Open access • Proceedings Article • DOI:10.1109/NTMS.2018.8328733

# Digitizing, Securing and Sharing Vehicles Life-cycle over a Consortium Blockchain: Lessons Learned — Source link

Kei-Léo Brousmiche, Thomas Heno, Christian Poulain, Antoine Dalmieres ...+1 more authors

**Institutions:** Institut de Recherche Technologique SystemX

**Published on:** 27 Feb 2018 - New Technologies, Mobility and Security

# Digitizing, Securing and Sharing Vehicles Life-cycle Over a Consortium Blockchain: Lessons Learned

Kei Brousmiche, Thomas Heno, Christian Poulain, Antoine Dalmieres, Elyes Ben Hamida

# Digitizing, Securing and Sharing Vehicles Life-cycle Over a Consortium Blockchain: Lessons Learned

Kei Leo Brousmiche*, Thomas Heno*†, Christian Poulain*†, Antoine Dalmieres*‡, Elyes Ben Hamida*
*IRT SystemX, Paris-Saclay, France, Email: {kei-leo.brousmiche, elyes.ben-hamida}@irt-systemx.fr
†Groupe PSA, Route de Gisy, 78140 Vélizy-Villacoublay, Email: {thomas.heno, christian.poulain}@mpsa.com
‡Covéa, 86-90 rue Saint Lazare 75009 Paris, France, Email: adalmieres@gmf.fr

***Abstract*—Nowadays, vehicles odometer fraud is becoming a growing problem internationally, and is costing European consumers between €5.6 to €9.6 billion per year. This is partly due to the lack of unified vehicles life-cycle management, and to the fact that vehicles data are currently spread across multiple stakeholders that do not trust each other or collaborate together. In this paper, we propose a Blockchain-backed Vehicles Data and Processes Ledger framework to streamline the management of vehicles life-cycle and data history, and hence to provide more transparency and collaborations between the involved stakeholders. The architecture and lessons learned from the first implementation phase are discussed, followed by future research challenges.**

## I. Introduction

Today's world is a world of data. As the information gets digitized, its use is multiplied across several distinct information systems that take it as a reference to provide value-added services. This directly implies a growing need to reconcile its value in a manner that can be trusted by all the involved stakeholders (*i.e.* consumers, producers). In this case, the information will even gain a much bigger value than when it was only accessible physically, its current observable aspect giving a very relative trust in its real nature.

The first obvious example for a vehicle is its mileage, which is the very first information that will impact its current value. On today's second-hand car market, the lack of trust is the main reason for devaluation. If a consumer wants to buy a vehicle from a private or professional entity, he/she may have serious doubts regarding the authenticity of the vehicle's maintenance history, displayed mileage or actual value/state. This is due to the fact that vehicles fraud (*e.g.* odometer frauds, wrecked or salvaged vehicles for sale, etc.) is currently becoming a growing problem internationally.

For instance, despite the introduction of digital odometers within modern vehicles, mileage fraud is currently affecting up to 30% of the used cars in Europe, costing the European consumers approximately €5.6 to €9.6 billion per year [1]. The vehicle's mileage is usually checked by authorized professionals during its regular maintenance or repair operations. These can be performed, either at the official car dealership networks or at any independent repair shops that will fulfill the warranty conditions.

Another example of vehicles fraud that has great economic and societal impacts concerns the *rolling wrecks*, *i.e.* vehicles that experienced severe damages and that have been declared as wrecks by an insurance expert, and hence that are no longer allowed to go on the roads. Nevertheless, some wreck vehicles are put back onto the second-hand car market, with the help of corrupt professionals. These *rolling wrecks* are often the cause of severe accidents, involving injured people, and costing insurance companies and consumers a lot of money.

Today, the only link between the involved stakeholders (*i.e.* consumers, automakers, repair shops, insurance companies, *etc.*) is typically a paper-based car log book which, in some situations, might be incomplete, corrupted or missing. In this context, new initiatives have been recently launched around the world (*e.g.* Germany [2], France [3], or Switzerland [4]) to digitize and secure the vehicles mileages using the *Blockchain technology* [5]; *i.e.* a tamper-proof, secure-by-design and decentralized ledger, and whose content is verified and validated by consensus of a majority of its participants. While the proposed approaches aim at minimizing the impact of vehicles frauds, they are still at an early stage of research, and several challenges still need to be addressed, including incentives mechanisms, governance, data privacy, scalability, and so on.

In this paper, we propose an innovative Blockchain-backed Vehicles Data and Processes Ledger framework to digitize the vehicles life-cycle over a consortium Blockchain [6], that enables the aforementioned stakeholders to collaborate through the secure sharing of vehicles data and maintenance history. Our main objective is to allow the secure sharing of some parts of the vehicles data and processes between stakeholders, that own them, and others that will exploit them to provide value-added services (*e.g.* vehicles mileages could be used for *pay-as-your-drive* insurance models or predictive maintenance). This represents the basic framework that will enable all an ecosystem of services to grow around the proposed framework.

The remainder of this paper is organized as follows. Section II will introduce the general context of this research work and will present the considered case study. Section III will describe the architecture and implementation of the proposed Vehicles Data and Processes Ledger framework. Section IV will analyze the key lessons learned during the first phase of the evaluation of the proof-of-concept, and will highlight the future research challenges and planned improvements. Finally, Section V will conclude the paper.

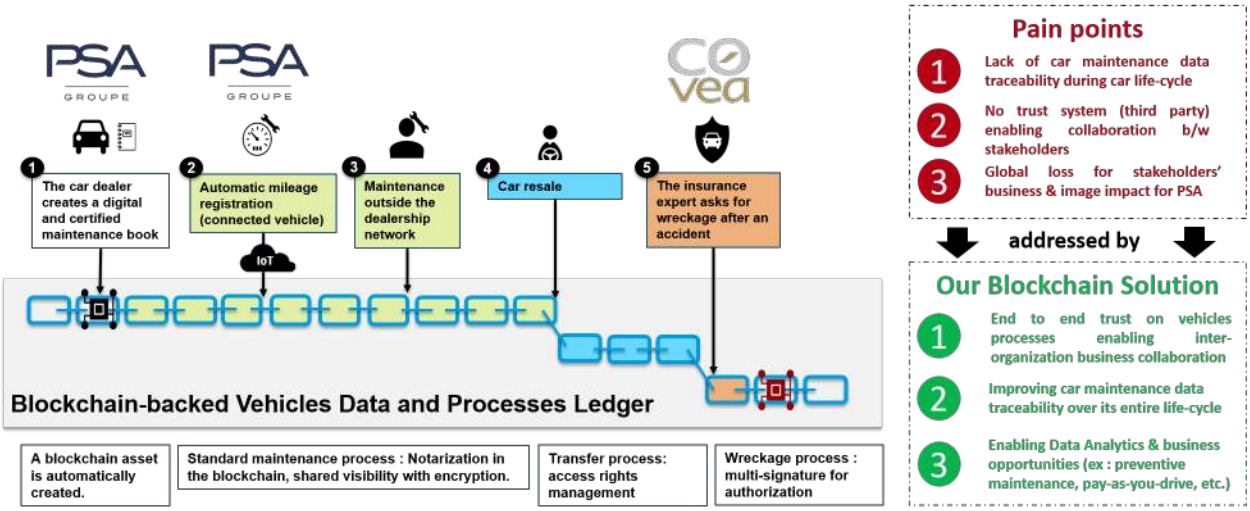


Fig. 1. Digitizing Vehicles Life-cycle over a Consortium Blockchain: Pain Points and Benefits of our Framework.

## II. Use case overview

The present research work is conducted within the scope of the *Blockchain for Smart Transactions* (BST) research project [7] that has been recently launched by IRT SystemX in partnerships with key industrial and academic partners, and whose main objective is to unlock the potential of Blockchain-based architectures by developing new usages based on human-centric data empowerment.

The first case study that has been addressed by the project was sparked by the need for innovative and viable technologies to address the challenges that are currently affecting the automotive industry, mainly: 1) the lack of collaborations and data sharing between the involved stakeholders; and 2) the lack of transparency and trust on used-car markets due to various types of frauds, as already discussed in the previous section.

In this context, we propose an innovative Blockchain-backed Vehicles Data and Processes Ledger to digitize the vehicles life-cycle over a consortium Blockchain. The initial stage of the developed Proof-of-Concept includes already major actors from the industry, including: 1) *PSA Group*: a leading French automotive manufacturer; 2) Covéa: a leading French mutual insurance company; and 3) Docapost: a leading provider of document management services (*i.e.* invoices, certificates, etc.). The integration of additional members is underway.

As shown in Figure 1, the benefits of our proposed framework is highlighted across five main steps of a typical vehicle life-cycle. During *step one*, when a consumer acquires a new vehicle, the automotive manufacturer (*e.g.* PSA Group) creates a new digital and secure car book on the consortium Blockchain, and whose access is initially restricted to only the actual car owner and the automotive manufacturer, including the members of its dealership network (*e.g.* official repair shops). Eventually, the car owner may grant an access to the secure car book to his insurance company (*e.g.* Covéa).

During *step two*, as modern vehicles already include sensing and communication capabilities, the current mileage of the vehicle is automatically transmitted to the carmaker's cloud infrastructure at regular intervals, and is written on the secure car book, at a reasonable frequency to attest the value of the vehicle.

During *step three*, the car owner may service or repair his vehicle within or outside the dealership network. In the first case, since the automotive manufacturer is already a member of the consortium Blockchain, and have already access to the secure car books, all vehicles operations and data (*e.g.* repair, maintenance, invoices, etc.) can thus be recorded on the Blockchain. In the second case, a consumer might also decide to select an *independent repair shop*, who is not an actual member of the consortium Blockchain, and hence grant him a temporary access to his secure car book. This independent repair shop will hence have access to the complete data history of vehicle and will be able to record new information and operations through the APIs that are exposed by the actual members of the consortium. Once the operations are done, the access to the secure car book is revoked, and the independent repair shop will not have access to any future information.

During *step four*, the car owner may decide to sell his vehicle on a used-car market. The interest that can be found in having this secure car book is then obvious. The current owner can prove the good maintenance state of his vehicle and certify its mileage and actual value, increasing thus transparency and trust with the potential buyers. We believe that this can help in minimizing the problem of odometer frauds and related costs. In this case, the current vehicle owner will transfer the ownership of his secure car book to the new owner.

Finally, during *step five*, in case of accidents, the insurance company, who has already access to the secure car books of its customers, will be able to better evaluate the damages on the vehicle and provide adequate compensations. The result of the insurance expertise will be permanently recorded to the secure car book. Depending on the severity of the damages, the insurance expertise could allow the vehicle to go again on the roads, or could declare the vehicle as a wreck. In this later case, the owner will thus transfer the property of his vehicle to his insurance company, who will take care of destroying the vehicle, limiting thus the frauds related to rolling wrecks.

## III. ARCHITECTURE

### A. General Architecture

The global architecture of the designed and implemented Blockchain-backed Vehicles Data and Processes Ledger comprises two main components, as highlighted in Figure 2 and discussed in the following sub-sections.

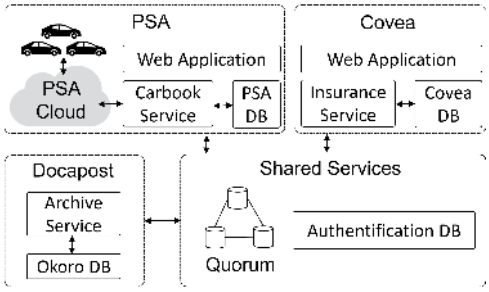


Fig. 2. General architecture

*1) Shared Services:* The consortium support a common infrastructure in order to share some core services.

*a) Quorum based Blockchain:* key component of this project, this Blockchain stores car maintenance log books, pseudonymized accounts information and their associated access rules. This technology derived from Ethereum enables to (1) control nodes access using a white list (*i.e.* consortium Blockchain), (2) validate blocks using Quorum Consensus [8] that do not requires mining and (3) handle private transactions using cryptographically secured channels. In this project, we use (1) to secure the access to the Blockchain and (2) in order to speed up the validation time. However, (3) is not used to manage privacy as it will be explained in sub-section III-B.

*b) Identity Database:* this database centralizes accounts information to authenticate users. It stores accounts names, passwords hashes, Blockchain keys and identifiers. Each services that needs to authenticate a given user will access this database (see sub-section III-B).

*2) Entities Services:* Each consortium member supports a server with a common architecture composed of three layers. The Blockchain connector that enables to access their Quorum nodes, a business services layer that handles business workflows coupled with a database and finally a web service layer that includes web interfaces to expose functionalities through the web. In order to access a functionality, web services first authenticate the user based on the shared identity database (see sub-section III-B). Once authenticated, an user is associated to a role that enables access to permissionned actions such as: create a car book (limited to the car maker), declare a vehicle as wreck (limited to car recyclers) and so on. This role-based permission is the first layer of our access control. In addition, once authenticated, users have access to their Blockchain keys enabling them to access on-chain functions through transactions (see sub-section III-B). As in every Blockchain, transactions are cryptographically signed and verified by the validators that constitute our second layer of access control. Lastly, a final layer secures on-chain reading access using a novel cryptographic protocol (see sub-section III-B). In the following sections we describe the services exposed by each entities of the consortium.

*a) Car Book Service:* supported by the car constructor, this service allows: the creation of accounts and car books, authenticate users, access on-chain data and its embodied database. An integrated data ingestion module writes automatically mileage into the on-chain car books. These data are provided by connected cars that push periodically their mileage to the car manufacturer's cloud service. The embodied database of the service layer stores meta data about its cars such as the brand, model name, the manufacture date. This service provides access to: car dealers, car owners and car repair shops. Dealers are able to create car books and associate them to car owners. Owners have access to their car books and are permitted to ask the writing of data called $record$ corresponding to a tuple $< mileage, label, date, document >$ where the $mileage$ is automatically retrieved from the connected car, the $label$ mentions the type of vehicle's operation (*e.g.* private maintenance), the $date$ is retrieved from the Blockchain's latest block's time stamp, and $document$ includes a pointer to a eventual document (*e.g.* a receipt) that is stored in external cloud archiving service (see sub-section III-A-c ). Owners have also the possibility to grant a temporary access to their car books to independent car repair shops (*i.e.* not affiliated with the car marker or not part of the members of the consortium). Once an access is granted, the independent car repair shop will be able to read and write into their customers' car books. These accesses are either manually revoked by the owner or automatically by the car book smart contract after a period of time (parameter of the system).

*b) Insurance Service:* provided by the car insurer, it proposes to car owners to insure their car based on their on-chain car books. Owners can insure their cars by tying their car books to an on-chain insurance smart contract. The insurer has full reading access to all their contractors car books. When opening a claim, an expert is mandated by the insurer, and which will be able to access the car book and write his diagnosis. Depending on the diagnosis, the insurer will take charge for repairs or propose the owner to redeem the broken car. The redeem takes place when the owner transfers the car book to the insurer, which can then sell it to recyclers.

*c) Cloud Archiving Service:* proposes to store and archive vehicles documents (*e.g.* invoices) into their secured and regulatory compliant databases. While archiving, the service also puts a transaction into the Blockchain with the hash of the document in order to prove its existence and to guarantee its authenticity.

### B. Vehicle data security and privacy

Multiple measures at different levels have been designed and implemented to limit the visibility of the data on Blockchain and to secure the data access to all car books (smart contracts).

*a) Blockchain access management:* As mentioned in previous sections, the Quorum-based Blockchain filters participating nodes using a predefined white list of members. It

is thus not possible to be part of the consortium without the agreement of its current members.

*b) Hybrid storage:* Our solution mixes classic database and Blockchain technology for storage. Data that have to be secured by the consortium are stored directly in the Blockchain using smart contracts. Other complementary data or member specific business data are stored in their local databases.

*c) Authentication:* While identity management is a central topic in a consortium system, we do not put emphasis on this problem in this work. Nevertheless, our services authenticate users based on a centralized, shared identity database before letting them access their data. Once an user identity has been verified based on his username and password knowledge, the service provides him a JSON Web token (JWT).

*d) Writing access:* Any writing access to a car book is cryptographically secured using Blockchain transactions. Only users that have access to their private key are able to sign their transaction. These signatures are then verified by smart contracts before executing any instructions.

*e) Reading access:* Data stored on a Blockchain are accessible to all its participants. This raises the problem of privacy within the consortium, indeed access to some strategic data have to be limited. For example, in this project, the car maker wants to limit the visibility of the $records$' labels to the car book's current owner and the actors that have bee explicitly authorized. We describe in the following section a novel hybrid cryptographic protocol to enable a fine grained data access over Blockchain.

*f) Hybrid cryptographic protocol:* While Quorum offers the possibility to send and share private transactions (*i.e.* data) among a subset of the Blockchain members, the list of the authorized members remains static. In other words, we cannot add or revoke a member's access to a data field in a transaction or in a smart contract. To tackle this limitation, we have implemented a novel protocol that enables the sharing of ciphered data and cryptographic keys over the Blockchain. In this protocol, each user is given an additional asymmetrical RSA key pair. Before writing a secret data $d$ on the Blockchain, the writer generates a symmetrical key $k$ and encrypts his data using AES. Once the ciphered data $cd$ is stored on the Blockchain, only the writer is able to decrypt it using $k$. In order to let another user $reader$ to decipher the data, the writer encrypts $k$ using the public key of $reader$ and publish the resulting cyphered key $ck^{reader}$ on the Blockchain (*i.e.* in a smart contract). The $reader$ retrieves the cyphered data and the cyphered key $ck^{reader}$, decrypts it to obtain $k$ using his private key and RSA. Finally, he decrypts $cd$ using $k$ with AES to obtain the clear data $d$.

The detailed description, validation and evaluation of the proposed security protocol is beyond the scope of this paper, and will be covered in a future article.

### C. Car maintenance log book smart contract

A number of smart contracts have been implemented in Solidity (*i.e.* a programming language proposed by Ethereum and supported by Quorum) to enable the afford-mentioned functionalities. In this section we focus on some specific features of the *CarBook* contract and its related contracts. The link between the *CarBook* smart contract and its corresponding car is done through the hash of the car's VIN (*i.e. Vehicle Identification Number*) written in a field of the contract. The use of the hash enables to anonymize the car identity over the Blockchain. Similarly, the ownership of a car book (*i.e.* the link between a car owner and the smart contract) is based on the Blockchain address of the owner that is generated at the time the account is created. Those two information are given by the car maker at the initialization of the contract. Also, in order to easily find the list of *CarBooks* that are owned by a user, we have put in place a *Registry* and *UserLibrary* contracts. The *UserLibrary* contains the list of *CarBooks* owned by a user, these contracts are themselves identified in the Registry contract. Using this latter contract, one is able to find a *UserLibrary* corresponding to a user address. The use of two contract instead of one contract that could have contained a mapping of addresses and lists of addresses is due to the limitation of the EVM (*i.e. Ethereum Virtual Machine*): structures, including maps, cannot store dynamic arrays. Each functions are protected by *modifiers* (*i.e.* Solidity functionality that checks some conditions before executing a function) that filter the transactions origin. Using them, we are able to control access according to the known addresses: *e.g.* functions limited to the owner, to the car maker, to the insurer if the owner subscribed to an insurance service. The format and content of new *records* is checked by the smart contract before storing them. Indeed, if the format does not match the expected pattern, the request is rejected. Also, the mileage of the record is checked so that it is not inferior to the last known value. To summarize, the usage of Smart Contracts for implementing *CarBooks* and its related functionalities guarantees the enforcement and sharing of common data model, processes and protocols over the consortium Blockchain.

## IV. Lessons learned and future challenges

### A. Lessons Learned

In comparison with traditional centralized architectures and databases, our Blockchain-backed Vehicle Data and Processes Ledger framework offers the following benefits.

*a) Collaborative architecture:* Based on an enterprise Blockchain technology, our solution enables the secured sharing of data, control and execution of workflows among the stakeholders without a central authority that would monopolize the power within the consortium.

*b) Shared data structure and workflows:* By modeling a car book and its life-cycle in the form of smart contracts, consortium members share a common, standardized data structure and workflows. This homogeneous environment facilitates collaborations between stakeholders and the development of new services based on common processes.

*c) Data and workflow security:* By inheriting the security level of the Blockchain, data stored in car books along with their processes are secured by design, thus preventing odometer fraud or *rolling wrecks*. Indeed, CarBook smart

contracts filter the writers and do not accept any request whose cryptographic signature does not match with an authorized Blockchain account. Moreover, the ledger being duplicated in each stakeholder server, car book data are tamper proof as long as attackers do not hack more than the half of the total consortium servers or identities.

*d) Data privacy:* Users identities as well as vehicles identifiers (*i.e.* VINs) are stored in separate databases, private to each stakeholder, in order to preserve data privacy. As for on-chain data, in order to limit the visibility of strategic information within consortium members, we have put in place a hybrid cryptographic protocol that enables the sharing of secrets and cyphering keys over smart contracts.

*e) Openness to additional services:* While the current implementation of the solution is limited to three stakeholders proposing their own services, our architecture is easily expendable to integrate additional members with complementary services based on the existing data. These extensions can be implemented without the need to develop data adapters that traditional databases usually require to ensure compatibility: data models in the Blockchain are shared among the consortium.

### B. Perspectives

We discuss hereafter the main challenges that still need to be investigated to accelerate the adoption and mass-market deployment of the proposed framework.

*a) Business model and incentives:* Business model is not shared between actors: the behavior of a car book is defined, but a consortium member is free to define its own business value above the blockchain using its web application. The consortium has to define a billing and cost sharing protocol based on read, write and mining operations on the Blockchain. As read operations are free on the ledger, billing on read operations is not possible, but authorized readers are identified via generations of keys. Thus, it would be possible for instance to put in place a data market place where each access to a strategic data is charged by its owner.

*b) Decentralized user authentication and identity management:* Current implementation use a unique database holding identities and Blockchain identifiers. This solution is not realistic in production environments where each web application has potentially its own set of user accounts. One possible way to tackle this issue would be to use smart contract representing a user and federating the created accounts on the different web applications. In that case, car books would use addresses of these smart contracts, instead of Blockchain identifiers of the users' accounts.

*c) Volume and transaction rate:* In case of mass adoption, transaction volume and rate would increase tremendously. A potential solution to scale our architecture would be to exploit the concept of *sharding*, often used is standard databases. As native Blockchain sharding mechanism is not yet implemented on Ethereum, a use-case specific sharding method based on substrings of VIN (*e.g.* year, serial number, etc.) or the hash of VIN could be used to choose one Blockchain among several instances. To prevent inserting a car book in a wrong Blockchain, a genesis block containing the sharding rules and smart contracts could check the request.

*d) Car book versioning:* Updating the behavior and version of a *CarBook* smart contract is mandatory in production environments (*e.g.* bug fixing, consortium membership evolution, new business model, etc.). Techniques exist to implement such functionalities. For instance, a proxy smart contract pointing to the right version of the actual *CarBook* smart contract could be designed.

*e) Regulatory compliance:* Immutability is a key concept in Blockchain, where data is persisted forever. However, with the emergence of new regulations, such as the *General Data Protection Regulation* (GDPR), the right to be forgotten or the portability of users' data should be guaranteed. Advantageously, in the case of consortium Blockchain, such as Quorum, it is theoretically possible to modify the past transactions with the consent of all its members [6].

## V. Conclusions

In this paper, we proposed a novel Vehicles Data and Processes Ledger framework to secure and automate vehicles lifecycle over a consortium Blockchain. The proposed framework aims at fostering data sharing and collaborations between the stakeholders in the automotive industry. The main objective is to increase transparency and trust on the used-car markets, which are currently affected by various types of frauds, such as odometers frauds. The lessons learned from the developed proof-of-concept have been discussed, and several research and technical challenges have been highlighted.

## Acknowledgment

This research work has been carried out under the leadership of the Institute for Technological Research SystemX, and therefore granted with public funds within the scope of the French Program Investissements d'Avenir.

## References

[1] T. Willemarck, H. Graafland, C. Gonderinger, J. Cobbaut, B. Lycke, J. Hakkenberg, and M. Peelman, "Protect european consumers against odometer manipulation," October 2014, accessed: 2017-11-13. [Online]. Available: goo.gl/CnQuYg

[2] Bosch and TUV Rheinland, "A solution for odometer fraud," July 2017, accessed: 2017-11-13. [Online]. Available: http://goo.gl/XPJQHV

[3] Renault, "Groupe renault teams with microsoft and viseo to create the first-ever digital car maintenance book prototype," July 2017, accessed: 2017-11-13. [Online]. Available: http://goo.gl/YxTtye

[4] ICT Journal, "La blockchain pour retracer l'historique complet des voitures," October 2017. [Online]. Available: goo.gl/Mx4wVb

[5] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[6] E. Ben Hamida, K. L. Brousmiche, H. Levard, and E. Thea, "Blockchain for Enterprise: Overview, Opportunities and Challenges," in *The Thirteenth International Conference on Wireless and Mobile Communications (ICWMC 2017)*, Nice, France, Jul. 2017.

[7] IRT SystemX, "Blockchain for smart transactions (bst) research project," accessed: 2017-11-13. [Online]. Available: http://www.irt-systemx.fr/en/project/bst/

[8] "GitHub - jpmorganchase/quorum: A permissioned implementation of Ethereum supporting data privacy," accessed: 2017-10-20. [Online]. Available: https://github.com/jpmorganchase/quorum