Bussecon Review Social Sciences

Bussecon Review of Social Sciences

BRSS VOL 4 NO 2 ISSN: 2687- 2285

Available online at www.bussecon.com
Journal homepage: https://www.bussecon.com/ojs/index.php/brss

Emerging blockchain solutions in the mobility ecosystem: Associated risks and areas for applications

Cemal Zehir [(a)]* *Melike Zehir* [(b)]

[(a)] *Professor, Faculty of Economics and Administrative Sciences, Yildiz Technical University, Davutpasa Cad., Esenler, 34220, Istanbul, Turkey*
[(b)] *Research Assistant, School of Business, Ibn Haldun University, Ulubatli Hasan Cad., No: 2 Basaksehir, 34494, Istanbul, Turkey*

ARTICLEINFO

Article history:
Received 25 November 2022
Received in rev. form 25 Dec 2022
Accepted 04 January 2022

Keywords:
Carbon Footprint, Data Marketplace, Digital Vehicle Identity, Distributed Ledger, V2X

JEL Classification:
M10, O32, O33

ABSTRACT

This study aims to identify the most influential blockchain types for potential implementation areas in the transforming mobility ecosystem, considering application area-specific needs such as transparency, transaction speed, scalability, energy usage, security, and operating cost. The study demonstrated the hybrid blockchain suitability for most of the 13 distinguished mobility applications, while private and consortium blockchains are found applicable based on the needs of specific use cases. A public blockchain is only found suitable for two of the use cases. Proof of Authority and Proof of Stake matches well with most use cases, while Practical Byzantine Fault Tolerance and Proof of Work could be suitable in particular.

Introduction

Mobility sector has been recently undergoing major transformations, mainly driven by the decarbonization of transport, decentralization of operation, data storage and management, and digitalization of user experience and services. Major sector players across the world have recently started to collaborate to develop integrated novel solutions by adopting promising technologies.

An expanding global nonprofit consortium, Mobility Open Blockchain Initiative (MOBI) is one of the key forces behind the digital transformation of the mobility sector. It consists of over 120 member organizations, ranging from vehicle manufacturers (BMW, Hyundai, Toyota, Honda, General Motors, Ford) to tech companies and consultancies (Accenture, Amazon Web Services, Bosch, IBM, IOTA, Quorum Control and many other), logistics to suppliers, blockchain protocol developers to e-mobility groups, fintech and lenders to insurers, utilities to governments, nongovernmental organizations (NGOs) (European Commission and other) and academic/research institutions (IEEE, Ontario Tech University, Texas A&M Transportation Institute and other). The consortium has been collaboratively identifying use cases, forming working groups, developing standards and taking part in field pilots aiming blockchain integration into wide range of mobility use cases.

Throughout the lifetime of a car, around 13 use cases have been identified for blockchain compatible vehicle digital identity. The use cases range from digital vehicle registration to DLT-based vehicle wallet, immutable maintenance and recall records to odometer fraud prevention, electric vehicle (EV) charging to vehicle-to-grid (V2G) services, road usage charge to smart parking management, traffic congestion management to vehicle and trip carbon footprint management, usage-based insurance and transportation services to connected data marketplace, vehicle-to-everything (V2X) communications to vehicle finance. Blockchain can allow effective,

---

* *Corresponding author. ORCID ID: 0000-0003-2584-4480*

http://dx.doi.org/10.36096/brss.v4i2.394

secure and autonomous verification, monitoring, traceability, operational optimization and transactions handling (Hacioglu and Aksoy, 2020).

Blockchain is not a solution that works in all situations or a one-size-fits-all approach with a single implementation that will be advantageous in all contexts, environments, and scenarios. Depending on the adoption setting, it has a variety of forms and design variations that may or may not be appropriate. Careful consideration of the tradeoffs between the implementation dynamics of private, consortium and public blockchains in terms of network access, pseudonymity, authentication, consensus mechanism, security, transaction speed, energy usage, system costs and individual costs is essential in planning and deployment of novel applications (Andoni et. al., 2019; Hassija et. al., 2021). It is a major challenge for decision-makers, technology experts and managers to assess and choose the most appropriate blockchain type and design. Moreover, there are inevitable risks that need to be carefully assessed in potential applications (Hacioglu, 2019).

There is a lack of studies on determining the suitable blockchain types and characteristics based on mobility applications and processes in detail. Furthermore, the possible risks and drawbacks of integration options have not been discussed satisfactorily.

The novelty and original contributions of this study are listed as:

i. Investigation of blockchain implementation opportunities in detail in mobility;
ii. Identification of the most suitable blockchain types, consensus algorithms and possible risks specific to the needs of each potential mobility use case.

The second section comprehensively explains the blockchain's possible applications in current and emerging mobility sector applications; while the third section summarizes the main blockchain types, commonly used consensus mechanisms and associated risks considered in the scope of this work. The fourth section determines use case specific suitable blockchain types and consensus algorithms, together with their risks. The last section summarizes the findings and provides directions for future works.

Literature Review

The relevant studies from the literature are presented in this section. Most of the studies in this area in the literature are published in recent years, mostly after 2018. Especially after 2020, the interest in related topics has significantly increased.

A study published in 2018, investigated blockchain applications for intelligent vehicles (Kim, 2018). Usage-based insurance, driving data sharing and car transactions are discussed as promising concepts. Scalability, transaction speed, computing power and transparency were listed as the primary challenges. In 2019, blockchain for usage-based insurance is investigated considering Pay As You Drive (PAYD) and Pay How You Drive (PHYD) schemes (Kumar et al., 2019). Another study on 2019 experimentally explored public blockchain with Proof of Work consensus protocol for usage-based insurance and incentives (Singh et al., 2019). The experiments conducted on a testbed proved the practicality of the developed solution. There is a study on consortium blockchain development for secure parking management (Al Amiri et al., 2020). In a different study, dedicated blockchain system and Proof of Work consensus protocol for traffic management through connected vehicles is explored (Astarita et al., 2020). An important possible real-time implementation challenge is stated as heavy computing load and scalability.

Furthermore, the experimentally developed solution's practicality is validated in the case study. Smart parking management preserving privacy and providing reputation management is investigated in another study (Badr et al., 2020). The proposed approach is found secure and sufficiently privacy preserving, while requiring low computing load. Use of blockchain for Vehicle to everything communication security is discussed in a review study in 2020 (Shresta et al., 2020). The issues are listed as performance, scalability, security and privacy. The same study also discussed big data, machine learning and 5G integration with blockchain, which is also focused on in other prominent studies centered around blockchain ecosystems (Hacioglu, 2020). Another study provides a thorough discussion of blockchain for electric vehicle energy trading activities (Al-Saif et al., 2021).

Theack of standards, guidelines, regulatory frameworks, and technological understanding are the important challenges to using blockchain in the energy exchange for electric vehicles. Information security, transaction speed, and privacy are identified as the main implementation challenges.

A summary of all the mentioned studies is given in Table 1.

Table 1: The Summary of the Prominent Related Studies in the Scientific Literature

Author (Date)	**Subject**	**Methods**	**Findings**
Kim (2018)	Traffic Management with Intelligent Vehicles	Case Study	Scalability, transaction speed, computing power and transparency are listed as the main challenges. Usage-based insurance, driving data sharing and car transaction concepts are discussed.
Kumar et al., (2019)	Usage-based Insurance	Conceptual Study	Pay As You Drive and Pay How You Drive concepts are discussed.
Singh et al., (2019)	Usagae-based Insurance and Incentive	Experimental Testbed Case Study using Public Blockchain with Proof of Work Consensus Mechanism	Transparency for effective data sharing between shareholders and authorities. Practicality of the approach is demonstrated with the experiment.
Al Amiri et al., (2020)	Secure Parking Management	Consortium Blockchain Experimental Development	Practicality of the proposed scheme is validated.
Astarita et al., (2020)	Traffic Management through Connected Vehicles	Dedicated Blockchain System and Proof of Work Consensus Mechanism	In future practical implementations, possible challenges are stated as heavy computing load and scalability.
Badr et al., (2020)	Smart Parking System	Consortium Blockchain for Privacy Preservation and Reputation Management	The proposed system is found sufficiently secure and privacy preserving, requiring low computing load.
Shresta et al., (2020)	Secure V2X Communication	Review Study	Performance, scalability, security and privacy challenges are discussed. 5G, big data and machine learning integration with blockchain are mentioned.
Al-Saif et al. (2021)	Energy Trading Activities of Electric Vehicles	Investigation of Requirements, Opportunities and Challenges	Lack of standards, guidelines, regulatory frameworks, understanding are identified as the main barriers. Information security, performance and privacy are listed as the challenges.

Source: Authors

The Overview of the Adopted Methodology

A repeatable and trustworthy research process is created to identify the best blockchain solutions for the most popular use cases in the mobility sector that are currently emerging. The developed methodology is not only suitable for the mobility sector, and a similar approach can be adopted to determine the most suitable blockchain technology integration solutions in other diverse sectors. The overall methodology is shown in Figure 1.

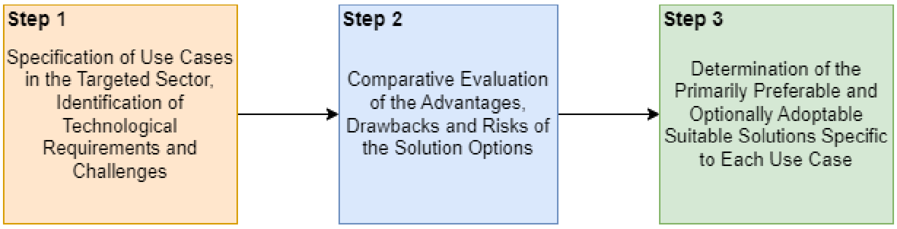
Step 1
Specification of Use Cases in the Targeted Sector, Identification of Technological Requirements and Challenges
Step 2
Comparative Evaluation of the Advantages, Drawbacks and Risks of the Solution Options
Step 3
Determination of the Primarily Preferable and Optionally Adoptable Suitable Solutions Specific to Each Use Case

Figure 1: The Overview of the Adopted Methodology

In the first step, the prominent emerging use cases in the targeted industry (mobility) for the integration of the considered technology (blockchain) is specified based on the scientific studies, technical reports, reliable whitepapers, technological road maps and regulatory guidelines, along with use case-specific technological requirements and challenges. In the second stage, the availabilities, advantages and disadvantages of the considered technology solution options (blockchain types and consensus mechanisms) are comparatively evaluated including the associated risks. In the last stage, the primarily preferable and optionally adoptable suitable solutions for each of the specific use cases are determined.

Digital Vehicle Registration

Digital vehicle registration, created using blockchain technology, ensures the traceability of the vehicle throughout its lifetime. The digital identity of the vehicle includes recording of all processes from the birth of the vehicle such as birth certificates, recalls and maintenance and repairs, safety checks, emission information, accident information, and original parts. Vehicle ID (VID) provides a clean and transparent history throughout a car's lifecycle (MOBI, 2021a).

Used car trading is fraught with an information imbalance between buyer and seller. Sellers may not share information such as accidents, modify odometers, original parts, warranties, or insurance transactions with buyers transparently. This creates information asymmetry between buyers and sellers. The vehicle registration system created with blockchain will ensure that all information and details of the vehicle are shared with other parties transparently, thus eliminating any distrust between the sides and reducing the damages that may arise. Through the virtual record created from the birth of the vehicle, the details of the provided maintenance services can be verified. It is even possible to identify the replaced or repaired parts of the vehicle. Furthermore, this method enables the immutable and sequential recording of the car's title deed information, assuring the prospective buyer that the true value of the vehicle can be ascertained and thereby preventing title fraud (MOBI, 2021e).

By enabling stakeholders to securely exchange data with one another and guaranteeing that the possibility of fraudulent activity related to ownership, odometer, and other information is significantly reduced or eliminated, digital registration of vehicles can offer a future-proof, contemporary solution to these issues. Digital vehicle ID added to car registration will make it simple to verify online who owns a particular vehicle.

Tracing the end-of-life of vehicles is necessary to guarantee that original vehicle parts, particularly those related to safety, are disposed of or recycled appropriately. To prevent the IDs of these parts from being used on counterfeit parts, it is important to record them. By using blockchain technology to trace these parts, dealers and repair shops can verify their authenticity. This traceability can improve security by reducing the incidence of fraudulent parts at the end of a vehicle's life.

DLT-Based Vehicle Wallet

A vehicle wallet is an application that allows transactions between customers, vehicles and other infrastructures to be carried out autonomously and securely. The vehicle wallet enables vehicles to facilitate transactions for repair services, toll payments, and the acquisition of information within the ecosystem through the exchange of funds. Vehicles with fixed wallets can convert this information transferred between parties into money in real-time, using smart contracts that issue payment orders and provide financial reconciliation. Smart contracts distribute payments among various stakeholders and data infrastructure according to the terms of the contracts (MOBI, 2021e).

Smart contracts on the blockchain ensure that payments are made automatically when the conditions set between the parties are met. In addition, since smart contracts keep immutable records of transactions, buyers and sellers cannot refuse transactions and related payments (Al-Saif et al., 2021). Smart contracts will also enable new road and infrastructure pricing systems.

In order to facilitate vehicle-initiated payments, it is necessary to verify the identity of the payee and confirm receipt of the payment. This can be achieved through the use of digital vehicle identification, which is linked to the vehicle's wallet. The integration of e-wallet technology and the incorporation of wallet functionality into various tools have made machine-to-machine payment transactions more convenient. However, the effectiveness of vehicle-based wallets in facilitating payments between vehicles and infrastructure relies on the availability of a digital vehicle ID.

Immutable Maintenance & Recall Records

Maintenance services and related part replacements can cause information asymmetry between the buyer and the seller. Some information that significantly affects the value and warranty coverage of the vehicle, such as how regularly the vehicle is maintained, the quality of the replaced parts and whether they are original, and what changes have been made to the vehicle, are sometimes not conveyed to the vehicle owners by the service providers that provide maintenance services, and grievances may occur.

Identifying vehicles that need to be recalled can also pose a serious challenge in part recalls. It can be challenging for companies to accurately identify the current owner of a vehicle and the corresponding parts when the warranty period has ended or when the vehicle is no longer in a rental or financing period. This tracking difficulty is because the motion flows in the transactions are not visible. For this reason, companies often have to recall more vehicles than they need (MOBI, 2021e).

For all these reasons, annual maintenance, parts replacement, and recall records need to be closely monitored for transparency. Blockchain technology ensures that all these records are kept securely and that even the smallest changes are simultaneously visible and traceable between the parties.

Odometer Fraud Prevention

The odometer reading is frequently used as a proxy for a vehicle's market value. As a result, there is a risk of fraudulent activity involving the alteration of odometer readings in the context of second-hand automotive sales, particularly in cross-border transactions, with the aim of artificially increasing the perceived value of the vehicle. This situation is very common and poses a serious problem for the automotive industry.

To combat fraudulent practices such as odometer tampering, the incorporation of a publicly accessible mileage log linked to a digital identity has been suggested as a potential deterrent. In recognition of this, numerous companies, including BMW and Bosch, have developed applications that utilize blockchain technology to secure odometer readings. The European Parliament has also acknowledged the potential of blockchain technology in addressing this issue (MOBI, 2021e).

Odometer tampering can undermine the integrity of the aftermarket and specialized vehicle sales industries. Implementing mileage readings linked to a digital vehicle identification and recorded on open, unchangeable ledger systems has the potential to enhance confidence in the used car market.

Electric Vehicle Grid Integration

Managing energy trading operations in electric vehicles is important. Systems used for this purpose are generally centralized and less reliable because they are vulnerable to data changes and hacker attacks. Blockchain securely enables these trade transactions to take place without intermediaries.

In the classical system, purchase and sale transactions in the electricity market are carried out through intermediaries. However, blockchain allows these transactions to be made by anyone without the need for intermediary institutions. In this way, electric vehicles can not only consume energy, but also sell their excess energy to neighbouring vehicles at an appropriate rate for both. Energy trading done in this way enables electric vehicles to maximize their financial benefits (PankiRaj et al., 2019; Leong et al., 2018).

The electricity price varies depending on the supply and demand conditions in the market. Electricity pricing varies during peak and off-peak hours. The price formation takes place in the market through bilateral agreements and open competitive market mechanisms between large buyers and power plants.

Blockchain-based smart contracts can facilitate energy auctions by automating the bidding process and eliminating the need for intermediaries, thus the trading of energy for electric vehicles will have lower transaction costs. The trustworthiness of these transactions is enhanced by the use of blockchain technology (Al-Saif et al., 2021).

Smart contracts can also be used in the management of energy demand and supply in the electric vehicle market. By collecting energy requests from multiple electric vehicle owners, smart contracts can help smart grid operators to determine the additional energy needed to meet the demand and maintain a balance between supply and demand in the market. This is achieved by analyzing data on energy demand and available storage capacity (MOBI, 2021c).

Blockchain technology can be utilized to facilitate the exchange of renewable energy between various stakeholders in a smart grid system. Through the use of a blockchain platform, energy producers, such as wind, solar, and hydroelectric power plants, can sell their excess energy to charging stations that supply energy to electric vehicles. The electric vehicles, in turn, can purchase energy from the charging stations and may also have the option to sell excess or flexible energy stored in their batteries back to the grid during times of high demand for profit. This process allows for the efficient distribution of renewable energy and helps to balance supply and demand within the grid (Al-Saif et al., 2021).

Road Usage Charge

Road usage charges can be used for a variety of purposes, such as refinancing road infrastructure or regulating traffic. Data provided by the blockchain can also be used to determine road tolls. Using smart contracts and payment applications of the blockchain, automatic collection and tracking of road tolls are also possible.

Smart Parking Management

The problem of searching for a parking place, which has become one of the biggest problems of drivers, especially those living in crowded cities, creates many problems along with it. It causes drivers to waste time, traffic jams, and air pollution. Around 30% of traffic congestion in crowded cities is caused by the problem of searching for a parking space (Giuffrè et al., 2012).

Smart parking systems aim to address the issue of limited availability of parking spaces by providing drivers with real-time information about the location and availability of empty spaces (Al Amiri et al., 2020). These systems utilize Internet of Things devices to detect empty spaces and communicate this information to drivers seeking parking. Smartphones can also be used to make online reservations in these systems.

Smart parking systems have gained significant attention in recent years, leading many companies to invest in these systems in various cities worldwide (Inrix, 2015; SpotHero, 2022). The use of a centralized server in smart parking systems can create vulnerabilities in terms of security and privacy. As all information is processed and stored by a single server, it can be more easily targeted by cyber attacks or unauthorized access. Additionally, the centralized nature of the system means that personal data and information related to parking transactions may not be adequately protected (Inrix, 2015; SpotHero, 2022). This leaves users vulnerable to the potential compromise of the system. In addition, the low transparency of central systems can lead to dissatisfaction among drivers. In a centralized management system, certain parking spaces may be given priority by the manager by being reserved first, putting some parking space owners out of pocket and making it more difficult for drivers to obtain parking nearby.

Implementation of a blockchain network for the management of parking services can address security concerns in the following ways. Firstly, decentralization of the parking system through the use of blockchain technology enhances its resistance to attacks that may disrupt the availability of the service. Secondly, blockchain technology can improve transparency within the system and ensure the integrity of data by recording all parking offers from various parking lots in a shared, unalterable ledger that is validated by the blockchain and can be audited by relevant parties (Badr et al., 2020).

However, the implementation of a blockchain system may not completely address concerns about location privacy if drivers choose to disclose their intended destinations on the blockchain. Additionally, blockchain validators may not have the ability to assist drivers in finding parking spaces outside of their area of jurisdiction.

Congestion Management

Using blockchain technology, connected vehicles can share traffic density in real-time. This situation informs the drivers about the development of the traffic and can direct them to alternative transportation methods that will reduce the density of the traffic. These real-time data also constitute an important source for traffic forecasts. Using the data obtained through simultaneous sharing of traffic information; useful traffic management strategies can be implemented, such as real-time regulation of traffic signals and better management of public transport systems (Astarita et al., 2020).

In order to promote adoption of the system, various incentives may be implemented such as parking privileges, access to restricted traffic areas, and payment in cryptocurrencies. These incentives can ensure that the system benefits both society and drivers.

Carbon Footprint Management

In the automotive sector, the fact that data such as the production, physical transportation, service life, and end of life of the product cannot be followed enough, causing the emission estimates to be misleading. In carbon footprint management, tracking and traceability of data throughout the supply chain are very important.

The transparency of data in an e-mobility ecosystem also presents an opportunity for a circular economy, in which all products are optimized for maximum reuse, particularly resources that are scarce or in demand. Reusing EV batteries after their "first life" is especially desirable. To determine the most appropriate use for a battery in its second or third life, it is crucial to provide as much data as possible about the battery's condition. Blockchain can facilitate the circular reuse of batteries by enabling stakeholders to securely share battery data with other parties and track battery health throughout its lifespan.

Traffic management applications for smart cities, such as reducing traffic congestion and parking search time provided by blockchain technology, also significantly reduce the carbon footprint.

Usage-Based Insurance and Transportation Services

Usage-Based Insurance (UBI) is a major innovation in the automotive insurance industry, comprising of Pay As You Drive (PAYD) and Pay How You Drive (PHYD) schemes (Kumar et al., 2019). It determines a driver's insurance premium and coverage based on their driving behavior.

Pay As You Drive (PAYD) is a popular form of Usage-Based Insurance where the insurance premium is determined by the number of kilometers traveled in the insured period, offering lower premiums to customers who drive less. The insured period can be customized to the customer's needs.

Pay How You Drive (PHYD), another form of Use-Based Insurance, has gained widespread adoption in the industry due to its benefits. PHYD calculates insurance premiums based on the make and model of the vehicle, the age of the driver, the driver's occupation, etc. rather than solely the vehicle, taking into account how the vehicle is used. This method of evaluation is more accurate because driving patterns are a significant indicator of the likelihood of making a claim, for example, a reckless driver is more prone to accidents and therefore more likely to file a claim (Kumar et al., 2019).

Usage-Based Insurance (UBI)-based solutions not only benefit insurance companies and customers, but also society as a whole. Customers will benefit from a fair premium payment policy that is based on their driving behavior. By linking the amount that a driver pays for insurance to their driving behavior, UBI can incentivize safer driving practices. As a result, the frequency and severity of traffic accidents may decrease, as drivers are more aware that their behavior is being monitored and will be reflected in their insurance premiums. This can lead to increased feelings of safety and security for drivers, as they are more confident in their ability to avoid accidents. In addition, the use of UBI may foster a sense of connection among drivers, as they are all working towards the shared goal of improving their driving habits and reducing the likelihood of accidents.

UBI also allows customers to access a range of value-added services such as vehicle diagnosis and emergency services. This can be particularly useful in the event of an accident, as efficient driving can lower the likelihood of accidents and therefore decrease the number of damage claims made. Insurance companies can also benefit from UBI, as it allows them to monitor real-time driving behavior and quickly generate evidence in the event of a claim, reducing the number of false claims and minimizing losses. By lowering overall premium costs and making policies more attractive to customers, UBI can help insurance companies to remain competitive. Finally, UBI can encourage drivers to choose better routes and limit vehicle use, leading to reduced fuel consumption, pollutant emissions, and traffic accidents (Singh et al., 2019).

UBI has been implemented in various regions around the world, with a significant presence in the United States, Europe, and Japan (Singh et al., 2019).

Connected Mobility Data Marketplace

Today, vehicles, trains, even bicycles and, scooters are becoming more and more connected and smart. Accordingly, infrastructures such as highways, bridges and ferries are equipped with sensors, and digital identity devices to generate and share data. Data can be shared seamlessly and easily with these devices. The interoperability of these obtained data is very difficult and important. It provides a suitable layer for secure data sharing between the parties by ensuring the authentication of the stakeholders in the blockchain ecosystem and the immutable and reliable recording of information.

Blockchain allows entities to authenticate each other, as well as immutably record and securely share collected information with each other. In order to achieve this, Connected Mobility Data Marketplace Standards (CMDM Standards), which contain regulations for the identity, data and functions of assets, have been created.

The CMDM Standard provides a universal data-sharing framework for devices to communicate and share information with each other and also addresses functional interoperability. CMDM compatible systems will produce clean, easily parsed and similarly organized data. (MOBI, 2021b).

Vehicle-to-Everything (V2X) Communications

Vehicle-to-everything (V2X), is the term and concept used to describe smart communication between vehicles and many other systems. It encompasses a variety of applications including vehicle-to-vehicle, vehicle-to-infrastructure, vehicle-to-road, vehicle-to-human, and vehicle-to-sensor communication.

Traditional security and privacy mechanisms are insufficient to defend intelligent and autonomous vehicles against cyberattacks. Smart transportation involves the sharing of a vast amount of data within vehicle ecosystems, including accident reports, traffic information, weather updates, infotainment messages, etc. Managing such a large amount of data is both costly and challenging. V2X communication is particularly vulnerable to security risks due to the sensitive nature of data shared between smart vehicles (Park, Park, 2017; Kim, 2018).

Blockchain enables information to be transmitted in a secure and distributed manner by storing it in a transparent and immutable way. Through its decentralized verification feature, it provides rapid verification of information sharing within the ecosystem. In this way, information such as accident history, traffic conditions, etc. can be shared between vehicle networks rapidly and accurately. In case of accident events, the information stored on the blockchain can be utilized by traffic police, law enforcement agencies, and insurance companies to resolve specific incidents. Participating vehicles can utilize the event information stored on the blockchain and act accordingly, as the information stored on the blockchain can be considered a reliable source.

Blockchain offers a number of benefits, such as defending the security and privacy of the data contained in these blocks against various kinds of sophisticated cyberattacks. On blockchains, every event or transaction has a time stamp and is confirmed using private keys. Vehicle owners can trace occurrences or transactions at a specified moment and safely monitor the history of transactions (Shrestha et al., 2020).

Vehicle Finance

Blockchain and smart contracts can enable a seller to better track and manage multiple maturities of loans that finance their vehicles (Hacioglu and Aksoy, 2021). This makes it easier for dealers to follow loan terms and eliminates the problem of not noticing that most of these loans are due at the same time.

Smart contracts enable the automatic enforcement of traditional contract arrangements in vehicle sales and financing. Smart contracts can distribute interest and principal payments to investors and collect transaction fees from interested parties. While performing these transactions, reduces the transaction costs by eliminating the need for intermediaries thanks to the reliable structure of the blockchain.

Verifiable credentials provided by the blockchain will facilitate transactions during the loan application process. Blockchain allows the creation of digital identity, unlocking the real-time potential of using other indicators to create a reputable asset profile for consumers who would otherwise have no credit (MOBI, 2021d).

The technological requirements and challenges of the identified use cases are listed in Table 2.

Table 2: Overview of Technological Requirements and Challenges Specific to the Identified Cases

Use Case	**Technological Requirements**	**Challenges**
Digital Vehicle Registration	Transaction Speed - Moderate Operational Cost - Moderate Transparency - High	Security - High Scalability - High Energy Consumption - Low
DLT-based Vehicle Wallet	Transaction Speed - High Operational Cost - Moderate Transparency - Low	Security - High Scalability - High Energy Consumption - Moderate
Immutable Maintenance & Recall Records	Transaction Speed - Low Operational Cost - Moderate Transparency - High	Security - High Scalability - Moderate Energy Consumption - Low
Odometer Fraud Prevention	Transaction Speed - Low Operational Cost - Low Transparency - High	Security - High Scalability - High Energy Consumption - Low
Electric Vehicle Grid Integration	Transaction Speed - High Operational Cost - Moderate Transparency - Moderate	Security - High Scalability - High Energy Consumption - Moderate
Road Usage Charge	Transaction Speed - High Operational Cost - Moderate Transparency - Low	Security - High Scalability - Moderate Energy Consumption - Moderate
Smart Parking Management	Transaction Speed - Moderate Operational Cost - Low Transparency - Moderate	Security - Moderate Scalability - Moderate Energy Consumption - Low
Traffic Congestion Management	Transaction Speed - High Operational Cost - Moderate Transparency - Low	Security - High Scalability - High Energy Consumption - Moderate
Carbon Footprint Management	Transaction Speed - Moderate Operational Cost - Low Transparency - High	Security - Moderate Scalability - High Energy Consumption - Low
Usage-based Insurance and Transportation Services	Transaction Speed - Moderate Operational Cost - Moderate Transparency - High	Security - High Scalability - High Energy Consumption - Low
Connected Mobility Data Marketplace	Transaction Speed - High Operational Cost - Moderate Transparency - High	Security - High Scalability - High Energy Consumption - Moderate
Vehicle-to-Everything (V2X) Communications	Transaction Speed - High Operational Cost - Moderate Transparency - Moderate	Security - High Scalability - High Energy Consumption - Moderate
Vehicle Finance	Transaction Speed - Moderate Operational Cost - Moderate Transparency - Moderate	Security - High Scalability - High Energy Consumption - Moderate

Source: Authors

Comparative evaluation of blockchain types in terms of technological requirements, challenges and the associated risks

There are four types of blockchain technology, including private, consortium, public, and hybrid. Private blockchain is a permissioned type, in which access is restricted to known, verified, and trusted participants who have the ability to read and write data. A single authority serves as the system provider and is responsible for evaluating and approving new applicants seeking access to the network and data. In private blockchain, the system provider has the ability to reverse certain processes and delete sensitive historical information to mitigate security vulnerabilities and operational errors. The transaction validation process is faster and operational costs are lower in private blockchain compared to other options, and energy consumption is also lower. However, participants cannot remain anonymous (no pseudonymity), new nodes must go through a pre-validation and evaluation process, and reliance on a single authority increases the risk of failure due to cyber-attacks. Proof of Stake (PoS), Proof of Authority (PoA), and Practical Byzantine Fault Tolerance (PBFT) are commonly used consensus algorithms in private blockchain applications (Zehir et al., 2022). The following subsection provides more detail on these consensus algorithms.

Similar to private blockchain, consortium blockchain is a permissioned blockchain type. On the other hand, it has a semi-decentralized structure because it is governed by a group rather than a single authority (Li et al., 2021). Blocks can only be validated by individuals who have been verified and trusted. As it has a middle ground in terms of energy consumption, operating costs, and transaction speed between private and public blockchain, consortium blockchain serves as a middle ground solution. The three most widely used consensus protocols are Proof of Work (PoW), Proof of Stakes, and Proof of Authority (PoA).

Public blockchain, also known as a permissionless blockchain, is accessible to any participant and assigns random IDs to users who do not have to disclose their personal information (Albrecht et al., 2018). Public blockchain is the foundation of Bitcoin and most Ethereum networks and lacks a central authority to evaluate new applicants or control ongoing traffic. Large-scale participation and a highly dispersed organization improve security, but also lead to slower transaction speed, higher energy consumption, and higher system costs. PoW and PoS are the most commonly used protocols in public blockchain.

Hybrid blockchain combines the favourable features of private and public blockchains, controlled access and freedom (Le, Hsu and Chen, 2021). In hybrid blockchain, the members have the power to decide who can join and which transactions can be made public. Its security, speed, and costs fall between those of consortium and public blockchain.

Consensus Mechanisms

There are more than 30 commonly used consensus methods for different applications. (Lu, Huang et al., 2019). Four of these consensus mechanisms are widely used and provide the basis for most of the others. This subsection comparatively introduces these four algorithms.

Proof of Work (PoW) enables any willing miner in a network to validate new data blocks, while allowing participating nodes to remain anonymous (Zhao, Fan and Yan, 2016). It involves extensive computation and verification of a transaction by several other nodes.

Proof of Stake (PoS) relies on the participation of stakeholders who own coins, assets, or smart contracts (Kaur et al., 2021). Those with significant stakes are permitted to validate new blocks and are referred to as "minters." They reserve a portion of their coins or assets as a security deposit in order to be selected as validators. If a validator engages in fraudulent or mistaken validation, they stand to lose their staked tokens. The potential loss of stakes serves as an incentive for participants to act fairly, as the potential benefits of fraud are relatively low.

Proof of Authority (PoA) includes the validation of transactions by particular authorized nodes. whose authorization is based on their disclosed organizational identities. These validators are subject to external regulations and binding agreements outside of blockchain platforms.

Practical Byzantine Fault Tolerance (PBFT) involves the authorization of a group of trusted validators by a single authority, with consensus reached through voting. This approach is used to decrease the risk of centralization, energy consumption, and costs, while increasing scalability in private blockchain applications (Hu, et al., 2020).

Risks

Blockchain has inevitable risks that need to be carefully considered and assessed when deciding on the most suitable solution and when adopting to a certain context. Standard risk considerations, value transfer risk considerations, and smart contract risk considerations are the three primary categories used by Deloitte to group risks (Deloitte, 2017).

Standard risk consideration is divided into eight subcategories. Strategic risk is the risk involved in an organization's decision to adopt a new technology at an early stage of its development or to wait for its further advancement and wider adoption before implementing it. This risk also includes decisions related to which network to join and which platform to use.

Business continuity risk refers to the potential interruption of network service due to operational circumstances or cyberattacks, which requires a rapid response and a short recovery period. Reputational risk is associated with compliance with legacy infrastructure. Information security risk involves the vulnerability of participant accounts or wallet registries and the security of transactions, particularly in private blockchain networks. Regulator risk is concerned with compliance with various regulatory requirements, which is more critical in international transactions. Operational and IT risks relate to speed, scalability, and interoperability with legacy systems during the implementation phase. Contractual risk involves the need for service-level agreements between participants and the network administrator. Supplier risks are associated with third-party technology providers.

Value transfer risk refers to the potential risks associated with transferring value, or assets, through a blockchain network. This type of risk can be further divided into four subcategories: consensus protocol risk, key management risk, data confidentiality risk, and liquidity risk. Consensus protocol risk refers to the potential vulnerabilities or operational problems that may arise with the chosen consensus algorithm, which is the process by which new transactions are verified and added to the blockchain. Key management risk refers to the possibility of an unauthorized party taking over control of an account or wallet, potentially leading to the irreversible loss of assets. Data confidentiality risk is concerned with the potential leakage of sensitive participant and transaction data to unauthorized parties. Liquidity risk refers to the risk of disputes arising in transactions and the need to resolve them based on predetermined regulations.

Smart contract risk considerations are divided into four subcategories; business and regulatory risks, contract enforcement, legal liability, and information security risks. Business and regulatory risks refer to the various business, economic, and legal considerations that need to be taken into account when determining the terms of a smart contract. This can include issues such as taxation, consumer protection laws, and other regulatory requirements. Contract enforcement risks refer to the potential difficulties that may arise in enforcing the terms of a smart contract, particularly in cases where the parties involved are located in different countries with different legal systems. Legal liability risks refer to the potential risks associated with fraudulent or mistaken use of smart contracts. Information security risks are related to the possibility of cyberattacks that could obtain, modify, or delete information contained within a smart contract. This could potentially lead to serious consequences for all parties involved.

In a study by Zhao and Chan (2020), seven general risks are identified in the use of blockchain technology. These risks include legal risk, which refers to the potential regulatory and legal issues that may arise, as well as the risk of business and regulatory problems. Technical risk refers to the potential operational and IT issues that may arise when implementing and using blockchain technology. Protocol risk is similar to consensus protocol risk and also has a connection to operational and IT risk. Cyber risk is closely related to key management risk and information security risk. Privacy risk is identical to data confidentiality risk. Validation risk is similar to legal liability. Market risk has similarities to strategic risk and reputational risk.

In this context, Table 3 presents a comparative evaluation of the various blockchain types.

Table 3: Comparative Evaluation of Blockchain Types in Terms of Technological Requirements, Challenges and the Associated Risks

Blockchain Types	Technological Requirements	Challenges	Dominant Risks
Public	Transaction Speed - Low Operational Cost - High Transparency - High	Security - High Scalability - High Energy Consumption - High	Legal risk Cyber risk Privacy risk
Private	Transaction Speed - High Operational Cost - Low Transparency - Low	Security - Moderate Scalability - Low Energy Consumption - Low	Technical risk Cyber risk Validation risk Protocol risk
Consortium	Transaction Speed - High Operational Cost - Low Transparency - Low	Security - High Scalability - Moderate Energy Consumption - Moderate	Validation risk
Hybrid	Transaction Speed - Moderate Operational Cost - Moderate Transparency - Moderate	Security - High Scalability - Moderate Energy Consumption - Moderate	Privacy risk Protocol risk

Source: Authors

The comparative evaluation of the considered consensus mechanisms is provided in Table 4.

Table 4: Comparative Evaluation of Consensus Mechanisms in Terms of Technological Requirements, Challenges and the Associated Risks

Blockchain Types	**Technological Requirements**	**Challenges**	**Dominant Risks**
PoW	Transaction Speed - Low Operational Cost - High	Security - High Scalability - High Energy Consumption - High	Privacy risk
PoS	Transaction Speed - Moderate Operational Cost - Moderate	Security - Moderate Scalability - Moderate Energy Consumption - Moderate	Validation risk Protocol risk
PoA	Transaction Speed - High Operational Cost - Low	Security - Low Scalability - Low Energy Consumption - Low	Validation risk
PBFT	Transaction Speed - High Operational Cost - Moderate	Security - Moderate Scalability - Low Energy Consumption - Moderate	Privacy risk Protocol risk

Source: Authors

Findings and Discussions

Findings

Consortium blockchain may be more suitable for use cases which satisfies any or a couple of the following: do not involve any or large number of vehicle owners/renters, where stake-holders does not change rapidly, which require high transaction speed or which does not have extreme scalability potential. Some suitable use cases could be road usage charge, smart parking management, vehicle finance, and usage-based insurance and mobility.

Hybrid blockchain is a type of blockchain that allows members to customize their network by determining which participants can join and which transactions will be made visible to the public. This type of blockchain is particularly well-suited for a wide range of use cases due to its ability to be customized to fit the specific needs of each individual member. Especially parts and recalls, maintenance and accidents, V2X communication, sale and registration, vehicle wallet and payments, odometer fraud prevention, V2G, traffic congestion management, carbon footprint, connected mobility marketplace could be favourable areas of use for hybrid blockchain.

Public blockchain with PoW consensus mechanism can be another alternative for vehicle registration and sale and digital wallet and payments, allowing higher scale applications with high security and pseudonymity, if high operational costs are feasible and relatively lower transaction speed is sufficient for the targeted application.

Among the identified applications for which consortium blockchain and hybrid blockchain applications could be suitable, the applications with lower risk of being targeted by cyberattacks can use PoS, while the applications with higher risk of cyberattacks could prefer PoA. V2G and V2X applications, traffic congestion management, vehicle wallet and payment, sale and registration are considered as the use cases that are highly likely to be targeted by cyber criminals.

Private blockchain does not seem to be the primarily preferable option for any of the potential applications. Although it has relatively lower costs and higher transaction speed compared to the other alternatives, its limited transparency and scalability, higher risk of data leakage, tampering and deletion in case of successful cyberattacks make it a low priority solution.

The overall view of suitable blockchain types and consensus algorithms are shown in Figure 2, where primarily suitable solutions are connected with solid arrows and optionally suitable applications based on project-specific availabilities are linked using dashed arrows. The arrows that leave the same criterions (transparency, transaction speed, scalability, energy consumption, security and operational cost) share the same color. In a similar manner, the arrows that are directed to the same blockchain type has the same color.

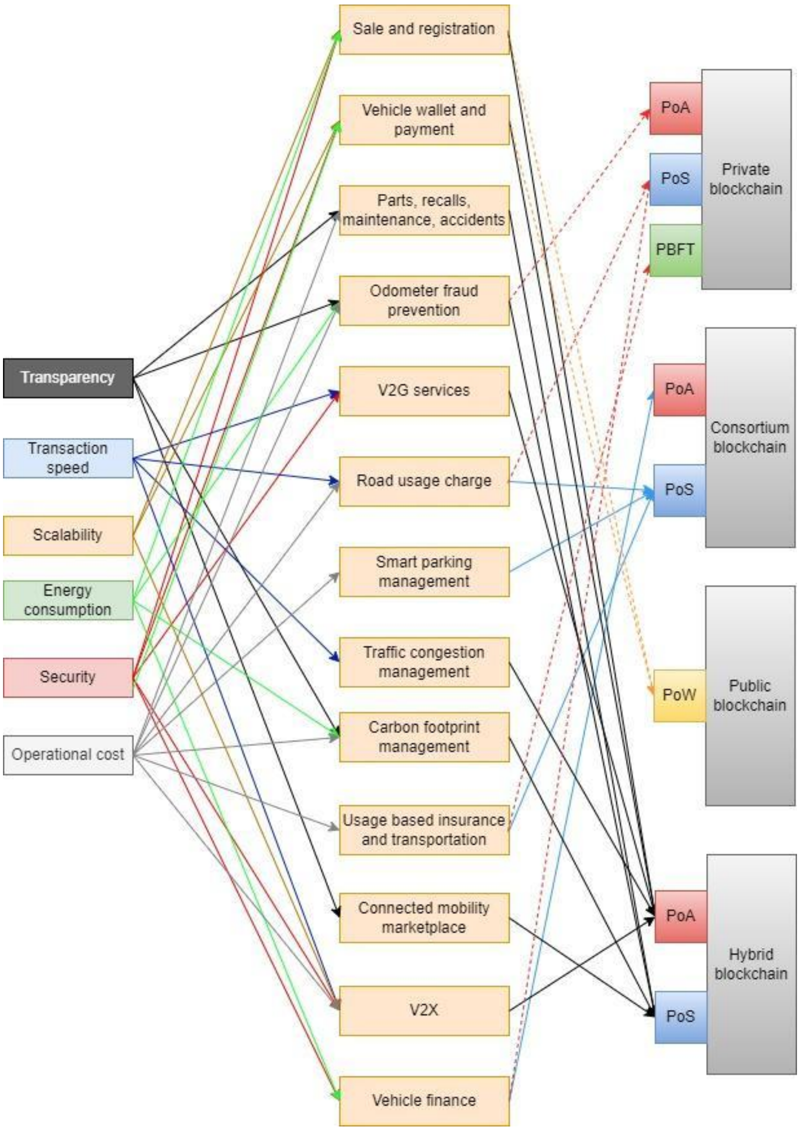

Figure 2: Suitable Blockchain Types and Consensus Algorithms based on Use Cases and Related Requirements; *Source:* Authors

Discussion

The majority of the use cases identified in the mobility ecosystem involves seamless data sharing between authorized stakeholders. Consortium blockchain and hybrid blockchain can address the needs of several different use cases. Public blockchain is only found suitable for

Although private blockchain could not be the primarily preferable solution, the use cases with the needs listed below could optionally prefer private blockchain if there are project-specific availabilities and considerable additional benefits compared to consortium blockchain:

i. Mainly based on data creation dominantly by a single stakeholder organization;
ii. Require fast transaction speed;
iii. Aim low operational costs;
iv. Have limited scalability.

Some optionally potential areas could be road usage charge, vehicle finance, odometer and usage-based insurance and mobility. For applications that that require higher security, such as odometer fraud, and vehicle finance, PoA could be more suitable than PoS. For low energy consumption targeted applications with limited scalability such as usage-based insurance and mobility, PBFT could be preferred over PoS.

Considering the risks, for critical infrastructure applications such as V2G, V2X, traffic congestion management, operational and IT risks and information security risks need to be taken into account. Odometer fraud prevention can also have operational and IT risks due to scalability, while V2G, V2X and smart parking management use cases may face supplier risks due to intense involvement of third-party technology providers. For vehicle wallet and payment, sale and registration and vehicle finance, key management risk and legal liability risk come to the fore. Contractual risk has higher importance in sale and registration, parts, re-calls, maintenance and accidents and smart parking management. Vehicle wallet and payment also has information security risk too. Vehicle finance also has liquidity risk, just as road usage charge. For regulatory or intensively multi-stakeholder applications such as carbon footprint management, connected mobility marketplace, parts, recalls, maintenance and accidents, usage based insurance and transportation, regulatory risk, reputational risk and contract enforcement risks become prominent.

Conclusions

This paper comprehensively presented the emerging use cases of blockchain in the transforming mobility ecosystem. 13 use cases are presented, each of which has different requirements for blockchain adoption. The multi-stakeholder environment, the need for wide sharing of data between several entities, interrelations between stakeholder's products and services, cybersecurity of critical infrastructure and data are strong drivers for wide deployment of blockchain in mobility use cases. Based on the availabilities, limitations and risks of blockchain types and consensus algorithms, suitable blockchain implementation opportunities that can accurately address the use case needs are highlighted. In overall, consortium blockchain and hybrid blockchain are stated to be the suitable options for most of the use cases in mobility. Public blockchain is explained to be a preferable option for use cases needing high scalability, with tolerable transaction speed, energy consumption and feasible costs. Private blockchain does not seems to be the primary solution for any of the identified use cases. Still, it can be optionally preferred in use cases that need high transaction speed, low energy consumption and costs, with tolerable scalability.

Future studies need to focus on case studies involving industrial actors to develop high technology readiness level (TRL) solutions and pilot demonstration of applications in the field.

Acknowledgement

All authors have read and agreed to the published version of the manuscript.
Author Contributions: Conceptualization, M.Z. and C.Z.; methodology, C.Z.; investigation, M.Z.; resources, M.Z.; writing—original draft preparation, M.Z..; writing—review and editing, C.Z.
Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.
Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to restrictions.
Conflicts of Interest: The authors declare no conflict of interest.

References

Al Amiri, W., Baza, M., Banawan, K., Mahmoud, M., Alasmary, W., & Akkaya, K. (2020). Towards secure smart parking system using blockchain technology. *17th IEEE Annual Consumer Communications and Networking Conference*, 1–2. https://doi.org/10.1109/CCNC46108.2020.9045674

Albrecht, S., Reichert, S., Schmid, J., Strüker, J., Neumann, D., & Fridgen, G. (2018, January). Dynamics of blockchain implementation-a case study from the energy sector. In *Proceedings of the 51st Hawaii International Conference on System Sciences*. https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/abc4d788-862f-421c-8ac9-dc549e333585/content

Al-Saif, N., Ahmad, R. W., Salah, K., Yaqoob, I., Jayaraman, R., & Omar, M. (2021). Blockchain for Electric Vehicles Energy Trading: Requirements, Opportunities, and Challenges. *IEEE Access*, 9, 156947–156961. https://doi.org/10.1109/ACCESS.2021 .3130095

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., ... & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews*, *100*, 143-174.

Astarita, V., Giofrè, V. P., Guido, G., & Vitale, A. (2020). The use of a Blockchain-based System in Traffic Operations to promote Cooperation among Connected Vehicles. *Procedia Computer Science*, 177, 220–226. https://doi.org/10.1016/j.procs.2020.10.031

Badr, M. M., Al Amiri, W., Fouda, M. M., Mahmoud, M. M. E. A., Aljohani, A. J., & Alasmary, W. (2020). Smart parking system with privacy preservation and reputation management using blockchain. *IEEE Access*, 9, 150823–150843. https://doi.org/10.1109/ACCESS.2021 .3130095

Giuffrè, T., Siniscalchi, S. M., & Tesoriere, G. A. (2012). A novel architecture of parking management for smart cities. *Procedia - Social and Behavioral Sciences*, 53, 16–28. https://doi.org/10.1016/j.sbspro.2012.09.856

Hacioglu, U. (Ed.). (2019). *Handbook of research on strategic fit and design in business ecosystems*. IGI Global.

Hacioglu, U. (2020). *Digital Business Strategies in Blockchain Ecosystems: Transformational Design and Future of Global Business*. Cham: Springer Nature Switzerland AG.

Hacioglu, U., & Aksoy, T. (2021). *Financial Ecosystem and Strategy in the Digital Era: Global Approaches and New Opportunities.* Springer Nature.

Hassija, V., Zeadally, S., Jain, I., Tahiliani, A., Chamola, V., & Gupta, S. (2021). Framework for determining the suitability of blockchain: Criteria and issues to consider. *Transactions on Emerging Telecommunications Technologies*, *32*(10), e4334. https://doi.org/10.1002/ett.4334.

Hu, X., Zheng, Y., Su, Y., & Guo, R. (2020). IoT Adaptive Dynamic Blockchain Networking Method Based on Discrete Heartbeat Signals. *Sensors*, *20*(22), 6503. https://doi.org/10.3390/s20226503

Inrix. (2015). 9. Accelerates INRIX Development of Smart Parking Services for Drivers Worldwide. https://inrix.com/press-releases/parkme-english/ [Accessed December 8, 2022].

Kaur, M., Khan, M. Z., Gupta, S., Noorwali, A., Chakraborty, C., & Pani, S. K. (2021). MBCP: Performance analysis of large scale mainstream blockchain consensus protocols. *IEEE Access*, *9*, 80931-80944. https://doi.org/ 10.1109/ACCESS.2021.3085187

Kim, S. (2018). Blockchain for a trust network among intelligent vehicles. *Advances in Computers*, 111, 43–68.

Kumar, A., Prasad, A., & Murthy, R. (2019). Application of Blockchain in Usage Based Insurance. *International Journal of Advance Research, Ideas and Innovations in Technology*, 5(2), 1574–1577.

Le, T. V., Hsu, C. L., & Chen, W. X. (2021). A Hybrid Blockchain-Based Log Management Scheme with Non-Repudiation for Smart Grids. *IEEE Transactions on Industrial Informatics*. https://doi.org/10.1109/TII.2021.3136580

Leong, C. H., Gu, C., & Li, F. (2018). Auction mechanism for P2P local energy trading considering physical constraints. *Energy Procedia*, 158, 6613–6618. https://doi.org/10.1016/j.egypro.2019.01.045

Li, M., Lal, C., Conti, M., & Hu, D. (2021). LEChain: A blockchain-based lawful evidence management scheme for digital forensics. *Future Generation Computer Systems*, *115*, 406-420. https://doi.org/10.1016/j.future.2020.09.038

MOBI. (2021a). Blockchain For Vehicle Identity Business Whitepaper. https://dlt.mobi/wp-content/uploads/2021/03/MOBI-VID0001-2021.pdf [Accessed December 5, 2022].

MOBI. (2021b). Connected Mobility Data Marketplace Business Whitepaper. https://dlt.mobi/ wp-content/uploads/2021/03/MOBI-CMDM0001-White-Paper-2021. pdf [Accessed December 5, 2022].

MOBI. (2021c). Electric Vehicle Grid Integration Business Whitepaper. https://dlt.mobi/wp-content/uploads/2021/02/MOBI-EVGI-0001-White-Paper-2021.pdf [Accessed December 7, 2022].

MOBI. (2021d). Finance, Securitization & Smart Contracts. Business White Paper. https://dlt.mobi/wp-content/uploads/2021/06/MOBI-FSSC0001WP2021-Version-1_compressed.pdf [Accessed December 7, 2022].

MOBI. (2021e). Vehicle Identity II: Use Cases and Business Requirements https://dlt.mobi/ wp-content/uploads/2021/02/MOBI-VID0002-Use-Case-2021.pdf [Accessed December 7, 2022].

PankiRaj, J. S., Yassine, A., & Choudhury, S. (2019). An auction mechanism for profit maximization of peer-to-peer energy trading in smart grids. *Procedia Computer Science*, 9, 156947–156961. https://doi.org/10.1016/j.procs.2019.04.050

Park, J. H., & Park, J. H. (2017). Blockchain security in cloud computing: Use cases, challenges, and solutions. *Symmetry*, 9(8), 1–13. https://doi.org/10.3390/sym9080164

Shresta, R., Nam, S. Y., Bajracharya, R. & Kim, S. (2020). Evolution of V2X communication and integration of blockchain for security enhancements. *Electronics*, 9(9), 1–33. https://doi.org/10.3390/sym9080164

Singh, P. K., Singh, R., Muchahary, G., Lahon, M. & Nandi, S. (2019). A blockchain-based approach for usage based insurance and incentive in its. *TENCON 2019*, 1202–1207. https://doi.org/10.1109/TENCON.2019.8929322

SpotHero. (2022). SpotHero App. https://www.excellentwebworld.com/best-app-of-the-week/spothero-app/ [Accessed December 8, 2022].

Zehir, C., Zehir, M., Borodin, A., Mamedov, Z. F., & Qurbanov, S. (2022). Tailored Blockchain Applications for the Natural Gas Industry: The Case Study of SOCAR. *Energies*, *15*(16), 6010. https://doi.org/10.3390/en15166010

Zhao, J. L., Fan, S., & Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financial innovation*, *2*(1), 1-7. http://dx.doi.org/10.1186/s40854-017-0059-8

Publisher's Note: Bussecon International stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.