Distr.: Restricted
19 August 2019

English only

Economic Commission for Europe

Inland Transport Committee

Working Party on Rail Transport

Group of Experts on Permanent Identification of Railway Rolling Stock

First session
Geneva, 2–4 September 2020
Item 5 (b) of the provisional agenda
Development of the Unique Rail Vehicle Identification System: Technological component

Use of blockchain for rail rolling stock assets registration

Submitted by European Union Agency for Railways (EUAR)

I. Introduction

1. Although falling short of high expectations, the blockchain technology has now been successfully implemented, in numerous areas where there is a need for accuracy and security of information, such as finance trade and assets registry. Besides specific business-oriented solutions, blockchain applications are already being used to support the SDGs and the blockchain is seen as a key facilitator of world trade by the UNECE[1].

2. Blockchain provides an alternative model to proof-of-existence and possession of legal documents. By leveraging the blockchain, a user can simply store the signature and timestamp associated with a document in the blockchain and validate it at any point using native blockchain mechanisms. To register ownership of an asset, a transaction is created with a reference to the physical asset. This information is stored on a blockchain record and can be associated with all manner of goods or services. The owner of the private key to that public record is then registered as the owner of that asset.

3. At a conceptual level, the properties of blockchain make it particularly suitable candidate for the task of maintaining an asset registry:

i) The system is resilient, without a single point of failure or corruption

ii) Cyptographic proofs provide integrity to the information contained in the ledger

iii) The information is traceable and auditable, thereby providing enhanced transparency

4. The implementation of blockchain in public domains has several challenges due to existing legal and organisational frameworks, which are further accentuated in the international context, however there are successful pilot projects available[2]. Off-the-shelf' block-chain packages are now offered by main software providers. Nevertheless, blockchain implementations are nowadays predominantly based on open source software.

5. The aim of this note is to provide some background information on the technology and its potential for use under Luxembourg protocol. It includes a specific proposal for the use of the blockchain under the Luxembourg protocol, as first outlined by Dylus in his article "The International Blockchain Registry of Mobile Assets"[3].

II. Blockchain technology for asset registration

6. A blockchain is a cryptographic protocol that allows separate parties to increase the trustworthiness of a transaction because the ledger entries in its database cannot be easily falsified (i.e. once data is written it is extremely difficult to change, albeit provided the data was correct from the outset).

At a more technical level, a blockchain is a time-stamped series of immutable records of data that is managed by a cluster of computers not owned by any single entity. Each of these blocks of data (i.e. block) is secured and bound to each other using cryptographic principles (i.e. chain). The system creates the first block consisting of a header and data related to transactions taking place within a time period, using the block's timestamp to create a string called a hash. The following blocks in the ledger use the previous block's hash to calculate their own. However, before a new block is added to the chain, the system validates its

[1] UN/CEFACT (2019), White Paper Blockchain in Trade Facilitation, UNECE

[2] Pignatelli F. et al. (2019) Blockchain for digital government, JRC science for policy report, JRC115049

[3] Dylus, Erich P. 'The International Blockchain Registry of Mobile Assets'. Air & Space Law 44, no. 1 (2019): 45–52.

authenticity by consensus, meaning that the majority of nodes in the network must agree that the new block's hash was correctly calculated. This ensures that all copies of the distributed ledger share the same state.

7. Each exchange of an asset from one party to another can be created as a transaction; timestamped; verified by all parties via a pre-agreed consensus mechanism; digitally signed and authenticated by relevant stakeholders, and then committed to an immutable ledger that is maintained as a node by all the participating agents.

8. An asset registry can be described as a book of records that maintains the ownership status of such assets (and are generally maintained by legal authorities). Asset registry/transaction is an area where one witness the maximum disputes, and hence a lot of time and money is spent on resolving asset ownership claims.

9. Blockchain may offer a more efficient and secure mechanism for the identification of the rail rolling stock assets, eliminate risks of syntax errors and noncontiguous asset histories and mitigate potential liability of the Registrar. A blockchain registry system does not need to affect the Supervisory Authority's approval process or confidentiality protocols, which remain essential for the protection of sensitive entity data and Protocol compliance.

10. A specific blockchain solution for an international blockchain registry under the Cape Town convention has been proposed by Dylus. The solution might also be viable under the Luxembourg protocol if the parties wishes so.

At a technical level, a standard such as ERC72116 would be used to 'tokenize' each registered asset, or to assign each asset a unique digital ID and function values to be transacted on the IR blockchain as a 'token' representing that asset.

The front-end user interface of the register need not to be complicated by a transition onto the blockchain, so that the users and site visitors could still search for assets by various combinations of name, model, or abbreviations thereof, or they could input an asset's specific blockchain address to locate the relevant token by which it is represented. When the asset token is found, the blockchain would disclose the set's current IR status along with its entire transactional history – all confidential information concerning the asset would be available only to permissioned entities, encrypted with the level of privacy and carrying any other attributes or data deemed acceptable by the Supervisory Authority. Creditors would be assured by their possession of their asset's token and blockchain security that the asset's registration status and thus their priority in interest would be incontrovertible until the next transaction event is validated. Furthermore, the blockchain's encrypted and decentralized method of information storage would provide added security for the IR, as well as reduce overhead, maintenance liabilities, and human error risks.

11. Albeit its straightforward implementation, there are some challenges for the implementation of the blockchain under the Luxembourg protocol.

i) Confidentiality of information: As per design, all transactions and all transaction information is visible to anyone on the blockchain. Although the transacting parties are pseudonymous and identified by public keys generated using mathematically derived algorithms, it remains possible to connect the identity of an individual with their public key. The turnaround is to only encode business non-sensitive information and introduce a proper management of public keys.

ii) Need for coordination: So called data fluidity is a prerequisite for an efficient application. It is facilitated by the use of standards and by a common IT architecture. The latter could be difficult to assure among all

parties involved under the Luxembourg protocol, but possible to overcome by limiting the number of parties on top of the central registrar.

iii) Implementation cost: Setting up the initial blockchain infrastructure is expensive and there are also maintenance costs involved. They could be effectively reduced by using an already proven application, by seeking synergies with other use cases (e.g. maritime and aviation transport equipment) and by using shared infrastructure with a low level of de-centralization.

III. Possible further steps

12. Validation of the use case: An inventory or issues encountered with the application of the Cape Town protocol represents a good starting point in understanding the weaknesses of the current centralized legacy system. This could be accompanied by a more specific potential risk inventory for railway application (e.g. due to the much higher number of parties involved).

13. Feasibility assessment: A proof-of concept might be necessary to demonstrate the feasibility of a blockchain application under the Luxembourg protocol. Several options should be assessed, notably a hybrid blockchain implementation alongside the fully fledged blockchain implementation. A more comprehensive analysis of challenges and opportunities, carried out in consultation with relevant external experts would provide further evidence for possible development.