Blockchain and Distributed Ledger Technologies for Intelligent Transportation Systems: a Survey

Giuseppe Loseto, Filippo Gramegna, Saverio Ieva, Agnese Pinto, Floriano Scioscia, Michele Ruta
Department of Electrical and Information Engineering (DEI)
Polytechnic University of Bari – Bari, Italy
name.surname@poliba.it

***Abstract*—Intelligent Transportation Systems (ITSs) aim to provide novel services to drivers and passengers, increasing safety, efficiency end environmental sustainability. Trustworthiness, reliability and auditability of distributed software and data are increasingly necessary from both a technical and a regulatory perspective, particularly as ITSs evolve towards autonomous driving. Unfortunately, heterogeneity of virtual counterparts of users and vehicles along with their intrinsic volatility make coordination and trust management difficult for cooperation. To solve these issues, blockchain and Distributed Ledger Technologies are increasingly adopted in ITSs. This paper surveys key aspects of blockchain research and usage in ITS and automotive sectors, comprising the main technological trends and open issues, the most significant application scenarios and an analysis of relevant DLT platforms.**

***Keywords*—Intelligent Transportation Systems, Blockchain, Distributed Ledger Technologies**

ACRONYMS

CVIM	Common Vehicle Information Model
DAG	Direct Acyclic Graph
DAO	Decentralized Autonomous Organization
DBMS	Data Base Management System
DLT	Distributed Ledger Technology
DSRC	Dedicated Short-Range Communication
EOV	Execute-Order-Validate
EVM	Ethereum Virtual Machine
IoT	Internet of Things
IoV	Internet of Vehicles
ITS	Intelligent Transportation System
MEC	Mobile Edge Computing
PBFT	Practical Byzantine Fault Tolerance
PoET	Proof of Elapsed Time
PoS	Proof of Stake
PoW	Proof of Work
RSU	Road-Side Unit
SC	Smart Contract
SGX	Software Guard eXtensions
SOA	Service-Oriented Architecture
TEE	Trusted Execution Environment
UTXO	Unspent Transaction Outputs
VANET	Vehicular Ad-hoc NETwork
VM	Virtual Machine
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything

I. INTRODUCTION

ITSs aim to provide novel and improved services to drivers, riders and passengers, increasing safety, efficiency end environmental sustainability of transportation [1]. ITS platforms integrate four main technological layers: (i) *sensing* internal and environmental data of vehicles and the road network; (ii) *processing* in distributed and multi-core architectures by means of artificial intelligence techniques for decision support and autonomous control; (iii) *communications* in Vehicular Ad-hoc NETworks (VANETs) comprising Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Everything (V2X) links through Dedicated Short-Range Communication (DSRC) or cellular infrastructures; (iv) *Service-Oriented Architectures* (SOA) to discover and exchange situational awareness information, multimedia resources and application services among vehicles, in addition to basic emergency data; (v) *human-machine interfaces* designed to present information effectively and properly for drivers.

Due to the high-speed mobility of vehicles, VANETs suffer from high device churn, with consequent unpredictable volatility of host and resource availability. This makes coordination and trust management difficult for device cooperation. Anyway, reliability, trustworthiness and auditability of distributed software and data are increasingly necessary from both a technical and a regulatory perspective, particularly as ITSs evolve towards autonomous driving [2]. Hence, even more research solutions tend to adopt *blockchain* technology in ITS pilot projects [3]. Blockchain denotes a data structure and protocol for peer-to-peer *trustless* distributed transactional systems. In traditional distributed databases, a trusted intermediary is needed to prevent *censorship* (*i.e.*, all valid transactions are committed) and ensure *irreversibility* (*i.e.*, no committed transaction can be reverted or altered). Blockchain systems avoid intermediaries by approving transactions through a distributed *consensus* approach, which guarantees no single host or small group of colluding hosts can force addition, removal or modification of data. Transactions approved in a given time period are grouped in *blocks*, which are appended sequentially. The blockchain works as a *distributed ledger* of transactions, and research on *Distributed Ledger Technologies* (DLT) is investigating several types of data structures, consensus protocols and architectural variations for DLT platforms.

The blockchain potential as general-purpose distributed database was understood soon after the introduction of the technology with the *Bitcoin* open source platform for digital currency. In particular, DLTs enable practical implementations of the *Smart Contract* (SC) idea [4], *i.e.*, programs encoding and enforcing cooperative processes like the terms of a contract among two or more parties. Consensus about SCs on

 ISBN: 978-1-61208-886-0

a blockchain is reached through a parallel execution in the network, effectively making every SC-enabled DLT a general-purpose application platform based on a distributed Virtual Machine (VM).

Due to the above features, ITS applications and projects are increasingly adopting DLT platforms. This survey provides a compact but comprehensive overview of the state of the art about blockchain and DLTs for ITSs.

The remainder of the paper is as follows: Section II briefly recalls the most important features of blockchain and DLT technologies, while Section III discusses on relevant applications of them in the ITS field. An analysis of four DLT platforms among the most adopted and technologically significant ones for ITS follows in Section IV, before conclusion.

II. Blockchain and Distributed Ledger Technologies

Blockchain and DLT systems are increasingly different in architecture, technologies and applications. Useful surveys exist, focusing on their integration in the Internet of Things (IoT) [5]–[7]. DLT types can be classified with respect to key design policies [8]:

Network access - *Permissionless* blockchains allow any host to join –even anonymously– at any time. Conversely, hosts are uniquely identified in *permissioned* platforms and only authorized ones can connect. This choice affects the blockchain project: permission-less chains usually have to reward participants for their computational effort, *e.g.*, Bitcoin allows hosts to generate (*mine*) and keep new currency for the validation of transaction blocks. Permissioned chains are instead adopted in more controlled collaboration contexts, where access itself is a reward, as it enables selling and buying services or resources.

Consensus protocol - Permissionless systems require stricter consensus methods, such as *Proof-of-Work* (PoW), which guarantees data security unless hosts collectively possessing the majority of computational power in the network are colluding to subvert the blockchain: *Byzantine fault tolerance* [9] is, in fact, typically required. For adding the next block to the chain, PoW elects a leader among all hosts having candidate blocks. Election requires solving a cryptographic challenge, and implies high computational and energy cost with commodity hardware, low transaction throughput and the need for *mining* (a reward to transaction validators participating in the consensus by means of small digital currency amounts). *Proof-of-Stake* (PoS) consensus, instead, elects the host with the highest value of *coin-age*, that is the product of the amount of owned currency and the time since the host has been holding it without spending. This mechanism avoids high computational costs and mining. Permissioned systems –where each host is accountable– may relax consensus constraints to *crash fault tolerance* guarantees [9]. Permissioned blockchains can follow either the *private* or the *consortium* model: in the former consensus is managed by hosts from a single organization, giving up some of the benefits of decentralization in exchange for higher transaction throughput; the latter adopts a trade off where a subset of all hosts, belonging to multiple organizations, can participate in the consensus.

Transaction model - *Assets* can be registered or transferred by means of transactions on a blockchain. In the *unspent transaction outputs* (UTXO) model, an $A \rightarrow B$ transfer implies *consuming* (*i.e.*, deleting) records for A's spent assets and *producing* (*i.e.*, adding) new ones for B's received assets. In the *account-based* model, instead, every host has an account reporting all its assets, which is updated by transactions. The former is simpler to manage and fits the digital currency use cases, but it is not general-purpose; the latter is required to support SCs [8].

SC language - Blockchains can adopt any formalism for SC specification and execution, such as procedural programming languages, logic programming or automata [10]. Industry proposals mostly adopt computationally complete programming languages, either existing (*e.g.*, Java in the *Iroha* framework) or created for the purpose (*e.g.*, Ethereum's *Solidity*).

Centralized information management models are clearly not scalable enough for the ever-growing IoT and the Internet of Vehicles (IoV) [11]. They pose issues with respect to cost and performance, as well as security and trust. The viability of blockchain and DLT technologies for the IoT is analyzed in [7] and strategies are outlined to combine security and scalability. Running IoV resource/service marketplaces with minimal or no human intervention [8] requires a cross-application peer-to-peer middleware layer comprising several building blocks. Recent proposals include the *Inter-Planetary File System* (IPFS) distributed storage protocol [12], intelligent service discovery [13] and billing services [14].

Research on blockchain scalability is very active, mainly by optimizing performance of consensus protocols [13], [15] and by introducting parallelism in a blockchain through *sidechains* and/or *sharding* [16]. Basically, the use of sidechains transforms the chain structure in a Direct Acyclic Graph (DAG). On the other hand, sharding is a parallelization technique borrowed from Database Management Systems, consisting in splitting data elements (*e.g.*, rows in relational databases) horizontally across host subsets in a cluster. Research results, however, are not mature enough [17] for building efficient, robust, large-scale IoT-oriented blockchains.

III. DLT solutions for Intelligent Transportation Systems

Emerging blockchains increasingly refer to novel transparent and trustless models, particularly fitting needs and requirements of sectors like transportation [18].

A reference ITS-oriented blockchain model has been proposed in [19], with seven conceptual layers characterizing and standardizing the typical architecture of blockchain systems:

1) *physical*: concerning devices, vehicles and physical assets;
2) *data*: core data structures and cryptographic primitives of the digital ledger;
3) *network*: peer-to-peer networking primitives;

4) *consensus*: implementing the supported consensus protocol(s);
5) *incentive*: policies for the issuance and allocation of incentives to miners;
6) *contract*: SC execution environment and SC instances;
7) *application*: ITS applications and services implemented on top of the previous layers.

According to the proposed framework, a real-time decentralized ride-sharing service has been also implemented to prove its applicability. In [20], the authors have extended previous modeling approaches to combine IoT and blockchain technologies for smart logistics and transportation in a general-purpose and reliable architecture fitting different ITS scenarios. Anyway, the layered architectural model is useful to guide a systematic analysis of the state of the art.

Physical layer. *Collaborative Vehicular Edge Computing* [21] maps the typical VANET architecture to the Edge Computing paradigm: vehicles and other mobile hosts belong to the infrastructure layer, where local computation and direct communication among nearby devices occur. Analogously, Road-Side Units (RSUs) enable the Edge Computing layer, which interconnects clusters of local devices and supports both vertical and horizontal collaboration through software-defined networking for dynamic resource provisioning and management. In [21] this general model has been specialized to include the three most popular approaches to Edge Computing: Mobile Edge Computing (MEC), Fog Computing, and Cloudlets.

Data layer. In VANET-based blockchains, security and privacy still have several relevant open research questions. Blockchain networks are not immune to cyberattacks and frauds. Attackers could exploit vulnerabilities in blockchain infrastructure to penetrate protected systems, compromise data, overload networks, and cause potentially severe risks to users. In [22], a consortium blockchain and SCs improve security in data exchange and storage within VANETs, while a reputation model enhances the quality of shared data. Information interoperability among heterogeneous hosts is a further largely open problem, and semantic-based structured representations of blockchain assets exploiting Semantic Web technologies have been proposed for that [13]. Defining interoperable methods to assess vehicle reputation and level of trustworthiness, based on both its prior actions and nearby vehicles information, is one of the main goals.

Network layer. As highlighted in [23], current vehicles basically integrate wireless communication and sensing devices providing high speed connectivity and a huge amount of gathered data. Information can be stored and manipulated by a distributed computing platform to create innovative smart applications. 5G is seen as a key enabling technology to overcome bandwidth, reliability and security problems of DSRC. The combination of both technologies simplify process automation in several ITS scenarios, including transmission of tracking information in fleet management applications, monitoring of resource flows and the administration of logistics processes. In fact, 5G communication improves the connectivity of IoT devices by maximizing channel transfer capacity, reducing network latency and increasing the density of interconnected devices, whereas blockchain ensures secure, verifiable and auditable storage of transaction data [24].

Consensus layer. From this perspective, scalability is the main open issue, as PoW and SCs still have a significant impact in terms of transaction throughput [8], [25] and cost of energy. For this reason the MEC blockchain architecture proposed in [26] offloads PoW computation to nearby Edge Computing hosts. Furthermore, the amount of computing resources required by a SC cannot be predicted, as it may recursively invoke further SCs. Approaches to solve this problem include associating currency costs to computation or preventing recursive SC calls [13]. Decentralized energy and charging service marketplaces for electric vehicles and Smart Grid integration are among the scenarios where the benefits of blockchain are most evident, as they need supporting secure and verifiable commercial transactions and providing facilities of service discovery, negotiation, selection and resource allocation. The Cloud-Edge architecture proposed by Liu *et al.* [27] aims to manage interactions concerning vehicular information and energy flows simultaneously. Following Cloud-Edge and information-energy interactions, they identify four categories of context-aware applications and propose a PoS consensus protocol based on *data coins* and *energy coins*.

Incentive layer. Blockchain can facilitate interoperable vehicle data exchanges among car makers, but the hardest obstacle to such cooperation is the historically competitive and secretive nature of the automotive industry. Several initiatives have been launched to overcome this limitation: most recently, the *AutoMat* [28] Horizon 2020 project has defined a Common Vehicle Information Model (CVIM) to represent and share hierarchically organized information about vehicles in an interoperable way, as well as an architecture for a cloud-based Big Data marketplace. Despite the adoption of blockchain and SCs is not in the AutoMat proposal, it is easy to see it would be a natural fit *e.g.*, with the European Blockchain Services Infrastructure (EBSI) [29], possibly granting stronger security, traceability, verifiability and flexibility to the data marketplace.

Contract layer. The adoption of DLTs and SCs can improve the automation of complex logistic procedures by introducing the following benefits [30], [31]: component traceability with real-time data transmission and identification of new resources; persistent and reliable storage of complex data, usually pre-processed by means of data mining and machine learning algorithms; user and data privacy, exploiting different encryption methods, which is particularly useful in industrial e-procurement scenarios where strict regulations must be applied; definition of simple testing procedures required to optimize business processes and automation procedures. All the above capabilities are very important for ITS-based supply chain and logistics applications, where DLTs can be exploited to reduce wait times and management costs and to improve (i) timely delivery of goods, (ii) use of connected devices according to current regulations, (iii) accuracy and efficiency of customer services, and (iv) monitoring of goods while transiting.

Application layer. In latest years, several automotive companies have been proposing interesting solutions for ITS, combining novel communication technologies and blockchain. BMW Group has been particularly active, developing pilot projects for several real-world ITS scenarios. The *VerifyCar* project, based on the *VeChainThor* [32] blockchain platform, has introduced a digital car registration document to store information about mileage, accident history, inspections, maintenance procedures and other useful information related to the lifecycle of a vehicle. Each car results equipped with an up-to-date and certified data log which can be properly accessed by authorized parties at any time and cannot be tampered with. This constitutes a very important benefit not only for vehicle servicing, but also for insurance and for the overall car market. Since 2019 BMW Group has also been working on a blockchain-based system called *PartChain* [33], aiming to improve the supply chain management in the automotive industry. The project has defined an industrial solution to share data of production tasks and simplify all the procedures for tracing the origin of each vehicle component. The company is planning to use the system also for the management of raw materials, focusing on the traceability of the most critical resources involved in vehicle manufacturing. Moreover, BMW is one of the founding members of *MOBI* (Mobility Open Blockchain Initiative) [34], a nonprofit consortium including over 100 companies in the automotive and information technology sectors. MOBI aims to define reference standards and control models for developing new platforms for ITS. Dedicated working group have been established for: vehicle identity, aiming at an extension of VerifyCar towards a vehicle digital twin; usage-based mobility and insurance; electric vehicle grid integration; connected mobility data marketplace; finance, securitization, and SCs; supply chain. The latter working group would extend the PartChain project to all companies interested and involved in the initiative, in order to facilitate cross-industry data exchange and speed up the integration of blockchain-based platforms in different automotive and transportation scenarios.

IV. Analysis of relevant platforms

Blockchains and DLTs can be classified and compared according to several criteria, including data structures, consensus protocols and SCs, allowed data security and privacy [8]. Four of the most relevant platforms are discussed in what follows, while Table I summarizes benefits and potential limitations from an ITS perspective.

Ethereum [37] is a permissionless blockchain; it allows integrating SCs for developing Decentralized Autonomous Organizations (DAOs) interacting without the intervention of a central authority [38]. The platform core is the *Ethereum Virtual Machine* (EVM) [39], *i.e.*, a *quasi-Turing-complete* execution environment for general-purpose transactions and SCs, replicated on each participating host for validation. Since Turing-completeness would open the platform to abuses and security risks, the EVM associates a cost in *gas* units to code execution, which must be paid in Ethereum's currency, *Ether*. When a host invokes a transaction or a SC, it must pay gas for that in advance; if execution does not complete before running out of the prepaid amount of gas, it is rolled back completely, otherwise it is committed and the possibly remaining gas is refunded. Ethereum is currently the largest SC platform. Several languages can be used: the most popular and mature one is *Solidity* [40]. Ethereum adopts a PoW consensus algorithm called *Ethash*. It aims to be less computationally intensive and more memory intensive than Bitcoin's PoW, in order to limit the recourse to specialized mining hardware and to concentrating computational power in few large mining pools. However, it does not solve the high energy consumption and limited scalability problems. With this motivation, the Ethereum Foundation and community are currently transitioning to Ethereum 2.0, which will adopt a PoS consensus algorithm to increase transaction throughput, reduce computational costs and make the platform fairer and more accessible. Chain sharding will be also employed to partition the validation load among validators and therefore increase platform scalability.

IOTA is a DLT designed specifically for Internet of Things scenarios. It is based on a Direct Acyclic Graph (DAG) data structure, the *tangle*, where each node stores a transaction [41]. Starting from a genesis node n_0, in order to accept a new node n_j the issuer must validate 2 or more transactions $n_{i_k}, k \geq 2$ already in the tangle; then n_j will be added to the tangle with edges from each of the nodes n_{i_k}. This consensus mechanism creates tamper-proof records of network participants' transactions, as older transactions are validated by newer ones either directly or indirectly (through a DAG path). Further key tangle properties are: scalability, because the validation load is spread across all participants; throughput, since a low number of validations is required to accept a new transaction; robustness, in case of network partitioning the tangle may fork temporarily, but it will merge again when connectivity is restored; no reward mechanism for validators is required, avoiding the potential distortions of hosts' behavior related with mining; a snapshot mechanism allowing the periodic removal of very old transactions from the DAG safely, so reducing ledger storage requirements for each peer. IOTA claims the protocol is as secure as PoW, however no formal proof has been produced yet. Based on the IOTA DLT, the *IOTA Streams* protocol (formerly known as *Masked Authenticated Messaging*) has been designed for secure and metered access to IoT data streams. It adopts a publish/subscribe model, integrating both cryptography for controlled data sharing and payment in the IOTA cryptocurrency. Its features make IOTA Streams particularly suitable to vehicular applications [42]. A IOTA based solution for ITS system has been proposed by the ORCHESTRA consortium [35].

Hyperledger Sawtooth is an open source project within the *Hyperledger* initiative for a business-oriented blockchain platform with support for SCs. By design, Sawtooth allows applications to dynamically select transaction rules, authorizations, and consensus protocol, based on business requirements.

TABLE I
COMPARISON OF BDLT PLATFORMS

BDLT	Benefits	Limitations	ITS Implementations
Ethereum	• SC support • DAO development	• PoW-related limitations • Low throughput, high resource consumption	• Xiong *et al.* [25]
IOTA	• Fast, inexpensive consensus • No transaction fee • Low energy consumption • High scalability when transactions increase • DAG snapshot mechanism • IoT-oriented data stream access services	• Limited SC support • Unproven consensus security	• ORCHESTRA [35]
Hyperledger Sawtooth	• SC support in several programming languages • Permissioned and permissionless blockchain support • Relatively high transaction throughput • Low energy consumption of PoET	• Specific hardware required for trusted execution environments	• Salesforce blockchain [36]
Hyperledger Fabric	• Permissioned blockchain support • High transaction throughput and low latency • SC support in several programming languages • Private data areas with privacy-preserving authentication	• Relatively higher architectural complexity	• PartChain [33]

Its architecture [43] clearly separates the application layer from the main platform layer, and in particular it isolates consensus from transaction semantics. The consensus mechanism is selected during the network configuration and can also be modified later on a running blockchain, by means of specific transactions. Sawtooth currently supports four types of consensus protocols: Practical Byzantine Fault Tolerance (PBFT) [44]; Proof of Elapsed Time (PoET) [45], implementing a fair lottery-based leader election system without the power consumption disadvantages of PoW; *Raft* [46], a consensus strategy optimized for small networks. In particular, a Byzantine fault tolerant PoET variant is enabled if a Trusted Execution Environment (TEE) is provided by the hosts' platform, such as the Software Guard Extensions (SGX) instructions of Intel CPUs, otherwise a less robust crash fault tolerant variant is implemented purely in software (essentially used for development purposes but not recommended in production environments). Similar flexibility is achieved for SC support, as an interface abstraction mechanism allows developers to write contract logic in multiple programming languages, including Python, JavaScript, Go, C++, Java, and Rust. Finally, Sawtooth includes a scheduler that splits transactions to parallel flows, mutually isolating their execution. Whenever possible, transactions run in parallel, allowing for a significant increase in performance over sequential execution. Salesforce introduced a blockchain solution for supply chain management based on Sawtooth [36].

Hyperledger Fabric [47] adopts an *Execute-Order-Validate* (EOV) transaction processing model: peers *endorse* transactions by checking their correctness, then *order* them by consensus and finally *validate* them against a particular *endorsement policy*, before committing them to the ledger. Conversely, the majority of DLT platforms adopt an *Order-Execute* model, where transactions are individually validated, then ordered and propagated to all peer hosts, which must execute them sequentially to commit the updated system state in the ledger. The EOV model grants parallel transaction execution and pluggable consensus protocols. Further Fabric peculiarities include: (i) *Zero-Knowledge-Proofs* for privacy-preserving authentication, which is particularly valuable in promiscuous environments like vehicular networks [48]; (ii) high modularity, since responsibilities within the EOV model are divided among *clients*, *endorsing peers*, *orderers* and *committing peers*, which may run on independent hosts.

V. PERSPECTIVES AND CONCLUSION

This paper has explored most relevant aspects of blockchain and Distributed Ledger Technologies for Intelligent Transportation Systems. The proposed outline of the main technological trends, results and open problems has shown the increasing adoption and importance of DLTs for both the automotive and transportation industries. While research must continue on technical issues, it is clear from this survey that, more and more, challenges for the success of DLTs in ITSs go beyond purely technological aspects, intertwining with complex societal, legal and business matters.

Blockchain, DLTs and SCs have been conceived to impact how people and organizations transact business, coordinate, and cooperate. Since their inception, they have been continuously debated with growing interest from technological, financial, regulatory, social and environmental viewpoints. This is a feature they have in common with transportation technologies, and in particular with Intelligent Transportation Systems; perhaps this is at the core of why each one of them is so relevant for the future of the other.

REFERENCES

[1] L. Zhu, F. R. Yu, Y. Wang, B. Ning, and T. Tang, "Big Data Analytics in Intelligent Transportation Systems: A Survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 1, pp. 383–398, 2018.
[2] M. Obaidat, M. Khodjaeva, J. Holst, and M. B. Zid, "Security and privacy challenges in vehicular ad hoc networks," in *Connected Vehicles in the Internet of Things*. Springer, 2020, pp. 223–251.
[3] G. Falco and J. E. Siegel, "A Distributed "Black Box" Audit Trail Design Specification for Connected and Automated Vehicle Data and Software Assurance," *SAE International Journal of Transportation Cybersecurity and Privacy*, vol. 3, no. 2, pp. 97–111, 2020.

[4] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, 1997.
[5] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 179–190, 2018.
[6] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT Integration: A Systematic Survey," *Sensors*, vol. 18, no. 8, p. 2575, 2018.
[7] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's Adoption in IoT: The Challenges, and a Way Forward," *Journal of Network and Computer Applications*, vol. 125, pp. 251–279, 2019.
[8] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[9] S. Liu, P. Viotti, C. Cachin, V. Quéma, and M. Vukolić, "XFT: Practical fault tolerance beyond crashes," in *12th USENIX Symposium on Operating Systems Design and Implementation*, 2016, pp. 485–500.
[10] F. Idelberger, G. Governatori, R. Riveret, and G. Sartor, "Evaluation of logic-based smart contracts for blockchain systems," in *International Symposium on Rules and Rule Markup Languages for the Semantic Web*. Springer, 2016, pp. 167–183.
[11] W. Xu *et al.*, "Internet of Vehicles in Big Data Era," *IEEE/CAA Journal of Automatica Sinica*, vol. 5, no. 1, pp. 19–35, 2017.
[12] M. Naz *et al.*, "A Secure Data Sharing Platform Using Blockchain and InterPlanetary File System," *Sustainability*, vol. 11, no. 24, p. 7054, 2019.
[13] M. Ruta, F. Scioscia, S. Ieva, G. Capurso, and E. Di Sciascio, "Semantic blockchain to improve scalability in the Internet of Things," *Open Journal of Internet Of Things (OJIOT)*, vol. 3, no. 1, pp. 46–61, 2017.
[14] R. Yaqub, S. Ahmad, H. Ali, and A. ul Asar, "AI and Blockchain Integrated Billing Architecture for Charging the Roaming Electric Vehicles," *IoT*, vol. 1, no. 2, pp. 382–397, 2020.
[15] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *International Workshop on Open Problems in Network Security*. Springer, 2015, pp. 112–125.
[16] K. Croman *et al.*, "On scaling decentralized blockchains," in *International Conference on Financial Cryptography and Data Security*. Springer, 2016, pp. 106–125.
[17] H. Wang, K. Chen, and D. Xu, "A maturity model for blockchain adoption," *Financial Innovation*, vol. 2, no. 12, pp. 1–5, 2016.
[18] V. Pureswaran and P. Brody, "Device democracy: Saving the future of the Internet of Things," IBM Institute for Business Value, Tech. Rep., September 2014, available: http://www-935.ibm.com/services/us/gbs/thoughtleadership/internetofthings, retrieved: August 2021.
[19] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*. IEEE, 2016, pp. 2663–2668.
[20] M. Humayun, N. Jhanjhi, B. Hamid, and G. Ahmed, "Emerging smart logistics and transportation using IoT and blockchain," *IEEE Internet of Things Magazine*, vol. 3, no. 2, pp. 58–62, 2020.
[21] K. Wang, H. Yin, W. Quan, and G. Min, "Enabling Collaborative Edge Computing for Software Defined Vehicular Networks," *IEEE Network*, vol. 32, no. 5, pp. 112–117, 2018.
[22] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4660–4670, 2018.
[23] M. Zichichi, S. Ferretti, and G. D'Angelo, "Are Distributed Ledger Technologies Ready for Intelligent Transportation Systems?" in *3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, ser. CryBlock '20. ACM, 2020, p. 12–17.
[24] I. Jovović, S. Husnjak, I. Forenbacher, and S. Maček, "Innovative Application of 5G and Blockchain Technology in Industry 4.0," *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, vol. 6, no. 18, pp. 1–6, 2019.
[25] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When Mobile Blockchain Meets Edge Computing," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 33–39, 2018.
[26] M. Liu, F. R. Yu, Y. Teng, V. C. Leung, and M. Song, "Computation offloading and content caching in wireless blockchain networks with mobile edge computing," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 11 008–11 021, 2018.
[27] H. Liu, Y. Zhang, and T. Yang, "Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing," *IEEE Network*, vol. 32, no. 3, pp. 78–83, 2018.
[28] J. Pillmann, C. Wietfeld, A. Zarcula, T. Raugust, and D. C. Alonso, "Novel common vehicle information model (CVIM) for future automotive vehicle big data marketplaces," in *2017 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, 2017, pp. 1910–1915.
[29] I. Williams, "Cross-chain blockchain networks, compatibility standards, and interoperability standards: The case of European Blockchain Services Infrastructure," in *Cross-Industry Use of Blockchain Technology and Opportunities for the Future*. IGI global, 2020, pp. 150–165.
[30] K. Valtanen, J. Backman, and S. Yrjölä, "Creating value through blockchain powered resource configurations: Analysis of 5G network slice brokering case," in *2018 IEEE Wireless Communications and Networking Conference Workshops*. IEEE, 2018, pp. 185–190.
[31] M. B. Mollah *et al.*, "Blockchain for the internet of vehicles towards intelligent transportation systems: A survey," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4157–4185, 2021.
[32] VeChain Foundation, "VeChain Whitepaper 2.0 – #Creating valuable TXs," 12 2019, www.vechain.org/qfy-content/uploads/2020/01/VeChainWhitepaper_2.0_en.pdf, retrieved: August 2021.
[33] D. Miehle, D. Henze, A. Seitz, A. Luckow, and B. Bruegge, "PartChain: a decentralized traceability application for multi-tier supply chain networks in the automotive industry," in *2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)*. IEEE, 2019, pp. 140–145.
[34] L. M. Powell, J. Schwartz, and M. Hendon, "The Mobility Open Blockchain Initiative: Identity, Members, Technologies, and Future Trends," in *Revolutionary Applications of Blockchain-Enabled Privacy and Access Control*. IGI Global, 2021, pp. 99–118.
[35] European Commission, "Coordinating and synchronising multimodal transport improving road, rail, water and air transport through increased automation and user involvement," 2021, https://cordis.europa.eu/project/id/953618, retrieved: August 2021.
[36] D. Harrison, R. Bohm, T. Flynn, and V. Nadi, "Blockchain: the building block of trust," Salesforce, Tech. Rep., 2018, https://www.salesforce.com/content/dam/web/en_us/www/documents/white-papers/finserv-blockchain.pdf, retrieved: August 2021.
[37] V. Buterin, "A next-generation smart contract and decentralized application platform," Ethereum Foundation, Tech. Rep., 2013, https://github.com/ethereum/wiki/wiki/White-Paper, retrieved: August 2021.
[38] K. Wüst and A. Gervais, "Do you need a blockchain?" in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. IEEE, 2018, pp. 45–54.
[39] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum Foundation, Tech. Rep., 2021, https://ethereum.github.io/yellowpaper/paper.pdf, retrieved: August 2021.
[40] C. Dannen, *Introducing Ethereum and Solidity*. APress, 2017, vol. 318.
[41] S. Popov, "The Tangle," IOTA Foundation, Tech. Rep. 1.8.3, 2018, https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf, retrieved: August 2021.
[42] P. C. Bartolomeu, E. Vieira, and J. Ferreira, "IOTA feasibility and perspectives for enabling vehicular applications," in *2018 IEEE Globecom Workshops*. IEEE, 2018, pp. 1–7.
[43] K. Olson *et al.*, "Sawtooth: an introduction," Hyperledger – The Linux Foundation, Tech. Rep., 2018, https://www.hyperledger.org/wp-content/uploads/2018/01/Hyperledger_Sawtooth_WhitePaper.pdf, retrieved: August 2021.
[44] M. Castro, B. Liskov *et al.*, "Practical byzantine fault tolerance," in *OSDI*, vol. 99, no. 1999, 1999, pp. 173–186.
[45] A. Corso, "Performance Analysis of Proof-of-Elapsed-Time (PoET) Consensus in the Sawtooth Blockchain Framework," Master's thesis, University of Oregon, 2019.
[46] D. Huang, X. Ma, and S. Zhang, "Performance analysis of the Raft consensus algorithm for private blockchains," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, pp. 172–181, 2019.
[47] E. Androulaki *et al.*, "Hyperledger Fabric: a distributed operating system for permissioned blockchains," in *Thirteenth EuroSys Conference*, 2018, pp. 1–15.
[48] D. Gabay, K. Akkaya, and M. Cebe, "Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5760–5772, 2020.