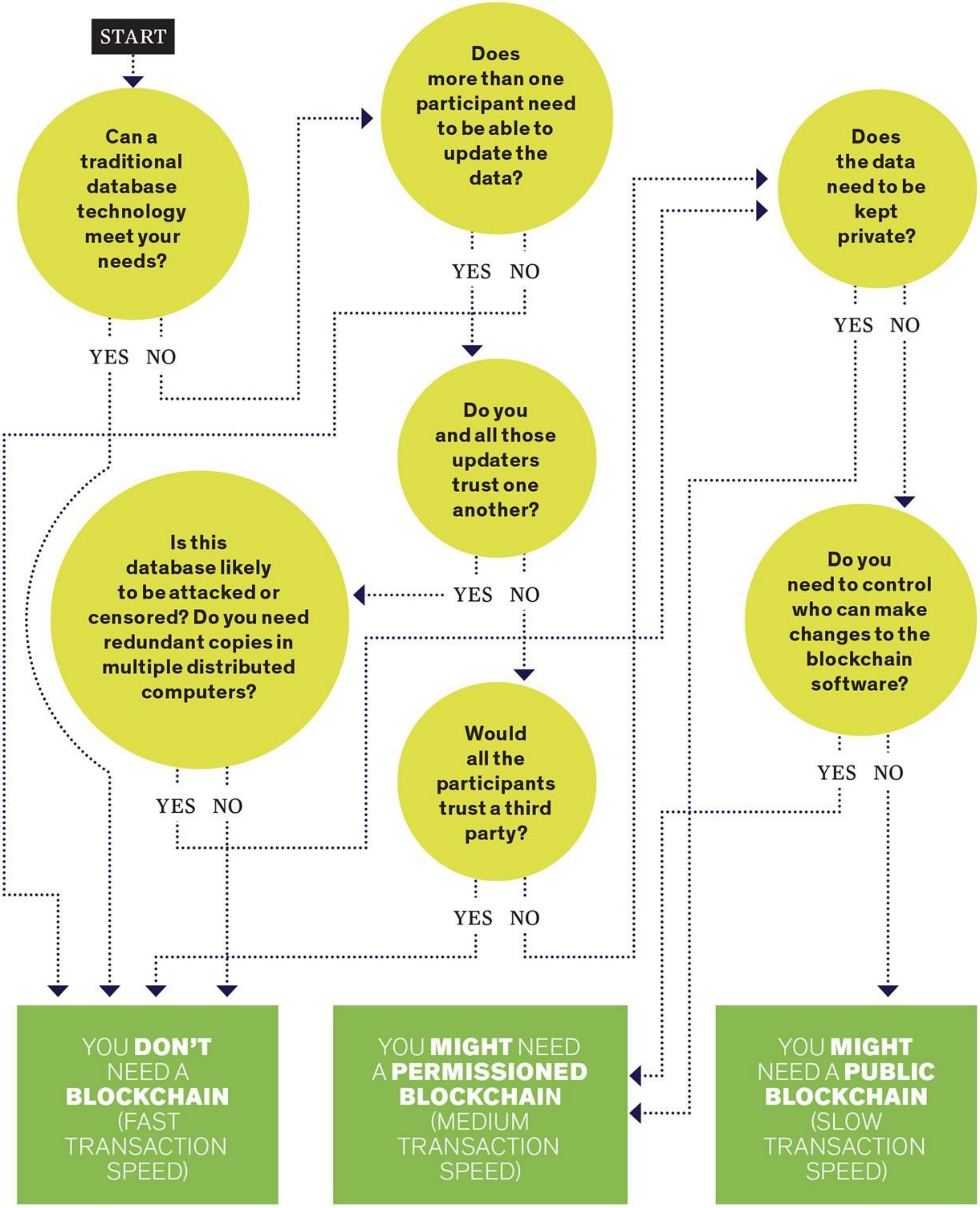

START
Can a traditional database technology meet your needs?
YES
NO
Does more than one participant need to be able to update the data?
YES
NO
Do you and all those updaters trust one another?
YES
NO
Is this database likely to be attacked or censored? Do you need redundant copies in multiple distributed computers?
YES
NO
Would all the participants trust a third party?
YES
NO
Does the data need to be kept private?
YES
NO
Do you need to control who can make changes to the blockchain software?
YES
NO
YOU DON'T NEED A BLOCKCHAIN (FAST TRANSACTION SPEED)
YOU MIGHT NEED A PERMISSIONED BLOCKCHAIN (MEDIUM TRANSACTION SPEED)
YOU MIGHT NEED A PUBLIC BLOCKCHAIN (SLOW TRANSACTION SPEED)

Figure 3: A simple flowchart to assess if a use case needs a blockchain. *[6]*

3 The Railways Ecosystem Asset Management: *As-Is* analysis

3.1 Overview

To better identify relevant use cases for WP4, it is important to understand the *AS IS* of asset maintenance inside the railways ecosystem. To do so, Cefriel and UNIGE have conducted interviews with RFI employees to better understand the governance and operational processes used in the ecosystem.

Not all what composes the railways ecosystem may be considered in scope with WS2: the overall goal of WS2 is to pave the way towards Intelligent Asset Maintenance, aiming at supporting the deployment, usage and maintenance of railway assets in a more effective and cost-efficient way. Given that, all the components and processes inside the Railways Ecosystem that deal with the integration and automation of the asset management (considering also the relative supply chain) can be considered in scope for WS2. It is important to define that for *asset it is* intended all the physical and non-physical entities that compose the railway infrastructure. So, for example, a train is an asset only if it is considered as an object that is employing a specific line of the infrastructure preventing others to use it; but it is not an asset *per se*, as it is not owned by the Infrastructure Manager (IM) (and its maintenance is not a responsibility of the IM)

In this Chapter an overview of the current operational workflow and the participants involved in the management of railway assets are presented, concluding with a list of derived requirements that the DLTs and Smart contracts use cases should fulfil to be considered for the project. In this perspective, also legal constraints will be taken into consideration thanks to the analysis conducted by KUL regarding legal aspects of the application of smart contracts in the ecosystem.

3.2 Main Roles of the Railways asset management workflows

Even if the Railways ecosystem is composed by a multitude of different actors, talking about the Asset Management, three main actors have been identified:

- The IM, responsible of the physical infrastructure
- The Supplier, that provides assets and services to the IM
- The Maintainer, responsible of the maintenance of a specific physical asset on behalf of the IM

In task 4.1 information have been gathered through interviews with the following actors, each of which maps a specific role of the ones defined:

- RFI (IM)
- Ansaldo STS (Supplier)
- Strukton (Maintainer)

A railway network is managed by a company that has the role of IM (in IN2DREAMS this role is represented by RFI); managing the network means controlling access to the (and usage of) infrastructure, planning and performing maintenance and upgrading railway lines when needed. The IM makes sure that all the maintenance activity does not disrupt network traffic and ensures reliability and safety.

Ansaldo STS is one of the main supplier of RFI; it designs and manufactures the railways components, according to the technical specifications that RFI requires; it also offers services to the IM for the revamping and maintenance of existing structures.

The IM schedules maintenance intervention with the goal of keeping a desired standard of service and to preserve the reliability of the network. These tasks are planned according to some criteria chosen from RFI. Maintenance teams, in coordination with the Traffic Management, take care of the maintenance tasks working with the maintenance contractors. Maintenance can be performed both by the IM or by maintenance subcontractors. The subcontractors are selected by a public tender call.

The installations of new asset that upgrade or extend the railway network follows a different workflow. RFI is in charge of taking investment decisions on the network and takes care of drafting calls for public tender and selecting the companies and professionals that can take part in the calls or can directly see themselves appointed to RFI to supply services or components.

In Figure 4, a simplified representation of the roles within the ecosystem and the links between the various participants is illustrated.

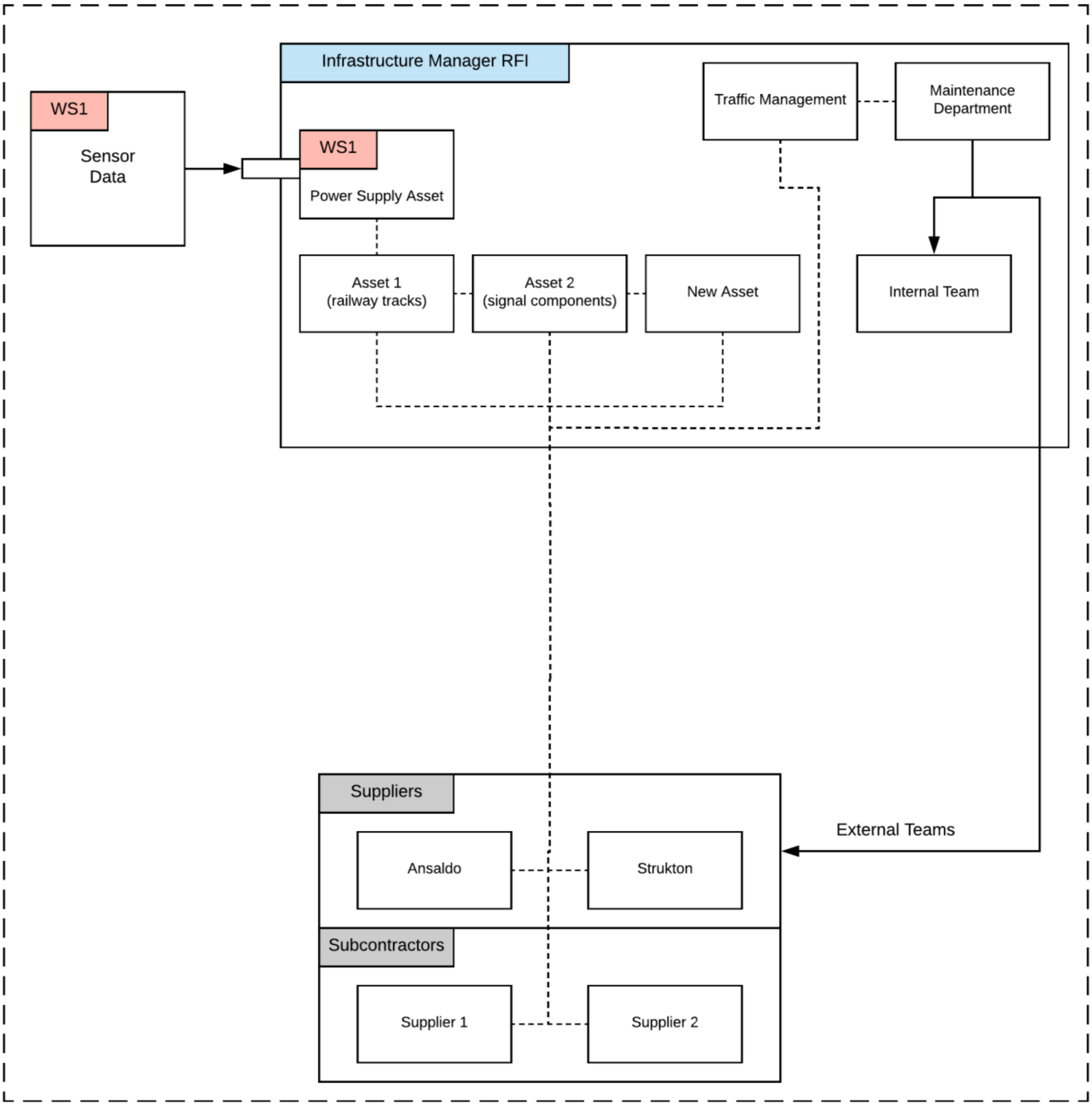


Figure 4: Entities involved in the railways ecosystem asset management

3.3 Asset Maintenance

Maintenance techniques that are currently employed by the IM are based on periodic and extraordinary inspections from specialised teams that evaluate the state of the infrastructure.

Asset maintenance operations can be classified in two categories:

- **Ordinary maintenance**
    - Maintaining the asset integrity and efficiency;
    - Guaranteeing the lifetime of the asset keeping a low wearing rate;

  - Preventing accidental damages or faults;
- **Extraordinary maintenance**
  - Not frequently recurring and not repeatable;
  - High capital cost; usually capitalised since it influences assets values;
  - Aimed at prolonging asset lifespan after it reaches expiration and needs revamping.

In this regard, RFI, Ansaldo STS, and Strukton are the actors that provided useful information and insights on the processes. Ordinary maintenance interventions are carried out due to:

- Activation of maintenance plans (preventive, cyclic or predictive maintenance);
- The need to optimise assets durability over time
- Detection of faults and troubleshooting.

In case of an anomaly on railway assets, RFI personnel is in charge of a first assessment of the problem. After an evaluation on the entity of the damage and the expected impact on traffic, RFI establishes if the problem can be solved internally or, in the case of a contract in place, which is the supplier that has to be notified. In this case, the intervention request is forwarded to the specific asset supplier that will contact its subcontractors to satisfy the request. The process is depicted in Figure 5 .

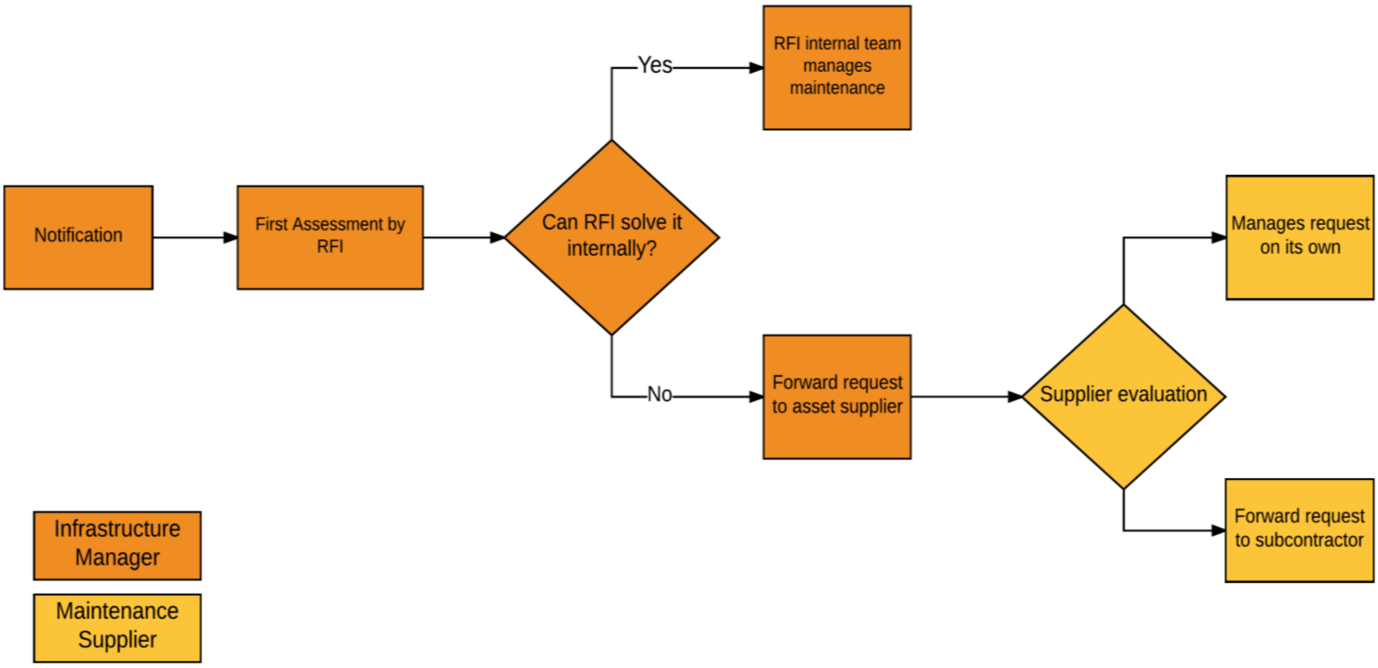

Notification
First Assessment by RFI
Can RFI solve it internally?
Yes
RFI internal team manages maintenance
No
Forward request to asset supplier
Supplier evaluation
Manages request on its own
Forward request to subcontractor
Infrastructure Manager
Maintenance Supplier

Figure 5: Workflow for maintenance due to fault detection

3.4 New Assets Procurement

This section provides an analysis of the criteria and procedures adopted by the Infrastructure Manager to choose its suppliers. The deployment of new assets on the railway network has to respect standards in terms of transparency, fairness and free competition between the qualified actors.

The IM is a company that manages the railway network thanks to a public grant by the railway owner. It takes investment decisions in order to improve the reliability and maintain the efficiency of the network. Suppliers of services in charge of the deployment of new assets cannot be selected arbitrarily but they have to participate to an open public call.

The IM uses two methods to select a supplier of a service:

- **Selection of a supplier through a public tender**: RFI regularly publishes calls for suppliers and service providers on a dedicated web portal. The phases of a public tender are the following:
    - *Definition of the details and requirements for the call;*
    - *Qualified suppliers participate in the tender by making an offer;*
    - *Offers that do not meet formal requirements are rejected;*
    - *Technical Evaluation by RFI;*
    - *Results of the technical and economic evaluation leads to election of a winner.*
- **Selection of a specific supplier**: if there is only a capable supplier for a specific work (e.g. for improving an existing system) RFI can select the specific supplier without a public call. This procedure is not preferred by law and so RFI have to justify it by producing a detailed technical report.

In any case the selection of the suppliers is made using a qualified suppliers list, both in case of Asset Maintenance or New Assets Procurement: RFI uses a procedure called "qualification system" [7] to draft a list of qualified actors and proven professionals in the field; companies and professionals in this list can provide services to RFI in the field they are qualified. There are predefined requirements and processes to be part of a qualification system (proven technical capabilities and expertise, economic and financial strength, production capabilities etc.). RFI selects a qualified supplier that has to draft a proposal for the service to be supplied; RFI will assess if the offer matches with industry benchmarks and consequently accept it or decline it.

The details and requirements of the tender specified by RFI must follow applicable law and notably public procurement law as provided for in EU directive 2014/25/EU[1] and national law.

[1] Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC

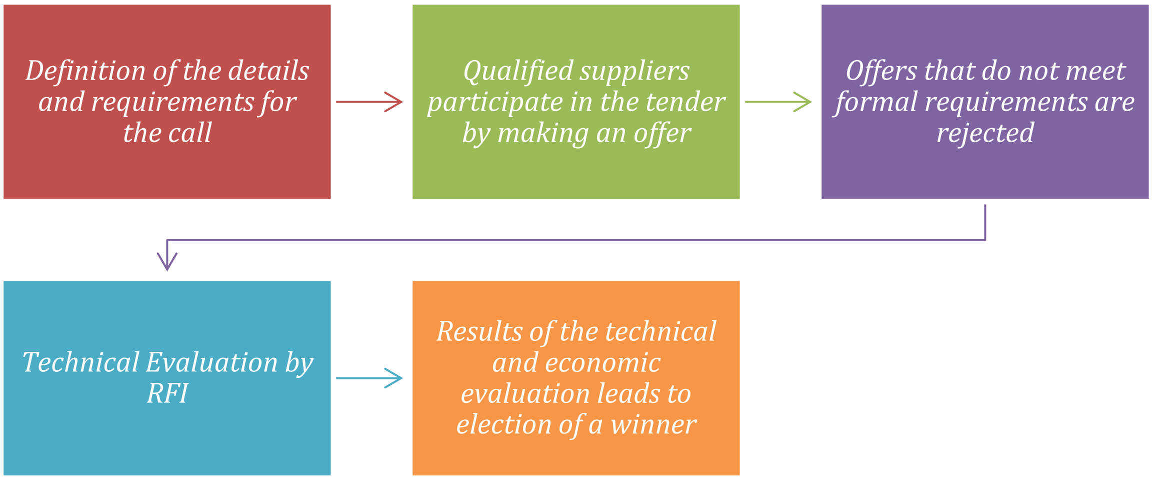

Definition of the details and requirements for the call
Qualified suppliers participate in the tender by making an offer
Offers that do not meet formal requirements are rejected
Technical Evaluation by RFI
Results of the technical and economic evaluation leads to election of a winner

Figure 6 Phases of public procurement (simplified workflow)

3.5 Train path allocation process

A train path is defined as "the infrastructure capacity needed to run a train between two places over a given period[2]". Train paths are the main services offered by the IM to transport companies; the IM drafts the rules and processes for the allocation of railway infrastructure capacity, the requirements that need to be fulfilled to get access to the network and the track access charges connected to its usage.

When a transportation company requests a train path to transport people or goods, it needs to submit an application to the IM; the IM takes care of the allocation of the railway infrastructure capacity respecting principles of transparency, non-discrimination as well as EU and national law regulating access to the railway infrastructure[3].

The main goal of this activity is to reach an optimal allocation of railway capacity, avoiding conflicts and delays.

In the following statements is summarised the capacity allocation process (see [8] paragraph 4):

[2] Article 3, 27° of Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area
[3] Directive 2012/34 (ibidem) and transposing national law.

1) The IM, on an annual basis and consistently with the international agreements on the date of entry into force of the new train timetable in the European states, shall disclose in its institutional website the schedule setting out the deadlines for each of the stages of the process for the allocation of the train path and rail-related services.
2) The RU shall be required to submit its requests for train paths and rail-related services via the RU – IM communications platform called ASTRO-IF for requests relating to the next or applicable working timetable period, or via the PIC WEB portal, in the case of short-notice requests.
3) For International transport service requests the RU may – in accordance with the RNE Agreement (see [8] paragraph 1.10) – present its request through the PCS (Path Coordination System).

Submission of the application for a train path: companies that want to be allocated a train path need to submit an application to the IM; the IM publishes annually, on the institutional website, the deadlines for every step of the application process for train path allocation. [8] The application made by the transportation company contains a series of information on the train and on the desired path such as the followings:

- Destination and route
- Number of wagons
- Physical characteristics of the trains
- Reference average speed
- Description of the material carried
- Timeslots needed and frequency

The path allocation is a quite long iterative process (see [8] paragraph 4.3.1 “Schedule for Capacity Requests for the purpose of the Framework Agreement”) involving different IT systems, IM and RU companies and the respect of specific international rules.

3.6 Requirements and *features* of potential use cases

The Railways Ecosystem has some specific requirements regarding the potential use and adoption of a blockchain framework and smart contracts. It is a quite complex context and the industrial application of blockchain should take into account the regulatory framework.

During the scenarios identification phase, some constraints, derived by the understanding of how the Railways ecosystem works, have been considered. The followings are the *necessary but not sufficient* conditions that a DLT solution in a railways ecosystem *must* satisfy to be employed:

1. Compliance with the European and national regulatory framework;
2. Confidentiality of asset related data;
3. Coexistence of blockchain with traditional payment systems;
4. Sustainability of the proposed architecture in term of operational costs (in respect of the current processes employed)

In addition to these ones, in accordance to the current maturity level of DLTs and the legal responsibilities that an IM has, it is wise to add as a necessary condition that the use cases shall not be affected by specific legal requirements about safety and liability.

Which are, instead, the requirements and *features* that the use case should have to be a suitable candidate for the usage of DLTs? If the reference is the section 2.6, it is possible to easily see that the most important condition that a use case should satisfy to justify the use of a DLT is the presence of multiple actors, as a single actor would not experience clear benefits using a DLT.

Talking about *nice-to-have* features, instead, followings have been identifies. Please note that a use case doesn't need to possess all of these features, as these are considered *nice to have*; of course, the more of these features it possesses, the more it is considered a suitable candidate.

- The use case taken in consideration should have a certain amount of human interaction that could be automated bringing benefits in terms of scalability
- Processes involved in the use case need/may benefit from a sort of certification of steps completion.
- It is not completely clear who should have a governance role in the processes depicted in the use case
- It is clear who has a governance role in the processes depicted in the use case, but transparency between the *leader* and all the other actors is considered an added value
- There is not a *leader* who can or wants to host a central infrastructure.

4 Introduction to the legal aspects of DLTs, smart contracts and related safety and security considerations in the railway sector

Smart contracts can be defined both from a feature-based (technical) perspective and from a functional perspective. Technically, smart contracts are a network of computer messages comprised of "if x then y" statements executed on a blockchain or DLT. From a functional perspective, smart contracts are designed so as to enable automation of (part of) the execution of an agreement where automation refers to the computer-based execution without direct human intervention. [9]

Blockchain-based smart contracts can be defined as "a piece of software code, implemented on a blockchain platform, which ensures self-performance and the autonomous nature of its term, triggered by conditions defined in advance and applied to blockchain-titled assets" [10]. Against this background, smart contracts seem more efficient – with a view to the actual performance of the agreement to the benefit of the parties – than a traditional written contract where the parties would merely *commit* to perform. By ensuring automated execution, smart contracts avoid non-performance of the agreement and thus seem to deprive recourse to judicial dispute-resolution process of any usefulness.

There is no specific regulation of blockchain-based smart contracts in Europe. This section thus examines smart contracts from a contract law perspective given their ambition to achieve functional equivalence with the performance of a legal contract. However, attention should be paid to the fact that – depending on the regulatory environment in which they operate – smart contracts may be governed by different frameworks. This section aims to (1) introduce the essential characteristics of a legal contract, (2) identify some of the challenges smart contracts pose before contract law, (3) describe the safety and security framework which governs the railway industry and (4) suggest some preliminary recommendations on the legal effect of smart contracts and preliminary guidelines for the selection of use cases. Complete analysis and further elaboration of these issues will be provided in Deliverable 4.5 'Legal aspects for smart contract adoption'.

4.1 The legal notion of contract

As contract law is not harmonised at EU level [11] [12], this analysis operationalises the common principles of contract law in the national laws of the EU Member States. By way of example, even if not a binding source, the latest revision of the Draft of a Common Frame of Reference (DCFR) provides an academic vision of what harmonised contract law in Europe could be on the basis of European substantive law and common principles in national law of the Member States. [13] [14]

4.1.1 Fundamental features of a legal contract

A legal contract is defined as an agreement vested with legal character.[4] While contracts are very diversified, they are generally vested with common intertwined fundamental features which are presented here with references to the specific features typical of the railway sector.

(i.) **A contract is a set of promises.** The legal character of the agreement entails the existence of an obligation between the parties which means reciprocal rights and duties among them. An obligation is a *duty* to perform which one party to a legal relationship, the debtor, owes to another party, the creditor.[5] A contract is thus, in essence, forward-looking: the parties agree when concluding the contract to respectively execute a duty in the future. The contract aims at removing uncertainty in human relations. [15] It governs the willingness of the parties to perform an agreement.

(ii.) **The intention of the parties to vest their agreement with legal character.**[6] Vesting the agreement with legal character means that the parties to it agree that their respective promises can be enforced on them by legal means. [16] While the parties may decide to deprive an agreement of its legal effect, this right is not unlimited. Examples include mandatory rules [16] which cannot be circumvented in any case.

(iii.) **Material scope of the agreement**. Unless prohibited by law[7], the parties are free to regulate their respective substantial commitments one to another.[8] Contractual commitments are legally binding in that they can be enforced before a court by the aggrieved party. However, it is a general principle of contract law that the content of the contract, its material scope, is legally binding only upon the parties to it.[9] In addition to the agreed substance of the contract, parties must also comply with any mandatory legal rules

[4] See article II.–1:101(1) DCFR: "a contract is an agreement which is intended to give rise to a binding legal relationship or to have some other legal effect […]" and article 1101 Belgian Civil Code (freely translated from French version): "the contract is an agreement by which one or several parties oblige herself / themselves to one or several parties to give, do, or not do something" or in US law "a contract is a legally enforceable agreement", Restatement (first) of contracts §1 (1932) as quoted by M. Raskin, The law and legality of smart contracts.

[5] Article III.-1:102 DCFR

[6] See II.– 4:101 DCFR "A contract is concluded, without any further requirement, if the parties: (a) intend to enter into a binding legal relationship or bring about some other legal effect […]. II.-4:102 DCRF: "The intention of a party to enter into a binding legal relationship or bring about some other legal effect is to be determined from the party's statements or conduct as they were reasonably understood by the other party".

[7] See II.-1:102 DCFR: "Parties are free to make a contract or other juridical act and to determine its contents, subject to any applicable mandatory rules".

[8] As stated in French and Belgian law (respectively article 1103 and 1134 of the Civil code): (free translation from French): "Legally-formed contract serves as law for the parties".

[9] See DCFR, explanatory report – Princ. 4 – contractual freedom – paragraph 4: Limitation with regard to third parties: "Parties can contract only for themselves, unless otherwise provided. A contract can produce an effect only in so far as it does not result in an infringement or unlawful modification of third party rights".

and principles stemming from sector-specific legislation or general principles of law such as the duty of good faith[10] which applies throughout a contract's lifecycle.

Railway legislation and contracts

Every branch of law comes with complementary duties and prohibitions applicable to the respective contracts (*lex specialis)*.

The legal relations between a railway infrastructure manager and its customers are highly regulated by sector-specific regulation as part of the liberalisation of this utilities industry. European law imposed structural unbundling between the activities of railway infrastructure management, on the one hand, and the use of the infrastructure (running of trains), on the other hand. The first activity remains monopolistic (as an "essential facility") whereas the second is open to competition. The infrastructure manager thus became the monopolist player of the newly-build market of the use of the infrastructure (characterised by the granting of train paths in exchange for track access charges) towards its customer (railway undertakings).

In order to protect the customers (and especially the new entrants in this new market) of potential abuse by the infrastructure manager of its position of power and to enhance the creation of a genuinely competitive of the transport activity (use of the infrastructure), European law has created a body of sector-specific rules based on principles of competition law and on the supervision of the infrastructure manager's activities by a national "regulatory body".

Figure 7: Railway legislation and contracts

(iv.) **Competence of the judicial authorities**. The legal character of the contract implies a right of recourse of the parties to an administrative and/or judicial authority to have the contract enforced and to resolve disputes related to it. In the EU, sector-specific railway legislation provides for a mandatory authority of an administrative "regulatory body"[11] with regard to contractual relationships between the infrastructure manager and its customers. The regulatory body has even broader competences that a traditional judiciary court e.g., *ex ante* competences on its own initiative.[12] In any case, a contractual clause strictly preventing any right of recourse of (one of) the party(ies) would typically be null and void and deprived of any legal effect.

4.1.2 The lifecycle of a contract

A contract's lifecycle typically involves four steps:[13] (i.) negotiation; (ii.) formation of the contract; (iii.) performance; (iv.) enforcement and dispute-resolution phase.

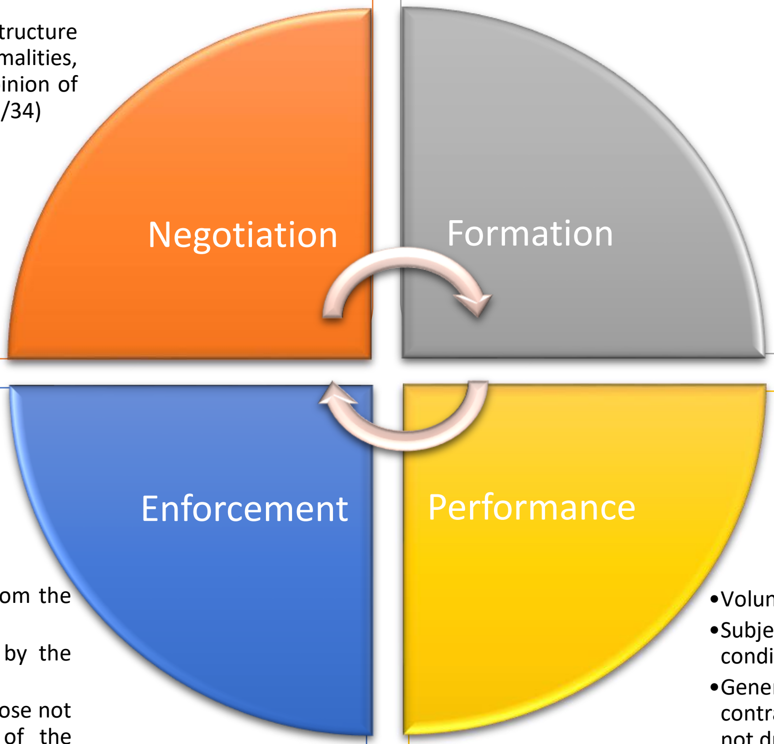
The schema below provides an overview of a contract's lifecycle and outlines the main issues and conundrums that need to be considered at each step.

[10] See article III.-1:103(1) DCFR: " A person has a duty to act in accordance with good faith and fair dealing in performing an obligation, in exercising a right to performance, in pursing or defending a remedy for non-performance, or in exercising a right to terminate an obligation or contractual relationship".

[11] See article 55 and following articles of Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area

[12] See article 56.2 of the directive 2012/34

[13] See DCFR explanatory report, paragraph 45.



- Natural or legal persons must have legal capacity to enter into contractual arrangements
- Agreement must be reached on the essential subject-matter of the contract
- Subject-matter must be legal and must not contradict mandatory legal requirements
- In the railway sector, contracts between the infrastructure manager and its customers are subject to prior formalities, such as a preliminary – binding or non-binding – opinion of the regulatory body (cf. Article 27 of e Directive 2012/34)

- Parties to a contract must have validly consented to it
- Unless specified otherwise, assent does not require a written *instrumentum* for a contract's valid formation

- Right of a party to go to court to claim remedies from the party which failed to perform its contractual duties
- Alternative dispute resolution systems recognised by the law also exist
- Enforcement is not an obligation, so a party may choose not to claim remedies in case of non-performance of the contract by the other party
- Remedies may include forced execution of a contract, payment of damages etc.
- Enforcement and dispute-resolution is dealt with by the external independent judicial system to prevent self-help and the stronger party obtaining satisfaction due to the imbalance in the power it may exert over the weaker party

- Voluntary execution of the parties' duties
- Subject to interpretation where the agreement's terms and conditions are not clear
- General principle that in case of doubt – the terms of the contract must be interpreted in favour of the party that did not draft it or in favour of the debtor
- Available exemption of the contractual obligations on the basis of “force majeure” or impossibility to comply

4.1.3 Beyond contract law: other legal implication

It should be mentioned that - for reasons pertaining to public interest - persons vested with police authority may be granted the authority to enforce preventive measures without prior recourse to a judge (while being subjected to judiciary review afterwards). The railway sector is driven by security and safety concerns which give rise to such exceptional regulations. The EU railway legislation provides for the compulsory competence of the Safety National Authority to "restrict[…] or suspend[…]" the train operations in case it identifies "a serious safety risk"[14] and other further provisions are often stated in national law.[15] Such preventive measures may thus interfere with the normal course of contracts.

It should be kept in mind that relationships between entities may also be governed by legal acts other than contracts. On the basis of criteria such as public funding, unilateral decision-making power towards the stakeholders in case of the performance of activities of general interest and/or the quality as company governed by public law by statutory regulation, the relationships between the infrastructure manager and the stakeholders – customers and/or service providers - may be (wholly or in part) considered public law acts (e.g. administrative decisions) of the infrastructure manager. There are, however, subject to national laws which differ significantly from one Member State to another.

4.2 Confrontation between legal contracts and smart contracts

Smart contracts are often (falsely) considered (either wholly or partially) replacements of legal contracts. They bring new challenges which are, however, diversified also depending on the regulatory environment within which they could be implemented. While from a technical perspective smart contracts are seen as a set of self-executing instructions, their legal assessment vary significantly ***depending on the function they are expected to fulfil***. The context of a smart contract implementation is therefore essential. Furthermore, as smart contracts are a techno-driven concept, terms used might have a different meaning from a legal perspective. [17] Blockchain-based smart contracts are rather new and have therefore not (yet) been challenged in courts of law in Europe. Conversely, legal research is still at its infancy. The following paragraphs provide an overview of smart contracts from a legal perspective as well as preliminary guidance on the legal requirements for their implementation in the railway sector.

4.2.1 Are smart contracts self-executing contracts?

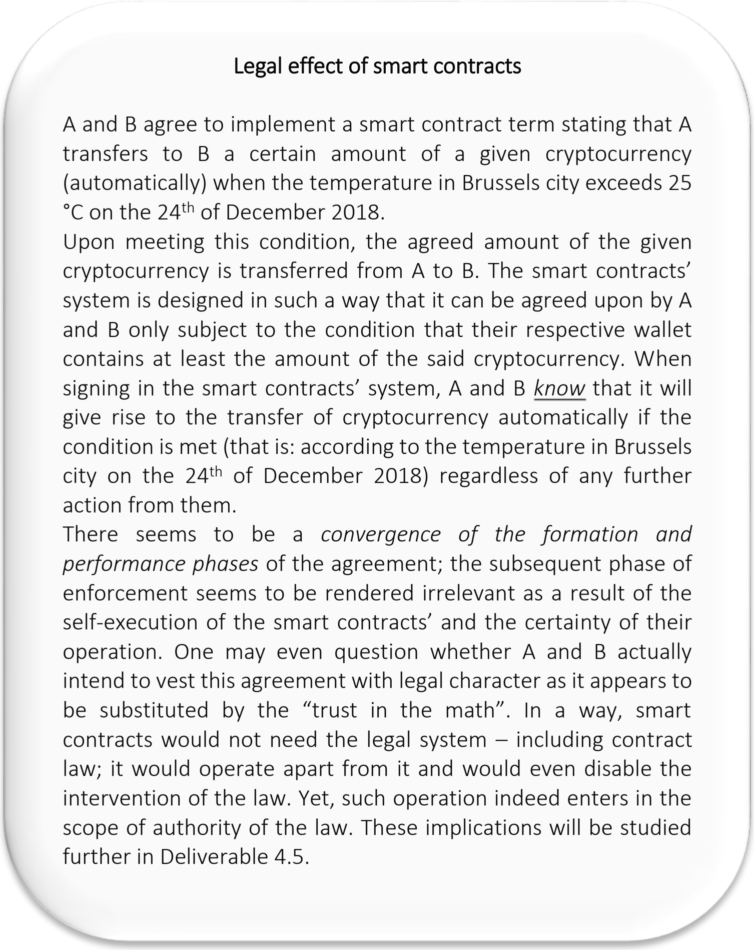
The main feature of smart contracts is that they enable automation of their terms without further intervention of the participants in the transaction. It is sometimes described as a form of "self-execution of the contract". Smart contracts would allow "self-enforcement" of the contract by actually taking away the

[14] See article 17 of Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety

[15] In Belgium the railway infrastructure manager is also provided with this competence to order that trees neighbouring the railway tracks be cut down (article 4 of the law of the 25th July 1891 revising the law of the 15th April 1843) since such trees could fall on the tracks and cause accidents.

risk of non-performance of the contract by the parties. In their most advanced form, smart contracts would cover the full lifecycle of a contract from its formation to its execution while enforcement would not be needed anymore. “Self-execution” of smart contracts would seem to take away performance by the parties as the subject-matter of their agreement, and hence the need to resort to legal enforcement. [10]

This feature of “self-execution of a contract” is an oxymoron itself, as a contract is traditionally defined by the reciprocal promise of the parties to do something that – if not properly performed – may be challenged before a judiciary authority. It is, however, undisputed that participants to a smart contracts’ system may give a valid consent[16] to the operation. This gives rise to reasonable questions about the legal effect of this consent, whether it qualifies for being a legally enforceable agreement[17] what its subject-matter may be.



Legal effect of smart contracts

A and B agree to implement a smart contract term stating that A transfers to B a certain amount of a given cryptocurrency (automatically) when the temperature in Brussels city exceeds 25 °C on the 24th of December 2018.
Upon meeting this condition, the agreed amount of the given cryptocurrency is transferred from A to B. The smart contracts’ system is designed in such a way that it can be agreed upon by A and B only subject to the condition that their respective wallet contains at least the amount of the said cryptocurrency. When signing in the smart contracts’ system, A and B *know* that it will give rise to the transfer of cryptocurrency automatically if the condition is met (that is: according to the temperature in Brussels city on the 24th of December 2018) regardless of any further action from them.
There seems to be a *convergence of the formation and performance phases* of the agreement; the subsequent phase of enforcement seems to be rendered irrelevant as a result of the self-execution of the smart contracts’ and the certainty of their operation. One may even question whether A and B actually intend to vest this agreement with legal character as it appears to be substituted by the “trust in the math”. In a way, smart contracts would not need the legal system – including contract law; it would operate apart from it and would even disable the intervention of the law. Yet, such operation indeed enters in the scope of authority of the law. These implications will be studied further in Deliverable 4.5.

Figure 8. Smart contract example

Our understanding of the legal effects of smart contracts in the context of the example in Figure 8 fits in the traditional lifecycle of a contract. Thus, the obligation not to challenge the result of the bet is assumed after the formation of the agreement. It comes with a transfer of the contractual subject-matter “downstream”: the actual contract formed between the parties by the smart contract in this example is not a “bet contract” but rather a(nother form of) contract. In this case, a blockchain is used by the parties as a certification authority. Importantly, this reasoning also restores the authority of judicial authorities: the agreement of the parties may well be legally enforced in a following phase subject to contract law so that A and B may rely on the smart contract. In this respect, it conversely entails that the contract could also be found null and void by a court, e.g. in case the oracle would actually be controlled by one of the parties without the other knowing about it (vitiated consent) or in case of misrepresentation by one of the parties. [18][18] Finally,

[16] Valid in the sense of contract law, cf. supra.

[17] For some the question of the legal value of smart contracts would simply be irrelevant by their virtue of circumventing the need for (legal) enforcement.

[18] This may however come with further legal but also practical questions: the parties may not know each other (which would presumably not be the case in B to B relations in the railway sector); it may be difficult to assert applicable law

it should be observed that the contractual arrangement itself is not included in the smart contracts system because the lines of code do not literally constitute the contract's *instrumentum*. Nonetheless, entering into a smart contracts system with (an)other party(ies) may well qualify as the formation of a legal contract whose content is, however, different from the source code and can thus have certain legal effects as a contract in its own right.

4.2.2 Execution of contractual arrangements by means of smart contracts

In the railway sector, smart contracts could facilitate part of the execution of the existing system of long-term and complex contractual relationships. The means may differ depending on the phases of the lifecycle of the contract affected by the deployment of smart contracts. They may be used to automate part of the *performance* of the contract by the parties or may incentivise the debtor to perform or enforce a sanction on a non-performing party. In this regard, smart contracts may automatically allocate liability in case of non-performance and trigger compensation to the benefit of the aggrieved party. A great variety of mechanisms can be used to incentivise the debtor to perform, such as temporarily blocking access of the non-performing party to a digital asset (or to a digitally controlled physical asset) [9, 19] in case of non-performance, triggering the (temporary) payment of a monetary security. Concerning the initial contract, such mechanisms could be said to be taking place during the phase of its enforcement or dispute-resolution.

Three main categories of issues in the railway context are particularly noteworthy: (i) trust and the position of the infrastructure manager; (ii) smart contract initiation and (iii) smart contract enforcement.

(i.) **Trust and the position of power of the infrastructure manager**. One of the benefits of smart contracts is that they bring trust between actors. However, a blockchain does not – and cannot – bring trust as to the content of the smart contracts code which is to be written by the participants as subject-matter of the smart contract. The automation of part of the performance of the contract cannot do away with the power imbalance in the market positions of the railway infrastructure manager and its customers. Under certain circumstances, it may even reinforce the stronger party's position which is in the position to implement smart contracts. Furthermore, the ambiguity of natural languages in which existing contracts are implemented will require interpretation on the part of the smart contract developer. [19] It will be their interpretation of the terms and conditions that will make it into the code creating thereby the risk of altering the parties' intentions and implementing an alternative regulatory system with its own rules. This could put the infrastructure manager in the position of unilaterally interpreting the applicable legal regime and notably the terms of the contract. In doing so, the infrastructure manager could circumvent the specific legal regime applicable to the formation of contracts with its customers and notably with regard to the *ex ante* competence of the regulatory body.[19] This power would then be reinforced by the self-executing character of the smart contracts so that affected parties – notably the customer as contracting party and

and to prove invalidity ground (e.g. with relation to the oracles). Further questions would undoubted arise as to the interpretation of contracts based on smart contracts

[19] See notably article 27 and 56 of the directive 2012/34.

the regulatory body as supervisory authority – would only be able to act against the infrastructure manager *ex post*.

(ii.) **Immutability of the blockchain vs. unexpected events in the lifecycle of contracts – the initiation of smart contracts**. Smart contracts run automatically as soon as the conditions embodied in their code are met and without further intervention needed or even possible. However, the lifecycle of a contract is not always linear. For example, in the railway sector, the regulatory body may impose modifications in contractual arrangements or implementation between the infrastructure manager and its customers[20]; National Safety Authority, the railway infrastructure manager or security authorities may suspend the train traffic or impose other preventive measures on grounds of safety or security. These circumstances and the dynamics of a contract's lifecycle should be accounted for in the design of smart contracts.

(iii.) **Smart contracts vs. legal enforcement**. Smart contracts could render legal enforcement of contracts and dispute resolution redundant. A great variety of dispute prevention or private enforcement smart contract-based mechanisms can be implemented [9] that could blur the distinction between the different phases of a contract's lifecycle. As smart contracts could in some cases extend the scope of the agreement between the parties to procedural aspects, they would then actually do much more than merely implementing the initial contract. While smart contracts cannot do away with the role of judicial enforcement mechanisms, they will likely change the subject of the procedural claims. Thus, the party that brings an action to court would typically not be the party aggrieved by the non-performance of the initial contract (traditional scenario) but rather the party aggrieved by the operation of the smart contract (presumably, the other party). Such mechanisms generally raise fundamental legal challenges as to the limits of contractual freedom of the parties that call for further research.

In the railway sector, given the monopolist position of the infrastructure manager vis-à-vis its customers, using smart contracts mechanisms as private enforcement tools may in certain circumstances qualify as unfair practices or abuse of dominant position. By relocating the (potential) dispute relating to the contract further in the lifecycle of the contract, such practices could indeed circumvent the procedural guarantees granted by the law to the weaker parties.

(iv.) **Multi-node complex smart contracts systems**. Use-cases contemplated in this project aim at dealing with the complexity in the railway environment and especially with the great variety of actors involved, by setting up smart contracts-based systems consisting of a large amount of transactions. Smart contracts operate on the basis of node-to-node transactions forming a complex network of transactions. Yet different legal meaning may attach to such – single or groups of - transactions so that the technical picture of transactions may quite differ from traditional legal relations.

Firstly, not all node-to-node transactions have legal or similar effect. Examples include:

[20] Article 56 of the Directive 2012/34

- *The parties*: transactions between nodes representing agents of the same company (intra-company transactions) are deprived of any contractual character; the same would apply to transactions between an oracle controlled by the company and an agent of the same company (intra-company transactions).
- *The subject-matter*: even when involving different parties, such transactions may not form a contract, in particular where their subject matter lacks the essential features thereof – lack of mutual promises. This could be the situation of smart-contracts systems dealing with administrative procedures or operational execution of contracts. This may become troublesome and lead to confusion in the case where other transactions *in the same system* would be vested with legal character (contractual or otherwise, e.g. administrative decision of an infrastructure manager onto stakeholders).
- *A single smart contract function* may in itself be deprived of any legal meaning, yet be considered – from a legal perspective – as forming part of a contract or other legal act constituted by a network of smart contracts.

Furthermore, smart contracts-based systems may execute direct technical transactions between entities which do not have direct legal relationships, allowing third parties to intervene in contracts contrary to the principle of relativity of contracts. Such complex situations are likely to blur the legal nature and delineation of transactions taking place and consequently pose accountability problems. As “nodes” are not necessarily “parties to a contract” but mere electronic agents, in complex situations and notably in a big data environment where transactions include oracles nodes, it may be difficult to identify on whose behalf the electronic agent has been acting at a certain point in time.

Finally, attention should be paid to confidentiality or secrecy issues in complex smart contracts networks. Indeed, the different “nodes” may not have the same access rights to the various data chains exchanged on the network. In the railway sector, the infrastructure manager is notably subjected to the obligation of respecting the confidential character of information that is “commercially sensitive” as regards its customers;[21] Where relevant, confidentiality shall also apply with regard to elements of the tendering procedure in compliance with public procurement rules.[22] Finally, secrecy obligations may be imposed by safety and security regulations.

4.3 Distributed ledger technologies and safety and security in the railway sector

The railway sector is governed by various safety and security frameworks. Security and safety should be distinguished. Railway safety refers to operational industrial safety that consists of technical and organisational rules implemented to prevent incidents caused by technical failures or human errors. The safety regime is thus closely related to the industrial and network character of the railway sector. Unlike

[21] See notably articles 29 and 39 of the Directive 2012/34

[22] See article 40.3 of the Directive 2014/25.

safety, security is not specific to the railway sector: it refers to the means implemented in order to prevent damages intentionally and maliciously caused by third parties to gain profit or cause harm [20] [21] [22].

4.3.1 Railway safety and security

Railway safety is regulated by Directive 2016/798 ("Safety Directive")[23] supplemented by implementing and delegated acts of the European Commission as well as by measures in the national laws of the Member States. Railway safety is closely related to interoperability[24] and forms part of railway specific regulation. It consists of a large set of rules regulating railway operations.

The Safety Directive targets the "main actors in the Union rail system"[25] - the infrastructure manager and the railway undertakings – as the ones bearing main responsibility for the safety[26] of the operation of their part of the railway system, in their capacity as professionals. As such, they are bound to respect safety rules and, respectively, have to establish their own internal rules, known as "safety management system" ("SMS").[27]

The railway actors are also subject the rules on critical infrastructures pursuant to Directive 2008/114 ("ECI Directive")[28], as variously implemented in Member States' national laws. The ECI Directive only provides for minimum harmonisation. [23] This matter is mostly regulated at national level since Member States retain the primary responsibility for ensuring public security. European critical infrastructure comprises "asset[s], system[s] or part thereof […] which [are] essential for the maintenance of vital societal functions […] and the disruption or destruction of which would have a significant impact [in at least two Member States] as a result of the failure to maintain those functions".[29] The directive also provides for a list of "ECI sectors"[30] which also includes rail transport. The owner/operator of the critical infrastructure is notified by the Member State of its designation.[31]

Finally, the railway sector is also subject to the rules of the NIS Directive[32] which targets the security of "network and information systems"[33] and thus harmonises the rules on security of network and information systems with regard to two categories of actors: "operators of essential services" and "digital service

[23] Directive (EU) 2016/798 of the European Union and of the Council of 11 may 2016 on railway safety (recast)
[24] Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union
[25] Recital (7) of the Safety Directive
[26] See recital (7) and (8) and article 4 of the Safety Directive
[27] See article 9 of the Safety Directive
[28] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
[29] Article 2(a) and (b) of the ECI Directive
[30] Annex I of the ECI Directive
[31] Article 4 of the ECI Directive
[32] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
[33] Article 1st of the NIS Directive

providers".[34] The essential service providers must be identified by the respective Member States on the basis of the criteria laid down in the NIS Directive. Railway infrastructure managers may be identified as operators of essential services[35] on the condition that and in so far as[36] they (1) provide a service "which is essential for the maintenance of critical societal and/or economic activities" which (2) "depends on network and information systems" where (3) an incident on the later would have a "significant disruptive effect of the provision of that service".[37]

4.3.2 The design of DLT based systems for railway infrastructure management and safety and (cyber)security regulation: guidelines for the selection of use cases

The use cases that are being contemplated within WS2 – though diversified - all aim at delegating part of the railway infrastructure manager's activities to a DLT system. Consequently, they may be subject to the safety and (cyber)security directives mentioned above and to further national regulation in this regard – provided they are designed as 'critical' by the respective Member States in the case of ECI and NIS.

The following guidelines are aimed at facilitating the choice of use cases in light of the obligations stemming from the safety and security frameworks applicable to the railway sector.

[34] Digital service providers are operators providing "online marketplace", "online search engine" or "cloud computing services": they do not have to be further "identified": every entity providing a digital service falls within the scope of the directive. See recitals (15), (16) and (17), article 4 points (5), (17), (18) and (19) and Annex III

[35] Article 4, point 4 and Annex II of the NIS Directive

[36] See recital (22) of the NIS Directive

[37] See article 5 and 6 of the NIS Directive

Matter	Recommendation	Applicable legislation
Use case subject matter	The more related the subject matter of the use case is to the core activities of railway infrastructure management, the more likely it is that it will be subject to the full scope of the applicable safety and security requirements.	Directive 2016/798 (Railway Safety Directive) Directive 2008/114 (European Critical Infrastructures Directive)
Digitalisation of railway infrastructure management processes	Digitalisation of certain processes in the management of railway infrastructure could have a bearing on its designation as 'critical', such as the NIS Directive where reliance on network and information systems for the provision of the essential services is a relevant triggering factor for the application of the directive.	Directive 2016/1148 (Network and Information Security Directive)
Confidentiality	Designation, detailed description and functioning of critical or sensitive assets as well as the specific measures to protect them are likely to be considered 'secret' which may not be compatible with the transparency of data transaction on a permissionless blockchain.	National legislation on confidentiality and protection of classified information
Responsibility and control	In assigning the responsibility to control safety-related activities to the infrastructure manager, the actor-based approach of safety legislation might collide with the distributed design of a blockchain where lack of control of a single node over the system is a prominent feature. Any DLT-based system should thus be assessed against the premises of the applicable technical and safety legislation. The following specific issues need to be considered: • internal rules of the operator may not allow for the delegation of part of safety- or (cyber)security-related activities outside the internal organisation to a decentralised network; • any substantial change in the safety management of the infrastructure manager must be notified to the National Safety Authority and may give rise to a revision of the safety authorisation; • assessment of the degree of control an end-user may have over a decentralised DLT-based system against the centralised concept of control in railway safety and security frameworks; • the difficulties in identifying the entities actually operating the network may leave the infrastructure manager as end-user deprived of an accountable counterpart; • immutability of the blockchain coupled with its openness may make it difficult to revise the system over time according to dynamic risk analysis and return of experience of the operator.	Directive 2016/798 (Railway Safety Directive) Directive 2008/114 (European Critical Infrastructures Directive)

Cybersecurity and blockchain as a “digital service”	Blockchain-based systems may under certain circumstances qualify as a “digital service” within the meaning of the NIS directive and, more precisely, as a “cloud computing service”. The legal definition of a cloud computing service refers to “a digital service that enables access to a scalable and elastic pool of shareable computing resources”. From a functional perspective, the public distributed infrastructure in this way very similar to traditional cloud computing services. It could be considered as a kind of cloud computing service where the computing resource is constituted by the network-powered platform (Platform as a Service) and the computing resources are provided and allocated according to the governance rules applicable to the platform. Pending further authoritative guidance, to the extent a blockchain service may be considered a cloud computing service, the obligations under the NIS Directive need to be taken into account.	Directive 2016/1148 (Network and Information Security Directive)

Table 3. Preliminary legal guidelines for the selection of use cases in WS2

5 Scenario Analysis: requirements and selected use cases

As result of the AS-IS analysis of the asset management operations performed by RFI and its suppliers, keeping into account all the requirements and features a suitable use case for DLT should have (section 3.6), four use cases for the application of blockchain (also considering scenarios developed in IN2SMART) have been identified:

1) Asset Maintenance;
2) Public procurement;
3) Data Monetisation;
4) Train Paths allocation.

All these use cases are related to asset management. Use Case 1) is in common with In2SMART and it is considered one of the main challenge of the future. The ability of the ecosystem to improve the efficiency of maintenance is crucial to the sustainability of the transport ecosystems, since it is the highest operational cost sustained by IMs.

Use Case 2) is strictly related to 1), but it is originally derived from the discussion with the main industry actors in field. Use Case 3) is derived from the discussion of potential evolution in In2SMART, since the data lakes that they are building still lack sustainable business models. The Use Case 3) is considered as more visionary and long-term; the last scenario, regarding tracks paths, is indirectly related to asset management since tracks paths are services build upon assets (tracks) and track paths management has a direct impact on assets.

In the following sections, each use case will be described by presenting the context and motivation, the business needs, the potential benefits of using blockchain and (when possible at this stage) the proposed architecture.

Some of these use cases, more precisely 1) and 3), are cross-WP use cases: the Data Monetisation use case is in common with WP5, while the Asset Maintenance one will be one of the inputs of the Data Visualisation use case, also part of WP5. Both use cases will be part of D5.1 deliverable. Please note that the “big picture” of IN2DREAMS WS2 use cases will also be better defined and described in D5.1.

5.1 Asset Maintenance

The following use case refers to the ordinary maintenance as described in section 3.3.

Ordinary maintenance is of paramount importance for IMs since:

- It extends the lifetime of the physical assets
- It prevents accidents that may cause delays, service interruption or even disasters

Currently, the administrative workflow followed to plan a maintenance activity, and to certify its execution, has three major drawbacks:

- It is time-consuming due to administrative procedures and non-automatic ways of forwarding data and delegating tasks between the different maintainers.
- Responsibilities at each step of the workflow could be difficult to understand.

- Lack of trust between the different actors makes it difficult to certify in an incontestable way the time of execution of all the workflow steps. This is especially important both from a legal and a SLA enforcement point of view.

Employing the blockchain technology in the ordinary maintenance scenario, it could be possible to improve the current situation. With the creation of smart contracts that correctly resemble the content of officially approved procedures, it is possible to automatise this workflow. Moreover, at each step it would be clear who is responsible of which action. Each action would be recorded in a transparent, secure, and immutable way on the blockchain, thus giving a trustable way to audit what has been done at each step of the workflow.

Given as an assumption that the content of the smart contracts is correct and has been accepted by all the actors of the use case, no rejection or objection could be made in case of contention.

Moreover, migrating the whole process and data to a blockchain will give the owner (RFI) and their partners a single source of data populated with core and valuable information about their assets. This source of information will be resistant to data tampering, thus making all the actors completely sure about the veracity of the information they will work with.

The whole process will be automated and updated in real time; human interaction, at least the one currently needed to communicate the correct execution of a workflow's step, will be put to a minimum.

In Table 4, a summary of the issues of today implementation, with the related benefits that comes with the adoption of DLTs, is presented.

Today's Issues	*Applying DLT and smart contracts*
Lack of security and trust between actors	Enhanced Security thanks to crash tolerance and secure timestamping.
Business logic enforced by third parties through contracts	Business logic automation through smart contracts
Enforcing subjective rules making the business non -transparent	Enhanced transparency through ledger auditability
Limited process efficiency due to dated communication methods	Potential efficiency gains in terms of time and complexity

Table 4 Comparison between business as usual with today's issues and application of DLT for the maintenance scenario

The proposed solution, that implies blockchain technology and smart contracts to manage the whole maintenance workflow, allows different actors (internal teams, suppliers and subcontractors) to exchange information about assets and their status. Indeed, the blockchain will act like an automated ticketing system which stores information in the ledger to manage the maintenance workflow and to provide a tamperproof and immutable record of the processes. Information about the assets will be feed to the blockchain, together with scheduled maintenance and assigned maintainer. The smart contracts deployed in the blockchain will act as an orchestrator of the workflow, automatically granting access to the data to the chosen maintainer and recording each completed step of the process. When the scheduled maintenance is completed, the maintainer will be able to record the completion of the process through the smart contract, thus informing eventual controllers or auditors. Since each step completion is recorded on the blockchain with a timestamp, verifying SLA infringement would be extremely easy and potentially free from contentious.

This leads to overall benefits to all parties involved in the process in terms of efficiency and accuracy. It brings the possibility to RFI to be able to plan its maintenance schedule more accurately, to improve the traceability of the parts and to increase the speed of flow of goods in a just-in- time network. The suppliers will be easily included in the digital workflow and can be managed and controlled by RFI easily so that all included parties will contribute to boost the efficiency of the railway ecosystem.

In Figure 9, the logical architecture of the asset management, with the blockchain acting as an underlying technological block of the asset maintenance, is illustrated.

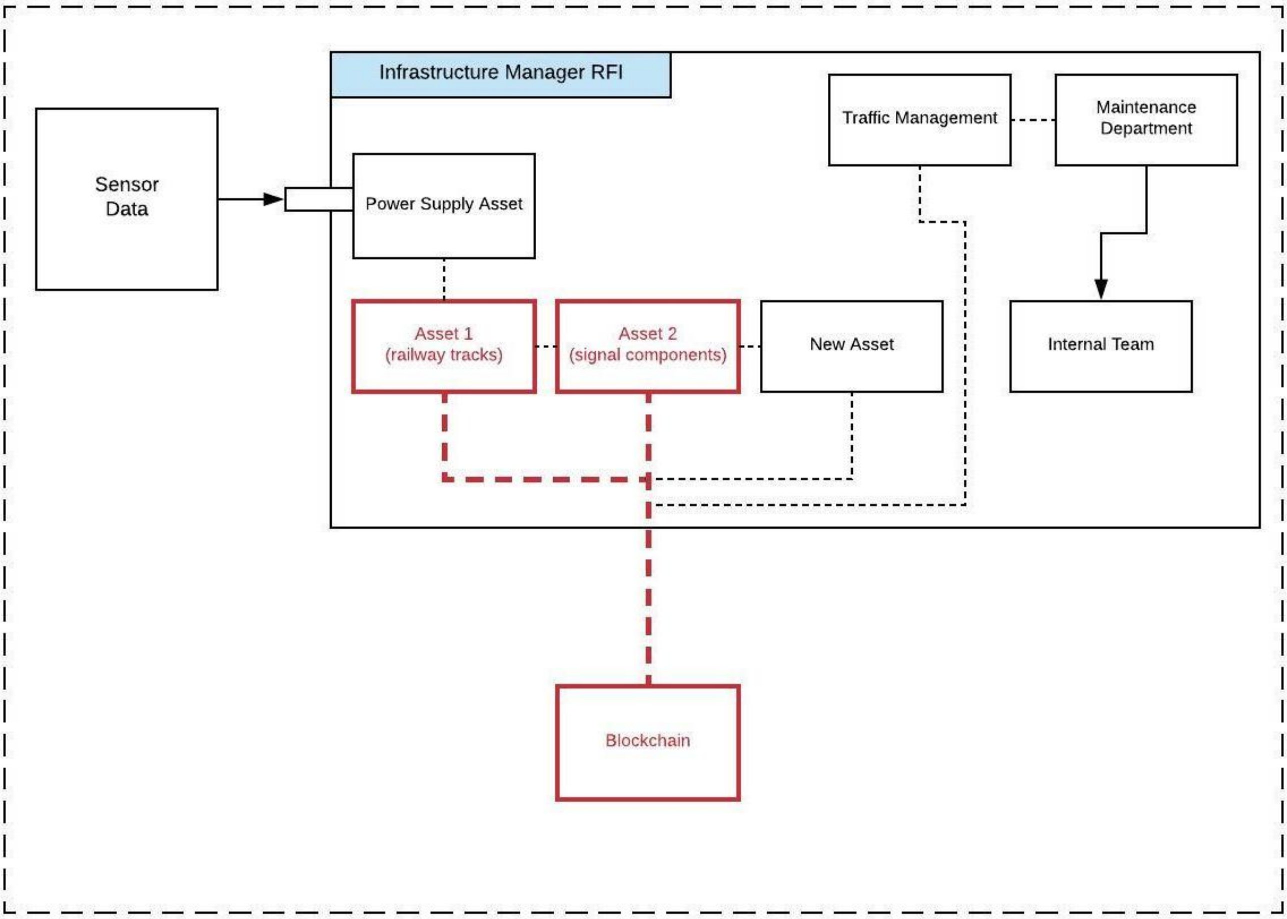


Figure 9: Logical architecture of asset management with the maintenance part based on a blockchain

5.2 Procurement

The following use case refers to the process of selection of a supplier and assignment of a contract for the deployment of a new asset, as described in section 3.4. The selection of a supplier is done through a public tender or, only in very special occasions and anyway if it was not possible to do it otherwise, by direct selection of suppliers through previous predefined benchmarks.

The public procurement process involves a great amount of resources and the analysis are time-consuming. Moreover, the IM has to guarantee transparency in the process and fairness with the parties involved in it and keep a historical record of all the data regarding past public procurements.

In Figure 10, a representation of the workflow of a public tender is pictured.

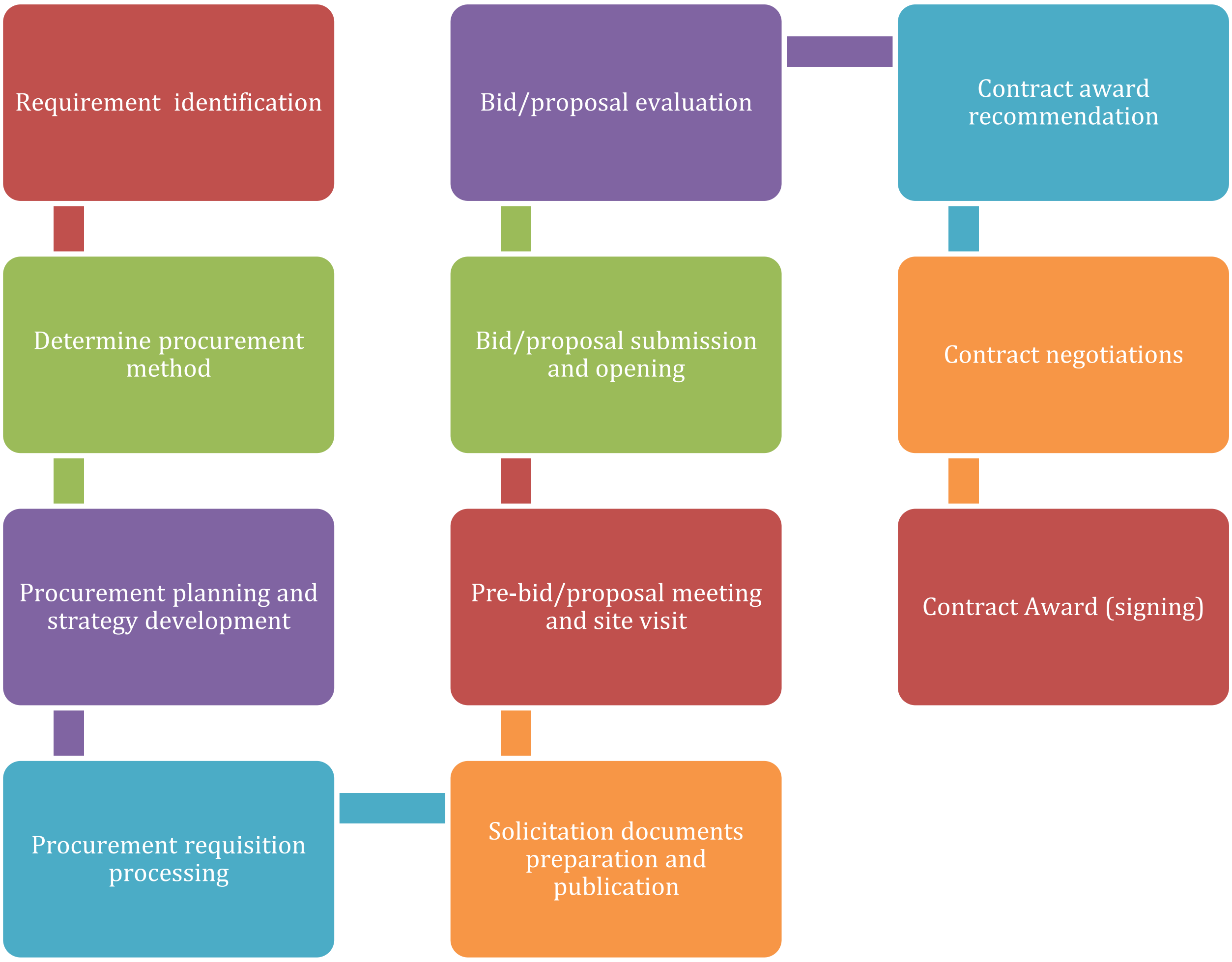

Requirement identification
Determine procurement method
Procurement planning and strategy development
Procurement requisition processing
Solicitation documents preparation and publication
Pre-bid/proposal meeting and site visit
Bid/proposal submission and opening
Bid/proposal evaluation
Contract award recommendation
Contract negotiations
Contract Award (signing)

Figure 10: Representation of the different phases of a public tender

This scenario is one of the main interest in potential application of blockchain, in fact there are already some experimentation [24] going on.

The characteristics required by procurement processes is of interest for the application of blockchain technology, since the technology has the potential to enhance process efficiency and transparency.

All of the previous flaws can be mitigated via blockchain thanks to the fact that the technology leads to simplification and automation of the bid process, management of the bidders' identities and overall security of the data involved in the process. The process transparency is enhanced through trusted timestamping and digital signatures on the final agreement and everything is recorded on a ledger that is immutable and tamperproof.

The owner can perform analysis and forecasting based on historical data that is easily accessed and processed through the ledger, enabling visibility into spending patterns and forecasting the future procurements based on this data. The owner could also opt for a direct procurement choosing a supplier based on certain benchmarks that are certified by the historical data.

In Table 5, a list of the issues related to the current procurement workflow is presented together with the potential benefit that the adoption of a DLT would bring.

Today's Issues	Potential Benefits applying DLT
The public procurement process involves a great amount of resources and is really time consuming.	Simplification and Automation of the bid process; Managements of bidders identities; Security of the data involved in the process;
The public company must demonstrate the transparency of the procurement process but it is an expensive activity	Enhance process transparency through: Trusted timestamping and digital signatures; Ledger auditability and immutability;
Keeping historical data from all of the previews interaction for future statistics	Distributed, auditable and immutable ledger can ensure autenticity of hystorical data.
Process bottlenecks due to lack of automation	Smart contracts technology can automate decisions and boost efficiency
No clear understanding of the money flow	Having a strong understanding of company spending
Nonvisible opportunities enforcing company outdated rules	Allowing organisations to negotiate better contracts
Accessing and processing historic data is time consuming and not often applicable	Visibility into spending patterns and forecasting the future procurement based on historic data
Lack of trust and competitive empowering	Optimised purchasing process will lead to more efficient sourcing- quality of goods and service delivered on time

Table 5 Comparison between business as usual and application of DLT for the procurement scenario

The proposed solution implies a blockchain to maintain a record of all the bidders received for a public procurement. For each procurement, a smart contract will be deployed on the blockchain acting as a digital notary certifying the receipts of bids in a secure and trustable way.

In case of an invitation only procurement, given the programmable nature of the smart contract, it would be possible to limit the bidder sets to a list of already identified companies, allowing only those ones to bid.

At the closing of the time window participants have to present their bids, the smart contract will automatically stop accepting bids. Eventually, when a winner is selected by the commission, also the final choice will be recorded on the blockchain for auditing purposes, letting the smart contract automatically notify participants of the result (either transparently proclaiming the winner or just saying individually if they won or not).

In a more advanced version of the proposed solution, it could also be possible to let the smart contract manage the agreed payment related to the winning bid: the organiser of the procurement would transfer funds to the smart contract that in turns would turn them to the winner according to the agreed schedule, thus guaranteeing the winner that the payment will be received.

In Figure 11, the logical architecture of the asset management, with the blockchain acting as an underlying technological block of the procurement of new asset, is illustrated.

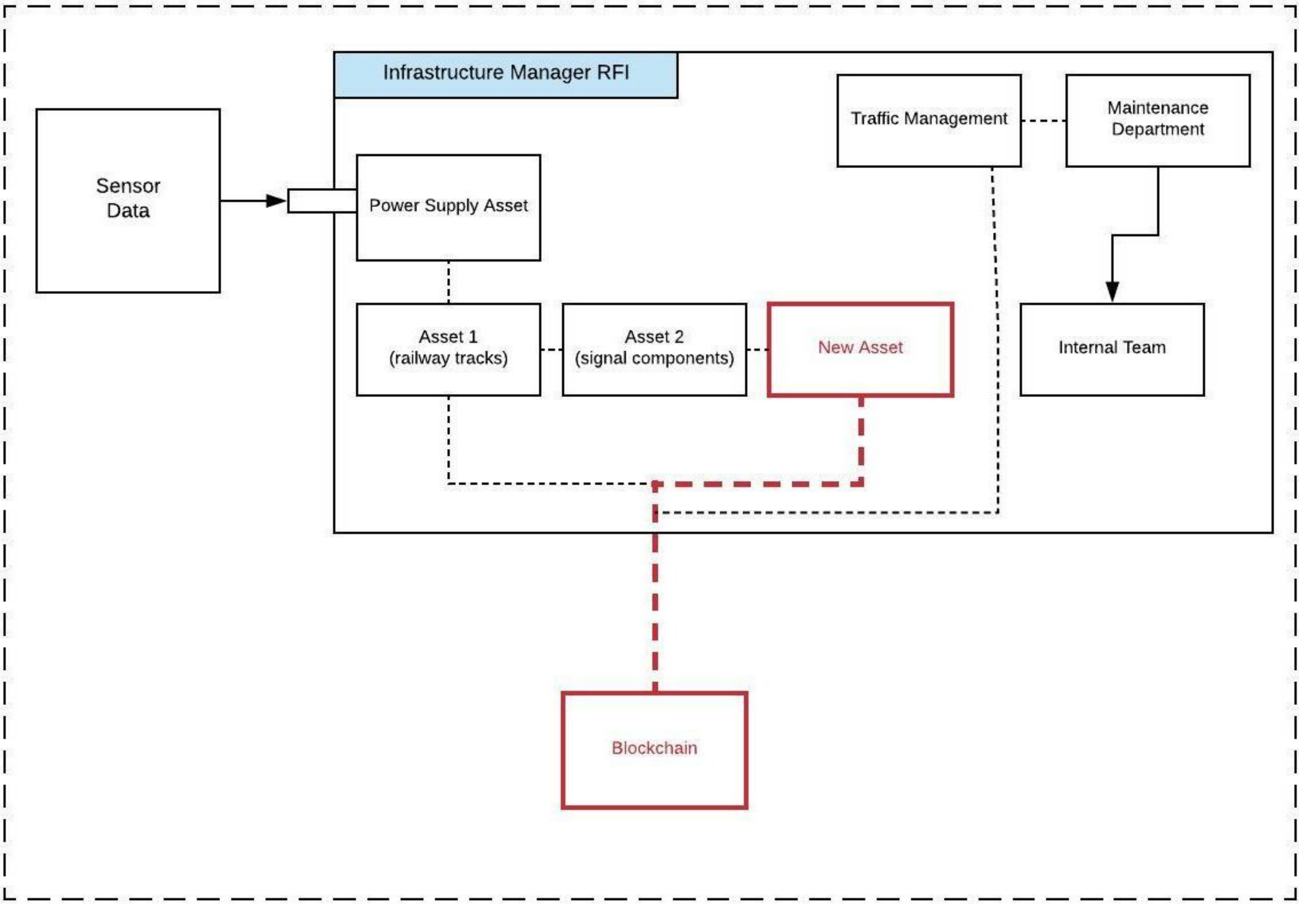


Figure 11: Logical architecture of asset management with the procurement of new asset build on a blockchainData

5.3 Marketplace for Monetisation and Servitisation

The Data Marketplace for Monetisation and Servitisation Use Case refers to the data sources ecosystem for asset management which will be defined by Shift2Rail project In2SMART (WP7). As output of this currently ongoing project, a system for the exchange of data sources will be designed. This system may play a crucial role in the European Railways Ecosystem, especially considering the Open Market scenario envisioned by the EC. In this use case, actors will be IMs, suppliers, or any other entity that is involved in data creation and data utilisation in this field. The system will have to consider the legal aspects of exchanging data sources, since there may be relevant issues related to the “ownership of data”.The system will collect all the data sources produced and used in the ecosystem by all actors and would have the main goal to allow their business exploitation.

A still open question of this platform is how to tackle the economic and business sustainability: how to turn data sources assets into value, how to monetise them and how to promote the demand for services (data marketplace).

All the actors involved are aware that this imply a paradigm shift from the “customer to supplier logic” to the ecosystem logic, where the involved “actor” may play different roles at a time, and then pass from the rigid governance rules based on “command&control” to “soft and simple rules” that are just enough to “allow” the collaboration among actors, but at the same time not too restrictive to block innovation and new services.

The railway ecosystem is composed by a heterogeneous group of actors that during their business activity produce data or consume data as an input for their products and services. The main challenges are: the lack of trust between the users in the network, the quality of the data and their analytics and the lack for a sustainable monetisation model.

In this context it is possible to apply blockchain (as SW infrastructure) and smart contract (as application layer) as the underlying technological enablers to facilitate the direct exchange of data sources in a trusted environment, even combined with direct reward mechanism for the exchange of data sources. Similar approaches have been recently proposed in [12].

Therefore, a digital marketplace is envised:

- The Actors involved in the process can manage and control their data without the need of intermediary third party or centralised repository
- The exchange of the data is regulated by adopting open standards and could be improved by adopting smart contracts that will enable data monetisation of the data exchange
- Thus, the monetisation for the exchange of data in digital ecosystem (precisely B2B) and the automation of governance logics in the digital ecosystem are enabled
- All parties involved in the exchange have access to the same data, this will lead to acceleration of data acquisition\sharing, and improving the quality of data and data analytics
- The adoption of smart contracts could tackle the problem of managing the marketplace dynamically. Data will be decentralised and will have dynamic value based on the usage or other

predefined characteristics. Unlike current data exchange markets, this solution requires no trusted third-parties

- Data producers and customers can cooperate together to build up a network of data-based value transfer. The core part of the network is a set of protocols which are followed by all the participants. The network will automatically record transaction logs which help data owners to audit the use of their data. The solution can help to promote data circulation, and to promote data-intensive applications. [10]

To support this use case, a generic discussion of the use of blockchain as SW connectors ca be find in [11].

The business expectation will be that this will empower companies to profit from their data while allowing sustainable data monetisation and enhancing trust between actors.

There are several possible proposed architectures for the data marketplace, depending on the specific blockchain and smart contracts frameworks adopted.

Table 6 sums up the expected benefits of a data marketplace, as described above.

Opportunity	*Potential Benefits applying DLT*
Define a new exploitation model for Data Monetisation of Data Sources among the Railway ecosystem	• Direct Exchange of value among actors • Simplified governance and managements of data sources
Provide a sustainable model for exchanging data sources based on incentives	• There is a reward mechanism based on incentives for data sources • The actors can exchange value without knowing each other in a complete transparent way
Tracking the use of data sources	• Having an auditable and immutable ledger can ensure authenticity of historical data and their usage

Table 6 Opportunity and potential benefits by applying DLT

5.4 Train Path allocation process

This section analyses a possible scenario that emerges from the complexities of coordination in the process of railway infrastructure capacity allocation when different countries are involved. In section 3.5, the process describing the train path allocation is described from a national perspective. When multiple countries are involved, different transportation companies and Infrastruture managers have to collaborate to optimally allocate the capacity and respecting their own networks and regulatory constraints.

Within the European railway ecosystem, a lot of effort has been put towards the harmonisation of the various railway systems with the goal to facilitate the development of an international railway system.

When a transportation company asks for an international train path it has to draft an appropriate path request; the different IMs involved in the path have to cooperate and provide the railway infrastructure capacity required to successfully satisfy the request. Each of them schedules the train passage in its corresponding path section according to the timetable drafted by the IM involved in the previous section.

When all the IM have scheduled railway capacity for the train passage, the path offer is submitted to the transportation company that evaluates it and eventually accepts it.

The creation of information systems that support processes and relationships between IMs and transport companies of different countries is of great value to achieve the harmonisation.

Currently, at the EU level, the harmonisation of international train path allocation processes is governed by RNE, that deployed the *Path Coordination System* [25]: an information system responsible of managing the communication and coordination processes for the demand and supply of international train paths.

In this context, the application of blockchain technology opens interesting scenarios about the automation of the path request and the tariff owed to the different IMs; path offerings are made of the sum of the different path section offered by every IM; every one of them can apply their track access charges according to their readiness to allocate train paths at some point in time.

Smart contract allow for a great flexibility in this sense thanks to the possibility of using a computer program to dinamically accept path requests if certain conditions are met. IMs can publish a smart contract on a blockchain to allocate capacity through auctions open to only trustworthy transportation companies providing proofs of the authenticity of their requests using timestamping and digital signatures.

A blockchain integrated Path coordination system has the potential of keeping track of path allocations agreement and enforce sanctions by making every party accountable for their commitments expressed in a smart contract.

Problems	*Potential benefits applying DLT*
Coordination between different IM is complex and time-consuming task	Process automation of path allocation Having a strong understanding of company spending
Nonvisible opportunities enforcing company outdated rules Different transportation companies have conflict of interest	Enhanced transparency between parties involved
Limited flexibility in tariff schemes	Smart contracts to manage dynamically the train path fees

Table 7 Comparison between business as usual and application of DLT to the path allocation scenario

The proposed solution implies a blockchain system where smart contracts are deployed to manage the workflow of international train paths allocation. As usual, the blockchain will act as a secure and trustable record of all the transactions between the different actors, while the smart contracts will be the orchestrators of the workflow.

When a new request comes up for an international train, the transportation company should send a transaction to the smart contract notifying all the needed information like point of origin and destination, and desired time window. The smart contract would automatically notify the IMs whose competent countries are involved that a new train path request is waiting for approval. Each IM would then either approve the proposed plan, reject it, or propose an alternative sending its answer to the smart contract. When all the IMs agree to the proposed allocation plan, that one will be considered final and the workflow closed; if not another round of discussion would be carried out always with the automatic orchestration of the smart contract.

In a more advanced version of the proposed solution, the train company that started the procedure would have to send the overall payment related to the train path to the smart contract. The payment would then be divided between all IMs according to the respective track access charges schemes and percentage of coverage of the all path, and automatically sent to them.

6 Conclusions and Use Case selection

As a result of T4.1 activities, the data exchange scenarios and four relevant use cases have been defined, taking into account both current processes and data exchange flows between the different parties involved, and future scenarios derived by the vision and the direction that the whole ecosystem is taking.

To accomplish this task at the widest level possible, T4.1 has acted in collaboration with other Shift2RAIL relevant recipients (In2SMART and In2STEMPO).

Throughout the analysis of the possible use cases carried out in Chapter 5, the main benefits that DLTs could bring to the Railways Asset Management ecosystem have been identified:

- Cut off third parties by enabling the direct exchange of trusted information
- Transparency
- Tamper-proof source of data
- Ability to run trusted self-executing logics (smart contracts)

Thanks to them, DLTs may contribute to the smart evolution of the Railways Ecosystem in term of growth, sustainability and openness of the market aimed at achieving a Single European Railway Area (SERA). Of course, considering that these technologies represent such a young and novel approach, and the frameworks, both legal and technical, are not as mature as required at the moment (even if they are evolving at a fast pace), it is necessary to experiment in a safe environment like the In2Dreams project to reach a deep understanding of the potential impacts of these technologies.

The identified use cases described in Chapter 5 have been presented to RFI that has driven the selection according to its business requirements.

The chosen use case is the Asset Maintenance one (described in Section 5.1). This has come by exclusions of the other use cases for the following reasons:

- The Procurement use case (Section 0), has been judged as not attractive since, considering that at this stage the legal implications related to the employment of a blockchain are unclear, in this specific use case the blockchain could merely be employed as a secure record of public procurements applications, without directly coordinating the overall process. In this way the benefits derived from its employment for procurements would be minimum.
- The Data Monetisation use case (Section 5.3) is considered interesting as a future evolution of the Railways Ecosystem. Nevertheless, the presence of a cryptocurrency in the proposed solution makes its success unclear if it is considered that at the moment cryptocurrencies have proved to be unfit to the exchange of monetary value: Bitcoin, for example, is currently used as a speculative investment and not as a payment system given the high instability of its value.
- The International Train Path allocation use case (Section 5.4) needs different IMs that interact with each other. Considering that there is only one IM involved in IN2DREAMS, the original idea was to rethink the use case within the context of the National Train Path allocation workflow, that involves multiple Command&Control centres each responsible of a specific Region. RFI nevertheless argued

that in such a case a decentralised trustless infrastructure is not needed as the different Command&Control centres are already coordinated at the national level.

The Asset Maintenance use case (Section 5.1), instead, is in line with the business needs of RFI and do not present any significant drawback or failure risk. Considering the AS-IS regarding asset maintenance, RFI has concluded that the employment of blockchain could bring great benefits to the use case in terms of reduced time consumption and clearly defined responsibilities at each step of the workflow.

References

[1] M. E. PECK, "How Blockchains Work," *IEEE Spectrum,* 2017.

[2] Blockgeeks, "What is Blockchain Technology? A Step-by-Step Guide For Beginners," 2016. [Online]. Available: https://blockgeeks.com/guides/what-is-blockchain-technology/.

[3] V. Gramoli, "From blockchain consensus back to Byzantine consensus," *Future Generation Computer Systems,* 2017.

[4] A. M. Antonopoulos, Mastering Bitcoin: unlocking digital cryptocurrencies, O'Reilly Media Inc., 2014.

[5] "Ethereum Wiki - Proof Of Stake FAQ," 2017. [Online]. Available: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ.

[6] M. E. PECK, "Do You Need a Blockchain?," *IEEE Spectrum,* 2017.

[7] "Rete Ferroviaria Italiana Official Website," RFI, [Online]. Available: http://www.rfi.it/.

[8] "Prospetto informativo della rete," [Online]. Available: http://www.rfi.it/rfi/SERVIZI-E-MERCATO/Accesso-alla-rete/Prospetto-informativo-della-rete.

[9] M. Ruskin, The law and legality of smart contracts, Law Technology Review 304 (2017), Georgetown (USA).

[10] A. Savelyey, Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law.

[11] E. O. O'Connor, The limits of contract law harmonization, European Journal of Law and Economics, Vol. 33, Issue 3 (2011).

[12] F. G. Pomar, The harmonization of contract law through European rules: a law and economics perspective, InDret, 2/2008 (2008).

[13] O. Lando, "Principles of European Contract Law: An Alternative or a Precursor of European Legislation", The Rabel Journal of Comparative and International Private Law, vol. 56, no. 2 (1992).

[14] "The Draft Common Frame of Reference (DCFR), Sellier European law publishers (2009)," [Online]. Available: https://www.law.kuleuven.be/personal/mstorme/2009_02_DCFR_OutlineEdition.pdf.

[15] Q. DuPont and B. Maurer, Ledgers and law in the blockchain, Kingsreview (2015).

[16] P. Wéry, Droit des obligations, Brussels, Larcier (2011).

[17] E. Mik, Smart contracts: terminology, technical limitations and real world complexity, Law, Innovation and Technology, 9:2 (2017).

[18] P. Cuccuru, Beyond Bitcoin: an early overview on smart contracts, International Journal of Law and Information Technology 25 (2017).

[19] P. De Filippi and S. Hassan, Blockchain technology as a regulatory technology: from code is law to law is code, in First Monday, vol. 21 n°12 (2016).

[20] E. Albrechtsen, Security v. safety (2003).

[21] E. Albrechtsen, Major accident prevention and management of information systems security in technology-based work processes, Journal of Loss Prevention of the Process Industry, Vol. 36 (2015).

[22] E. A. M. Bartnes Line, Examining the suitability of industrial safety management approaches for information security incident management, Information & Computer Security, Vol. 24, n°1 (2016).

[23] P. C. a. G. d. Búrca, EU Law: Text, Cases, and Materials (OUP Oxford 2011).

[24] G. D. A. Program. [Online]. Available: https://www.ge.com/digital/sites/default/files/Global-Partner-Summit-2017-Guaranteeing-IoT-Data-Integrity-Blockchain-Rail-Use-Case-Ericsson.pdf.

[25] RailNetEurope, "Path Coordination System (PCS)," [Online]. Available: http://pcs.rne.eu/.

[26] M. D. A. D. a. M. L. Steve Cheng, "Using blockchain to improve data managament in the public sector," February 2017. [Online]. Available: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector.

[27] Y. X. Jinchuan Chen, "Bootstrapping a Blockchain Based Ecosystem for Big Data Exchange," *IEEE International Congress on Big Data,* 2017.