Avrupa Bilim ve Teknoloji Dergisi
Sayı 21, S. 473-485, Ocak 2021

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
No. 21, pp. 473-485, January 2021

Research Article

Towards Adoption of Blockchain Technology for Enhancing Communication in Smart Transportation

Busra Ozdenizci Kose[1*]

[1*] Gebze Technical University, Faculty of Business Administration, Departmant of Management, Kocaeli, Turkey, (ORCID: 0000-0002-8414-5252), busraozdenizci@gtu.edu.tr

(First received 8 November 2020 and in final form 26 January 2021)

(**DOI:** 10.31590/ejosat.823102)

ATIF/REFERENCE: Ozdenizci Kose, B. (2021). Towards Adoption of Blockchain Technology for Enhancing Communication in Smart Transportation. *European Journal of Science and Technology*, (21), 473-485.

Abstract

Today, IoT (Internet of Things) revolution and V2X (Vehicle-to-Everything) paradigm are collaboratively making a deep impact on a wide range of industrial areas, especially on transportation and automotive industry. Efficient and value added business models are highly appreciated to revolutionize transportation services and environments over the world; and to establish autonomous transport systems without the need of minimum possible human intervention. On the other hand; currently transportation ecosystem stakeholders are facing some problems including data integrity, non-repudiation, and trust. Data manipulation, missing information, and inconsistencies are examples of serious problems in the context of automated mobility and heterogeneity. This study aims to explore the potential of Blockchain technology in smart transportation. In this context, a communication model is presented for smart transportation ecosystems that provides solutions to problems, and also ensures data integrity, non-repudiation and trust by utilizing Blockchain technology. The proposed smart contract based model allows trustless users to negotiate on immutable and transparent data without the need for a trusted third party which can provide further innovative services. The proposed model is evaluated in aspects of appropriateness of technology, technical features, and adoption and diffusion of technology. Taking all this into account, it is possible to point out that the proposed model, not only have the potential of supporting development of V2X and smart transportation ecosystems, but also is feasible to other various smart environments having high heterogeneity and mobility.

Keywords: Blockchain; Communication; Heterogeneity; Mobility; Smart Transportation; Adoption of Technology.

Akıllı Ulaşımda İletişimin Geliştirilmesi için Blockchain Teknolojisinin Benimsenmesi

Öz

Günümüzde IoT (Nesnelerin İnterneti) devrimi ve V2X (Vehicle-to-Everything) paradigması, özellikle ulaşım ve otomotiv endüstrisi olmak üzere, çeşitli endüstriyel alanlar üzerinde işbirliği içinde derin bir etki yaratmaktadır. Verimli ve katma değerli iş modelleri, ulaştırma hizmetlerinde dünya çapında devrim yaratmak ve insan müdahalesine ihtiyaç duymadan otonom ulaşım sistemleri kurmak için büyük ilgi görmektedir. Diğer yandan; şu anda ulaşım ekosistemi paydaşları hareketlilik ve heterojenlik bağlamında veri bütünlüğü, inkar etmeme ve güven gibi bazı sorunlarla karşı karşıyadır. Veri manipülasyonu, eksik bilgiler ve tutarsızlıklar ciddi sorunlara örnektir. Bu çalışma, akıllı ulaşımda Blockchain teknolojisinin potansiyelini keşfetmeyi amaçlamaktadır. Bu bağlamda, akıllı ulaşım ekosistemleri için olası sorunlara çözümler sağlayacak ve aynı zamanda Blockchain teknolojisini kullanarak veri bütünlüğü, inkar etmeme ve güven sağlayacak bir iletişim modeli sunulmaktadır. Önerilen akıllı sözleşme tabanlı model ile, birbirine güvenmeyen kullanıcıların, güvenilir bir üçüncü tarafa ihtiyaç duymadan daha fazla yenilikçi hizmetler sağlayabilecek, değişmez ve şeffaf veriler üzerinde pazarlık yapmasına olanak tanımaktadır. Model teknolojinin uygunluğu, teknik özellikleri, teknolojinin benimsenmesi ve yayılması yönlerinde değerlendirilmiştir. Tüm bunları hesaba katarak, önerilen modelin sadece V2X ve akıllı ulaşım ekosistemlerinin gelişimini destekleme potansiyeline sahip olmadığını, aynı zamanda yüksek heterojenliğe ve hareketliliğe sahip diğer çeşitli akıllı ortamlar için de uygulanabilir olduğunu belirtmek mümkündür.
Anahtar Kelimeler: Blockchain; İletişim; Heterojenlik; Hareketlilik; Akıllı Ulaşım; Teknolojinin Benimsenmesi.

[*] Corresponding Author: busraozdenizci@gtu.edu.tr

1. Introduction

IoT (Internet of Things) can be described as a network of smart devices those have embedded technologies such as sensors and actuators in order to sense and collect data, communicate with each other, integrate and exchange data, and therewithal be remotely accessible over Internet (Atzori et al., 2010; Al-Fuqaha et al., 2015). IoT refashions telecommunication paradigm through providing connection between the physical world and machine-based systems, and also allows people to integrate with value adding technologies and processes. With the help of various enabling wireless and wired technologies, significant number of physical objects are connected to the Internet and plays a remarkable role in various application areas with innovative solutions including -but not limited to- smart home, smart infrastructure, energy management, transportation, supply chain management, logistics, healthcare, social applications and many others (Gubbi et al., 2013; Lee and Lee, 2015). Billions of heterogeneous, distributed, and intelligent devices connected to the Internet will proceed to provide new service opportunities and generate valuable smart environments -like homes, buildings, companies, schools, and many other establishments- with the purpose of monitoring and control, data analytics, and information sharing with collaboration (Whitmore et al., 2015; Li et al., 2015).

Today, IoT revolution is making a deep impact on automotive and transportation industry. Both researchers and practitioners are investigating on how to revolutionize transportation services; how to establish intelligent transport systems without much need of human intervention; and how to advance V2X (Vehicle-to-Everything) communication models. V2X is a novel paradigm which stands for interconnected vehicles, pedestrians, and infrastructures that collects and exchanges real time information about the environment via wireless communication technologies (Chen et al., 2017). GSMA (GSM Association) highlights that connected car market -as a main component of V2X paradigm- is one of the highest growth areas of the IoT, with a potential application revenue (GSMA, 2019). Recent cellular technologies provide valuable features for the advancement of V2X which are high speed, low latency and wide area connectivity. With the intensive usage of 4G-5G technologies, V2X started to gain great importance including a set of technologies that allow vehicles to communicate with each other and also with other smart transportation solutions (GSMA, 2020).

In order to achieve full coverage, mobility, availability, and continuity of various smart transportation services, V2X systems including connected cars are utilizing innovative hardware and software technological developments. GSMA -as one of the important organization in this context- is currently working with Mobile Network Operators (MNO), automotive Original Equipment Manufacturers (OEMs), suppliers, industry associations, and regulatory bodies to accelerate the growth of the connected car and also V2X market by agreeing a common approach to security and infrastructure solutions (GSMA, 2020). One of the recent popular advancement is the use of secure smart car kit including a UICC (Universal Integrated Circuit Card) based secure element (SE) or SIM card based SE infrastructure to enable Over the Air (OTA) connection via cellular network (Turkcell, 2020). In that specific example, smart car kit provided by a MNO is attached on a vehicle. It allows to create a secure connection with the vehicle, aggregates various sensor data (i.e., IoT data) on vehicle, and transfer data to third parties with the aim of providing value-added services and more pleasant, safe driving conditions. Vehicle’s status can be tracked and monitored, which provides safety alerts –such as increase in engine temperature or low battery voltage of the car- and special value-added services like emergency, first aid, health, fire and so on. Another advancement, being embedded LTE (Long Term Evolution) solutions, are considered as next generation opportunity for V2X industry (Gemalto, 2020). A virtual embedded SIM card, namely eSIM, could be soldered in a device and then programmed to remotely connect the device to a chosen network carrier. eSIMs enable remote subscription management over the air to vehicles with an MNO of user’s choice. With the support of high-speed and low latency connectivity, eSIM technology on vehicles can provide advanced driving experiences for both drivers and passengers (Gemalto, 2020). Examples for these experiences are real-time navigation, telematics, insurance services, breakdown services, emergency functions, remote diagnostics, secure ID-based ignition, integrated NFC (Near Field Communication) and mobile wallet applications.

All these technological developments enable the collection and exchange of vast amount of user data. On the other hand, this expanding vision brings some challenging issues that should be handled in the context of smart transportation. Stakeholders of transportation ecosystem (e.g., police agencies, medical agencies, repair and maintenance companies, insurance companies, rental companies etc.) generally prefer to use their own proprietary data management platforms. Data sharing among diverse platforms can create inconsistencies and even repudiation problems. For instance, in case of a traffic accident, accurate data collection -such as vehicle speed, engine temperature, seat belt usage state, and timestamp information- from sensors of a connected car would be beneficial for all stakeholders The integrity of such data is critical to provide proper emergency services as well as insurance services accurately and timely. In a possible accident, it is important that the driver could not deny the fact of over speed driving or hide any improper crucial activity caused by herself. Furthermore, in context of IoT environments, monitoring activities of the user such as location or driving behavior brings security and privacy issues. Unauthorized, malicious third party activities may try to intercept and utilize sensitive user data as well (SIM Alliance, 2017). Data manipulation, information loss, inconsistencies, and spoofing are serious problems in the environments of increasing automated mobility and heterogeneity. Therefore, establishment of a sustainable communication opportunity is highly required for smart transportation ecosystem; where all stakeholders trust each other, all stakeholders are authenticated on a private network and where all authorized stakeholders benefit from each other’s sensitive data to provide value-added services.

This study aims to present a comprehensive communication model for smart transportation ecosystem having high heterogeneity and mobility. The model ensures particularly data integrity, non-repudiation and trust among the stakeholders by utilizing Blockchain as a promising technology. In research context, Blockchain technology has a significant opportunity for allowing trustless users to negotiate on inconvertible data -without the need for a trusted third party- and making it possible to record events -or facts- in a way that cannot be rewinded. The proposed Blockchain based model offers value-added services for the development of sustainable intelligent transportation ecosystem.

The structure of the paper is as follows: Section 2 presents the research background including challenging issues of smart environments, essentials of Blockchain technology, and use of Blockchain in smart transportation. Section 3 presents our proposal as the Blockchain based business model with system design considerations and business model examples -particularly car rental and car accident cases based usage scenarios- in order to embody the proposed model. Section 4 evaluates and discusses the proposed Blockchain based communication model in aspects of appropriateness of Blockchain technology for smart transportation; technical features and considerations; adoption and diffusion of innovation. Finally, Section 5 concludes and presents future research directions.

2. Material and Method

In this section we present recent challenging issues of smart environments, related work on Blockchain technology with its technical infrastructure, and use of Blockchain technology in smart transportation environment.

2.1. Heterogeneity and Mobility

IoT is the concept of connected things and people in order to sense, collect, and share data about the way they are used and about the environment around them (Ashton, 2009; Clark, 2016). IoT expands the concept of machine to machine (M2M) communication to intelligent communication which can be conducted between human and machine as well as between machine and machine. IoT systems are able to connect billions of heterogeneous devices and create smart environments with various applications that touches almost every daily life activity.

Smart environments are also facing some challenges (Hameed et al., 2019; Silva et al., 2018; Zhang et al., 2014; Singh et al., 2014) which need full attention from researchers and practitioners. One considerable issue is that smart environment allows to interconnect billions or even trillions of heterogeneous objects through the Internet (Elkhodr et al., 2016; Jabbar et al., 2017). Heterogeneity and large-scale networks are critical factors that distinguish the security of IoT from the security issues of traditional networks. Interoperability of all different devices and platforms is essential for enabling security and guaranteeing trust over the network (Atzori et al., 2010). At the same time, these heterogeneous devices generate and transfer massive volume of data in almost all IoT systems; smart home, smart transportation, smart city, connected cars, smart health. During this exchange, secure storage of data, protection of sensitive user behaviour and interaction data, and also powerful processing is required. In fact, the study of Zhang et al. (2014) identifies some valuable requirements for the security of smart environments and IoT systems. These are object identification, authentication and authorization, privacy, lightweight cryptosystems and security protocols, software vulnerability and malware.

As mentioned, smart transportation and V2X systems including connected cars are gaining great attention from practitioners. Smart transportation environments will enhance with the integration of cellular communication; especially with the 4G-5G technologies (Lee et al., 2017). It is clear that the technologies like eSIM, virtual SIMs technologies will have deep impact on connected car evolution and continue to be paved the way for new opportunities and value added transportation services. In addition to high heterogeneity and scalability concerns, high mobility of things in smart transportation environment requires more secure and efficient data exchange between various entities, protection of sensitive data, data integrity, non-repudiation and authenticity (Lei et al., 2017; Gemalto, 2020).

2.2. Essentials of Blockchain Technology

Blockchain technology comes to scene after the introduction of Bitcoin cryptocurrency by Satoshi Nakamoto –which is a nickname- in 2008 (Nakamoto, 2008). Blockchain provides decentralized data storage network with a tamper-resistant shared ledger including chained blocks in distributed networks (Casino et al., 2019; Shin, 2019; Wang et al., 2019); which can record and secure transactions using cryptography between two or more parties efficiently and in a verifiable and permanent way (Zheng et al., 2017). It allows trustless users agree on an immutable and irreversible data without the need of a trusted third party as a referee. These key features enable Blockchain technology receive extensive attention from various fields such as finance, health, government and public sector.

Figure 1 illustrates a sample Blockchain template (Zheng et al., 2018; Fernández-Caramés and Fraga-Lamas, 2018; Panarello et al., 2018). Blockchain is a list of blocks linked together using -mainly- cryptographic hash functions. Each block contains hash of its previous block that allows users to agree on undeniable and immutable data. The first block in the chain is named as Genesis Block. A block consists of a block header and a block body. In addition to hash value of parent (next) block, the block header has other fields such as block version, timestamp, nonce etc. The block body has also a counter indicating the number of transactions generated so far. Each one of these blocks can be described as a container that holds information related to specific transactions, such as the financial transactions. As new transactions are created, the list keeps growing subsequently. Transactions are created by entities (called as nodes) within the network. Once a transaction is created by a node, the transaction is broadcasted by that node to all other nodes. The transaction is validated by miner nodes in the network before being accepted by other nodes and thereafter being added to the chain.

Blockchain technology integrates several core technologies such as cryptographic hash, digital signature, and distributed consensus mechanism (Zheng et al., 2018; Fernández-Caramés and Fraga-Lamas, 2018). Consensus algorithm is the most significant component of Blockchain in order to reach an agreement between untrustworthy nodes which is considered as the transformation of Byzantine Generals (BG) Problem (Zheng et al., 2018). PoW (Proof-of-Work) is the original consensus algorithm and the most commonly used algorithm in order to confirm transactions and create new blocks on the chain. Bitcoin and Ether are the two most famous cryptocurrencies using PoW. The algorithm used over the network ensure that shared ledger in different nodes are consistent with each other (Zheng et al., 2018; Fernández-Caramés and Fraga-Lamas, 2018).

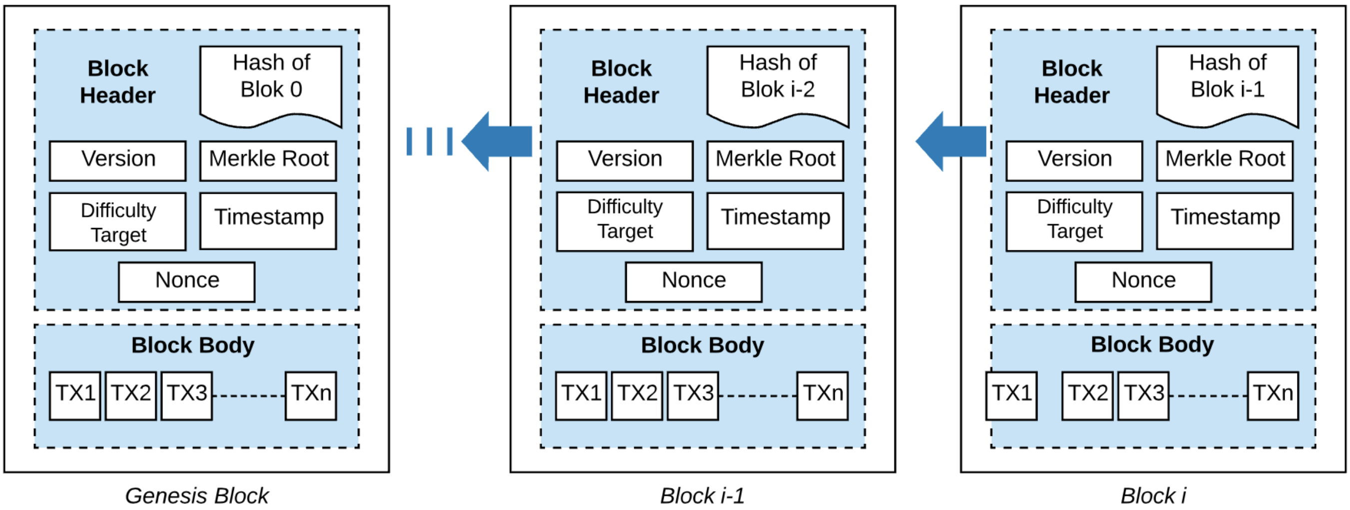


Figure 1. Blockchain Structure (Panarello et al., 2018; Zheng et al., 2018)

Another essential component of Blockchain is smart contract which is defined as a crypto economically secured execution of code (Wang et al., 2019); a code fragment is executed by the miners automatically (Zheng et al., 2017); a self-operating computer program (Nguyen et al., 2019). Without intervention of any third parties, smart contract self-executes the contractual statements and defined rules as codes independently on every node in the Blockchain network. Several projects such as Ethereum and Bitcoin implemented smart contract. Since all actions are recorded and verified in the decentralized ledger of Blockchain, smart contract provides real-time auditing services and also undeniable transactions (Macrinici et al., 2018; Wang et al., 2019; Nguyen et al., 2019). In terms of IoT, use of smart contracts helps to translate various and assets into virtual identities in Blockchain, and allows them to interact with other assets automatically with defined rules in trackable, auditable and undeniable manner.

Blockchain networks can be classified into three categories; public, consortium, and private Blockchains (Zheng et al., 2018). In public Blockchain -such as Bitcoin-, anyone can join the network and all records are visible to the public. Most Blockchain platforms are public systems; Bitcoin and Ethereum are two most famous public Blockchain examples. In private Blockchain though, write permissions are kept centralized to one organization; whereas read permissions can be public or restricted to a specific level. In consortium Blockchain, only a pre-defined set of nodes are allowed to join the network. Hyperledger is a popular consortium platform that is mostly used in developing business Blockchain frameworks; Ethereum is yet another example. In case of private Blockchain systems, there are also various companies implementing private networks for efficiency and auditability (Zheng et al., 2018; Fernández-Caramés and Fraga-Lamas, 2018).

2.3. Blockchain in Smart Transportation

Blockchain is a revolutionary distributed ledger technology which provides decentralized and transparent data management in an auditable, immutable and irreversible manner based on consensus among different parties. Blockchain is used or being though as a solution in various fields of IoT (Kshetri, 2017) - such as government, energy, financial transaction, transportation, fleet monitoring and management, smart cities, healthcare, farming, defense and public safety, logistics and more- with the aim of secure IoT data transfer and storage (Panarello et al., 2018), data exchange with access control policies among connected things as cars (Alsadi et al., 2019a; Alsadi et al., 2019b), identity management and authentication (Shafagh et al., 2017; Pinno et al., 2017; Nuss et al., 2018; Hammi et al., 2018), monitoring IoT assets (Ouaddah et al., 2016), time stamping and similar high security related services to enhance trust between IoT entities (Fernández-Caramés and Fraga-Lamas, 2018).

Currently, the potential of Blockchain technology is an emerging research area for transportation ecosystems (Yuan and Wang, 2016; Leiding et al., 2016; Lei et al., 2017; Alsadi et al., 2019b). Lei et al. (2017) highlights the challenging issues of heterogeneity of wireless network and emphasizes on the necessity of timely delivery of cryptographic materials in Vehicular Communication Systems (VCS) in order to provide safer and intelligent transportation environment including entities of vehicles, infrastructures and roads. The study presents an optimized Blockchain based model on “dynamic key management” for intelligent transportation systems in order to handle challenges of high mobility, large volume, and frequent handoffs of vehicular nodes in intelligent transportation systems. The study compares the performance of proposed Blockchain based key management model with traditional network models; results with performance optimization in secure key transfer; shortens the key transfer time among mobile nodes.

Another study by Yuan and Wang (2016) highlights that Blockchain can be utilized to establish a secured and decentralized autonomous intelligent transportation systems (ITS) ecosystem. A seven layer conceptual model for blockchain is proposed and a preliminary study on the potential of Blockchain in transportation research is conducted. The study of Singh and Kim (2017) proposes an intelligent vehicle data sharing framework between vehicles without interfering or disturbing other intelligent vehicles by using Blockchain technology. Vehicles are connected with Blockchain and store a unique crypto number. During communication, this crypto number is attached to message format and then message is transmitted to build trust and reliable peer-to-peer data sharing among intelligent vehicles.

In terms of business model perspective, the study of Leiding et al. (2016) proposes a preliminary model of self-managed, Ethereum Blockchain based vehicular ad-hoc network (VANET). The presented concept aims to provide transparent and self-regulating smart contracts based system without a central managing authority; and proposes use of some applications - traffic regulation, vehicle tax, vehicle insurance, traffic jams and weather forecasts notification- with the help of self-managed VANET. Another relevant business model study, Li et al. (2018) implements Blockchain technology on transportation insurance use case through a prototype in order to establish a trustable ecosystem among drivers, transport operators and insurance companies. Data about drivers and vehicle usage -which are extracted from IoT data that are collected from car sensors- are saved on an immutable, traceable, transparent distributed ledger; and with the IoT data analytics module, insurance premium is assessed which promotes fairness among drivers and encourages safer driving style.

Recent studies on use of Blockchain in context of smart transportation generally presents proprietary data management solutions among vehicles in order to handle heterogeneity and mobility issues, or to support a specific business domain of applications. A comprehensive Blockchain based framework for smart transportation ecosystem is highly required that handles aforementioned problems with a wider interaction model among various stakeholders. This study aims to fill this gap by presenting a trustworthy Blockchain based communication model, and ensuring data integrity and non-repudiation.

3. Proposed Model

The proposed communication model benefits from Blockchain technology with ‘self-regulating smart contracts’ to handle issues of data manipulation, missing information, inconsistencies, repudiation, and consensus problems among stakeholders in the context of automated mobility and heterogeneity. With the Blockchain utilization in smart transportation ecosystem, the following contributions are provided and presented in this study:

- A communication design over Blockchain network is introduced for establishing trust among various entities in smart transportation ecosystem,
- A smart contract based communication on an Ethereum Blockchain platform is designed and two business scenarios are implemented with a preliminary prototype,
- Evaluation of proposed model is performed in terms of appropriateness of Blockchain in this context, technical features, and diffusion of innovation; further design science issues and improvements are also assessed for transportation ecosystem.

3.1. Design Considerations

A typical transportation environment includes various stakeholders -drivers, insurance companies, medical agencies, police agencies, rental companies, repair companies and more- who are dealing with several interrelated effort-based tasks and operations. Today, connected cars are also considered as a significant stakeholder with the advances in intelligent transportation systems. In addition to effort-based services of human actors, with the support of innovative embedded hardware or software technologies on cars, various sensitive sensor data (such as accident notification, safety belt usage state, speed value, location, driver behavior and more) can be automatically produced. This collected valuable data can be used for supporting effort-based services of all stakeholders and providing new transportation services.

Efficient and secure communication among all stakeholders can promote value added services -such as emergency, maintenance, and insurance services- and can enrich the capabilities of governmental organizations and citizens. To ensure efficient and secure data sharing, the proposed model benefits from Blockchain network infrastructure where each stakeholder becomes a node that can provide various data in the form of transactions into the Blockchain network as shown in Figure 2.

The transactions generated by the nodes are stored on the Blockchain network in a distributed and shared manner. Various kinds of interrelated transactions regarding nodes’ requirements can be generated on the network. In order to embody, some examples of the nodes (i.e., stakeholders) with potential usage areas are emphasized as follows:

- Node of Drivers represents the registered users of cars; personal information and identity details of drivers should be transferred and stored on the Blockchain network.
- Node of Smart Cars represents the connected cars which have necessary embedded technologies and capabilities that provide sensitive sensor data –such as OBD (on-board diagnostics) data, GPS (location) data, start and end time of trip, collision data, maximum speed during the trip, safety belt usage, and similar data- to the Blockchain network.
- Node of Insurance Companies provides data about the insured vehicles and their policy details to the Blockchain network for the use of other nodes (i.e., entities like police, medical etc.) in case of emergency or maintenance conditions.
- Node of Repair (Maintenance) Companies transfers required data in case of supporting an accident situation (e.g., operations of a tow truck for the related car, examination of the car), or in case of a troubleshooting or technical problem of the smart car. This actor transfers data about the solution related to vehicle problem to the Blockchain network. Similarly, other actors (e.g., an insurance company) may monitor the securely stored data on Blockchain network.
- Other entities (such as police departments, medical agencies, gas station firms, rental companies) can also join the proposed model as a node. In this case they can generate critical data about transportation environment. For example, a rental company or a policeman may monitor the securely stored data on Blockchain network in case of emergency condition. Authorized and registered nodes are able to make use of validated and approved secure data by all entities on Blockchain network in order to promote safer and efficient transportation and value added services.

A consortium type of Ethereum Blockchain (https://ethereum.org) network infrastructure among stakeholders is proposed for system design and implementation which is suitable for establishing the corresponding smart transportation environment. It allows for authorized entities to participate in the consensus process, but network ownership belongs to multiple entities instead of a centralized authority.

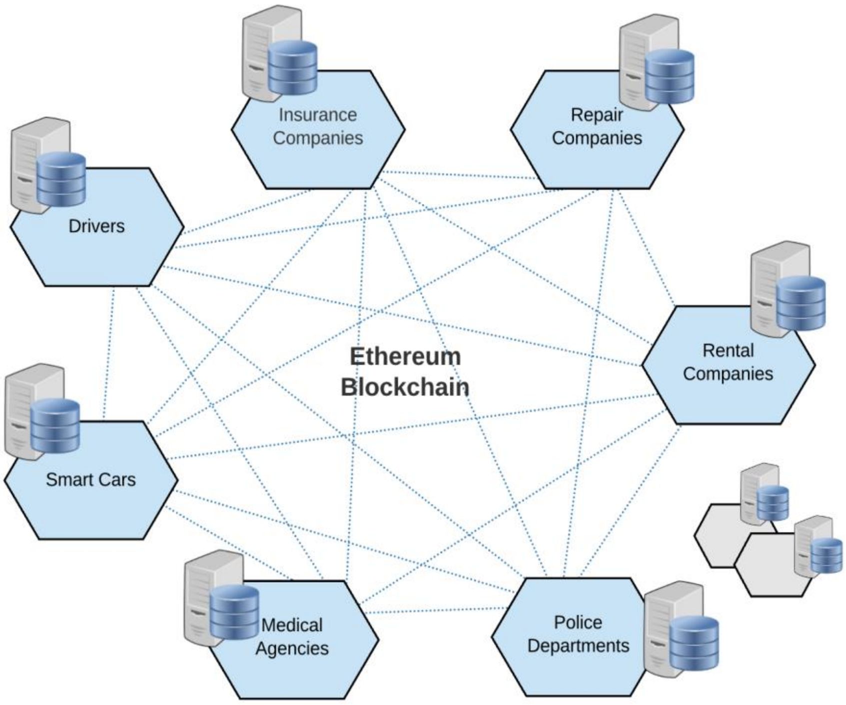


Figure 2. Adopting Blockchain into Smart Transportation Ecosystem

In order to realize preliminary functionality of the proposed model, Ganache-Truffle (https://www.trufflesuite.com/ganache) framework is used to provide an in-memory Ethereum node (which means that records will be deleted once Ganache platform is closed) as shown in Figure 3. Ganache framework allows to develop Ethereum Blockchain networks for deploying smart contracts with advanced mining controls, run tests, execution commands, and other actions on the chain without any cost. Ganache framework is widely used by developers during testing smart contracts, request processing scenarios, and monitoring the changes on Blockchain. The interface allows to reach the details about not only nodes, but also the blocks and transactions. All data is stored on a local database server used by each node during system implementation.

In order to interact on Ethereum Blockchain network, each user needs to register to the system by creating an account in related node (e.g., driver, car, insurance company, policy agency etc.). After registration, a unique address for each account is created to allow data sharing within the network layer; and also a private key and a public key pair is created for each account in the node. Every transaction made by nodes is transferred to the network with the use of web3js (i.e., a JavaScript library). All securely stored data on the Blockchain network is also displayed in the same manner. The validity of a new transaction is determined and confirmed by miner nodes. PoW (Proof of Work) algorithm is used by miner nodes to verify signed transactions to achieve a secure, tamper-resistant consensus among all stakeholders.

As self-executing codes with various functions and predefined rules, smart contracts are developed to realize value added transportation services such as report accident, rent car, driving behavior record, car insurance status detection and more. The code including contractual statement is distributed on Ethereum Blockchain network which manages data exchange, requests and consensus among transportation stakeholders. Functions in the smart contract are triggered by a new transaction that is sent from an account. Smart contracts of some scenarios are developed by Solidity programming language on Truffle (https://www.trufflesuite.com/ganache) platform in proposed system. Truffle represents the developer environment that allows to build applications, manage smart contracts, and perform necessary configurations, and also allows efficient deployment and testing.

The application layer of proposed model represents cars, users, insurance companies, automotive repair services and all other actors of the system. The actors can communicate with the Blockchain network using smart contracts by a web-based application –called as distributed application (DApp). The developed DApp includes two parts: front-end as web client application, and back-end as server application which includes smart contracts that runs on Blockchain network. In the proposed system design, HTML5 and JavaScript language are used for developing the front-end application; and lite-server (lightweight development web server) is used for the back-end application. In order to access Ethereum Blockchain network, network settings (including network name, host name, port number and other details) as shown in Figure 3 are firstly defined in DApp. Actors can initiate data sharing (uploading or requesting) operations via DApp and accomplish operations with the help of self-regulating smart contracts on distributed ledger.

3.2. Use Cases

The proposed model is considered through business case examples including secure data uploading and transfer over Blockchain network. In order to explain easy-to-understand usage of proposed model for smart transportation environment, Rent Car Report Accident scenarios are used. Both scenarios are presented here to clarify the usage of the proposed model for smart transportation environment. Both cases highlight the necessity of efficient consensus among entities and also the necessity of transparent communication for providing valuable further services.

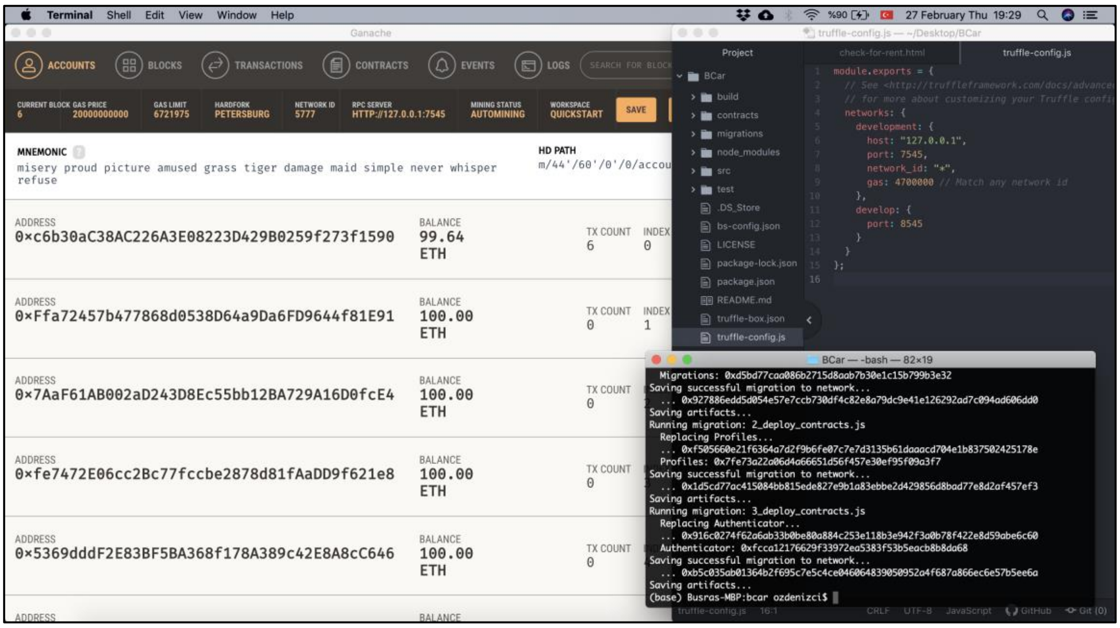


Figure 3. Ethereum Blockchain with Ganache framework on localhost.

We will now dive into Rent Car scenario in this section. The preliminary code script on smart contract that is designed for rent car operation as well as some functions with events are presented in Code Section 1. The general flow of scenario is described by a flow diagram in Figure 4a:

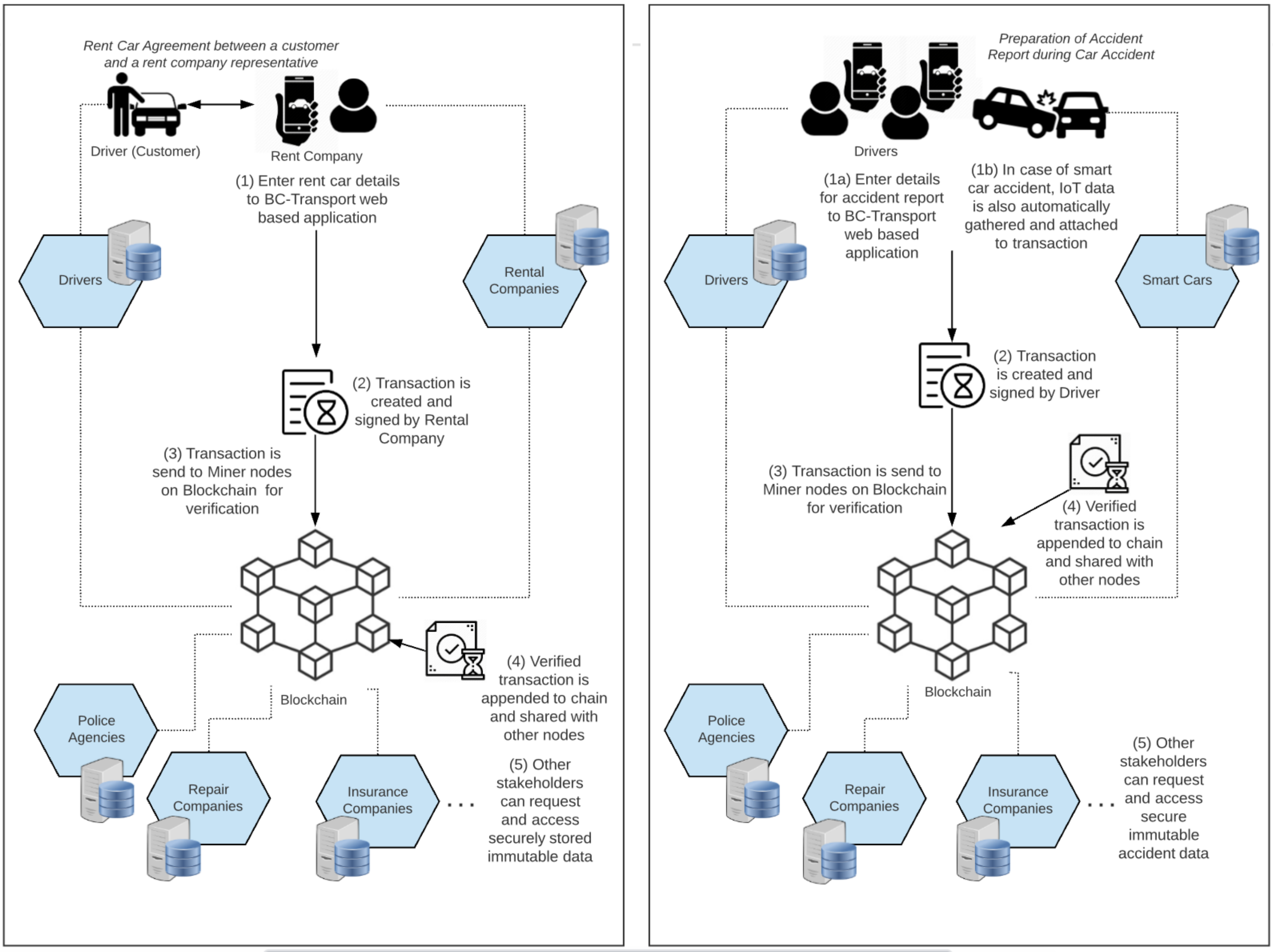
(1) A rental company (i.e., registered user in rental companies node) wants to prepare a rent car operation for a previously registered customer (i.e., registered user in drivers node) on the system. For this purpose, Rental company may access the web application of Blockchain network and prepare the details of rent car operation as a transaction on chain.
(2) The transaction is created in accordance with the functions defined in smart contract and signed with the private key of the user (i.e., rental company) for ensuring non-repudiation security requirement.
(3) The signed transaction is firstly sent to miner nodes on Blockchain via web3js JavaScript library for verification and confirmation. Consensus mechanism by PoW algorithm is applied over network –as explained previously.
(4) Verified -rent car agreement- transaction by miner nodes is appended to the chain and also is shared with other actors; policemen, rental companies, insurance companies and so on.
(5) Other entities can view and access the stored data by making requests and view reports. For example, a policy agency can request lists and some information of the currently rented cars; a rental company can request previous accident history of a customer (driver); or request GPS, speed and other similar sensor data coming from a currently rented smart car. When the driver checks-in the car, the same communication and process flow is performed by the corresponding rental company over web based distributed application.

Another valuable business scenario is about reporting an accident condition where smart cars can also play significant role. The general flow of scenario is given by a flow diagram in Figure 4b:

(1) Let's assume that a registered driver of the consortium network urgently needs to prepare an accident report, of course a secure and immutable one. The user (aka driver) may access the web based distributed application of Blockchain network to prepare the details of accident report -such as car ID; accident date and time; accident location; description; intervention of police, ambulance or tow track- on chain. In case of a smart car accident, sensors with smart kit gateway technology can provide additional real-time data such as speed, life belt usage, engine heat record and more; all of such sensor data can be attached to the accident report to be used for further value added services such as insurance handling operations.
(2) The transaction is created in accordance with the functions in smart contract and signed with the private key of the driver for ensuring non-repudiation.
(3) The signed transaction is sent to miner nodes on Blockchain via web3js, JavaScript library, for verification and confirmation through Blockchain's consensus mechanism.
(4) Verified -accident report- transaction is appended to the chain and concurrently shared with other nodes.
(5) Other entities can view the accident data by making transaction requests and also can get reports about the accident details. These authorized entities can also get reports about accidents those occurred in some period; accidents those will be charged to the insurance companies or to the individuals; accidents those required policeman, ambulance, and / or tow track attention; accidents that a specific car got involved; location, speed, and / or life belt usage information of currently rented cars etc. Notice that a rental company may query only its own cars, whilst policemen may query all. In case of an emergency situation, the triggered entities (police, medical, automotive service company) can make necessary interventions and assistance which also needs to be uploaded to the Blockchain network in the same manner over web based DApp.

```
contract CarProfile is Ownable {

struct AuthTokens {
        address add;
        bytes32 hashedToken;
    }
mapping(address => AuthTokens) tokenStructs;
struct Access {
       address accessOwner;
       uint v;
       uint ttl;
}
struct Car {
      string vin;
      string manufactor;
      string location;
      address carOwner;
      address renter;
      uint256 rentPrice;
      address[] accessList;
      mapping(address => Access) accessStructs;
}
mapping(string => Car) carStructs;
string[] carList;

// events
event newCarEvent(bool result, address creator, string vin);
event addAccessToCarEvent(bool result, address creator, string vin, address user);
event addAccessTokenEvent(bytes32 token);
event rentCarEvent(bool result, address user, string vin);

function newCar(string _vin, string _manufactor, string _location, uint256 _price) public
    returns (bool success)
      {
        carStructs[_vin].vin = _vin;
        carStructs[_vin].manufactor = _manufactor;
        carStructs[_vin].location = _location;
        carStructs[_vin].carOwner = msg.sender;
        carStructs[_vin].renter = 0x0;
        carStructs[_vin].rentPrice = _price;
        carList.push(_vin);
        newCarEvent(true, msg.sender, _vin);
        return true;
      }

function getCar(string _vin) public view
    returns(string vin, string manufactor, string location, address _owner, address _renter, uint256 _price, uint accessCount)
      {
        return(carStructs[_vin].vin, carStructs[_vin].manufactor, carStructs[_vin].location, carStructs[_vin].carOwner,
          carStructs[_vin].renter, carStructs[_vin].rentPrice, carStructs[_vin].accessList.length);
      }

function addAccess(string _vin, address _user, uint _v, uint _ttl) public
    returns(bool success)
      {
        carStructs[_vin].accessList.push(_user);
        carStructs[_vin].accessStructs[_user].v = _v;
        carStructs[_vin].accessStructs[_user].ttl = _ttl;
        addAccessToCarEvent(true, msg.sender, _vin, _user);
        return true;
      }

```

Code Section 1. A smart contract script for car profile and rent car data uploading.



(a) Rent Car Scenario *(b) Report Accident Scenario*

Figure 4. Scenarios for Smart Transportation

4. Evaluation of Model

The proposed Blockchain based model provides opportunities for the development smart transportation ecosystem and also for the management of problems arising from high heterogeneity and high mobility. The model demonstrates how self-regulating smart contracts on Blockchain can enhance the communication in transportation ecosystem, and also how business models can improve trust among entities with immutable data entries. Hereby, this section evaluates and discusses proposed model through three perspectives: appropriateness, technical features, and adoption and diffusion.

4.1. Appropriateness of Proposed Model for Transportation Ecosystem

The study introduced by World Economic Forum (Mulligan et al., 2018) provides a well-defined decision tree for initial assessment of whether Blockchain is an appropriate solution for a defined problem and identifies essential common characteristics and goals of Blockchain use cases. In the light of the aforementioned framework (Mulligan et al., 2018), the proposed communication model has the common goals that demonstrates appropriateness of Blockchain technology for various interrelated operations of stakeholders in smart transportation environment. The general features of the proposed model are evaluated hereunder:

Permanent digital assets: As the popularity of information technology is hyped, cost per storage media lowered, and proper security measures are provided; handling the data that has effects on legal issues switched from physical to digital media harmoniously. With the digital transformation of governments and public services, immutable and irrefutable digital assets are fostered instead of using physical assets over the world. In the context of smart transportation, the proposed Blockchain based communication model has an opportunity for developing permanent records and unalterable transactions of driving license reports, driver's history report, accident reports, insurance claims, rental contracts (agreements), repair and maintenance contracts, and many other. Critical information can be digitally stored and exchanged among nodes of Blockchain with appropriate consensus mechanism; in turn which allows to develop valuable reports, achieve operational excellence and trustworthy environment.

Shared repository by multiple entities: As mentioned, transportation or traffic ecosystem is a broad environment that encloses various operations that are governed and realized by various stakeholders. Existence of interdependencies between operations is highly seen in transportation ecosystem; for example, in an accident case scenario where police, insurance companies, medical agencies and many other entities need to create critical information about corresponding accident, request information about driver and car details, and so on. The proposed communication environment allows not only to create interaction and dependency between transactions by different entities; but also to generate transactions for the shared repository by multiple entities.

Improved trust: Usage of physical assets and weaknesses in integration of different platforms used by different actors (nodes) may result in occurrence of undesired events; such as inconsistencies, loss of data, illegal data modifications, illegal data alterations, even fraud or corruptions that many countries are suffering today. The potential capabilities of proposed model can foster an efficient agreement environment among transportation stakeholders. With the model, the stakeholders can have full control over the digitally stored immutable assets as well as the previous records. Registered end-users (drivers, rental companies, police agencies, insurance companies etc.) can produce, access, request and view irrefutable and transparent proof of transactions with high level of confidence.

Elimination of intermediaries: Another significant aim of the proposed model is to remove intermediaries between the end-users of transportation ecosystem, and allow for more lean and transparent communication environment. With the support of consensus mechanism; stakeholders can manage and handle claims, reports and other data about transportation status, which facilitates the digitalization of traffic management systems instead of using a central gatekeeper. Elimination of intermediaries (i.e., third party service providers and their own proprietary data management platforms) will reduce the cost of delivering services and allow for faster resolution of problems and claims, which means operational excellence and productivity.

4.2. Technical Features and Considerations of Proposed Model

Incorporating Blockchain with its core technologies presents valuable technical and security benefits for smart transportation that needs especially data integrity and non-repudiation of entities. In this regard, an evaluation of technical features and further technical improvements of the proposed model are presented hereunder:

Data integrity: Being immutable means that a block cannot be deleted or modified once it has been chained to the network; which guarantees data integrity among stakeholders. In the proposed model, the usage of shared ledger technology by stakeholders of transportation ecosystem -instead of proprietary data management platforms- will eliminate the data inconsistency problems and handles the heterogeneity problems. Sensitive information about drivers and cars will be shared between registered and authorized users without any change in consortium Blockchain. Data manipulation, lack of information, inconsistencies, spoofing, and other similar threats will be prevented via hashing functionality of Blockchain.

Non-repudiation of user: When a user -as a connected node- submits transaction details through a form -which will trigger corresponding function in smart contract-, the transaction is created and signed by user’s private key. Blocks are created through transactions which are sent among nodes of the Blockchain network. For a transaction to be valid, it has to be generated by an authorized node. With the proposed model, repudiation and consensus problems among stakeholders that do not trust each other will be prevented in digitalized transportation ecosystem.

Permissioned-public network: Different from public Blockchain systems, permissioned systems allow only authorized entities to join and benefit from Blockchain network. Consortium and private Blockchain platforms are examples of permissioned systems. In case of private blockchain, the network is owned and administered by a single entity (organization). However, using consortium Blockchain as a permissioned-public platform allows authorized entities to participate in the consensus process; and network ownership belongs to multiple entities, which is suitable for transportation ecosystem requirements. In this sense, consortium platform will be a beneficial setting for the proposed model and transportation ecosystem where multiple entities operate in the same industry as in transportation ecosystem which require a common ground to perform critical transactions and relay valuable information. Consortium network -with consensus procedures controlled by the present nodes- will mitigate the centralized control risks of permissioned and private Blockchain networks by streamlining the communication among entities.

Further improvements: There are also some other important technical issues that can be considered within context of this proposed model. First, the proposed model should definitely provide a scalable and manageable architecture which ensures reliable and robust interconnection between various nodes. There is a need to implement proposed system adapting scalable transportation scenario; while guaranteeing high quality user experience and reliable data sharing. Moreover, the model should allow users to access sensitive transportation data anytime and anywhere through a web based platform; users should interact with the system in a real time and dynamic manner. Optimization of data uploading and processing will allow for efficient transaction communication and low network latency.

Data access control among entities is another significant issue that can be considered when complex and special policies are defined by smart contracts. A flexible and dynamic access control policy -such as tokenization mechanisms- can be applied by smart contracts in order to allow or deny access to sensitive -traffic, driver, sensor or any other similar- data. An efficient access control policy will enhance the operations of smart transportation environment. For example, a driver can determine how the data is to be shared, can set access permissions and access periods to specific entities; and even can change permissions at any given time. In a vehicle malfunction scenario, a driver may need to collaborate only with insurance and repair companies; sensitive data of driver needs to be shared with certain entities instead of insurance companies or repair companies in the network. An access control architecture over proposed model must be able to achieve the user's (e.g., driver’s) proof of identity; and must enable users to authorize necessary entities for accessing private data based on the access control policy that user created. In this regard, tokenization models can be a beneficial way of implementing access control policy through smart contracts.

Finally, in order to manage access of end-users to distributed application, a multi-factor authentication (such as one-time-password, personal identifier number, biometrics) mechanism can be integrated. Such an authentication mechanism can provide identity management of end-users. Users can authenticate themselves to the system before using distributed application; after which they can access and use the Blockchain network. For example, even if the credential of a user is compromised, the authentication model will not authenticate any user without entering the correct one-time-password which is recently sent the user's smartphone.

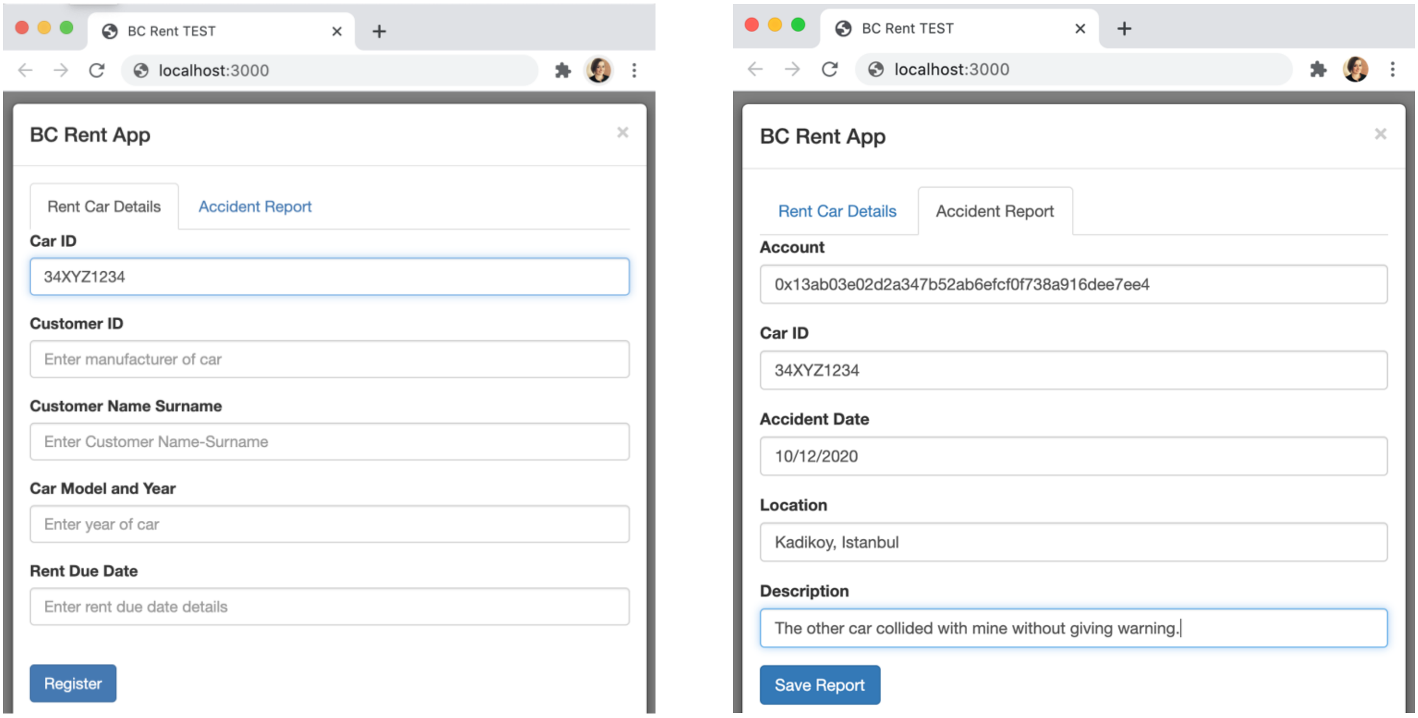
4.3. Adoption and Diffusion of Proposed Model

Besides technical capabilities and features, adoption and diffusion of the proposed model in transportation ecosystems should be considered as well. In this context, Technology Acceptance Model (TAM) (Davis, 1985) and Diffusion of Innovations (DOI) (Rogers, 2010) are essential theories which are being utilized extensively by researchers and practitioners in order to explore a variety of technological innovations adoption. In the light of adoption and diffusion theories, the preliminary implementation of the proposed model is assessed in order to comprehend and explore insights about the behavioral intention of stakeholders to use in a systematic way:

Relative Advantage: The concept of relative advantage is indicated as the value oriented aspect including constructs of perceived usefulness (Davis, 1985; Kamble et al., 2019). In accordance with explained potential characteristics and technical features in previous subsections, the proposed model can be evaluated as useful; since it increases productivity, simplifies underlying process, allows transparent and immutable record, reduces cost, time and user effort, and eliminates intermediaries in transportation ecosystem.

Complexity: As an effort-oriented aspect, complexity is the degree to which an individual is considered and perceived difficult to understand and utilize (Kamble et al., 2019; Yoo et al., 2019), which is the opposite of perceived ease of use. From end-user's perspective, simple user interfaces over web based application -as shown with some form examples from implementation in Figure 5- allow users to access to the proposed Blockchain based network easily, perform data sharing or request on distributed ledger, and exchange data. The designed interface ¬(i.e., web based application) of the proposed model is simple and straightforward, which also hides many complexities. The interface triggers self-executing programs via smart contracts, eliminates complexities in the foreground, and establishes trust relationship among stakeholders with a complex consensus mechanism in the background.

Compatibility: Compatibility is the degree to which technological innovation is considered as stable, consistent (steady) with user's existing values, needs, and experiences (Davis, 1985; Kamble et al., 2019; Cheung et al., 2000). The proposed model will serve as a common collaboration and communication platform for the stakeholders in order to realize interrelated operations and transactions regarding traffic and transportation services. Common needs of various agencies and drivers will be handled in a less time-consuming manner. After the establishment of the proposed Blockchain based network among government agencies and other entities; users will be able to seamlessly adopt, learn and use new platform. As performed by implementation, users do not require to acquire additional products to benefit from this service; new users can join the developed platform through an online user registration form on DApp easily.



(a) Rental Contract Screen *(b) Accident Report Screen*

Figure 5. User Interface Examples of Web Based Application

Observability and Trialability: Recently, Blockchain based implementations have very few observability and trialability opportunities for users. The concept of observability is defined as the degree to which the technology provides detectable, tangible, visible results to adopters, whereas trialability is the ability to test, experience and explore the innovation before adopting usefulness (Davis, 1985; Kamble et al., 2019). Due to restricted scalability in this study, a partial implementation of described business scenarios are conducted in order to comprehend establishment of a Blockchain network and its appropriateness. Within context of the proposed model, development of more advanced smart contracts about further scenarios (such as upload or request of driving license reports, driver's history report, insurance agreements, insurance claims, repair and maintenance contracts) will increase observability of benefits more in transportation environment. Also, with the dissemination of smart cars, it will be possible to make use of sensor data on transactions. Moreover, high fidelity prototypes and advanced smart contracts deployments will improve the observability and trialability metrics and diffusion of innovation.

4. Conclusions and Future Work

This paper explores the potential of Blockchain technology and implements a Blockchain based communication model for smart transportation ecosystem. The main purpose of Blockchain based communication scheme is to overcome challenges and issues of data manipulation, missing information, inconsistencies, repudiation, and consensus problems among transportation stakeholders that do not trust each other in the context of automated mobility, high heterogeneity and V2X paradigm.

In this regard, this study focuses on the design of a trustworthy model that provide valuable interrelated business services with the help of self-regulating smart contracts, efficient consensus mechanism and secure distributed, shared ledger capability. The proposed model's system design considerations, architecture requirements and business model examples within context of smart transportation are explained. A consortium network establishment and a preliminary implementation of some business models with smart contracts are performed to perceive conformity of Blockchain technology for the transportation ecosystem. The study also integrates a comprehensive evaluation of the proposed model for smart transportation.

Permanent and immutable digital asset management, shared repository by multiple stakeholders (e.g., drivers, insurance companies, medical agencies, police agencies, rental companies, repair companies and even connected cars), elimination intermediaries and improved trust are desired goals in smart transportation ecosystem; which also demonstrate appropriateness of Blockchain technology for interrelated operations of stakeholders in smart transportation environment. In terms of technical aspect, the proposed model supports goals of data integrity and non-repudiation of users with permissioned public Blockchain network deploying smart contract based communication. Moreover, in terms of adoption of model as user aspect, the proposed model can be assessed as useful, less complex and compatible with end user's needs depending on interrelated operations in transportation ecosystem. The proposed model provides transparent and immutable record management by Blockchain, simplifies underlying process, reduces cost, time and user effort, and eliminates intermediaries in transportation ecosystem.

Future research should focus on improving self-executing smart contracts with business scenarios, end-user identity management and access control policy developments on smart contracts, scalability and availability improvements for real-time transaction handling, and lightweight consensus design solutions for high QoS and low network latency for advancement of Blockchain based smart transportation. The further implementations can also increase the observability of benefits and trialability degree of the proposed communication model.

References

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE communications surveys & tutorials, 17(4), 2347-2376.

Alsadi, M., Gülseçen, S., Kara, S. Köse, B. Ö., & Coşkun, V. (2019a). A Blockchain Based Data Management Model. Journal of Information Systems and Management Research, 1(1), 31-36.

Alsadi, M., Yildirim, S., Gülseçen, S., Köse, B. Ö., & Coşkun, V. (2019b, October). Akıllı Araç Ekosistemlerinde Blockchain Tabanlı Güvenli Veri Yönetim Modeli. In 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), (pp. 1-5). IEEE.

Ashton, K. (2009). That 'internet of things' thing. RFID journal, 22(7), 97-114.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787-2805.

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics and Informatics, 36, 55-81.

Chen, S., Hu, J., Shi, Y., Peng, Y., Fang, J., Zhao, R., & Zhao, L. (2017). Vehicle-to-everything (V2X) services supported by LTE-based systems and 5G. IEEE Communications Standards Magazine, 1(2), 70-76.

Cheung, W., Chang, M. K., & Lai, V. S. (2000). Prediction of Internet and World Wide Web usage at work: a test of an extended Triandis model. Decision support systems, 30(1), 83-100.

Davis, F. D. (1985). A technology acceptance model for empirically testing new end-user information systems: Theory and results (Doctoral dissertation, Massachusetts Institute of Technology).

Elkhodr, M., Shahrestani, S., & Cheung, H. (2016). The internet of things: new interoperability, management and security challenges. arXiv preprint arXiv:1604.04824.

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. IEEE Access, 6, 32979-33001.

Gemalto (2020). Connected Cars. Retrieved from https://www.gemalto.com/automotive/connect-cars

GSMA (2020). IoT, Automotive. Retrieved from https://www.gsma.com/iot/automotive

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.

Hameed, S., Khan, F. I., & Hameed, B. (2019). Understanding security requirements and challenges in Internet of Things

(IoT): A review. Journal of Computer Networks and Communications, 2019.

Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. Computers & Security, 78, 126-142.

Jabbar, S., Ullah, F., Khalid, S., Khan, M., & Han, K. (2017). Semantic interoperability in heterogeneous IoT infrastructure for healthcare. Wireless Communications and Mobile Computing, 2017.

Clark, J. (2016). What is Internet of Things?, https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/

Kamble, S., Gunasekaran, A., & Arha, H. (2019). Understanding the Blockchain technology adoption in supply chains-Indian context. International Journal of Production Research, 57(7), 2009-2033.

Kshetri, N. (2017). Can blockchain strengthen the internet of things?. IT professional, 19(4), 68-72.

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4), 431-440.

Lee, J. H., & Kim, H. (2017). Security and privacy challenges in the internet of things [security and privacy matters]. IEEE Consumer Electronics Magazine, 6(3), 134-136.

Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P. A., & Sun, Z. (2017). Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet of Things Journal, 4(6), 1832-1843.

Leiding, B., Memarmoshrefi, P., & Hogrefe, D. (2016). Self-managed and blockchain-based vehicular ad-hoc networks. In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct (pp. 137-140).

Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: a survey. Information Systems Frontiers, 17(2), 243-259.

Li, Z., Xiao, Z., Xu, Q., Sotthiwat, E., Goh, R. S. M., & Liang, X. (2018). Blockchain and IoT Data Analytics for Fine-Grained Transportation Insurance. In 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS) (pp. 1022-1027). IEEE.

Macrinici, D., Cartofeanu, C., & Gao, S. (2018). Smart contract applications within blockchain technology: A systematic mapping study. Telematics and Informatics, 35(8), 2337-2354.

Mulligan, C., Scott, J. Z., Warren, S., & Rangaswami, J. P. (2018, April). Blockchain beyond the hype: A practical framework for business leaders. In World Economic Forum, White Paper.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for secure EHRs sharing of mobile cloud based e-Health systems. IEEE access, 7, 66792-66806.

Nuss, M., Puchta, A., & Kunz, M. (2018). Towards blockchain-based identity and access management for internet of things in enterprises. In International Conference on Trust and Privacy in Digital Business (pp. 167-181). Springer, Cham.

Ouaddah, A., Abou Elkalam, A., & Ait Ouahman, A. (2016). FairAccess: a new Blockchain-based access control framework for the Internet of Things. Security and Communication Networks, 9(18), 5943-5964.

Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and IoT integration: A systematic survey. Sensors, 18(8), 2575.

Pinno, O. J. A., Gregio, A. R. A., & De Bona, L. C. (2017). Controlchain: Blockchain as a central enabler for access control authorizations in the iot. In GLOBECOM 2017-2017 IEEE Global Communications Conference (pp. 1-6). IEEE.

Rogers, E. M. (2010). Diffusion of innovations. Simon and Schuster.

Shafagh, H., Burkhalter, L., Hithnawi, A., & Duquennoy, S. (2017). Towards blockchain-based auditable storage and sharing of iot data. In Proceedings of the 2017 on Cloud Computing Security Workshop (pp. 45-50).

Shin, D. D. (2019). Blockchain: The emerging technology of digital trust. Telematics and Informatics, 45, 101278.

Silva, B. N., Khan, M., & Han, K. (2018). Internet of things: A comprehensive review of enabling technologies, architecture, and challenges. IETE Technical review, 35(2), 205-220.

SIM Alliance (2017). eUICC for: Connected cars. https://simalliance.org/wp-content/uploads/2017/10/eUICC-for-Connected-cars_FINAL.pdf

Singh, D., Tripathi, G., & Jara, A. J. (2014). A survey of Internet-of-Things: Future vision, architecture, challenges and services. In 2014 IEEE world forum on Internet of Things (WF-IoT) (pp. 287-292). IEEE.

Singh, M., & Kim, S. (2017). Blockchain based intelligent vehicle data sharing framework. arXiv preprint arXiv:1708.09721.

Turkcell (2020). Kopilot. Retrieved from https://www.turkcell.com.tr/servisler/kopilot

Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., & Zheng, K. (2019). Survey on blockchain for Internet of Things. Computer Communications, 136, 10-29.

Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things—A survey of topics and trends. Information Systems Frontiers, 17(2), 261-274.

Yoo, K., Bae, K., Park, E., & Yang, T. (2019). Understanding the diffusion and adoption of Bitcoin transaction services: The integrated approach. Telematics and Informatics, 101302.

Yuan, Y., & Wang, F. Y. (2016). Towards blockchain-based intelligent transportation systems. In 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC) (pp. 2663-2668). IEEE.

Zhang, Z. K., Cho, M. C. Y., Wang, C. W., Hsu, C. W., Chen, C. K., & Shieh, S. (2014). IoT security: ongoing challenges and research opportunities. In 2014 IEEE 7th international conference on service-oriented computing and applications (pp. 230-234). IEEE.

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE International Congress on Big Data (BigData Congress) (pp. 557-564). IEEE.