



Blockchain for V2X: Applications and Architectures

JAMES MEIJERS  (Graduate Student Member, IEEE),
PANAGIOTIS MICHALOPOULOS (Graduate Student Member, IEEE), **SHASHANK MOTEPALLI**, **GENGRUI ZHANG**,
SHIQUAN ZHANG, **ANDREAS VENERIS** (Senior Member, IEEE), AND **HANS-ARNO JACOBSEN**  (Fellow, IEEE)
(Invited Paper)

Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada

CORRESPONDING AUTHOR: JAMES MEIJERS (e-mail: j.meijers@mail.utoronto.ca)

This work was supported by a grant from Huawei Canada.

ABSTRACT Modern vehicles rely on data from a vast array of sensors such as radar and GPS equipment that can be shared with surrounding vehicles and other interested parties. Vehicle-to-everything (V2X) is the collection of systems that enable such communication. Although this data sharing has the potential to improve both the safety and efficiency of vehicles, ensuring that what is shared has not been altered, deleted, forged, leaked, or otherwise tampered with remains a challenging problem. Today, blockchain technology allows a system's participants to come to an agreement (consensus) on the state of the system and its data in a decentralized, trustless manner. This new technology may be capable of securing V2X data, as well as enabling other useful V2X services such as payments. However, the V2X ecosystem poses several unique challenges that complicate the application of blockchain technology, not least of which is the vast number of communications that any proposed blockchain network will need to support. This paper gives an overview of V2X and blockchain technology, explores potential applications of blockchain within the V2X domain, and justifies its importance. It also reviews, analyzes, and discusses various blockchain architectures that could support V2X applications. Though there is a place for blockchain in the V2X environment, currently there is no robust or mature blockchain architecture available that could support the entire ecosystem's needs. As such, this paper proposes novel directions for future research towards the creation of such a blockchain.

INDEX TERMS Blockchain, communication, IoT, transportation, V2X.

I. INTRODUCTION

Modern vehicles have a multitude of different sensors on-board, ranging from cameras and radars to GPS and gyroscopes [1], rightfully earning their reputation as “computers on wheels” [2]. These sensors, combined with on-board computing facilities, have already enabled many new technologies, such as GPS navigation and certain driver assistance features. While current implementations of these applications mainly rely on intravehicle sensing and computing, many other potential applications require significant intervehicle communication to complement the functionality of those on-board facilities. Vehicle-to-everything (V2X) encompasses all potential vehicle communication systems that enable these smart applications.

Although such communications could unlock significant new capabilities for vehicles and infrastructure, they also come with safety and reliability concerns. Problems could range from minor inconveniences, such as incorrect traffic reports causing a car to take a suboptimal route, to more serious issues, such as a toll payment not being processed properly, to life-threatening problems that could cause accidents, such as a car misreporting its speed. Such issues could be the result of malfunctioning hardware [3], buggy software [4], or even attacks by malicious actors [5].

A blockchain is a type of distributed state-machine that, using cryptography, specialized data structures, peer-to-peer (P2P) networks, game-theoretical incentives, and fault-tolerant *consensus algorithms*, enables participants to come to

an agreement on changes to the state of a global database [6]. Using *smart contracts*, the rules for database updates can be defined by users through software programs, allowing them to design complex applications that utilize the shared database. It is clear that there are many potential applications of blockchain technology in the V2X space [7]. These include mechanisms to improve the security and reliability of V2X communications as well as a large number of applications requiring fast and efficient payments. There are several key reasons why blockchain technology is a good fit for the transportation sector. For example, the automotive sector has a diverse array of stakeholders, such as insurance companies, government agencies, and car manufacturers, among others. Using blockchain technology, stakeholders can consent to a protocol in which they all participate in the maintenance of the common ledger, each verifying its contents and maintaining records to ensure it is not being misused. The open nature of blockchains also allows a wide variety of participants to utilize the system on equal footing, without anyone being disadvantaged. Additionally, blockchains allow for accurate auditing of data, which is important for many V2X applications, especially accident investigations.

In this work, we argue for the inclusion of blockchain technology in the V2X technology stack by describing compelling applications of V2X communications that can be enabled or improved using blockchain technology. We also show why a blockchain can be an ideal platform on which to build these applications given the unique circumstances of the transportation sector. Later, we analyze various blockchain architectures that can be used to support these applications. In doing so, we determine what aspects of these systems need to be improved in order to support the distinct requirements of V2X systems and make blockchain for V2X a reality. We build on previous work [7] by specifying what features of blockchains are most utilized by V2X applications, allowing us to better justify the use of blockchains for these applications. Additionally, we delve into numerous blockchain architectures, both those that target the transportation sector and those that do not, in order to better determine what shortcomings future research into blockchain architectures for V2X should attempt to overcome.

The contributions of this work are as follows.

- 1) We investigate and analyze proposed applications of blockchain technology in the V2X ecosystem by highlighting the key services offered by blockchains and discussing how they can be utilized by V2X applications. We also discuss the advantages and disadvantages of using blockchains as opposed to other, centralized services.
- 2) We describe several blockchain architectures that may be used in the V2X ecosystem, including both generic blockchain architectures and designs specifically targeting IoT and V2X ecosystems. We analyze these architectures in order to see where they fall short of V2X system requirements.
- 3) We highlight several challenges to integrating blockchains into the V2X ecosystems and propose

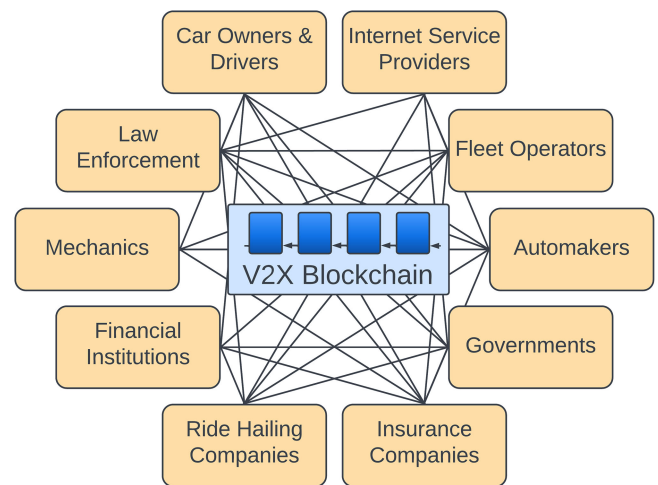


FIGURE 1. Major stakeholders who may be interested in using a V2X blockchain.

some directions for future research to follow in order to attempt to address these challenges.

This paper is organized as follows. Section II provides background on V2X and blockchain technology, summarizes the potential of V2X combined with blockchain technology, and discusses prior reviews in the space. Section III details the services that blockchains can provide to V2X applications, describes applications that can utilize these services, and analyzes the value-add of blockchains to these applications. Section IV illustrates various blockchain that have been proposed to support the special requirements of V2X applications and analyzes their designs. Finally, Section V presents some of the technological challenges standing in the way of this adoption as well as future research directions.

II. BACKGROUND

Here, we provide some background on V2X, blockchains, and the combination thereof. Definitions for some relevant terms are given in Table 1. We also describe some prior reviews in the area of blockchain for V2X.

A. VEHICLE-TO-EVERYTHING

V2X conceptualizes a vehicle communication system composing of vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-grid (V2G), and other communications. A V2V communication system is envisioned as a technology for vehicles to authenticate one another and exchange messages with the goal of improved safety by triggering related warnings and other such applications [8]. In a V2I system, infrastructure captures data generated by vehicles and returns advisory information on safety, mobility, or road conditions [9]. V2G communication aims to allow electric vehicles to communicate with, consume power from, and provide power to electrical grids in order to better manage demand for power [10]. Prior work and industrial projects have revealed the potential of V2X technology to improve

TABLE 1. Glossary of Terms

51% attack	An attack against blockchains in which a malicious user tries to take control of more than 50% of the validation authority on the network [17].
Blockchain	A specialized data structure paired with a distributed network that, using cryptographic primitives such as hashing and digital signatures along with a consensus algorithm, Sybil-resistance mechanism, and game-theoretical incentive designs, allows the network to cooperatively maintain an ordered collection of records [6].
Client / User	Someone who uses the services offered by a blockchain network [18].
Consensus Algorithm	An algorithm that coordinates server actions to agree on one or more values in the presence of faults [19].
Distributed Ledger Technology (DLT)	A decentralized system that allow users to read from and write to a shared ledger, commonly referred to as a blockchain, though some DLTs exist which are not technically blockchains [20].
Miners	Participants in a PoW blockchain network that expend computing power in an effort to create the next block and receive a reward [6].
Permissioned	A blockchain network that requires users to be given permission by some centralized authority in order to participate in the network, e.g., Hyperledger Fabric [20].
Permissionless	A blockchain network in which users do not need permission from any centralized authority in order to participate, e.g., Bitcoin [20].
Proof-of-Stake (PoS)	A Sybil-resistance mechanism in which stakers act as validators and a validator’s authority to create blocks increases with the size of their stake [21].
Proof-of-Work (PoW)	A Sybil-resistance mechanism in which miners act as validators and a validator’s ability to create blocks increases with the amount of computing power dedicated to the task [6].
Roadside Unit (RSU)	Compute nodes positioned near roads that offer services to passing vehicles, also known as fog nodes [22].
Stakers	Participants in a PoS blockchain network that stake (lock up) funds in order to obtain the authority to create blocks [21].
Sybil attack	An attack against distributed systems in which a single user takes on multiple pseudonymous identities which is prevented using a Sybil-resistance mechanism [23].
Trustless	A decentralized system that operates without requiring any users to trust any other individual user, only that a majority of users of the system are rational actors who are not colluding [20].
Vehicle-to-Everything (V2X)	The collection of all vehicle communication systems, including Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Grid (V2G) and others [22].
Validator	A participant in a blockchain network that is responsible for the operation of the network, including creating and validating new blocks of transactions [18].

transportation efficiency and safety while enabling new applications [11]. Some applications include traffic congestion controls [12], driving with enhanced fuel efficiency and travel time [13], and improved safety assistance [14]. Current V2X system proposals mainly rely on dedicated short range communication [15] and/or cellular communication [16] standards. For the remainder of this paper we assume that both standards provide sufficient latency, throughput, and reliability guarantees to support a blockchain network.

B. BLOCKCHAIN

Blockchains are specialized data structures paired with a distributed network that, using cryptographic primitives such as hashing and digital signatures along with a *consensus algorithm* and game-theoretical incentives for all users to participate fairly in the system, allow the network to cooperatively maintain an ordered collection of records [24]. These records are grouped into blocks, and each block contains a hash of the block that comes before it, forming a chain. It is ensured that a new block cannot be added to the chain without the agreement of a majority of participating nodes and that previously added records are immutable. These features allow blockchains to be used for a variety of applications.

The records appearing on a blockchain generally take the form of transactions that alter the state of a shared database. Bitcoin [6], the first blockchain, used such a system to implement a payment mechanism. In that system, the blockchain records transactions between pseudonymous users who are identified only by a public key. By signing a transaction with the corresponding private key and adding a record of this transaction to the Bitcoin blockchain, that owner is able to send the tokens (that today they have a monetary value that can easily be converted to fiat currency) to another user, also identified by a public key. This system of payments has several advantages over other traditional payment systems, but it also comes with some drawbacks. For example, the system is pseudonymous as users are only identified using a public key, which helps protect user privacy. On the other hand, the entire record of transactions is publicly visible, which reduces privacy. Another advantage is that anyone can be a participant in the system, and no one user can prevent another user from accessing it. This freedom comes at the cost of efficiency; Bitcoin transactions can be slow to be finalized and expensive when compared to traditional payment mechanisms such as Visa or PayPal.

Bitcoin was only the first blockchain network. The next generation of blockchain networks further expanded on the concepts Bitcoin introduced. For instance, Ethereum [25] works with similar primitives to Bitcoin, but instead of its transactions only representing the transfer of tokens from one user to another, its transactions take the form of bytecode which runs on a virtual machine with a global state that is updated with each transaction. This allows users to write complex programs, referred to as *smart contracts*, with APIs which can be called by clients. These smart contracts form the basis of *decentralized applications* (DApps) which can be used to run decentralized exchanges [26], voting protocols [27], and more.

Blockchains mainly fall into two categories: *permissionless* and *permissioned*. Generally, permissionless blockchains are openly operating distributed ledgers in which any user around the globe can freely join the network as a *validator*, the nodes that operate a blockchain network, or as a *user*, those that make use of the system's services. They use Sybil-resistance mechanisms to ensure no single participant can accrue too much power on the blockchain. Examples of such mechanisms include proof-of-work (PoW) [6], where *miners* create blocks by solving a randomized, cryptographic puzzle, demonstrating the computing power they have dedicated to the task; proof-of-stake (PoS) [21], where *stakers* lock up funds in order to obtain the ability to produce and validate blocks at a rate proportional to the size of their stake and risk losing their staked funds in response to bad behaviour, such as validating two incompatible blocks; and Proof-of-Elapsed-Time [28] which uses specially designed hardware to ensure validators wait a sufficient period before producing new blocks. These Sybil-resistance mechanisms are paired with consensus algorithms which allow the participants to come to agreement on the state of the blockchain. Applications built upon permissionless blockchains can operate at a large scale but often suffer from low throughput and high latency [29]. Nevertheless, modern technology advances in permissionless blockchains have managed to achieve significant performance gains.

On the other hand, permissioned blockchains can attain high throughput and low latency by only allowing specific authenticated nodes to act as validators. These chains can either be set up by a centralized entity that holds the power to invite new validators to the network, or a collection of entities who all work together to maintain the network and determine who can act as a validator. For example, the Diem network [18] was run by a collection of corporations; the group was led by Facebook (now Meta) and its members included blockchain companies, e-commerce companies, and payment processors, among others [30]. The primary concern of permissioned blockchains is to design efficient and effective Byzantine fault-tolerant (BFT) algorithms to tolerate arbitrary failures [31]–[33]. PBFT [34] and its variants (*e.g.*, BFT-SMaRt [35]), which achieve consensus using $O(n^2)$ messages, have been widely used in platforms such as Hyperledger Fabric [36] and R3 Corda [37]. In addition, SBFT [38],

HotStuff [39], and Prosecutor [40] optimize the message passing pattern and leverage threshold signatures, achieving consensus using only $O(n)$ messages, allowing permissioned blockchains to scale and enable large data transfers, such as those that may be required by some V2X applications.

Blockchains are the most common distributed ledger technology (DLT). DLT refers to all decentralized systems that allow users to read from and write to a shared ledger. Many non-blockchain DLTs are based on a directed acyclic graph (DAG) architecture. While in blockchains each block points to one previous block (its parent), and each block only has one child, in a DAG-based system blocks may have multiple parents and multiple children, forming a DAG [41]. Despite the fact that not all DLTs are technically blockchains, the term blockchain is often used to refer to all kinds of DLTs. In this paper we will follow this custom.

Though blockchains are generally considered to be very secure systems, they may be susceptible to various kinds of attacks and must be carefully designed in order to prevent them. One potential attack is the *51% attack*, in which an attacker attempts to control the network by taking control of a sufficient number of validators [17]. In permissioned networks, this attack is generally prevented by carefully selecting and protecting validators, ensuring both that the validators are trusted to not participate in such an attack, and that the machines holding their private keys are not vulnerable to attack. In permissionless networks, this attack is prevented by making it very expensive to carry out, either through the cost of computation needed for PoW, or through the cost of the stake required in PoS networks.

Another important attack against blockchains is a *Sybil attack*, in which one user takes on multiple identities [23]. This attack is made possible by blockchain's extensive use of pseudonymous identities. In permissioned networks, Sybil attacks are prevented using ID mechanisms. In permissionless networks, Sybil attacks are prevented using Sybil-resistance mechanisms, which either make the creation of identities expensive or prevent users from realizing any material advantages from the use of multiple identities.

C. BLOCKCHAIN-ENABLED V2X

There has been a lot of interest in applying blockchain technologies to the automotive sector [42]–[44]. When applied to V2X communication systems, blockchain networks would sit between the networking and application layers [42], as shown in Fig. 2. Here, blockchains can build upon advanced networking technologies such as 5 G, 6 G, Wi-Fi, P2P networks, and vehicular ad-hoc networks (VANETS), while providing services to the applications above. As using a blockchain network will introduce some delay, many applications would only rely on blockchains for certain features, such as data timestamping.

There will be many heterogeneous participants in a V2X blockchain network. Vehicles will of course utilize the blockchain for the applications they require. Additionally, infrastructure such as traffic lights, roadside units (RSUs),

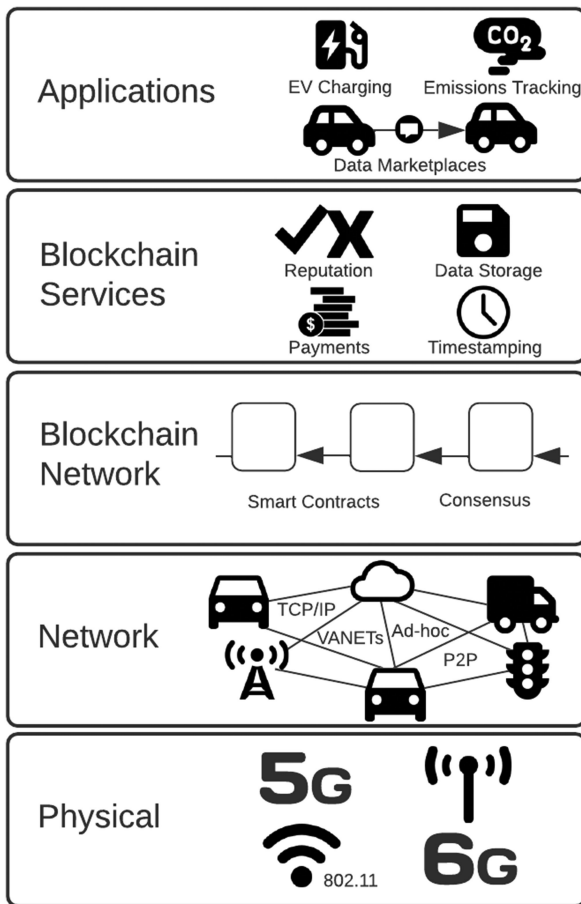


FIGURE 2. Layered view showing how blockchains fit into the networking stack.

and others play both an active and supporting role in the network. For example, parking meters, which may use a V2X blockchain to accept payments, would be active users in the blockchain. Meanwhile, RSUs (also known as fog nodes) can play a supporting role by providing extra services to passing vehicles, such as packet forwarding, data caching, and more. Other possible participants in the network include cloud service providers who could offer various services, such as data storage and cloud computing.

An important aspect of V2X communication is proper handling of data from the various sensors on the vehicle. In this scenario, data integrity must be maintained and sensitive data must be protected. Therefore, the application of a blockchain to V2X systems is tightly linked to its application within IoT systems as they share many common concerns. For example, both V2X systems and IoT systems may experience inconsistent internet connections, and location and geography may play a larger role in these systems than most blockchain applications. Nevertheless, there are certain differences that must be considered when developing V2X blockchains. First, though the energy and computational power available is limited, modern vehicles still have significantly stronger capabilities than most IoT devices which often rely on small capacity batteries and/or inconsistent power sources. Second,

the transportation industry is more heavily regulated than IoT in general, which could alter the pathway to adoption.

Adoption of blockchain-enabled V2X applications faces several obstacles. A major challenge is privacy. Vehicle data can reveal very personal information, such as one’s location. Care must be taken to ensure such data is not inadvertently revealed on a public ledger [44]. Another important issue faced is performance. Current networks are not able to fully support even a subset of the proposed blockchain-enabled V2X applications, and much more innovation is needed to create optimized architectures for the V2X space [7]. Additional issues are discussed in Section V.

D. PRIOR WORK

Huang *et al.* [45] describe many of the security and privacy challenges faced by V2X systems. A significant portion of these attacks can be addressed by blockchains, including bogus messages, message modification, and Sybil attacks. Because of this, multiple works have identified blockchain as a key component of the 6 G networks that will enable the V2X ecosystem [46], [47]. Other surveys have investigated possible applications of blockchain in IoT and transportation industries. Yuan and Wang [42] lay the groundwork for applying blockchain to transportation and demonstrate how blockchains can fit into the existing internet protocol stack in order to provide their services to applications. Fraga-Lamas and Fernández-Caramés [43] review how blockchains can be used to add resilience to the entire automotive industry and discuss how the industry’s wide array of stakeholders, some of which can be seen in Fig. 1, make the use of decentralized solutions especially important. Stoyanova *et al.* [48] survey forensics issues in IoT systems, including transportation systems, and how blockchain technology can be used to address these challenges. Mollah *et al.* [44] analyze many proposed blockchain-based applications for the internet of vehicles (IoV) and identify many challenges facing such applications.

III. V2X BLOCKCHAIN USE CASES

Prior research has demonstrated a wide array of applications that can be enabled or improved using blockchain technology. These applications differ in terms of what features of blockchain technology they utilize, and to what extent they rely on those features. A categorization of applications based on these and other factors can be found in [7]. In the remainder of this section, we describe the important services blockchains can provide to V2X applications, and we analyze how a variety of previously proposed applications of blockchain utilize these services.

A. V2X BLOCKCHAIN SERVICES

We have found that proposed V2X blockchain applications rely on blockchains for three key services: *payments and incentives, reputation and identity, and data authentication and timestamping.* Notably, many applications claim to use blockchains to increase user privacy. While it is the

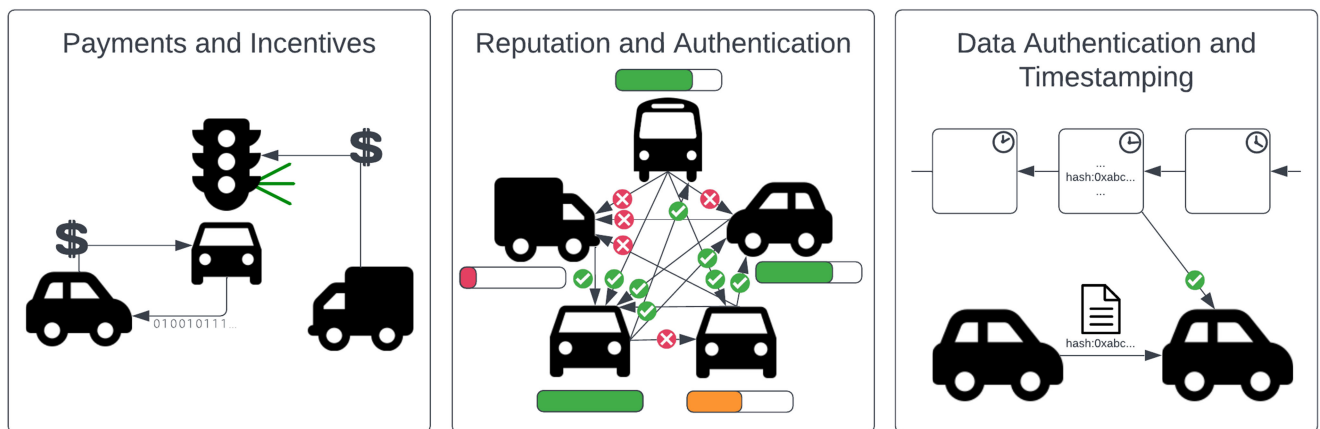


FIGURE 3. The three key services provided by blockchain to V2X applications.

case that many blockchain-based designs provide strong privacy guarantees using technologies such as zero-knowledge proofs [49], [50], blockchain's public and distributed nature make it an inherently less private platform than many other designs. As such, privacy in these applications is achievable *in spite* of the use of blockchain technology, not because of it. This is demonstrated by the fact that the privacy preserving techniques used in these designs, such as pseudonymous identities, data encryption, and zero-knowledge proofs, can just as easily be applied to centralized applications that do not use blockchain.

Here, we describe the most important services that blockchains provide for V2X applications, which can be seen in Fig. 3.

1) PAYMENTS AND INCENTIVES

Payment services are important to V2X systems because many applications, such as paid parking [51] and EV charging [52], require them. The first blockchain, Bitcoin [6] is an electronic cash system, and most modern blockchains continue to offer these services. Blockchain-based payment services offer several advantages over existing payment systems that are important for V2X applications. First, many applications, such as data marketplaces, require *microtransactions* which send very small amounts, as little as a fraction of a cent, between users. Current payment systems, such as Visa, Swift, and PayPal, are not only too expensive to support such transactions [53], but by-construction they were never designed to handle micro-payments. On the other hand, blockchain systems are able to provide these services [54]. Although Bitcoin transactions are expensive, other technologies exist that allow for much cheaper payments. For example, *Layer-2* solutions execute transactions off-chain and periodically settle balances on some major blockchain, such as Ethereum, in order to finalize these transactions in batches [55]. Many categories of *Layer-2* exist, including *payment channels* and *rollups*. For example, the Lightning Network is a system built on the Bitcoin blockchain that uses payment channels to enable low-cost transactions [56].

Layer-2 solutions generally present trade-offs between speed, efficiency, and security. By selecting from the available options, users can tailor their choice to their own specific needs and preferences. Additionally, new blockchain networks such as Solana [57] and Avalanche [58] have vastly more capacity than Bitcoin or Ethereum, allowing for cheaper transactions even without Layer-2 solutions. A second advantage of blockchains over legacy payment systems is that blockchains allow users to develop complex payment mechanisms that suit their purposes using smart contracts. For example, EV charging networks are able to easily support dynamic pricing, which allows users to act as both a buyer and seller of energy [52].

2) REPUTATION AND AUTHENTICATION

Reputation is a measure of how others perceive an entity's behaviour and is widely used both online and in real life to weed out bad actors and to inform others whether or not they should trust a particular identity. V2X systems require strong reputation mechanisms in order to protect against false or misleading data being shared among vehicles, among other uses. Many systems to track reputation on blockchain have been proposed [59]. These systems generally use reviews by users of their interactions in order to establish a reputation associated with a particular identity. Reputation can either be global, meaning all users calculate the same reputation score for a particular identity, or personalized, meaning that users may have different perceptions of the reputation of an identity, generally based on its past interactions with them or others in their social network [59]. As identities may be used to track users' activities, privacy is an important aspect of any reputation system [60]. Additionally, when user reviews are used to determine an identity's reputation, Sybils and other related attacks must be protected against [61]. This is often done using a permissioned system with semi-trusted authorities [62]. A key service related to reputation is authentication. Systems controlling sensitive data, such as the location data produced by vehicles, must be careful to give users access only to what they are authorized for while also managing

user privacy. Using blockchain-based identity and reputation, strong authentication systems can be developed [63].

3) DATA AUTHENTICATION AND TIMESTAMPING

Maintaining accurate records is very important to V2X systems. For example, in the event of an accident, vehicle data must be stored to assist with investigations [64]. Blockchains provide an immutable record of their own histories. This means that blockchains can be used to store an immutable record of any data. Additionally, because blockchain networks are able to remember the approximate time that a block was created, placing data onto a blockchain provides a timestamp for the data. These services have the potential to significantly improve the reliability and accuracy of vehicular digital forensics.

Storing all of the vast quantities of data produced by V2X systems on a blockchain is not possible, as all on-chain data must be stored by all nodes validating the blockchain. Instead, many applications can be supported by changing the type of storage required. For example, video feeds produced by a vehicle's camera(s) should not be stored on chain due to both the size of the data and privacy concerns, but a record of such data may be desired to ensure its authenticity in case of an accident investigation. In such cases, a hash of the particular data can be stored on-chain rather than the data itself [65]. This allows data to be authenticated and timestamped, but does not ensure that the data ever was or ever will be available; this may be acceptable for some applications. Such as system can also be used in combination with centralized cloud storage services in order to provide additional auditability [66]. In other cases, it may be required that the data was made available at some point in time, but does not need to be stored going forward. For example, insurance contracts may require drivers to regularly provide information about their driving habits to their insurance company. This can be achieved using data availability proofs. By augmenting blocks of data with Reed-Solomon erasure codes, nodes participating in the network can be confident that all data in a block has been made available to the network while only downloading a small subset of that data [67]. This solution ensures that the data in question was made available at some point in time, but does not ensure the data will continue to be made available. In some cases, this may not be enough and secure, decentralized, long-term storage of data is required. For example, this may be the case for data being used by accident investigations. Filecoin, built on top of the Interplanetary File System (IPFS), allows users to rent their available storage space to others in a decentralized fashion [68]. This allows users to store data in a reliable way using blockchain, much like can be done on Bitcoin. However, in this case only a fraction of the validators on the network will store the data, providing less guarantees of storage compared to Ethereum, for instance, or other established blockchain networks, albeit at a much lower cost.

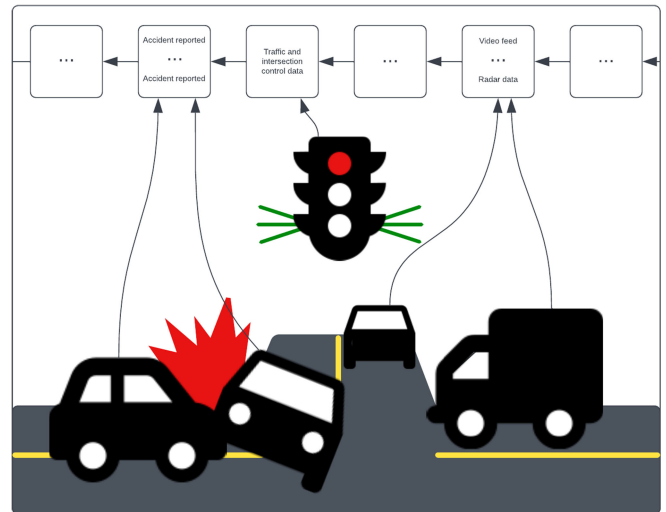


FIGURE 4. A demonstration of how blockchains could be used to store accident data.

B. V2X BLOCKCHAIN APPLICATIONS

In this section, we describe some previously proposed blockchain-based V2X applications and detail how they use the blockchain services described so far. This list is not exhaustive, but it does cover many of the most commonly proposed applications.

1) INSURANCE AND ACCIDENT INVESTIGATIONS

Insurance and accident investigations are important applications for blockchains in the V2X space as they can utilize all of the blockchain services described above. First, through payments and smart contracts, blockchains can be used to purchase dynamic insurance plans [69]. This allows users to purchase much more tailored plans, for example, only purchasing insurance for the time they spend driving. This has the potential to lower costs for many consumers while also reducing risk for insurance companies as they can better tune premiums to precise driving scenarios. Additionally, blockchains can be used to store information for insurance purposes. For example, records of a driver's behaviour could be stored on the blockchain and smart contracts could update the driver's premiums automatically based on these data [70]. In the event of an accident, surrounding vehicles that witness the event could automatically upload any pertinent data they captured so as to prevent forgery or missing data [64], [65], as shown in Fig. 4. The immutability guarantees offered by blockchains can greatly assist with vehicular digital forensics. Vehicles could also use blockchain consensus mechanisms to come to agreement on what occurred in an accident, with blockchain-based reputation and identity being used as a tool to help determine the trustworthiness of all parties [71].

2) DATA MARKETPLACES

Data are produced constantly by individuals, including while driving. Data from vehicles could be used for many purposes,

such as building highly accurate maps [72]. In spite of this, rather than realizing the value of data, users face barriers when trying to sell their data including high transaction fees and a limited set of buyers; blockchain technology can help solve these problems [54]. Blockchain-based payments can be used to pay for data [73]. Because individual sensor readings are generally worth very little, specialized techniques must be used to reduce transaction fees [54]. Additionally, smart contracts can be used to take advantage of more complex pricing models [74]. Reputation techniques can also be applied to this problem to ensure the quality of data [75] or to provide small loans to buyers and further reduce transaction fees [54]. Due to the cost of transferring data via blockchain relative to the value of most IoT data, it is not advisable to use blockchains to transfer or store these data.

Blockchains could also be used to more efficiently distribute important data such as maps and firmware updates. Baza *et al.* [76] describe a system where vehicles share large data files with nearby peers rather than having to download them from a centralized server. This reduces network congestion while improving download speeds for end users and reducing server costs for those providing the files. Blockchain-based payments could be used to incentivize users to share files and reputation and authentication systems could be used to verify data sources and ensure only authorized users are given access to the files.

3) EMISSIONS TRACKING

An important challenge for the transportation industry is how to reduce carbon emissions. One suggested mechanism for emissions reduction is a cap-and-trade scheme whereby individuals and companies are given a certain allotment of carbon credits, entitling them to a certain amount of emissions [77]. Individuals who use more than their allotment must then purchase credits from others who do not use their entire allotment. All of this can be tracked on a blockchain for efficiency, resilience, and ease of use [77], [78].

Such an application could use all of the blockchain services described above. Strong identity and reputation services could be used to determine the entities that are to be granted carbon credits, payment services and exchange smart contracts could be used to buy and sell credits, and records of actual emissions could be recorded on chain to track emissions and ensure that all users have the credits required to pay for their emissions.

4) TOLLS, PARKING, AND RIDE SHARING

Evidently, blockchain-based payments can be used to pay for tolls, parking, and ride sharing [79], [80]. Blockchains offer several advantages over traditional mechanisms. First, the open nature of blockchains allows for multiple parties to use a single shared interface to charge and pay for these services. This allows individuals to sell parking or rides that they have available, increasing the availability and utilization of cars and parking. It also allows even small municipalities to set up toll systems which may not otherwise be worthwhile

to operate. Despite these disparate sources of charges, end users can pay for all these services through a shared interface, increasing ease-of-use. Additionally, through smart contracts, blockchains can enable more dynamic pricing models for these services, including auction mechanisms, optimizing both the price and utilization of resources [51].

5) EV CHARGING

Another proposed application for blockchain in the V2X realm involves vehicle-to-grid (V2G) communications [81]. Proposed systems allow electric vehicles (EVs) to connect with electric grids in order to purchase electricity and even sell power back to the grid or to other vehicles to ensure a stable energy supply [10], [52], [82]–[84]. V2G systems bring many advantages. First, they contribute to the creation of a more robust power grid by distributing power sources. Second, through incentive compatible pricing models, it is possible to induce supply to meet demand, ensuring stability [10], [82]–[85]. By using blockchains to enable such systems, it can be made easy for any user to make and accept payments, allowing for a wider field of participants, and using microtransactions and smart contracts, more dynamic pricing models can be enabled using low cost blockchains [10], [52], [81], [83], [85]. When using blockchains to enable such services, one must be careful to protect users' personal information, such as their location. Designs have been proposed to address these concerns [86], [87].

C. USE CASE ANALYSIS

For any proposed blockchain-based application, an important initial question to ask is: *why blockchain?* In many cases a simple database can support all the same services as a blockchain at lower cost with more scalability [88]. Even many of blockchain technology's touted benefits, such as transparency and privacy can also be achieved by centralized solutions, though they are often not prioritized by such solutions. Therefore, the question of why blockchain must be asked of blockchain-based V2X applications as well.

We envision *four* major reasons supporting the use of blockchain in these and other V2X applications. First, the automotive sector has a diverse array of stakeholders [43]. As a decentralized database, blockchains are not controlled by any one entity. Therefore, they can be useful in areas with diverse stakeholders with potentially diverging interests, as is the case in the automotive sector. This feature becomes especially important in scenarios where participants may not be incentivized to act honestly, such as in accident investigations.

Second, blockchains natively support payments and can be used to efficiently pay for things such as tolls, electricity, and data. Though some existing blockchains suffer from high transaction fees, limiting their use for payments, others have improved in this area, resulting in blockchain-based payments that compete in cost with existing payment platforms [57].

Third, blockchains are inherently open systems which allow both large and small scale applications to take full advantage of their features, such as payments and reputation, while operating on a level playing field where all participants have equal access to data. This will allow, for example, anyone to rent their driveway in the same way companies might rent spots in a parking lot. This is an advantage over other systems run by private platform vendors, as such entities may be able to leverage their market position to extract unfair rents from their users or push out competitors. Although the field of V2X is too nascent to already have platforms with such control, lessons must be learned from other fields, such as retail, where Amazon has been accused of using its seller's data to gain an unfair advantage in their marketplace [93], and in mobile operating systems, where Apple and Google have been accused of using their dominant positions to charge unreasonable fees to developers [94]. Notably, Apple and Google both produce software for in-car infotainment systems.

Fourth, many applications require accurate timestamping of information. This is especially important in cases where users may wish to edit information after the fact, such as in accident investigations. Using blockchain, accurate, unforgeable timestamps can be created by anyone.

Despite the above advantages, using blockchain technology for these applications is not a panacea and does not come without cost. For instance, blockchains will generally be slower and have less throughput than other distributed database designs. This limits their applicability as some applications may require real-time responses or significant storage resources. Some blockchain designs can improve in these respects, though they often trade off on decentralization, potentially reducing some of the benefits of using blockchain. Additionally, due to its public nature, extra care must be taken and advanced cryptography techniques may be required to ensure privacy is maintained in blockchain-based systems. Finally, many applications require data collected by off-chain entities, such as emissions sensors. Ensuring that this data is accurate is a difficult problem which specialized applications called oracles attempt to solve, though imperfectly. This issue is discussed further in Section V.

IV. V2X BLOCKCHAIN ARCHITECTURES

An important question for any V2X application that requires blockchain services is: *which blockchain network should the application be built on?* Meijers *et al.* [7] analyzed several V2X blockchain applications in order to determine their underlying requirements in terms of throughput, data storage, and other factors. They show that none of the most popular networks currently have the capability to support all of these applications, even when limiting the scope to the province of Ontario, Canada. This is due to the massive volume of transactions and data that vehicles and infrastructure are capable of producing. Below, we summarize some efforts that have been made to increase blockchain capacity, both in generic blockchain networks and those tailored for IoT and transportation ecosystems.

A. GENERIC BLOCKCHAIN NETWORKS

Here, we describe several blockchain networks that could be used in the V2X ecosystem. A summary of the networks described here is given in Table 2. Note that the throughput is divided into two categories, low and high. Comparing precise throughput claims of different networks is difficult given that any claim is highly dependent on the network settings, the nodes running the network, the minimum transaction size, and other factors. Networks listed as having low throughput achieve less than 10 transactions per second (tps). Networks listed as having high throughput are capable of achieving in excess of 1000 tps under certain conditions. Additionally, it should be noted that networks that do not natively support smart contracts, such as Celestia, can still be used as a consensus mechanism for smart contract platforms [95].

1) BITCOIN AND ETHEREUM

Bitcoin [6] and Ethereum [25], both described in Section II-B, are early and extremely popular blockchains. However, due to Bitcoin's limited programmability (i.e., no Turing-complete smart contract functionality due to a lack of loops in its scripting language) and both Bitcoin and Ethereum's low throughput, high fees, and long confirmation time, they are not good choices to support V2X blockchain applications. The Ethereum network is in the process of being upgraded to Ethereum 2.0 which will move the network from a PoW based consensus scheme to one based on PoS [96]. The goal of this process is to eliminate these shortcomings by introducing orders of magnitude more transaction throughput, but it is yet to be seen whether or not this upgrade will be a success. If so, it may be able to support V2X applications in the future.

2) POS NETWORKS

Many other networks, such as Algorand [21] and Solana [57], already use PoS consensus to improve efficiency and throughput. These networks are theoretically able to achieve thousands of tps with very low latency [21]. Further scaling can be achieved using sidechains, sharding, and rollups, though such strategies generally come at the expense of latency. A major drawback of such networks is the centralization of control. Individuals with large stake can exert significant control over the network, raising questions about security and stability. As such, it is important to ensure that all actors in PoS networks are properly incentivized [97].

Avalanche [58] is a network that uses a different consensus algorithm, the Avalanche consensus protocol [90]. Though it uses PoS as a Sybil prevention mechanism, this algorithm operates much differently from many other PoS networks. A major advantage of the Avalanche consensus protocol is that any node can participate, even one with little computing power. This allows the validator set of the network to grow very large and prevents the centralization of the network around a few actors while still allowing the network to scale to many thousands of tps. This means that individual vehicles could

TABLE 2. Summary of Generic Blockchains

	Type	Sybil-Resistance	Consensus	Throughput	Transaction Fees	Smart Contracts
Bitcoin	Public	PoW	Nakamoto [6]	Low	High	Limited
Ethereum	Public	PoW	GHOST [84]	Low	High	Turing-complete
Algorand	Public	PoS	BA* [21]	High	Low	Turing-complete
Solana	Public	PoS	Proof-of-history [52]	High	Low	Turing-complete
Avalanche	Public	PoS	Avalanche [85]	High	Low	Turing-complete
Hyperledger Fabric	Private	Permissioned	<i>Flexible</i>	High	None	Turing-complete
Open Libra	Public	Delay Towers [86]	HotStuff [34]	High	Low	Turing-complete
Celestia	Public	PoS	<i>Unknown</i>	<i>Unknown</i>	Very Low	Not natively supported
IOTA	Public	PoW	Coordinator [87]	High	Very Low	Not natively supported
Conflux	Public	PoW	GHASt [36]	High	Low	Turing-complete

act as validators in the network without negatively affecting throughput.

Although such networks may provide enough performance to support certain V2X applications, it can be argued that a permissioned system is more suitable than PoS for the V2X system, even though a more open, decentralized system may be preferred for other applications. This is due to the large number of established, semi-trusted stakeholders in the V2X ecosystem, such as governments and automakers.

3) PERMISSIONED NETWORKS

Hyperledger Fabric [36] is an open-source blockchain implementation that allows groups to stage permissioned blockchain networks for their own use. Networks based on this implementation are able to achieve high throughput and low latency using a limited, permissioned validator set. Limiting the set of validators in this way eliminates the issue of Sybil attacks, which allows for more efficient Byzantine fault-tolerant algorithms to be used. Hyperledger's consensus algorithm is not able to accommodate a large number of validators due to communication overhead [98], though designs have been proposed to increase Hyperledger's performance [99]. New consensus algorithms, such as HotStuff [39], run more efficiently, allowing larger validator sets. A variant of HotStuff was used by the Diem network. Although the future of that network is unclear, other networks are utilizing its technology stack, including Open Libra (0 L) [91]. Despite the fact that the V2X ecosystem has semi-trusted stakeholders who may be willing and able to operate a blockchain network, it may be desirable to have vehicles themselves operate the network rather than cloud-based nodes in order to reduce communication latency. Unfortunately, even the HotStuff consensus algorithm is not able to scale to accommodate so many validators without a decrease in performance due to communication overhead.

4) MODULAR BLOCKCHAINS

Celestia [95] (previously LazyLedger), which is currently under development, promises to be a modular blockchain network. Celestia is modular in that it only provides ordering and data availability to its applications. It does not rely on the network to execute transactions for every application, unlike with

most other systems. This allows individual applications to customize the execution layer in order to suit their own needs. To provide these services efficiently, Celestia nodes randomly sample specially designed blocks to determine (with a chosen level of probability) that the data in the block has been made available to the network. Since they do not have to execute the transactions in the block, nodes do not even have to download the data from the entire block. Instead, nodes can simply download the transactions for applications they are interested in and track the state of only those applications. This reduces the work that needs to be done by individual nodes at the expense of ease-of-use for the application developer. This design could assist with solving the capacity problem of many current chains, as vehicles could record data on the blockchain without burdening all other vehicles on the network. However, additional effort would be needed for vehicles to support other services, such as payments, which could hinder development and limit interoperability.

5) DAG-BASED BLOCKCHAINS

DAG-based systems, such as IOTA [92], [100] and Conflux [41], have been proposed as a way of improving throughput. Unlike most blockchains, where each block contains the hash of its immediate predecessor (parent), in DAG-based blockchains each block contains the hashes of multiple predecessors. In IOTA, each block declares two parents. In Conflux, each block declares one parent and zero or more blocks that were created before the current block (uncles). This architecture allows blocks to be produced and processed in parallel, increasing scalability. A diagram of a DAG-based blockchain with Conflux-style uncles can be seen in Fig. 5. Note that because blocks are produced in parallel, the precise order in which blocks are produced may be unknown, and multiple orderings may be possible. Therefore, any solution that uses a DAG-based blockchain must either use a deterministic algorithm that finds the final ordering of blocks, as Conflux does, or disallow conflicting transactions, as is done by IOTA.

Conflux scales to at least 6000 tps, past which point it is limited by the compute capacity of its nodes [41]. IOTA claims to have infinite scalability, but these claims have not been proven [100]. Additionally, IOTA currently relies on a centralized coordinator node to operate, though plans are

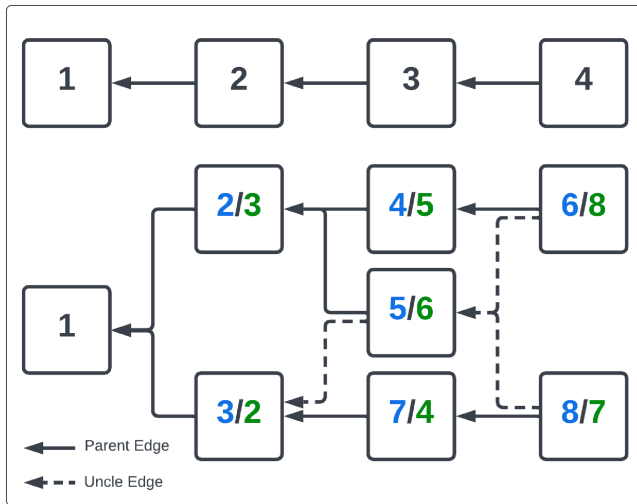


FIGURE 5. A diagram of a blockchain with its block ordering (above) and a DAG-based blockchain showing two possible block orderings (below) .

underway to remove that requirement. Such a system may be well suited to V2X systems because the fact that blocks can be created in parallel allows for different geographic regions to operate semi-independently of each other, potentially decreasing latency. Although such independence raises the risk of conflicting transactions which must be reverted in systems like payments, some V2X applications, such as data recording, do not have any chance of producing conflicting transactions.

B. NETWORKS TARGETING IOT AND TRANSPORTATION

Many blockchains and consensus designs have been proposed to better serve IoT and transportation industries. In order to reduce power consumption, most do away with PoW consensus in favor of a permissioned system or a custom consensus algorithm. Creators of such networks have pursued several different strategies to increase throughput, as described below.

One common approach is to use a DAG architecture [101]–[103]. Such designs can significantly increase throughput, but may require other strategies to deal with the large volume of transactions that can be created [101], [102].

One strategy to deal with these transactions is to reduce the amount of data that nodes need to store. This is especially important for V2X systems, in which vehicles can produce large amounts of data that must be stored for some period in case it is needed (for example, in case the car later gets into an accident), but which can be deleted after some amount of time. Dorri *et al.* [104] propose a memory-optimized blockchain in which transaction senders pay network participants to store a transaction’s data for a certain period of time. Once that period is up, the transaction may no longer be available to the network, though the sender can still store it if they wish. This prevents nodes from having to store large transaction and state histories, reducing their storage requirements. Yang *et al.* [102] introduce another design in which nodes only store data that are relevant to them, which, in the context

of transportation, is likely to be recent data that occurs near their geographic location.

Finally, another scaling strategy many proposed V2X blockchain networks have used is to break the blockchain into different pieces serving either different application types or geographic regions. Biswas *et al.* [105] propose a system where devices form smaller networks with trusted peers, such as devices from the same manufacturer. Transactions from these networks are later settled on a global blockchain. Similarly, Dorri *et al.* [106] propose dividing nodes into clusters which rely on cluster heads, who are selected based on a decentralized algorithm, to relay their transactions to the wider network. These cluster heads are similar to validators on other networks, as they produce and validate blocks, although, unlike validators in other networks, cluster heads are assigned specific users they must provide services to, such as relaying of transactions and messages. Speed and efficiency are increased by limiting the validator set and using a time-based consensus algorithm that is more energy-efficient than PoW.

Many V2X blockchain applications, such as parking, ride sharing, and data marketplaces, are impacted by geography. For example, a car is more likely to be interested in traffic information from a nearby vehicle than one that is far away. Therefore, V2X blockchain designs should account for this, ideally exploiting this aspect of some applications in order to maximize performance. Shrestha and Nam [107] argue that V2X blockchains are local in nature because most of the information transferred via these chains, such as traffic data, is only relevant in specific locations. Additionally, they show that even these smaller chains can be well-secured. Karlsson *et al.* [101] propose Vegvisir, a blockchain based on a DAG which allows users in different locations to add blocks to the chain separately, without incurring the delay required to maintain identical chains globally. However, this design only supports applications where transactions cannot conflict, meaning it does not support payments, among other services.

C. ARCHITECTURE ANALYSIS

A holistic design for a V2X blockchain architecture must make certain decisions about how to solve certain problems. In some cases, the correct choice is reasonably clear, in others, many possible solutions exist. Some of these decisions are described below.

1) PERMISSIONS

An important question for any blockchain network is that of its participants. In permissionless systems, the default answer is anybody. This is chosen to ensure maximum participation in and access to the system. This design opens the door to attackers, requiring robust consensus algorithms that may in some cases perform worse than those that could be used in a system where more trust can be placed in individual users. Unlike with the internet at large, in transportation systems a license is required to drive and cars must be registered. As such, using a permissioned system is consistent with these rules and

requirements and does not place too significant a burden on its users. This also allows the use of consensus designs that might not be safe to use in a permissionless environment.

In permissioned systems it must be determined who is allowed to act as a validator on the network. Should all vehicles be considered equals and able to contribute to the running of the network, or should some users (either vehicles, RSUs, or other participants) be able to participate in the validation of the chain while others are relegated to user status? The decision here is highly dependant on the choice of consensus algorithm, as some algorithms [90] support many more validators than others [36].

2) CONSENSUS, LATENCY, AND THROUGHPUT

Another important question is how to choose the correct consensus algorithm in order to ensure the network meets its latency and throughput requirements. Although Bitcoin and Ethereum provide high security, their low throughput is evidence that a basic PoW consensus algorithm is insufficient for V2X applications. Other designs, both based on PoS algorithms [21], [41] or higher throughput versions of PoW consensus (e.g., Layer-2 solutions), come closer to being able to support V2X applications. Many blockchain networks implement consensus algorithms that are able to achieve low latency and thousands of tps in throughput. However, these networks generally require participating nodes to have significant processing, storage, and networking capabilities, limiting who can participate in the network operation. This may be undesirable, especially if vehicles and RSUs, which may have unstable network connections at some times, are expected to participate. Other algorithms such as those proposed by IOTA and other DAG-based blockchains, as well as that of Avalanche, allow users of all capabilities to participate. Finally, there is the possibility of a layered architecture [106], which allows all users to participate, but gives certain users, who likely have more capabilities, increased responsibility to operate the network.

3) CAPABILITIES

What capabilities a V2X blockchain must have is another important question. As described in Section III-A, V2X blockchains must support three main services: payments and incentives, reputation and authentication, and data authentication and timestamping. The first service requires that a blockchain's consensus accounts for conflicting transactions (such as two transactions transferring the same token). The second requires that the blockchain supports some level of smart contract capabilities in order to allow for a robust reputation and authentication system. Finally, the third requires that the blockchain have some support for recording, verifying, and timestamping data. Notably, while these capabilities are all required in order to support the widest range of applications, it may be possible to divide them amongst multiple chains. For example, Vegvisir [101] can support large amounts of data authentication and timestamping, but it cannot support

payments. By combining this design with another chain that does support payments the advantages of both designs could be realized. Conversely, using multiple blockchain architectures increases complexity, makes application development more difficult, and increases the chances of fragmentation caused by different vehicles supporting different services. Celestia [95] offers the interesting opportunity to run multiple virtual machines on top of one consensus system, which could theoretically allow the use of multiple architectures with less significant concerns around complexity and fragmentation, however, this design has yet to be proven.

4) SCALABILITY

A major issue with any potential V2X-serving blockchain is its scalability. Given the number of vehicles on the road and the number of interactions future connected vehicles can be expected to have with each other, the number of potential blockchain transactions far exceeds the capacity of any existing blockchain [7]. Additionally, storing the data of those transactions for any significant period will exceed the capabilities of any participant outside of a large data center. As such, novel tools are needed to increase the scalability of the blockchain. For example, data storage could be distributed and pruned [104], or the entire blockchain could be divided up based on regions, reducing the amount of information any one node must account for [107]. It is in this area where generic blockchains generally fall short. Though modern designs offer significant scalability, supporting a global ledger of all V2X transactions would require validators to have massive storage and processing capabilities, disqualifying vehicles as significant actors in the network and potentially increasing latency as a consequence.

V. CHALLENGES & RESEARCH DIRECTIONS

There is clearly potential for blockchain technology to enable new and exciting applications within the V2X ecosystem, nevertheless, adoption of such technology still faces several challenges. Some are technical, and significant research has gone into solving these complex problems. Even so, more work remains to be done in order to tailor the technology to the V2X ecosystem. As discussed above, no existing blockchain has all the features and capabilities needed to support the entire V2X ecosystem. Additionally, there are certain challenges that are specific to V2X blockchains that also require more research. Even though we focus on technical challenges, notably there are also regulatory questions that must be addressed. These involve items such as how blockchain technology could be used for government operations, including toll collection and accident investigation. While these issues are significant and warrant more investigation, they are outside the scope of this work.

Finally, it should be noted that the ability to support blockchain networks in V2X systems is limited by the capability of the networking stack that underlies them. Significant

research has gone into enabling intervehicle networking technologies using standards such as Wi-Fi and 5 G which may be able to support blockchain networks, however, this aspect of the technology stack is outside the scope of this work as such communication protocols must support far more technologies and applications than just blockchain.

A. GEOGRAPHICALLY AWARE ARCHITECTURE

Most existing blockchains are global and geographically agnostic, but transportation systems are much more local in nature [107]. Global blockchains generally increase communication costs and latency while reducing scalability. Some proposals have suggested taking advantage of the regional nature of transportation systems to increase performance and scalability [102], [107]. Nevertheless, while localizing blockchain systems does give some advantages, there are certain applications, such as payments, that benefit from a global blockchain. Additionally, while transportation systems are local, vehicles are constantly moving between localities, and so systems must be interoperable, with vehicles being able to quickly switch from one system to another without compromising the safety or security of any vehicles or the applications running on the blockchain. Therefore, fast, reliable, and secure cross-chain solutions such as bridges, which facilitate the transfer of assets between blockchain networks, must be developed [108]. A system that pairs local consensus with global consensus for certain transactions while allowing vehicles to easily transfer between local networks could go a long way towards providing the scalability that V2X systems require.

B. DATA STORAGE

Efficiently storing and serving large amounts of data is a difficult problem for blockchains. Nevertheless, it is an important service that V2X blockchains must offer. Solutions have been proposed for more efficient blockchain-based storage systems. For example, MOF-BC [104] allows users to pay validators to store their transactions for long periods and Filecoin [68] allows participants to rent out disk space. Despite this, more research is required for designs specifically targeting V2X systems. Such designs could take advantage of the large number of vehicles that may be willing to offer their storage for use by the network, trusted hardware available on many vehicles which can be used to confirm that a vehicle is storing the data it claims, and the local nature of transportation systems which may allow data to be stored near where it is most likely needed, reducing access times and network usage.

C. OFFLINE SUPPORT

An important factor of any V2X blockchain system is the fact that at times vehicles may not have access to the internet, for example, when they are driving in geographically remote areas. Some of the use cases described in Section III require certain offline capabilities so that vehicles can continue to communicate with surrounding peers even when an Internet connection is unavailable. This is similar to the requirements

of central bank digital currencies, where users need be able to transact even when they are not online [53]. This is in contrast to current blockchains where all participating nodes must have a consistent connection to the Internet to participate. An application that requires a consistent Internet connection is limited, either in terms of where it can operate, or in how much it can be relied on by vehicles. Therefore, any blockchain for V2X design needs to have some level of support for offline use in order to enable the broadest possible range of applications.

One possible way to approach this problem is to allow vehicles that have become disconnected from the wider Internet to form a local networks with other peers so they can continue transacting on the blockchain, albeit less securely due to the decreased number of nodes [109]. Those “local offline side-chains” could be later synced with the main network when those vehicles come back online, similar to some Layer-2 solutions in existing networks [55]. Another possibility is to allow trusted execution environments (such as Samsung’s KNOX, ARM’s TrustZone, Intel’s SGX, etc.) to securely process/store certain operations offline before later syncing with the wider network [53]. Such a design could potentially achieve good performance and security, but it would place a lot of trust in these specialized parts and their manufacturers. We believe it is likely that this problem will be resolved through a number of different mechanisms. The exact nature, design, and capabilities of these mechanisms certainly present interesting areas for future investigation.

D. ORACLES

A major shortcoming of blockchain systems is the difficulty of verifying off-chain information. *Oracles* are blockchain applications that attempt to provide accurate information to blockchains from the outside world. Many systems have been proposed, including decentralized solutions where users vote to determine accurate information [110] and solutions based on trusted execution environments [111]. Such systems are very important for many V2X blockchain applications as almost all applications rely on information collected by vehicles. Voting and reputation-based systems may be sufficient for some applications, but others, such as accident investigations, will likely require solutions with higher security guarantees, such as those based on trusted computer hardware. Still, as even trusted hardware may have bugs or vulnerabilities, even more secure solutions, such ones relying on a variety of possible methods, may be desirable. Oracles are an important area of research within blockchains, and are especially vital for V2X blockchain systems.

E. PRIVACY

Blockchains, though often touted for privacy advantages, are inherently public platforms. Data on blockchains are shared between all validators, and though identities are often pseudonymous, techniques can be used to uncover private information from public data [112]. This is especially true of

review-based reputation systems, as a users' historical interactions could reveal their identities, past locations, contacts activities, and more. As such, specialized designs are needed to preserve privacy, and many have been proposed [113]. Many of the designs that offer the strongest privacy protections are based on zero-knowledge succinct non-interactive arguments of knowledge (ZK-SNARK) [114], which are capable of near-perfect privacy protection. However, to produce a transaction containing a ZK-SNARK takes significant computing power, limiting the potential scope of their application. Therefore, other designs that either use ZK-SNARKs more efficiently or that use other, more efficient cryptographic techniques are needed. Additionally, there has recently been significant push-back from governments regarding strong encryption and the inability of governments to break such encryption even if they obtain a warrant to access the encrypted information [115]. Because the transportation industry is heavily regulated by governments, privacy schemes that allow the government to access private information where warranted may be desired.

F. ROBUST BLOCKCHAIN ARCHITECTURES FOR V2X

Many researchers have recognized that the distinct problems posed by V2X-based blockchain systems require distinct solutions. Though previously proposed architectures targeting V2X applications offer advantages over existing systems, many of them fail to prove the security of the proposed design. Blockchain architectures can be made insecure in several ways, including by not properly incentivizing the participants to behave honestly, exposing the system to denial-of-service attacks, or by introducing a single point of failure. Designing blockchains that do not fall into these and other pitfalls is difficult, and as such, ground up designs, or designs which heavily modify existing systems, must be carefully scrutinized, as all blockchain applications wholly rely on the integrity of the network below.

One way to resolve this issue is to utilize and build on networks that have been proven to be robust, through both direct proofs and real-world usage. Given the high performance of some modern blockchains, this may be sufficient for many applications. Nonetheless, as discussed above, it is unlikely that existing blockchains are able to support the demands of the entire V2X ecosystem. Therefore, novel solutions should be developed, but in order to be accepted and used, these designs must be proven safe and secure. This can be done in part by building on top of the successful designs of generic blockchains, customizing them to perform optimally in the V2X domain.

VI. CONCLUSION

This paper presents an overview of both blockchain applications in the V2X space and available blockchain platforms that may be able to support them. Though significant work has been done to develop advanced applications and platforms, more research is warranted to develop a truly viable V2X blockchain that enables worthwhile applications. Specifically, while blockchain platforms targeting V2X systems have been

proposed, they often do not take advantage of the advances made by state-of-the-art blockchains. Meanwhile, while these advanced blockchains offer significant performance and features, they must be adapted in order to account for and take advantage of the many distinct aspects of the V2X ecosystem, such as the importance of location and the large number of potential users.

ACKNOWLEDGMENT

Special thanks to Robert Sun and Edward Au of Huawei Canada for their advice and support.

REFERENCES

- [1] J. Z. Varghese *et al.*, "Overview of autonomous vehicle sensors and systems," in *Proc. Int. Conf. Operations Excellence Serv. Eng.*, 2015, pp. 178–191.
- [2] F. Meissner, "The car will become a computer on wheels," Jan. 2020. [Online]. Available: <https://www.rolandberger.com/en/Insights/Publications/The-car-will-become-a-computer-on-wheels.html>
- [3] M. Stern, "Ford recalls F-150s to repair cruise control radar," Dec. 2021. [Online]. Available: <https://www.torquenews.com/3769/ford-recalls-f-150s-repair-cruise-control-radar>
- [4] D. Shepardson, "Tesla recalls nearly 12,000 U.S. vehicles over software communication error," Nov. 2021. [Online]. Available: <https://www.reuters.com/business/autos-transportation/tesla-recalling-nearly-12000-us-vehicles-over-software-communication-error-2021-11-02/>
- [5] K. B. Kelarestaghi, M. Foruhandeh, K. Heaslip, and R. Gerdes, "Vehicle security: Risk assessment in transportation," 2018, *arXiv:1804.07381*.
- [6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *White Paper*, 2008.
- [7] J. Meijers *et al.*, "Blockchain for V2X: A taxonomy of design use cases and system requirements," in *Proc. 3rd Conf. Blockchain Res. Appl. Innov. New. Serv.*, 2021, pp. 113–120.
- [8] U.S. Department of Transportation, NHTSA, "FMVSS no. 150 vehicle-to-vehicle communication technology for light vehicles," 2016.
- [9] U.S. Department of Transportation, ITS, "Vehicle-to-infrastructure (V2I) resources" ITS Deployment, 2020. [Online]. Available: <https://www.its.dot.gov/v2i>
- [10] Z. Zhou, B. Wang, M. Dong, and K. Ota, "Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 50, no. 1, pp. 43–57, Jan. 2020.
- [11] S. Widodo, T. Hasegawa, and S. Tsugawa, "Vehicle fuel consumption and emission estimation in environment-adaptive driving with or without inter-vehicle communications," in *Proc. IEEE Intell. Veh. Symp.*, 2000, pp. 382–386.
- [12] K. Katsaros, R. Kernchen, M. Dianati, D. Rieck, and C. Zinoviou, "Application of vehicular communications for improving the efficiency of traffic in urban areas," *Wireless Commun. Mobile Comput.*, vol. 11, no. 12, pp. 1657–1667, 2011.
- [13] B. Asadi and A. Vahidi, "Predictive cruise control: Utilizing upcoming traffic signal information for improving fuel economy and reducing trip time," *IEEE Trans. Control Syst. Technol.*, vol. 19, no. 3, pp. 707–714, May 2011.
- [14] D. Reichardt, M. Miglietta, L. Moretti, P. Morsink, and W. Schulz, "CarTALK 2000: Safe and comfortable driving based upon inter-vehicle-communication," in *Proc. Intell. Veh. Symp.*, 2002, pp. 545–550.
- [15] J. B. Kenney, "Dedicated short-range commun. (DSRC) standards in the United States," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.
- [16] 3GPP, "Vehicle-to-everything (V2X) services in 5G system (5GS); stage 3," 3rd Gener. Partnership Project (3GPP), Tech. Specification (TS) 24. 587, 2020. [Online]. Available: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3640>

- [17] S. S. Shetty, C. A. Kamhoua, and L. L. Njilla, "Overview of attack surfaces in blockchain," in *Blockchain for Distributed Systems Security*. Hoboken, NJ, USA: IEEE Press-Wiley, 2019, pp. 51–66, doi: [10.1002/9781119519621.ch3](https://doi.org/10.1002/9781119519621.ch3).
- [18] T. L. Association, "An introduction to Libra," 2019. [Online]. Available: <https://libra.org/en-US/white-paper/>
- [19] G. Zhang *et al.*, "Reaching consensus in the Byzantine empire: A comprehensive review of BFT consensus algorithms," 2022, *arXiv:2204.03181*.
- [20] S. Kadam, "Review of distributed ledgers: The technological advances behind cryptocurrency," in *Proc. Int. Conf. Adv. Comput. Technol. Manage.*, 2018. [Online]. Available: https://www.researchgate.net/publication/323628539_Review_of_Distributed_Ledgers_The_technological_Advances_behind_cryptocurrency
- [21] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling Byzantine agreements for cryptocurrencies," in *Proc. 26th Symp. Operating Syst. Princ.*, 2017, pp. 51–68.
- [22] S. Chen *et al.*, "Vehicle-to-everything (V2X) services supported by LTE-based systems and 5G," *IEEE Commun. Standards Mag.*, vol. 1, no. 2, pp. 70–76, Jul. 2017.
- [23] J. R. Douceur, "The Sybil attack," in *Proc. Int. Workshop Peer-to-Peer Syst.*, Berlin, Heidelberg: Springer, 2002, pp. 251–260.
- [24] K. Zhang and H.-A. Jacobsen, "Towards dependable, scalable, and pervasive distributed ledgers with blockchains," in *Proc. IEEE 38th Int. Conf. Distrib. Comput. Syst.*, 2018, pp. 1337–1346.
- [25] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, no. 2014, pp. 1–32, 2014.
- [26] H. Adams, N. Zinsmeister, and D. Robinson, "Uniswap V2 core," White Paper, 2020. [Online]. Available: <https://uniswap.org/whitepaper.pdf>
- [27] C. Killer *et al.*, "Æternum: A decentralized voting system with unconditional privacy," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency*, 2021, pp. 1–9.
- [28] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of Proof-of-Elapsed-Time (PoET)," in *Proc. Int. Symp. Stabilization, Saf., Secur. Distrib. Syst.*, Cham, Switzerland: Springer, 2017, pp. 282–297.
- [29] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Open Problems in Network Security*, J. Camenisch and D. Kesdoğan, Eds. Berlin, Germany: Springer, 2016, pp. 112–125.
- [30] M. Isaac and N. Popper, "Facebook plans global financial system based on cryptocurrency," *New York Times: Technology*, Jun. 2019. [Online]. Available: <https://www.nytimes.com/2019/06/18/technology/facebook-cryptocurrency-libra.html>
- [31] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," in *Proc. Concurrency: Works Leslie Lamport*, 2019, pp. 203–226.
- [32] G. Zhang and C. Xu, "An efficient consensus protocol for real-time permissioned blockchains under non-Byzantine conditions," in *Proc. Int. Conf. Green, Pervasive, Cloud Comput.*, Cham, Switzerland: Springer, 2018, pp. 298–311.
- [33] G. Zhang and H.-A. Jacobsen, "ESCAPE to precaution against leader failures," 2022, *arXiv:2202.09434*.
- [34] M. Castro *et al.*, "Practical Byzantine fault tolerance," in *Proc. OSDI*, 1999, vol. 99, pp. 173–186.
- [35] A. Bessani, J. Sousa, and E. E. Alchieri, "State machine replication for the masses with BFT-SMART," in *Proc. 44th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw.*, 2014, pp. 355–362.
- [36] E. Androutaki *et al.*, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf*, 2018, pp. 1–15.
- [37] R. G. Brown, J. Carlyle, I. Grigg, and M. Hearn, "Corda: An introduction," R3 CEV, 2016.
- [38] G. G. Gueta *et al.*, "SBFT: A scalable and decentralized trust infrastructure," in *Proc. 49th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw.*, 2019, pp. 568–580.
- [39] M. Yin, D. Malkhi, M. K. Reiter, G. G. Gueta, and I. Abraham, "HotStuff: BFT consensus with linearity and responsiveness," in *Proc. ACM Symp. Princ. Distrib. Comput.*, 2019, pp. 347–356.
- [40] G. Zhang and H.-A. Jacobsen, "Prosecutor: An efficient BFT consensus algorithm with behavior-aware penalization against Byzantine attacks," in *Proc. Middleware: 22nd ACM/IFIP Int. Middleware Conf.*, 2021, pp. 52–63.
- [41] C. Li *et al.*, "A decentralized blockchain with high throughput and fast confirmation," in *Proc. [USENIX] Annu. Tech. Conf.*, 2020, pp. 515–528.
- [42] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *Proc. IEEE 19th Int. Conf. Intell. Transp. Syst.*, 2016, pp. 2663–2668.
- [43] P. Fraga-Lamas and T. M. Fernández-Caramés, "A review on blockchain technologies for an advanced and cyber-resilient automotive industry," *IEEE Access*, vol. 7, pp. 17578–17598, 2019.
- [44] M. B. Mollah *et al.*, "Blockchain for the Internet of Vehicles towards intelligent transportation systems: A survey," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4157–4185, Mar. 2021.
- [45] J. Huang, D. Fang, Y. Qian, and R. Q. Hu, "Recent advances and challenges in security and privacy for V2X communications," *IEEE Open J. Veh. Technol.*, vol. 1, pp. 244–266, 2020.
- [46] L. U. Khan, I. Yaqoob, M. Imran, Z. Han, and C. S. Hong, "6G wireless systems: A vision, architectural elements, and future directions," *IEEE Access*, vol. 8, pp. 147029–147044, 2020.
- [47] T. Huang, W. Yang, J. Wu, J. Ma, X. Zhang, and D. Zhang, "A survey on green 6G network: Architecture and technologies," *IEEE Access*, vol. 7, pp. 175758–175768, 2019.
- [48] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues," *IEEE Commun. Surv. Tut.*, vol. 22, no. 2, pp. 1191–1221, Apr.–Jun. 2020.
- [49] E. B. Sasson *et al.*, "Zerocash: Decentralized anonymous payments from bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, 2014, pp. 459–474.
- [50] P. Biel, S. Zhang, and H.-A. Jacobsen, "A zero-knowledge proof system for OpenLibra," in *Proc. 22nd Int. Middleware Conf.: Demos Posters*, 2021, pp. 3–4.
- [51] V. Hassija, V. Saxena, V. Chamola, and F. R. Yu, "A parking slot allocation framework based on virtual voting and adaptive pricing algorithm," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5945–5957, Jun. 2020.
- [52] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.
- [53] A. Veneris, A. Park, F. Long, and P. Puri, "Central bank digital loonie: Canadian cash for a new global economy," White paper, 2021. [Online]. Available: https://www.rotman.utoronto.ca/-/media/Files/Programs-and-Areas/FinHub/BoC_ModelX_Final_Report.pdf
- [54] J. Meijers, G. Dharma Putra, G. Kotsialou, S. Kanhere, and A. Veneris, "Cost-effective blockchain-based IoT data marketplaces with a credit invariant," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency*, 2021, pp. 1–9.
- [55] "Layer 2 scaling," [Online]. Available: <https://ethereum.org/en/developers/docs/layer-2-scaling/>
- [56] J. Poon and T. Dryja, "The Bitcoin lightning network: Scalable off-chain instant payments," 2016. [Online]. Available: <https://www.bitcoinlightning.com/wp-content/uploads/2018/03/lightning-network-paper.pdf>
- [57] A. Yakovenko, "Solana: A new architecture for a high performance blockchain v0. 8.13," White paper, 2018. [Online]. Available: <https://solana.com/solana-whitepaper.pdf>
- [58] K. Sekniqi, D. Laine, S. Buttolph, and E. Gün Sirer, "Avalanche platform," *Netw. Distrib. Ledgers*, Jun. 2020.
- [59] E. Bellini, Y. Iraqi, and E. Damiani, "Blockchain-based distributed trust and reputation management systems: A survey," *IEEE Access*, vol. 8, pp. 21127–21151, 2020.
- [60] A. Schaub, R. Bazin, O. Hasan, and L. Brunie, "A trustless privacy-preserving reputation system," in *Proc. IFIP Int. Conf. ICT Syst. Secur. Privacy Protection*. Cham, Switzerland: Springer, 2016, pp. 398–411.
- [61] R. Dennis and G. Owen, "Rep on the block: A next generation reputation system based on the blockchain," in *Proc. 10th Int. Conf. Internet Technol. Secured Trans.*, 2015, pp. 131–138.
- [62] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.

- [63] Q. Feng, D. He, S. Zeadally, and K. Liang, "BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4146–4155, Jun. 2020.
- [64] C. Oham, S. S. Kanhere, R. Jurdak, and S. Jha, "A blockchain based liability attribution framework for autonomous vehicles," 2018, *arXiv:1802.05050*.
- [65] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4Forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 50–57, Oct. 2018.
- [66] S. M. Danish, K. Zhang, and H.-A. Jacobsen, "BlockAM: An adaptive middleware for intelligent data storage selection for Internet of Things," in *Proc. 2nd IEEE Int. Conf. Decentralized Appl. Infrastructures*, Oxford, U.K., J. Xu, S. P. Schulte Ruppel, A. Küpper, and D. Javad, Eds., 2020, pp. 61–71. [Online]. Available: <https://doi.org/10.1109/DAPPS49028.2020.00007>
- [67] M. Al-Bassam, A. Sonnino, and V. Buterin, "Fraud data availability proofs: Maximising light client security and scaling blockchains with dishonest majorities," 2018, *arXiv:1809.09044*.
- [68] Protocol Labs, "Filecoin: A decentralized storage network," Jul. 2017. [Online]. Available: <https://filecoin.io/filecoin.pdf>
- [69] F. Lamberti, V. Gatteschi, C. Demartini, M. Pelissier, A. Gomez, and V. Santamaria, "Blockchains can work for car insurance: Using smart contracts and sensors to provide on-demand coverage," *IEEE Consum. Electron. Mag.*, vol. 7, no. 4, pp. 72–81, Jul. 2018.
- [70] Z. Li, Z. Xiao, Q. Xu, E. Sotthiwat, R. S. M. Goh, and X. Liang, "Blockchain and IoT data analytics for fine-grained transportation insurance," in *Proc. IEEE 24th Int. Conf. Parallel Distrib. Syst.*, 2018, pp. 1022–1027.
- [71] H. Guo, W. Li, M. Nejad, and C.-C. Shen, "Proof-of-event recording system for autonomous vehicles: A blockchain-based solution," *IEEE Access*, vol. 8, pp. 182776–182786, 2020.
- [72] C. Lai, M. Zhang, J. Cao, and D. Zheng, "SPIR: A secure and privacy-preserving incentive scheme for reliable real-time map updates," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 416–428, Jan. 2020.
- [73] D. Wörner and T. von Bomhard, "When your sensor earns money: Exchanging data for cash with bitcoin," in *Proc. ACM Int. Joint Conf. Pervasive Ubiquitous Comput.*, 2014, pp. 295–298.
- [74] K. Liu, W. Chen, Z. Zheng, Z. Li, and W. Liang, "A novel debt-credit mechanism for blockchain-based data-trading in Internet of Vehicles," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9098–9111, Oct. 2019.
- [75] G. S. Ramachandran, R. Radhakrishnan, and B. Krishnamachari, "Towards a decentralized data marketplace for smart cities," in *Proc. IEEE Int. Smart Cities Conf.*, 2018, pp. 1–8.
- [76] M. Baza, M. Nabil, N. Lasla, K. Fidan, M. Mahmoud, and M. Abdallah, "Blockchain-based firmware update scheme tailored for autonomous vehicles," in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2019, pp. 1–7.
- [77] J. Eckert, D. López, C. L. Azevedo, and B. Farooq, "A blockchain-based user-centric emission monitoring and trading system for multimodal mobility," in *Proc. Forum Integr. Sustain. Transp. Syst.*, 2020, pp. 328–334.
- [78] W. Li, L. Wang, Y. Li, and B. Liu, "A blockchain-based emissions trading system for the road transport sector: Policy design and evaluation," *Climate Policy*, vol. 21, no. 3, pp. 337–352, 2021.
- [79] X. Deng and T. Gao, "Electronic payment schemes based on blockchain in VANETs," *IEEE Access*, vol. 8, pp. 38296–38303, 2020.
- [80] M. Baza, M. Mahmoud, G. Srivastava, W. Alasmay, and M. Younis, "A light blockchain-powered privacy-preserving organization scheme for ride sharing services," in *Proc. IEEE 91st Veh. Technol. Conf.*, 2020, pp. 1–6.
- [81] V. Hassija, V. Chamola, S. Garg, D. N. G. Krishna, G. Kad-doum, and D. N. K. Jayakody, "A blockchain-based framework for lightweight data sharing and energy trading in V2G network," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5799–5812, Jun. 2020.
- [82] C. Liu, K. K. Chai, X. Zhang, E. T. Lau, and Y. Chen, "Adaptive blockchain-based electric vehicle participation scheme in smart grid platform," *IEEE Access*, vol. 6, pp. 25657–25665, 2018.
- [83] M. Zhang, F. Eliassen, A. Taherkordi, H.-A. Jacobsen, H. Chung, and Y. Zhang, "Demand-response games for peer-to-peer energy trading with the Hyperledger blockchain," *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 52, no. 1, pp. 19–31, Jan. 2022. [Online]. Available: <https://doi.org/10.1109/TSMC.2021.3111135>
- [84] J. Pajic, J. Rivera, K. Zhang, and H.-A. Jacobsen, "EVA: Fair and auditable electric vehicle charging service using blockchain," in *Proc. 12th ACM Int. Conf. Distrib. Event-Based Syst.*, Hamilton, New Zealand, A. Hinze, D. M. Eysers, M. Hirzel, M. Weidlich, and S. Bhowmik, Eds., 2018, pp. 262–265. [Online]. Available: <https://doi.org/10.1145/3210284.3219776>
- [85] Y. Wang, Z. Su, and N. Zhang, "BSIS: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3620–3631, Jun. 2019.
- [86] S. M. Danish, K. Zhang, H.-A. Jacobsen, N. Ashraf, and H. K. Qureshi, "BlockEV: Efficient and secure charging station selection for electric vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4194–4211, Jul. 2021. [Online]. Available: <https://doi.org/10.1109/TITS.2020.3044890>
- [87] S. M. Danish, K. Zhang, and H.-A. Jacobsen, "A blockchain-based privacy-preserving intelligent charging station selection for electric vehicles," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency*, Toronto, ON, Canada, 2020, pp. 1–3. [Online]. Available: <https://doi.org/10.1109/ICBC48266.2020.9169419>
- [88] M. J. M. Chowdhury, A. Colman, M. A. Kabir, J. Han, and P. Sarda, "Blockchain versus database: A critical analysis," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng.*, 2018, pp. 1348–1353.
- [89] V. Buterin and V. Griffith, "Casper the friendly finality gadget," 2017, *arXiv:1710.09437*.
- [90] T. Rocket, M. Yin, K. Sekniqi, R. van Renesse, and E. G. Sirer, "Scalable and probabilistic leaderless BFT consensus through metastability," 2019, *arXiv:1906.08936*.
- [91] S. Motepalli and H.-A. Jacobsen, "Decentralizing permissioned blockchain with delay towers," 2021, *arXiv:2203.09714*.
- [92] S. Popov, "The tangle," *White Paper*, vol. 1, no. 3, 2018.
- [93] S. V. Dorpe and V. Manancourt, "Amazon knew seller data was used to boost company sales," Apr. 2021. [Online]. Available: <https://www.politico.eu/article/amazon-seller-data-company-sales/>
- [94] J. Nicas, K. Browning, and E. Griffith, "Fortnite creator sues Apple and Google after ban from app stores," Aug. 2020. [Online]. Available: <https://www.nytimes.com/2020/08/13/technology/apple-fortnite-ban.html>
- [95] M. Al-Bassam, "LazyLedger: A distributed data availability ledger with client-side smart contracts," 2019, *arXiv:1905.09274*.
- [96] "Upgrading Ethereum to radical new heights," [Online]. Available: <https://ethereum.org/en/upgrades/>
- [97] S. Motepalli and H.-A. Jacobsen, "Reward mechanism for blockchains using evolutionary game theory," in *Proc. 3rd Conf. Blockchain Res. Appl. Innov. Netw. Serv.*, 2021, pp. 217–224.
- [98] J. A. Chacko, R. Mayer, and H.-A. Jacobsen, "Why do my blockchain transactions fail?: A study of Hyperledger fabric," in *Proc. SIGMOD: Int. Conf. Manage. Data*, Virtual Event, China, G. Li, Z. Li, S. Idreos, and D. Srivastava, Eds., 2021, pp. 221–234. [Online]. Available: <https://doi.org/10.1145/3448016.3452823>
- [99] P. Nasirifard, R. Mayer, and H.-A. Jacobsen, "Fabric-CRDT: A conflict-free replicated datatypes approach to permissioned blockchains," in *Proc. 20th Int. Middleware Conf.*, Davis, CA, USA, 2019, pp. 110–122. [Online]. Available: <https://doi.org/10.1145/3361525.3361540>
- [100] S. Popov, "IOTA: Feeless and free," *IEEE Blockchain Tech. Briefs*, Jan. 2019. [Online]. Available: <https://blockchain.ieee.org/technicalbriefs/january-2019/iota-feeless-and-free>
- [101] K. Karlsson et al., "Vegvisir: A partition-tolerant blockchain for the internet-of-things," in *Proc. IEEE 38th Int. Conf. Distrib. Comput. Syst.*, 2018, pp. 1150–1158.
- [102] W. Yang, X. Dai, J. Xiao, and H. Jin, "LDV: A lightweight dag-based blockchain for vehicular social networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5749–5759, Jun. 2020.
- [103] V. Hassija, V. Chamola, G. Han, J. J. Rodrigues, and M. Guizani, "DAGIoV: A framework for vehicle to vehicle communication using directed acyclic graph and game theory," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4182–4191, Apr. 2020.

- [104] A. Dorri, S. S. Kanhere, and R. Jurdak, "MOF-BC: A memory optimized and flexible blockchain for large scale networks," *Future Gener. Comput. Syst.*, vol. 92, pp. 357–373, 2019.
- [105] S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang, "A scalable blockchain framework for secure transactions in IoT," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4650–4659, Jun. 2019.
- [106] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A lightweight scalable blockchain for IoT security and anonymity," *J. Parallel Distrib. Comput.*, vol. 134, pp. 180–197, 2019.
- [107] R. Shrestha and S. Y. Nam, "Regional blockchain for vehicular networks to prevent 51% attacks," *IEEE Access*, vol. 7, pp. 95033–95045, 2019.
- [108] I. A. Gasse, M. Abu Talib, and Q. Nasir, "Inter blockchain communication: A survey," in *Proc. ArabWIC 6th Annu. Int. Conf. Res. Track*, 2019, pp. 1–6.
- [109] Z. Yang, K. Zheng, K. Yang, and V. C. M. Leung, "A blockchain-based reputation system for data credibility assessment in vehicular networks," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun.*, 2017, pp. 1–5.
- [110] Y. Cai, G. Fragkos, E. E. Tsirapolou, and A. Veneris, "A truth-inducing Sybil resistant decentralized blockchain oracle," in *Proc. 2nd Conf. Blockchain Res. Appl. Innov. Netw. Serv.*, 2020, pp. 128–135.
- [111] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, "Town Crier: An authenticated data feed for smart contracts," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, pp. 270–282.
- [112] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in Bitcoin," in *Proc. Int. Conf. Financial cryptogr. Data Secur.*, Berlin, Heidelberg: Springer, 2013, pp. 34–51.
- [113] T. A. Butt, R. Iqbal, K. Salah, M. Aloqaily, and Y. Jararweh, "Privacy management in social Internet of Vehicles: Review, challenges and blockchain based solutions," *IEEE Access*, vol. 7, pp. 79694–79713, 2019.
- [114] N. Bitansky, R. Canetti, A. Chiesa, and E. Tromer, "From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again," in *Proc. 3rd Innov. Theor. Comput. Sci. Conf.*, 2012, pp. 326–349.
- [115] N. Perlroth, "What is end-to-end encryption? Another bull's-eye on big tech," Nov. 2019. [Online]. Available: <https://www.nytimes.com/2019/11/19/technology/end-to-end-encryption.html>

JAMES MEIJERS (Graduate Student Member, IEEE) received the B.Sc. degree in computer engineering in 2020 from the University of Toronto, Toronto, ON, Canada, where he is currently working toward the M.Sc. degree in computer engineering. His research interests include applications of blockchain technology in the IoT and transportation industries.

PANAGIOTIS MICHALOPOULOS (Graduate Student Member, IEEE) received the Diploma in electrical and computer engineering from the University of Patras, Patras, Greece, in 2017, and the M.Sc. degree in embedded systems from the Eindhoven University of Technology, Eindhoven, The Netherlands, in 2020. He is currently working toward the Ph.D. degree in electrical and computer engineering with the University of Toronto, Toronto, ON, Canada. His research interests include identity and trust systems, their applications on the Internet of Things, and distributed ledger technologies.

SHASHANK MOTEPALLI received the bachelor's degree in information technology and the master's degree in data science with the International Institute of Information Technology, Bangalore, India. He is currently working toward the Doctoral degree with the Middleware Systems Research Group, University of Toronto, Toronto, ON, Canada. His research interests include consensus protocols and mechanism designs for blockchains.

GENGRUI ZHANG received the M.Sc. degree from the University of Chinese Academy of Sciences, Beijing, China, in 2018. He is currently working toward the Ph.D. degree with the University of Toronto, Toronto, ON, Canada. His research interests include the development of efficient consensus algorithms for blockchains, cloud services, and distributed and parallel systems. His focuses on reinforcement learning with an emphasis on optimizing event processing systems.

SHIQUAN ZHANG received the bachelor's degree in information security from Shanghai Jiao Tong University, Shanghai, China, in 2018, and the master's degree in computer science from McGill University, Montreal, QC, Canada, in 2020. He is currently working toward the Ph.D. degree (second-year) with the Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON, Canada. His research interests include zero-knowledge proofs, V2X, and other applications in blockchain systems.

ANDREAS VENERIS (Senior Member, IEEE) received the Diploma from the Department of Computer Engineering and Informatics, University of Patras, Patras, Greece, in 1991, the master's degree from the University of Southern California, Los Angeles, CA, USA, in 1992, and the Ph.D. degree from the University of Illinois, Urbana-Champaign, Champaign, IL, USA, in 1998. He is currently a Connaught Scholar and Professor with the Department of Electrical and Computer Engineering, cross-appointed with the Department of Computer Science University of Toronto, Toronto, ON, Canada., He held joint faculty positions with the Department of Informatics, Athens University of Economics and Business, Athens, Greece, during 2006–2016, and with the Department of ECE, The University of Tokyo, Tokyo, Japan, during 2010–2011. For more than 20 years he worked in the field of CAD for VLSI synthesis, verification and debugging, with emphasis in formal methods, where he has authored or coauthored more than 150 conference/journal papers in peer ACM/IEEE venues. During 2013–2014, he was a part of the team that spearheaded Ethereum in Toronto, and since 2015 his research transitioned into cross-disciplinary aspects of distributed ledger (blockchain) technology. His current research interests include Central Bank Digital Currencies, mechanism and system design, distributed oracles, formal methods for smart contract verification, IoT and distributed systems, techno-legal blockchain matters, and crypto-economics. Prof. Veneris was the recipient of the ten-year Best Paper Retrospective Award, three other best paper awards and he holds many patents. He was the Member of the team in the first webcast ever (37th Grammy Awards, 1995), an event acknowledged by the American Congress. In 2020, he was commissioned by the Bank of Canada to lead a team of four faculty in compiling a proposal for Canada's digital currency. In February 2021, this work became public proposing Canada's Central Bank Digital Loonie – the first work of its kind that presents a comprehensive technological, regulatory/legal and economic model for a central bank digital currency. In 2021, he was honored to be given the opportunity to comment on a classified report by the Hoover Institution, edited by Darrell Duffie & Elizabeth Economy, prefaced by Condoleezza Rice, and coauthored by an extensive list of prominent world-thinkers. This report was released on March 1, 2022 and it is titled Digital Currencies: The U.S., China, And The World At A Crossroads. On March 8, 2022 the U.S. President Joe Biden signed an Executive Order following most of the recommendations of this Report.

HANS-ARNO JACOBSEN (Fellow, IEEE) is currently a Professor of computer engineering and computer science with the University of Toronto, Toronto, ON, Canada, where he directs the activities of the Middleware Systems Research Group. His pioneering research include the intersection of distributed systems and data management, with particular focus on blockchains, middleware abstractions, (complex) event processing, and cyber-physical systems. After studying and completing the Ph.D. degree in Germany, France, and the U.S., he engaged in Postdoctoral Research with INRIA near Paris, France, before moving to the University of Toronto in 2001. He has widely authored or coauthored and has filed more than a dozen patents. He has chaired International Conferences and led conference steering committees.