Integration of Blockchain with Connected and Autonomous Vehicles: Vision and Challenge

TOOSKA DARGAHI, University of Salford, UK
HOSSEIN AHMADVAND, Sharif University of Technology, Iran
MANSOUR NASER ALRAJA, Dhofar University, Oman
CHIA-MU YU, National Yang Ming Chiao Tung University, Taiwan

Connected and Autonomous Vehicles (CAVs) are introduced to improve individuals' quality of life by offering a wide range of services. They collect a huge amount of data and exchange them with each other and the infrastructure. The collected data usually includes sensitive information about the users and the surrounding environment. Therefore, data security and privacy are among the main challenges in this industry. Blockchain, an emerging distributed ledger, has been considered by the research community as a potential solution for enhancing data security, integrity and transparency in Intelligent Transportation Systems (ITS). However, despite the emphasis of governments on the transparency of personal data protection practices, CAV stakeholders have not been successful in communicating appropriate information with the end-users regarding the procedure of collecting, storing and processing their personal data, as well as the data ownership. This paper provides a vision of the opportunities and challenges of adopting blockchain in ITS from the "data transparency" and "privacy" perspective. The main aim is to answer the following questions: (1) Considering the amount of personal data collected by the CAVs, such as location, how the integration of blockchain technology would affect *transparency, fairness and lawfulness* of personal data processing concerning the data subjects (as this is one of the main principles in the existing data protection regulations)? (2) How the trade-off between transparency and privacy can be addressed in blockchain-based ITS use cases?.

CCS Concepts: • **Security and privacy** → **Pseudonymity, anonymity and untraceability**; • **Computer systems organization** → **Peer-to-peer architectures**.

Additional Key Words and Phrases: Connected and Autonomous Vehicles, Blockchain, Transparency, Privacy

ACM Reference Format:
Tooska Dargahi, Hossein Ahmadvand, Mansour Naser Alraja, and Chia-Mu Yu. 2021. Integration of Blockchain with Connected and Autonomous Vehicles: Vision and Challenge. 1, 1 (April 2021), 9 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

The world has entered the era of Connected and Autonomous Vehicles (CAVs) and their value will become increasingly prominent. According to the UK's Centre for Connected and Autonomous Vehicles [10], CAV technology not only improves the transportation system but also provides economic growth and job opportunities, such that the UK market could be worth £62 billion by 2035 [18]. In the modern Intelligent Transportation System (ITS), vehicles are equipped

Authors' addresses: Tooska Dargahi, University of Salford, Manchester, UK, t.dargahi@salford.ac.uk; Hossein Ahmadvand, Sharif University of Technology, Tehran, Iran, ahmadvand@ce.sharif.edu; Mansour Naser Alraja, Dhofar University, Oman, malraja@du.edu.om; Chia-Mu Yu, National Yang Ming Chiao Tung University, Taiwan, chiamuyu@nycu.edu.tw.

with several sensors, including cameras, GPS, Lidar and Radar and collect a huge amount of data, such as geolocation data. To handle the challenging driving tasks, CAVs make use of the data that are collected from either built-in sensors or the roadside units (RSU) and/or other vehicles to interpret the surrounding environment and make real-time decisions ensuring the efficiency and safety of the transportation system [40]. These vehicles communicate with each other (V2V), with the manufacturers, with the infrastructure (V2I) and with everything else (V2X). Although recent advancements in the vehicular industry sound promising, researchers argue that privacy, trust, access control, data ownership and transparency are among the most important issues that need to be addressed for society to accept this emerging technology [26, 28, 33, 50].

These vehicles can collect and store privacy-sensitive data about individuals, such as location, video and audio recordings. According to Lim and Taeihagh [36], insurance companies can use CAV data for calculating individual's credit scores, while location information and travel history could be misused against certain individuals. Governments, including the EU, UK, US, Australia, China, Japan and Singapore have already released regulations regarding data privacy and cybersecurity in CAVs [5, 36]. However, these guidelines are not quite clear on how proper implementation of those principles should look like. At the same time, some researchers believe that most of the privacy challenges with regards to transportation data relate to the centralised storage of the collected data by the service providers and lack of proper access control mechanisms [37]. This does not mean that the data is stored on a single server, rather the problem is the service provider who has the sole control over the users' data and users do not have any control over their data being shared with other service providers, e.g., insurance companies, legal authorities, etc. To tackle some of these challenges, various researchers in academia and industry suggest the integration of blockchain technology in transportation systems [31, 49]. Their main argument is that blockchain will improve data security, ownership, trust, transparency and auditability[37].

1.1 Blockchain for Smart Transportation

Blockchain is a trustless decentralized digital ledger of transactions that are stored in the form of a series of blocks on distributed nodes [47]. Each node in the blockchain network broadcasts the transaction to the other nodes and specific nodes, called “miners", verify the transactions, generate blocks and add them to the chain. Each node in the network stores a replica of each block that is secured by miners using cryptographic functions.

One of the main features of blockchain is *the transparency of information*, which is provided due to it being a public ledger thereby creating consensus and confidence in the direct communication between the associated parties, without the need for a trusted third party (TTP). For example, insurance of CAVs is different from normal cars, as there wouldn't be a driver who might be responsible for an accident, rather the car insurance providers require to have access to different kinds of data (e.g., accident data, car-related data, environment condition) to understand if the accident has happened due to malfunctioning of the AV itself, or an external incident/entity had an effect on the accident. The immutability nature of blockchain would protect the stored data against tampering without a consensus within the blockchain network. The usage of *smart contracts* in blockchain-based systems further helps in the removal of TTPs and instead develops immutable agreements between different untrusted parties in a decentralised manner through pieces of code [43].

Due to its promising features, such as decentralization, security, immutability and anonymity, blockchain has become a revolutionary technology and attracted the attention of the vehicular research community [41]. Decentralized blockchain-based intelligent transportation systems, to improve security, trust and privacy in different applications have been proposed in several research papers [30, 32, 46, 48, 49]. Moreover, a framework for the forensic investigation of AVs to store detailed vehicle data which can be used in post-accident scenarios by insurance companies is proposed in [27]. Also, a blockchain framework for securing CAVs is presented in [45], where activities of each entity, i.e., the vehicle or the in-vehicle IoT devices, are traced and recorded inside the blockchain to provide secrecy and transparency among the customers and drivers.

The existing body of literature on the blockchain-based solutions for ITS mainly concentrates on the benefits and use cases of integrating blockchain with IoV and ITS, with a few numbers of solutions for CAV. However, to the best of our knowledge, they do not take into account what personal data protection means from law enforcement and privacy regulations' perspective. Despite favourable features of blockchain, there is a trade-off between transparency (provided by a public blockchain) and privacy (provided by a permission blockchain) [35]. It is within each individual's right to know what kind of data is generated and gathered about them, especially when it comes to auditing, legal and ethical scenarios [22]. This became more challenging with the introduction of the General Data Protection Regulation (GDPR) [15], the EU data security and privacy law that came into effect on 25 May 2018.

1.2 Data Protection Law

GDPR [15] comprises 99 articles, which are organised into sections ranging from initial principles and specific definitions, through rights of the data subject, controllers and processors, and obligations of each. According to the UK Information Commissioner's Office (ICO) [17] GDPR sets out seven key principles. (1) *Lawfulness, fairness and transparency*: identification of valid grounds for collection and use of personal data; ensuring any action does not breach other laws; 'fair' use of data – that which is not detrimental, unexpected, or misleading to the individual; clarity, openness, and honesty in how data is used. (2) *Purpose limitation*: being clear about the purposes for processing from the start; recording these purposes and clearly signposting them for the individual (privacy policy); consent is obtained for any new use of data. (3) *Data minimisation*: the data collected is adequate to fulfil the purpose, is relevant to that purpose and is limited to only that which is necessary. (4) *Accuracy:* steps are taken to ensure correct and not misleading; if incorrect or misleading steps are taken to remedy as soon as is reasonably possible. (5) *Storage limitation*: keep data for no longer than it is needed, with justifications for time frames; policy of standard retention periods; erase or anonymise data that is no longer needed; offer the right to erasure for the individual. (6) *Integrity and confidentiality*: appropriate security measures must be in place to protect the data. (7) *Accountability*: to take responsibility for what is done with data and compliance with the other principles.

As discussed earlier in this section, blockchain and smart contracts have the potential to solve the security and trust challenges in vehicular systems. Introducing blockchain technology to CAVs will pave the way for additional services, e.g. insurance and secure software update, that can be explored if properly implemented. However, personal data protection according to the guidelines of the regulations remains an important challenge that we discuss here. This paper evaluates the effectiveness of adopting blockchain by the CAV industry considering the interplay between data confidentiality, data privacy and transparency. In the remainder of the paper, Section 2 reviews the opportunities provided by the adoption of blockchain in CAV, along with real-world use case scenarios, while Section 3 discusses existing challenges. Section 4 concludes the paper and highlights future research directions.

2 OPPORTUNITIES OFFERED BY INTEGRATING BLOCKCHAIN WITH CAVS

As discussed in the previous section, the adoption of blockchain technology in smart transportation is beneficial for both the stakeholders and the users in different ways. In this section, we review some of the opportunities provided by blockchain in real-world use case scenarios concerning privacy and transparency. Figure 1 shows the opportunities and challenges that we cover in this section and Section 3.

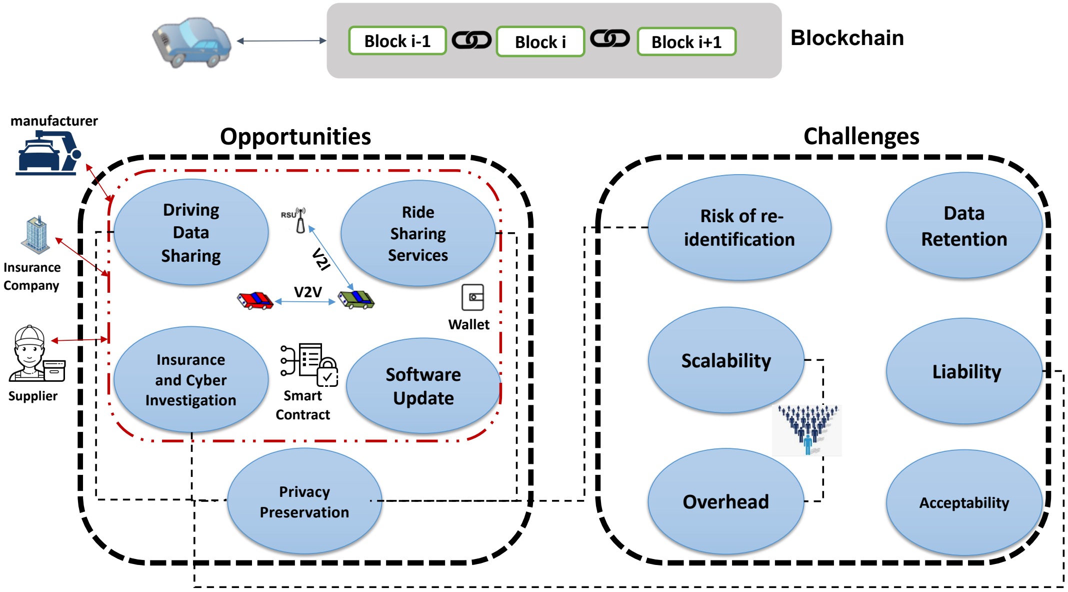

Fig. 1. Opportunities and challenges of integrating blockchain with CAV

2.1 Transparency in Data Sharing

The automotive industry has started to explore different ways of benefiting from blockchain in smart transportation. According to Toyota [20], blockchain will improve the interaction between different stakeholders, e.g., manufacturers, suppliers and dealers, due to the transparency and immutability of their transactions. It also facilitates driving and vehicle testing data sharing between the customers and the manufacturers to ensure safe and reliable operation of the vehicles, as blockchain assures that vehicle data has not tampered with. Toyota Research Institute (TRI) is working hand in hand with academic institutions and industry to integrate blockchain with autonomous vehicles to improve transparency, traceability and trust [20]. The TRI and its partners have focused on three prominent areas: driving data sharing, ride-sharing and car-sharing transactions and vehicle insurance [21]. In the open vehicle data platform proposed by Kaiser et al. [34], users can decide who can access what kind of data (e.g., anonymised data, vehicle-specific data or user-specific data). Moreover, a blockchain-based platform enables car/ride-sharing services by CAV, similar to Uber. This would allow owners to monetize their vehicles by selling ride services through smart contracts. The decentralization and data immutability features of blockchain provide transparency for the customers [20].

Insurance companies and cyber forensic investigators would also benefit from the immutability feature of blockchain-enabled CAVs [27]. Using blockchain, various kinds of data, such as vehicle information (e.g., event data recorder (EDR) data, vehicle usage data, parts supply chain, etc) and user-related information could be securely shared among service providers and authorities to improve information management and protect data integrity, while preserving data ownership through smart contracts. As mentioned in the Introduction Section, an important challenge regarding CAV data is that it is not clear who owns the data and only manufacturers have a holistic view of the data storage and access. However, using blockchain and smart contract will facilitate appropriate access arrangements between different stakeholders and users. Also, the insurance contracts can be stored in the blockchain [1, 29]. Ford, GM, Renault and BMW have formed a consortium to take advantage of blockchain opportunities in different domains, including vehicle identity and data tracking, supply chain tracking, as well as vehicle payments [8, 12]. In the latter case, the in-vehicle wallet will provide payment opportunity [2].

Another opportunity provided by the blockchain is related to security and defending CAVs against software/firmware vulnerability exploitation [39]. CAVs are composed of different components, where each component requires periodic software and firmware update. A recent large scale cyber attack against SolarWinds IT company has shown that a compromised software channel could lead to the installation of malicious software updates on customers' devices [19]. This scenario, if happens for CAVs, would lead to a hazard and put the public's safety in danger. While, as proposed in [25], the immutability feature of blockchain would help in ensuring the authenticity and integrity of software/firmware updates. CUBE [11], a network security company, also provides a blockchain-based AV security platform for different data consumers, such as insurance companies. Their platform provides an over-the-air (OTA) tool to securely upgrade vehicle's software and perform remote software diagnostics. Referring to Figure 1, these opportunities are shown on the left-hand side of the figure (inside the red rectangle), and examples of involved parties are provided. Usage of smart contracts will lead to increased trust and transparency and reduced risk of fraud [21]. Moreover, vehicle data could be shared with other vehicles and the infrastructure using blockchain without the need to have a TTP.

2.2 Privacy-Preserving Analysis

The privacy of the users should be considered in all the stages of a cyber investigation. Blockchain provides a platform for "trustless, traceable, and privacy-aware post-accident analysis" [27]. Using permission blockchain provides the possibilities of using anonymous identities by CAV users while sharing their vehicle data with the stakeholders. Using blockchain in CAVs, also provides an opportunity to use coin-mixer algorithms to benefit from privacy-preserving and anonymity by removing any logical relation between inputs and outputs of blockchain [24]. This will improve privacy for critical transactions and message exchange, however, more efforts to increase the level of transparency is required. Solutions for privacy-preserving authentication and trust management based on blockchain has been introduced in [38] for vehicular location-based services. The authors discuss the inefficiency of traditional privacy-preserving algorithms, e.g., k-anonymity, in the context of vehicular networks. They explain that their proposal enhances security, privacy and reliability, while the imposed overhead is negligible. Figure 1 shows privacy preservation as an opportunity that could positively affect other opportunities, i.e., investigation, location services and data sharing, demonstrated by lines between these components.

3 CHALLENGES

Although there are impressive opportunities in integrating blockchain with CAV, there are important challenges in terms of transparency requirements, specifically with regards to big data analysis, users' legal rights to delete/modify their own records, and the trade-off between privacy, transparency and usability, which should be taken into account. In this section, we discuss some of the main challenges as depicted in Figure 1. In this figure, the lines between some of the opportunities and challenges demonstrate the trade-off between the offered opportunity and the imposed challenge.

3.1 Data Retention

As discussed earlier, blockchain is a distributed ledger and a copy of the user's data and transactions are stored publicly by each of the miner nodes without any means for erasing such data. Although we could assume that all such data are encrypted and/or anonymised, a challenge still exists on how to explain to the data subject, where the data is stored and for how long. Chapter 3 of the GDPR [14] explains the rights of the data subject regarding transparency on collection and processing of the data and the right to be forgotten. Article 12 of GDPR [3] clearly states that the storage and processing of the users' data must be done in "a concise, transparent, intelligible and easily accessible form, using clear and plain language". Article 13 of GDPR provides further details on the information that must be provided to the data subject to ensure fairness and transparency [4]: "the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period". It also explains the right to rectification and erasure [4]: "the existence of the right to request from the Controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to the processing as well as the right to data portability". The trade-off between taking advantage of blockchain and GDPR compliance has been discussed by the EU Parliamentary Research Service in [35]. However, in the case of CAVs, this challenge is even more problematic when it comes to the video recordings captured by the CAV's camera, where pedestrians and other vehicles are identifiable, who clearly have not given consent for their data to be stored and processed in the blockchain. As another example, in a CAV sharing scenario, passengers may be required to choose their privacy settings, and they might have different privacy preferences. However, if such data is going to be stored on the blockchain, providing such privacy preference selection becomes challenging.

3.2 Risk of re-identification

In January 2020, the European Data Protection Board (EDPB) released guidelines on personal data processing in CAV [16]. It explains that three categories of data, including geolocation, biometric, and data that reveal a criminal offence, which is generated by CAVs are very sensitive. The EDPB suggests "local" storage and processing of such data where possible, and if external processing is required, proper security mechanisms must be in place to protect the data. In the case of blockchain, several cryptographic algorithms, as well as pseudonyms could be used to preserve the privacy of users and vehicles. In a very recent survey study, Mollah et al. [41] discussed the inefficiency of the existing methods and suggested the potential of applying differential privacy to enhance privacy in IoV applications. However, we argue that one of the main drawbacks of differential privacy, compared to other privacy-preserving methods, is that it does not give a clear idea to the end-user to what extent his privacy is preserved and what is the probability of re-identification. Considering that users' data is stored on the blockchain and replicated on several nodes, it is not clear how the risk of re-identification could be measured. Moreover, to the best of our knowledge, a proper privacy-preserving technology for streaming data that could guarantee a high level of privacy protection is still an open problem. We argue that decentralized storage of such sensitive data might affect the re-identification probability.

3.3 Scalability and Overhead

In any given blockchain, the number of blocks increases as the usage grows over time. For instance, there has been an increase in the size of the Bitcoin blockchain from a few megabytes in 2009 to 302GB in October 2020 [7]. This means that reaching a consensus would require much more computational capabilities and resources. As shown in figure 1 adoption of blockchain in vehicular networks could improve transparency and privacy to some extent, with the expense of increased computation overhead. Due to the huge amount of generated data and the necessity for real-time processing of such data, scalability and overhead are among the main issues of adopting blockchain in CAV. Efforts have been made to increase the block size, use different consensus mechanisms, and use optimization frameworks based on reinforcement learning to improve scalability [41]. A framework for reducing the computation of public-key signature for V2I communications is proposed in [23]. However, the challenge still exists in V2V (Vehicle to Vehicle) communications. Although, this approach improves transparency and data privacy in the data exchange to/from RSUs, the data generated by the On-board Units (OBUs) are still at risk. Ford and Volkswagen have used cryptocurrency based on blockchain for V2V and inter-vehicle communication [13], [9]. However, such a combination imposes communication and computation overhead. As discussed in [44] there is a trade-off between scalability, security and decentralization. Although permission blockchain might seem to be more scalable (and to some extent provide more privacy [35]), the security of the system might be reduced. Therefore, a proper combination of different parameters is required in the context of CAVs.

3.4 Liability and Acceptability

According to IBM [6], knowledge about blockchain among transport planners and policymakers is somewhat restricted. Blockchain implementation in the transport sector, especially for CAVs, will be restricted to innovative ideas and possibly small-scale projects, as otherwise, a large number of stakeholders should adopt distributed ledger, and new regulations are required. Although researchers believe that using blockchain is a good approach for liability attribution in CAV [42], we argue that the use of blockchain might raise some legal issues which need to be addressed. The liability for failures or other technical errors will be a significant legal concern especially in the case of forensic investigation and insurance (as shown in Figure 1). Since we rely on decentralized technology, the network will not be maintained by any centralized body. Therefore for large-scale adoption of blockchain for the automotive industry proper regulatory and legal measures should be in place.

4 CONCLUSION

In this “vision" paper, we answered the research questions that were set in the abstract by discussing the opportunities and challenges that integration of blockchain with CAV will bring about. As extensively explained, the most important benefits of using blockchain and smart contracts in this context include: (1) the integrity of the exchanged information due to their immutability feature, (2) transparency of transactions on CAV-related data between different stakeholders, (3) possibility of preserving privacy using permission blockchain, and (4) providing trust between stakeholders without a trusted third party. However, several challenges identified in this paper which would affect the privacy of data subjects. The most important challenge is *decentralisation vs privacy*. Considering that CAV data includes very sensitive information, new legislation is required to define specific use cases and applications of blockchain where decentralise data storage would not affect the user privacy rights according to GDPR (and/or other privacy regulations), in particular *right to be forgotten*. Although blockchain inherently provides transparency over data transactions, it might diminish users' privacy, in particular their control over how their personal data is stored and processed. Although some suggestions are provided in [35], such as usage of hybrid or permission blockchain, more investigation and research specific to CAV data type is required. Another identified challenge is *the imposed overhead* by the integration of blockchain with CAVs, which would affect the real-time processing of data. Possible solutions to consider for this challenge could be increasing the bandwidth for V2V and V2I communication, and improving the computation capabilities of RSUs and OBUs. Future research could concentrate on finding proper measures for defining an acceptable threshold for the trade-off between transparency and privacy. Possible directions could be considering data categorization, as suggested in [34], and defining fine-grained access control policies over the blockchain-based systems. Other approaches to look into could be consideration of off-chain transactions for specific data types and usage of proper privacy-preserving algorithms which are suitable for streaming data to deal with the risk of re-identification.

5 ACKNOWLEDGEMENT

We thank Abba Toko Gongulong and Thomas Bolton for their assistance during the data collection and the literature review. This research is supported by the UK Royal Society Award, Grant Number: IEC\R3\183047, by the Research Council (TRC), Sultanate of Oman (Block Fund-Research Grant), Grant Number: BFP/RGP/ICT/19/186, and by the Ministry of Science and Technology (MOST), Taiwan, Grant Number: MOST 110-2636-E-009-018 and 110-2927-I-009-510.

REFERENCES

[1] [n.d.]. 5 Ways Autonomous Vehicles Can Use Blockchain. https://innotechtoday.com/autonomous-vehicles-blockchain/. Accessed: 2020-11-25.

[2] [n.d.]. Analysis of Blockchain Technology in the Mobility Sector. https://philippsandner.medium.com/analysis-of-blockchain-technology-in-the-mobility-sector-1078e429615f. Accessed: 2020-11-25.

[3] [n.d.]. Art. 12 - GDPR Transparent information, communication and modalities for the exercise of the rights of the data subject. https://gdpr-info.eu/art-12-gdpr/. Accessed: 2020-11-26.

[4] [n.d.]. Art. 13 GDPRInformation to be provided where personal data are collected from the data subject. https://gdpr-info.eu/art-13-gdpr/. Accessed: 2020-11-26.

[5] [n.d.]. Automated Vehicles. https://www.lawcom.gov.uk/project/automated-vehicles/. Accessed: 2021-03-01.

[6] [n.d.]. Blockchain-powered autonomous automobiles can be the answer. https://www.ibm.com/blogs/blockchain/2020/04/blockchain-powered-autonomous-automobiles-can-be-the-answer/. Accessed: 2020-10-26.

[7] [n.d.]. Blockchain Size. https://www.blockchain.com/en/charts/blocks-size. Accessed: 2020-10-20.

[8] [n.d.]. BMW Blockchain. https://www.bmw.com/en/innovation/blockchain-automotive.html. Accessed: 2020-11-26.

[9] [n.d.]. CNNBlockchhain. https://www.ccn.com/uk-giant-seeks-patent-for-invention-mitigating-blockchain-attacks/. Accessed: 2020-11-24.

[10] [n.d.]. Connected and Automated Vehicles in the UK: 2020 information booklet. https://www.gov.uk/government/publications/connected-and-automated-vehicles-in-the-uk-2020-information-booklet. Accessed: 2020-11-28.

[11] [n.d.]. CUBEINT. https://cubeint.io/wp-content/uploads/2019/03/CUBEWhite_Paper-V2.2.pdf. Accessed: 2020-11-01.

[12] [n.d.]. Ford, Renault, GM, BMW, IBM co-found MOBI blockchain consortium. https://internetofbusiness.com/ford-renault-gm-bmw-ibm-co-found-mobi-blockchain-consortium/. Accessed: 2020-11-25.

[13] [n.d.]. FordBlockchain. https://news.bitcoin.com/ford-cryptocurrency-inter-vehicle-communication-system/. Accessed: 2020-11-24.

[14] [n.d.]. GDPR Chapter 3 - Rights of the data subject. https://gdpr-info.eu/chapter-3/. Accessed: 2020-11-26.

[15] [n.d.]. General Data Protection Regulation. https://gdpr-info.eu/. Accessed: 2020-11-26.

[16] [n.d.]. Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf. Accessed: 2020-11-29.

[17] [n.d.]. ICO - Information Principle (a): Lawfulness, fairness and transparency. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/. Accessed: 2021-03-05.

[18] [n.d.]. INNOVATION IS GREAT - Connected and Automated Vehicles. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/929352/innovation-is-great-connected-and-automated-vehicles-booklet.pdf. Accessed: 2020-11-28.

[19] [n.d.]. SolarWinds advanced cyberattack: What happened and what to do now. https://blog.malwarebytes.com/threat-analysis/2020/12/advanced-cyber-attack-hits-private-and-public-sector-via-supply-chain-software-update/. Accessed: 2021-03-01.

[20] [n.d.]. Toyota builds up Blockchain abilities. https://autovistagroup.com/news-and-insights/toyota-builds-blockchain-abilities. Accessed: 2020-10-30.

[21] [n.d.]. Toyota, MIT Lab Eye Using Blockchain in Insurance Rating of Driverless and Shared Vehicles. https://www.insurancejournal.com/news/national/2017/05/23/451913.htm. Accessed: 2020-10-30.

[22] Nadia Adnan, Shahrina Md Nordin, and Mohamad Ariff bin Bahruddin. 2019. Sustainable interdependent networks from smart autonomous vehicle to intelligent transportation networks. In *Sustainable Interdependent Networks II*. Springer, 121–134.

[23] Ikram Ali, Mwitende Gervais, Emmanuel Ahene, and Fagen Li. 2019. A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs. *Journal of Systems Architecture* 99 (2019), 101636.

[24] PSLM Barreto, Vincent Rijmen, et al. 2000. The Whirlpool hashing function. In *First open NESSIE Workshop, Leuven, Belgium*, Vol. 13. 14.

[25] Mohamed Baza, Mahmoud Nabil, Noureddine Lasla, Kemal Fidan, Mohamed Mahmoud, and Mohamed Abdallah. 2019. Blockchain-based firmware update scheme tailored for autonomous vehicles. In *2019 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 1–7.

[26] Cara Bloom, Joshua Tan, Javed Ramjohn, and Lujo Bauer. 2017. Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*. 357–375.

[27] Mumin Cebe, Enes Erdin, Kemal Akkaya, Hidayet Aksu, and Selcuk Uluagac. 2018. Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles. *IEEE Communications Magazine* 56, 10 (2018), 50–57.

[28] Riccardo Coppola and Maurizio Morisio. 2016. Connected car: technologies, issues, future trends. *ACM Computing Surveys (CSUR)* 49, 3 (2016), 1–36.

[29] Mehmet Demir, Ozgur Turetken, and Alexander Ferworn. 2019. Blockchain Based Transparent Vehicle Insurance Management. In *2019 Sixth International Conference on Software Defined Systems (SDS)*. IEEE, 213–220.

[30] Ali Dorri, Marco Steger, Salil S Kanhere, and Raja Jurdak. 2017. Blockchain: A distributed solution to automotive security and privacy. *IEEE Communications Magazine* 55, 12 (2017), 119–125.

[31] Yuchuan Fu, Fei Richard Yu, Changle Li, Tom H Luan, and Yao Zhang. 2020. Vehicular Blockchain-Based Collective Learning for Connected and Autonomous Vehicles. *IEEE Wireless Communications* 27, 2 (2020), 197–203.

[32] Feng Gao, Liehuang Zhu, Meng Shen, Kashif Sharif, Zhiguo Wan, and Kui Ren. 2018. A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks. *IEEE network* 32, 6 (2018), 184–192.

[33] Dorothy J Glancy. 2012. Privacy in autonomous vehicles. *Santa Clara L. Rev.* 52 (2012), 1171.

[34] Christian Kaiser, Marco Steger, Ali Dorri, Andreas Festl, Alexander Stocker, Michael Fellmann, and Salil Kanhere. 2018. Towards a Privacy-Preserving Way of Vehicle Data Sharing–A Case for Blockchain Technology?. In *International Forum on Advanced Microsystems for Automotive Applications*. Springer, 111–122.

[35] Mihalis Kritikos. 2018. What if blockchain offered a way to reconcile privacy with transparency? *European Parliamentary Research Service, Scientific Foresight Unit* (2018).

[36] Hazel Si Min Lim and Araz Taeihagh. 2018. Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications. *Energies* 11, 5 (2018), 1062.

[37] David Lopez and Bilal Farooq. 2020. A multi-layered blockchain framework for smart mobility data-markets. *Transportation Research Part C: Emerging Technologies* 111 (2020), 588–615.

[38] Bin Luo, Xinghua Li, Jian Weng, Jingjing Guo, and Jianfeng Ma. 2019. Blockchain enabled trust-based location privacy protection scheme in VANET. *IEEE Transactions on Vehicular Technology* 69, 2 (2019), 2034–2048.

[39] Subhrajit Majumder, Akshay Mathur, and Ahmad Y Javaid. 2019. A study on recent applications of blockchain technology in vehicular adhoc network (VANET). In *National Cyber Summit*. Springer, 293–308.

[40] Markus Maurer, J Christian Gerdes, Barbara Lenz, and Hermann Winner. 2016. *Autonomous driving: technical, legal and social aspects*. Springer Nature.

[41] Muhammad Baqer Mollah, Jun Zhao, Dusit Niyato, Yong Liang Guan, Chau Yuen, Sumei Sun, Kwok-Yan Lam, and Leong Hai Koh. 2020. Blockchain for the Internet of Vehicles towards Intelligent Transportation Systems: A Survey. *IEEE Internet of Things Journal* (2020).

[42] Chuka Oham, Salil S Kanhere, Raja Jurdak, and Sanjay Jha. 2018. A blockchain based liability attribution framework for autonomous vehicles. *arXiv preprint arXiv:1802.05050* (2018).

[43] Reza M Parizi, Ali Dehghantanha, Kim-Kwang Raymond Choo, and Amritraj Singh. 2018. Empirical vulnerability analysis of automated smart contracts security testing on blockchains. *arXiv preprint arXiv:1809.02702* (2018).

[44] Kaihua Qin and Arthur Gervais. 2018. An overview of blockchain scalability, interoperability and sustainability. *Hochschule Luzern Imperial College London Liquidity Network* (2018).

[45] Geetanjali Rathee, Ashutosh Sharma, Razi Iqbal, Moayad Aloqaily, Naveen Jaglan, and Rajiv Kumar. 2019. A blockchain framework for securing connected and autonomous vehicles. *Sensors* 19, 14 (2019), 3165.

[46] Sachin Sharma, Kamal Kumar Ghanshala, and Seshadri Mohan. 2019. Blockchain-Based Internet of Vehicles (IoV): An Efficient Secure Ad Hoc Vehicular Networking Architecture. In *2019 IEEE 2nd 5G World Forum (5GWF)*. IEEE, 452–457.

[47] Paul J Taylor, Tooska Dargahi, Ali Dehghantanha, Reza M Parizi, and Kim-Kwang Raymond Choo. 2020. A systematic literature review of blockchain cyber security. *Digital Communications and Networks* 6, 2 (2020), 147–156.

[48] Zhe Yang, Kan Yang, Lei Lei, Kan Zheng, and Victor CM Leung. 2018. Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet of Things Journal* 6, 2 (2018), 1495–1505.

[49] Yong Yuan and Fei-Yue Wang. 2016. Towards blockchain-based intelligent transportation systems. In *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*. IEEE, 2663–2668.

[50] Kum Fai Yuen, Lanhui Cai, Guanqiu Qi, and Xueqin Wang. 2020. Factors influencing autonomous vehicle adoption: an application of the technology acceptance model and innovation diffusion theory. *Technology Analysis & Strategic Management* (2020), 1–15.