Blockchain for V2X: A Taxonomy of Design Use Cases and System Requirements*

James Meijers†, Edward Au‡, Yuxi Cai†, Hans-Arno Jacobsen†, Shashank Motepalli†, Robert Sun‡, Andreas Veneris†, Gengrui Zhang†, Shiquan Zhang†
†University of Toronto, ‡Huawei Canada
{j.meijers, yuxijune.cai, shashank.motepalli, gengrui.zhang, shiquan.zhang}@mail.utoronto.ca,
{edward.ks.au, rob.sun}@huawei.com, {jacobsen, veneris}@eecg.toronto.edu

***Abstract*—Vehicles today contain a multitude of sensors creating vast amounts of data. For many applications, these data need to be shared with other entities so that they can also utilize it. Vehicle-to-everything (V2X) is the amalgamation of all potential vehicle communication systems. V2X technologies are enabling many smart-vehicle applications, such as autonomous vehicles. However, in utilizing these data from external entities, vehicles rely on the availability and trustworthiness of centralized entities who may be able to delete, forge, leak, or otherwise tamper with the underlying data. Blockchain technology provides a decentralized mechanism to allow vehicles to validate data they receive in a trustless manner. This paper explores potential applications of blockchain technology in the V2X space, categorizing and analyzing use cases based on their underlying blockchain requirements. It then uses this analysis to determine the key requirements behind an effective V2X blockchain.**

***Index Terms*—IoT, blockchain, V2X, taxonomy**

I. Introduction

Modern vehicles are rightfully also called "computers on wheels" [1] as they have a multitude of different sensors on-board, ranging from cameras and radars to GPS and gyroscopes [2]. These sensors, combined with on-board computing facilities, have already enabled many new technologies, such as GPS navigation and other autonomous self-driving capabilities. While current implementations of these applications mainly rely on on-board sensing and computing, many other potential applications require significant inter-vehicle communication to complement the functionality of those on-board facilities. For example, *platooning*, wherein cars coordinate their movements to increase safety and fuel-efficiency, requires reliable communication between vehicles [3]. Vehicle-to-Everything (V2X) encompasses all potential vehicle communication systems that enable these smart applications.

Achieving V2X communication in a safe and reliable way is a challenging task. In particular, the transportation space has a wide, heterogeneous array of stakeholders [4]. While good for competition, this heterogeneity introduces interoperability and/or security risks. For example, if for a new smart-vehicle application important vehicular data is to be stored in a traditional database, stakeholders can either develop and maintain their own databases, which may or may not be interoperable, or they could contribute to a single, centralized database, which forces them to cede control to some centralized authority which may be able to manipulate, falsify, or withhold data for its own gain.

Blockchains are a type of distributed state-machine database with special characteristics [5]. Without requiring the services of trusted third parties, they rely on reward mechanisms to enable trading, smart contracts, among others [6]. These are enabled by agreement on a shared protocol and state machine, followed by consensus on what transactions have been run on the state machine. In this context, there are many potential applications of blockchain technology within the V2X space. As outlined above, using traditional databases for V2X applications may be difficult due to the diverse number of stakeholders. However, using blockchain technology, stakeholders can consent to a protocol in which they all participate in the maintenance of the database, each verifying its contents and maintaining records to ensure it is not being misused. This shared database could then be used to record and distribute data, such as verified over the air software updates [7], recordings of a driver's behaviours and habits, and timestamped reports from vehicles involved in accidents [8]. A blockchain's ability to maintain a ledger of scarce resources could also be used in the V2X space. Blockchain technology could enable the purchase of energy for electric vehicles [9], the payment of tolls [10], or the purchase of sensor data [11] securely and pseudo-anonymously.

In this work, we categorize and analyze V2X applications that can utilize blockchain technology in order to learn the requirements of and guide the design decisions for a future V2X blockchain design. In contrast to previous taxonomies [12], [13], we divide applications into categories based on what they require from the underlying blockchain technology, rather than application type. By analyzing the requirements of specific use cases in each category, we determine what features are needed in a V2X blockchain in order to support a broad range of applications. In doing so, we argue that a permissioned blockchain with high throughput,

*This research has been supported by a grant from Huawei Canada.

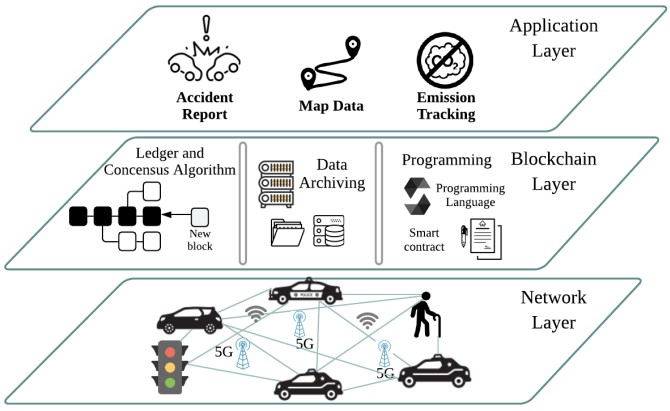

Fig. 1. V2X blockchain system overview.

strong privacy controls, and special features such as offline support, would best serve contemporary V2X blockchain applications. Such a blockchain could safely be operated by the many stakeholders in the transportation space. The contributions of this work include a detailed overview and analysis of V2X blockchain use cases, a determination of the requirements of a V2X blockchain, and an argument for the viability of permissioned blockchains in the V2X space.

This paper is organized as follows. Section II gives background on V2X and blockchain technology and summarizes its prior applications in the V2X space. Section III categorizes use cases of blockchain technology in the V2X space and analyzes them to determine their underlying requirements. Section IV uses this analysis to determine the requirements of an ideal V2X blockchain, comparing these requirements to the capabilities of existing blockchains. Finally, the paper concludes in Section V.

II. Background

A. V2X and Applications

V2X conceptualizes a vehicle communication system composing of Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Pedestrian (V2P) communications. A V2V communication system is envisioned as a technology for vehicles to authenticate and exchange messages with each other with the goal of improved safety by triggering related warnings and other such applications [14]. In a V2I system, infrastructure captures data generated by vehicles and returns advisory information on safety, mobility, or road conditions [15]. V2P communication aims to protect vulnerable nonvehicle occupants of the road by enabling communications between handheld devices and in-vehicle systems [16]. Prior work and industrial projects have revealed the potential of V2X technology to improve transportation efficiency and safety while enabling new applications [17]. Some applications include traffic congestion controls [18], driving with enhanced fuel efficiency and travel time [19], and improved safety assistance [20]. Current V2X system proposals mainly rely on dedicated short range communication [21] and/or cellular communication [22] standards as depicted in the network layer of Fig. 1. Both standards provide sufficient latency, throughput, and reliability guarantees. For the rest of the paper, we limit the discussion of latency, throughput, and reliability to the blockchain layer only.

Past work has analyzed V2X use cases. For example in [12] Willke et al. describe various connected vehicle applications, dividing them into four categories: information services, vehicle safety, individual motion control, and group motion control. In [13], the authors survey the entire landscape of connected vehicles, including an analysis of applications where they build on the work in [12]. In [23], the US Department of Transportation provides a list of connected vehicle applications on which their *Connected Vehicle Reference Implementation Architecture* is based.

B. Blockchain and Consensus Protocols

Blockchains, including those adapted for V2X applications, mainly fall into two categories: permissionless and permissioned blockchains. Generally, permissionless blockchains are openly operating distributed ledgers in which worldwide users can freely join the network. They often utilize consensus protocols such as Proof-of-Work [5], Proof-of-Stake [24], and Proof-of-Elapsed-Time [25] which uses specially designed dedicated hardware. Applications built upon permissionless blockchains can operate at a large scale but often suffer from low throughput and high latency [26]. Permissioned blockchains, on the other hand, can attain a higher throughput and lower latency by only allowing specific authenticated nodes to participate in the consensus process.

The primary concern of permissioned blockchains is to design efficient and effective Byzantine fault-tolerant (BFT) algorithms to tolerate arbitrary failures [27], [28]. PBFT [29] and its variants (*e.g.*, BFT-SMaRt [30]), which achieve consensus using $O(n^2)$ messages, have been widely used in platforms such as Hyperledger Fabric [31] and R3 Corda [32]. In addition, SBFT [33], HotStuff [34] and Prosecutor [35] 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.

C. Blockchain and V2X

There has been a lot of interest in applying blockchain technologies to the automotive sector. In [36], Yuan et al. propose a framework for automotive focused blockchains. In [37] Dorri et al. propose their own blockchain design to support privacy preserving V2X communication. In [38] Jiang et al. present a blockchain network architecture and analyze its performance. Blockchains designed for vehicular data-dissemination are proposed in [39] and [40]. In [41] the authors propose the use of directed acyclic graphs (DAGs)

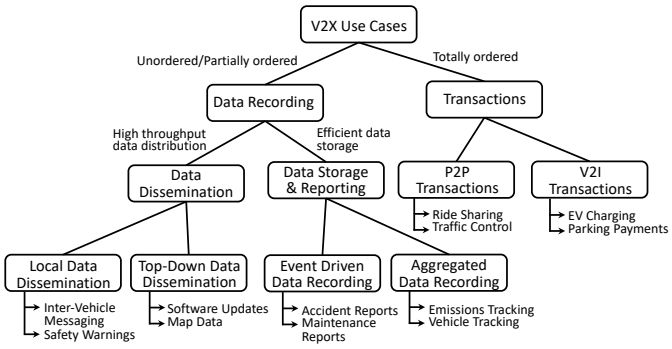

Fig. 2. V2X-blockchain use case taxonomy.

to enable V2V communication. A review of blockchain technologies for the automotive sector is presented in [42], where the authors demonstrate the value that a blockchain-based communication system can bring to the transportation landscape. This paper builds on this work by analyzing use cases to determine the requirements and guide the development of a blockchain meant to realize that value.

Many works have also investigated specific blockchain-based V2X applications. These applications include vehicle tracking and data security for insurance and accident investigation [8], securing and distributing firmware updates [7], enabling decentralized ride sharing [43], energy trading [44], [45], and trust management [46].

Blockchain technology is particularly well suited to the V2X space due to the automotive sector's diverse array of stakeholders. As a decentralized database, blockchains are not controlled by any one entity. As such 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. Additionally, blockchains natively support payments and can be used to efficiently pay for things such as tolls, electricity, and data. Finally, as vehicles and roadside infrastructure are equipped with more sensors and collect more data, ensuring that this data is distributed to those who need it efficiently, while still ensuring that it can be trusted becomes very difficult. Blockchains enable heterogeneous clients to communicate effectively in an environment where all interactions are recorded and validated. This ensures that all users can access new technologies without sacrificing safety.

III. V2X-Blockchain Use Case Analysis

In order to determine the requirements (in terms of latency, throughput, additional features, etc.) of a blockchain designed to support V2X applications, we must first determine the nature and requirements of those applications. However, as blockchains have been applied to a diverse range of V2X applications, performing this analysis on a random selection of use cases could cause one to miss important requirements not present in that selection. To avoid this pitfall we take a more systematic approach, categorizing the use cases we have found based on the requirements they have for underlying blockchains. We perform this categorization using a taxonomy-tree. The splits in the tree are selected such that applications have similar underlying requirements to those with which they share many branches in the tree. The resultant tree, shown in Fig. 2, has six categories that we believe offer a comprehensive summary of V2X use cases involving blockchain. To perform our analysis of V2X blockchain requirements, we take a use case from each category and determine its underlying requirements, taking those to be representative of the category as a whole.

A. Use Case Taxonomy

Here we will define each of the categories shown in Fig. 2, explain how blockchain can be applied to them, and give a high-level overview of their specific requirements for an underlying blockchain.

Data Recording: Applications where the primary purpose is to transmit and record unordered (or partially ordered) data. For example, users may wish to record the maintenance history of vehicles. Blockchains can assist in these applications by providing an immutable record of the data being sent. In these scenarios, redundant transactions or conflicting transactions may not need to be resolved and latency requirements are relatively loose as the data is not immediately actionable.

Transactions: Applications where a consensus must be reached on the ordering of the transacted data. For example, any application involving payments would fall into this category (such as road tolls, registration costs, fines, etc.), as total ordering is needed to prevent double spending. Blockchains can be used to reach this consensus on ordering. In these scenarios, redundant transactions must be removed and nodes must reach consensus on *conflicting transaction resolutions* by ordering the transactions; this is needed to enable the transfer of scarce resources. These applications require *low latency* as transactions may be used to trigger actions and *smart contract support* to allow more complex transactions, such as deferred payments.

Data Dissemination: Applications where the transmitted data need to be processed and consumed by a number of nodes in the network. For example, an application notifying local vehicles of traffic delays or accidents would fall into this category. Here, the blockchain serves as a secure channel for distributing the data. *High throughput* is required by the underlying system to efficiently distribute the data.

Data Storage & Reporting: Applications where the transmitted data are likely to be collected only by interested parties, a subset of the nodes in the network. For example, an application recording accident reports is likely to produce data only of interest to regulators and the involved parties. The blockchain serves as a secure channel for distributing,

authenticating, storing, and timestamping the data. These applications require blockchains with *high throughput* and *efficient data storage* capabilities to handle the large amounts of data.

P2P Transactions: Applications where the majority of the transactions happen between nodes of similar priority or capability (*e.g.*, vehicles). For example, ride sharing applications, where users sell rides to others, would fall into this category. Blockchains can be used to allow such nodes to transact safely, without trusting each other or a third party. These applications require *public verifiability* of transactions so that two untrusting nodes can validate transactions between themselves.

V2I Transactions: Applications where the majority of the transactions happen between any devices (*e.g.*, vehicles) and some specific parties (*e.g.*, infrastructures of highways). Electric Vehicle charging, where users purchase power from the grid, is one example of this. Blockchains can be used to support reliable payments without compromising privacy. These applications can run on public or private/consortium blockchains to improve *privacy* and may require a *public key infrastructure* (PKI) so that users can identify legitimate infrastructure.

Local Data Dissemination: Applications where the majority of data creation and transfer happens between nodes of similar priority or capability (*e.g.*, vehicles). Inter-vehicle messaging applications, where vehicles notify surrounding peers of important events, such as traffic jams, fall into this category. Blockchains can be used to validate the data and the sender. *Reputation* mechanisms are required to verify the data sent by nearby nodes [46].

Top-Down Data Dissemination: Applications where authorities (*e.g.,* government, car manufacturer, etc.) serve as the data sources. Software update applications fall into this category. Blockchains can be used to discover data, validate them when they are received, and to compensate the sender. A *PKI* is required to verify the data initially came from a trusted source.

Event Driven Data Recording: Applications where the transmitted data are unprocessed and triggered by events, such as accidents, which may or may not be periodical. Here, blockchains provide verifiable, immutable, timestamped records of the data. These applications require sophisticated *reputation* and *oracle* designs to ensure data is not tampered with before being uploaded to the blockchain.

Aggregated Data Recording: Applications where a consistent stream of data is recorded on chain. For example, emissions tracking applications fall into this category. Blockchains can be used both to record the data and to perform actions based on the data using smart contracts. Such applications require a blockchain with *high throughput* in order to handle all the data, and *smart contract support* in order to allow parties to act on the data.

B. Use Case Description and Analysis

We analyze a use case from each of the categories at the bottom of Fig. 2. We briefly describe the use case and analyze its underlying blockchain requirements. The requirements for the applications under consideration are summarized in Table I. Without loss of generality, we base these requirements off of the needs of the province of Ontario, Canada, which is indicative of the traffic today in other regions globally. In particular, Ontario had approximately 14 million residents and nine million registered vehicles in 2017 [47].

Inter-Vehicle Messaging: Vehicles' sensors can record data that is important not only to the vehicle itself, but to other vehicles around it. For example, if traffic is slow on a certain street, cars on surrounding roads may wish to know. However, the risk of malicious actors providing false data is high, and so a mechanism to gauge the reputation of message senders (vehicles) is required. Blockchains can assist this type of application by adding a trust management layer to the communication protocol, as proposed in [46]. In that system, vehicles can use a blockchain to optionally rate messages they receive, either positively if they found the message accurate or negatively if they found the message inaccurate. Vehicles' reputations can increase or decrease based on the ratings of the messages they send, and future messages from these vehicles can be accepted or rejected based on their reputation. In 2017 an estimated 144 billion km were driven in Ontario [47]. Assuming vehicles submit a batch of ratings every 10km, such a blockchain system would need to support an average of 500tps. Assuming each ratings batch is approximately 1KB in size, the blockchain must support 500KBps total data throughput. Low latency is not required and so delays of up to 10 minutes are acceptable. The only data that needs to be stored by the blockchain is the cumulative rating for each user, approximately 1GB of data. As all vehicles will submit ratings, the number of clients of the system is approximately 9 million. In addition to the above requirements, such a system would ideally be able to provide some functionality even in cases where vehicles are not connected to the wider Internet (*i.e.*, due to being in remote areas without a cellular connection); this issue is discussed further in Section IV-C.

Software Updates: Vehicle software needs to be updated for both road safety and system security reasons [7]. Software providers send out the updates infrequently and these packages must be distributed quickly to every vehicle system that needs it. Additionally, vehicles must only accept updates from trusted providers. The system proposed in [7] uses a blockchain to validate software updates and record attestations from vehicles that have received the update. A local P2P network is used for the actual data distribution and the blockchain may also be used to support network discovery. Around nine million vehicles were registered in Ontario in 2017 [47]. Assuming that an update package with a size of 1 MB needs to be sent to 90% of the vehicles in

TABLE I
BLOCKCHAIN REQUIREMENTS OF V2X APPLICATIONS

	Tx Throughput	Data Throughput	Max. Latency	Users	Storage	Special Requirements
Inter-Vehicle Messaging	500tps	500KBps	10 min	9 million	<1GB	Offline Use, Sybil Prevention
Software Updates	260tps	260KBps	10 min	9 million	9GB	PKI, Local Networking
Accident Reports	<1tps	10KBps	10 min	500 000	300GB	Offline Use, Hardware Oracles
Emissions Tracking	300tps	150KBps	10 min	14 million	9GB	Regulator Support, Hardware Oracles
Ride Sharing	50tps	50KBps	<1 min	1 million	12GB	Data Encryption, Payments
EV Charging	1tps	0.5KBps	<1 min	46 000	<1GB	PKI, Payments

one day, and attestations of reception are under 1KB, the blockchain system needs to sustain on average 260 tps and 260 KBps of throughput, along with 260MBps of throughput in the underlying P2P network. Latency of up to 10 minutes in the blockchain layer is acceptable. Only a record of the latest software installed on each vehicle needs to be kept, as such approximately 9GB of storage is required, 1KB for each vehicle.

Accident Reports: We consider the accident investigation and insurance use cases discussed in [8]. Data generated in this use case fall into two categories: *on-site* and *off-site*. On-site data is recorded and uploaded automatically by the vehicles, pedestrians, and infrastructure involved in the accident. It may include the vehicles' location, speed, number of passengers, hashes of camera feeds, among other items. On-site data contains key information from a relatively short period around the accident, which we estimate normally totals less than 1 MB per accident. Ideally this data could be recorded and verified by surrounding vehicles even in cases where the accident occurs in areas without an Internet connection. Off-site data, including the accident investigation reports and insurance bills are generated by the government and insurance companies. These data may be larger than the on-site data. The size of the reports can be up to 10 MB in size, depending on the scale of the accident. According to the Ontario road safety annual reports, around 200,000 road collisions happen per year, of which around 30,000 result in fatalities or personal injury. Assuming that, in addition to 1MB of on-site data, each minor accident requires an average of 100KB of data in the report and each fatal or personal injury accident requires an average of 1MB of data, the data storage requirements of the system can reach nearly 300GB per year. These data are not processed in real time, as such latency is not a major concern and latency of up to 10 minutes is acceptable.

Emissions Tracking: We consider the emissions monitoring scheme described in [48]. In this system, for every trip a user takes, carbon usage data is recorded on a blockchain. Carbon credits are used to pay for this usage. Additionally, credits can be traded between users. Simulation based on travel data for an Ontario town required approximately 2.7 transactions per user per day. Therefore, a blockchain supporting this application for the population of Ontario would require around 300 tps. Assuming each transaction is approximately 0.5KB, this equates to 150KBps of data throughput. Latency requirements for this application are not strict as carbon emissions need not be responded to in real time; we suggest that a latency of up to 10 minutes would be acceptable. Every traveller would need to submit transactions to this system, so the estimated number of clients is on the order of 10 million. As users pay for their carbon usage at the end of each trip, no data is required to be stored on chain other than the identities of users and their credit balances. This results in less than 1KB of data per user, and approximately 9GB for the system as a whole. More data may be stored for research purposes, however this is not strictly required. As this system handles potentially sensitive data, privacy is a major concern. All users on the system are pseudonymous, which provides some protection. Further privacy could be achieved through the use of temporary identifiers or private blockchains. Such a system would require strong support from relevant regulators.

Ride Sharing: In general, a ride sharing system allows passengers with close destinations to share a vehicle and divide the cost of the trip among themselves. We consider the ride sharing scenario described in [43]. Here, local computing resources are used to match drivers with passengers and a private blockchain is used to record information about trips taken and can further be used to facilitate payment. Data required to be stored on the blockchain in such a use case includes the distance of the journey, number of passengers and their pseudonymous ids, and the total cost for the trip. The size of the data is approximately 1 KB per ride. Assuming approximately 10% of the population uses ride sharing, and each of those takes approximately 2 trips per day, this system is required to support an average of 50tps of throughput, totaling approximately 4GB of total data per day. This throughput would have to rise to account for increased demand in peak hours. As payments are desired to be fast, latency should be relatively low, less than 1 minute. Transactions should be stored on chain for several months. As trip data may be sensitive, privacy is a major concern in this use case. It may be possible to encrypt some data, such as trip details, in order to preserve privacy, however other data, such as the total cost, must be available to system validators to facilitate the correct payment.

Electric Vehicle (EV) Charging: We consider the designs provided in [44] and [45] as examples of V2I transaction use cases. In both proposals, EVs are both users and suppliers

of power in the systems. A local aggregator (LAG) serves as a validator in the system, provides temporary storage of power between suppliers and users, and may perform as an extra power supplier when needed. Additionally, in [44] the LAG performs double auctions to determine the power price. Stakeholders include the EV owners, an authority responsible for regulation, and the LAG operators. Currently, there are more than 1,600 charging stations [49] and over 46,000 EVs in Ontario [50]. Transactions in the network include electricity requests and monetary payments. Each transaction is around 500 bytes in size [45]. Given an average annual distance of 15,200 km [51], an average travel distance per charge of 200 km [52], and assuming a uniform distribution of charges throughput the year, there are approximately 20 thousand charges daily, however a rapid growth in that number is targeted. Assuming the charges happen mostly in the 8 work hours, the throughput required is $2,500$ transactions per hour or roughly 1 tps. Latency requirements are the same as any other application involving cryptocurrency transactions (*i.e.*, less than 1 minute). As data in the system may reveal the location and identity of the vehicle owner, pseudo-anonymity is required. However, regulatory authority should be able to reveal the identity whenever required.

IV. Mapping to Blockchains

A. Blockchain Specifications

As shown in the previous sections, blockchains targeting V2X use cases have unique requirements. First, they must support large amounts of data. For example, supporting only the use cases in Table I requires supporting over 1000tps, nearly 1MBps of data throughput, and hundreds of gigabytes of storage. Additionally, due to the sensitive nature of vehicular data (as it can generally reveal a user's location), privacy of this data must be central to these blockchains. Due to the safety critical nature of blockchains, security is a major concern, and so well-known attacks, such as Sybil attacks and 51% attacks must be prevented. Vehicles need to be able to act as clients in the network, submitting transactions. V2X blockchains must support cryptocurrency transactions to support use cases such as EV Charging and Ride Sharing. Finally, certain applications may have special requirements, such as those that must include some method to support vehicles temporarily disconnected from the Internet.

One possibility is to have vehicles support different blockchains for different use cases tailored to suit the specific task. However, we argue that this is *not* the ideal solution for the following two reasons:

- Requiring vehicles to support multiple blockchains raises numerous interoperability concerns. If every vehicle runs on the same blockchain, applications can be made universal. However, if they run a wide array of blockchains, certain vehicles may be unable to run certain applications and/or present myriad of overhead layers (and associated costs/delays) for inter-chain-communication in such a segregated environment. This negates one of the major advantages of using blockchains in the V2X space and so should be avoided.
- Ensuring applications run on the same blockchain can allow them to build on each other. Further, this tactic also promotes a culture behind a "holistic" ecosystem where third-parties can build novel decentralized applications/services. For example, the reputation mechanism used in the Inter-Vehicle Messaging use case could be adopted by many of the other use cases, *e.g.*, it could help users of the Ride Sharing application to gauge their trust in a potential driver. Taking advantage of these synergies would be costly and/or cumbersome if these applications ran on different blockchains.

B. Blockchain Architectures: An Empirical Case Study

Here, we compare the above requirements to currently available blockchains. To enforce use case logic into the system, we only consider blockchains with Turing-complete smart contract languages. We summarize the design and features of some candidate chains in Table II. We select Ethereum, IOTA, and Algorand as examples of public blockchains, with Hyperledger Fabric and Facebook's Diem being our examples for permissioned networks. This selection is based on the fact that those networks present complementary characteristics.

Public blockchains, such as Ethereum, and Algorand can provide high levels of security and decentralization. IOTA [53], on the other hand, relies on Proof-of-Work to avoid resource exploitation and a trusted entity called Coordinator for transaction finalization. While throughput is extremely limited in some cases (*e.g.*, Ethereum), resulting in poor performance and high fees, upcoming layer-2 solutions such as Zk-rollups [54] may provide significant performance improvements. However, the biggest concern with these chains when it comes to V2X use cases is their lack of privacy. All data posted on these blockchains is public, and as such anybody can read it. While this may not be a major concern for some types of transactions, it is unacceptable for transactions that may reveal a user's location, as many do in the V2X space. Additionally, due to a lack of know your customer (KYC) requirements, applications on public blockchains are often susceptible to Sybil attacks.

Due to these factors, we suggest that permissioned blockchains are the clear choice for V2X applications. While these blockchains are more centralized than public chains, due to the large number of semi-trusted stakeholders in the V2X space (*e.g.,* governments, police services, insurance companies, car manufacturers, citizen groups, etc.), we argue a blockchain validated by these stakeholders would provide good security and sufficient decentralization while still providing great throughput and low fees. By limiting the set of validators to only known and trusted entities, the risk to user privacy is greatly diminished. These entities can ensure that smart contract rules surrounding the availability of data to

TABLE II
SUMMARY OF CANDIDATE CHAIN DESIGNS AND FEATURES

	Ethereum	**Hyperledger Fabric**	**IOTA**	**Algorand**	**Diem**
Type of blockchain	Public	Permissioned	Public	Public	Permissioned
Consensus	Proof of Work [5]	PBFT [31]	IOTA Proof of Work [53]	Proof of Stake [24]	HotStuff [34]
Transaction fees	very high	nil	low	low	nil
Throughput	low	high	high	high	high
Data Dissemination	Unhosted accounts	ideal	feasible	high	ideal
Data Storage and Reporting	privacy, high fees concerns	ideal	privacy concerns	privacy concerns	ideal
Transactions	Native or ERC20 tokens	Feasible	Feasible	Native	Native or Coins

third parties are enforced. Through government oversight of the validators, these concerns can be eased even further.

Unlike decentralized public blockchains such as Bitcoin, some permissioned blockchains only allow hosted wallets, *i.e.*, a few entities have the authority to issue accounts, often with a KYC process. This feature is crucial for some use cases such as Inter-Vehicle Communication and Accident Reports, hosted wallets are required to prevent Sybil attacks. Hosted wallets enable trusted authorities to track down users in order to resolve conflicts without compromising privacy. Due to the privacy concerns of revealing the true identity behind these wallets, we suggest only the most trusted validators (*e.g.*, governments) should have this ability.

It is important to note that vehicles' sensor data has a high collection frequency and volume, testing the limits of any distributed computing system. We suggest the systems to be designed to prune the data at regular intervals and to be augmented by layer-2 solutions such as Zk-rollups or payment channels [54] to maximize the number of possible use cases that can be supported by a single blockchain.

The special requirements of some applications, summarized in Table I also suggest open problems that require further investigation. Some applications require hardware oracles in order to provide trustworthy data to the blockchain. The Ride Sharing application requires that some data be encrypted in a way that preserves privacy while allowing users with the proper permissions to access it.

C. A Note on Offline V2X Operation

An important factor of any V2X blockchain system is the fact that at times vehicles may not have access to the network. Evidently, as noted earlier in this paper, some of the use cases described here 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 when they are not online [55]. Admittedly, this introduces a major gap with 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 [56]. Those "local 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 [54]. 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 [55]. Such a design could potentially achieve good performance and security, however 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.

V. CONCLUSION

This paper presents an overview of blockchain applications in the V2X space and analyzes these applications in order to determine the requirements of a V2X blockchain. We find that permissioned blockchains are the best option to enable the widest range of applications and ensure that throughput, user privacy, and KYC requirements are all met. However further work is needed to enable the vast amount of throughput required to process all the data produced by modern connected vehicles. Some interesting directions for future work on this topic include the development of a blockchain specially designed for the V2X space, layer-2 solutions built on top of permissioned blockchains to increase throughput, the development of novel blockchain features that may be applied to the V2X space, such as support for offline use, and real-world testing of blockchain based V2X applications.

REFERENCES

[1] 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

[2] J. Z. Varghese *et al.*, "Overview of autonomous vehicle sensors and systems," in *Int. Conf. on Operations Excellence and Service Engineering*, 2015, pp. 178–191.

[3] V. Milanés *et al.*, "Cooperative adaptive cruise control in real traffic situations," *IEEE Trans. on Intelligent Transportation Syst.*, vol. 15, no. 1, pp. 296–305, 2014.

[4] M. Usman *et al.*, "A business and legislative perspective of v2x and mobility applicat. in 5g networks," *IEEE Access*, vol. 8, pp. 67 426–67 435, 2020.

[5] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot, Tech. Rep., 2019.

[6] S. Motepalli *et al.*, "Reward mechanism for blockchains using evolutionary game theory," in *2021 3rd Conf. on Blockchain Research Applicat. for Innovative Networks and Services (BRAINS)*, 2021.

[7] M. Baza *et al.*, "Blockchain-based firmware update scheme tailored for autonomous vehicles," in *2019 IEEE Wireless Commun. and Networking Conf. (WCNC)*, 2019, pp. 1–7.

[8] M. Cebe *et al.*, "Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," *IEEE Commun. Magazine*, vol. 56, no. 10, pp. 50–57, 2018.

[9] S. M. Danish *et al.*, "Blockev: Efficient and secure charging station selection for electric vehicles," *IEEE Trans. on Intelligent Transportation Syst.*, pp. 1–18, 2020.

[10] M. Abraham *et al.*, "Blockchain and collaborative intelligence based next generation smart toll application," in *2020 2nd Conf. on Blockchain Research Applications for Innovative Networks and Services (BRAINS)*, 2020, pp. 206–207.

[11] J. Meijers *et al.*, "Cost-effective blockchain-based iot data marketplaces with a credit invariant," in *2021 IEEE Int. Conf. on Blockchain and Cryptocurrency (ICBC)*, 2021.

[12] T. L. Willke *et al.*, "A survey of inter-vehicle communication protocols and their applications," *IEEE Commun. Surveys Tutorials*, vol. 11, no. 2, pp. 3–20, 2009.

[13] J. E. Siegel *et al.*, "A survey of the connected vehicle landscape—architectures, enabling technologies, applications, and development areas," *IEEE Trans. on Intelligent Transportation Syst.*, vol. 19, no. 8, pp. 2391–2406, 2018.

[14] United States Department of Transportation, NHTSA, "FMVSS No. 150 Vehicle-To-Vehicle Communication Technology For Light Vehicles," 2016.

[15] United States Department of Transportation, ITS, "Vehicle-to-Infrastructure (V2I) Resources," *ITS Deployment*, 2020. [Online]. Available: https://www.its.dot.gov/v2i

[16] ——, "Vehicle-to-Pedestrian (V2P) Communications for Safety," *Research Archive*, 2020. [Online]. Available: https://www.its.dot.gov/press/2015/v2p_tech.htm

[17] S. Widodo *et al.*, "Vehicle fuel consumption and emission estimation in environment-adaptive driving with or without inter-vehicle communications," in *Proc. of the IEEE Intelligent Vehicles Symp. 2000*. IEEE, 2000, pp. 382–386.

[18] K. Katsaros *et al.*, "Application of vehicular communications for improving the efficiency of traffic in urban areas," *Wireless Commun. and Mobile Computing*, vol. 11, no. 12, pp. 1657–1667, 2011.

[19] B. Asadi *et al.*, "Predictive cruise control: Utilizing upcoming traffic signal information for improving fuel economy and reducing trip time," *IEEE transactions on control systems technology*, vol. 19, no. 3, pp. 707–714, 2010.

[20] D. Reichardt *et al.*, "Cartalk 2000: safe and comfortable driving based upon inter-vehicle-communication," in *Intelligent Vehicle Symp., 2002. IEEE*, vol. 2, 2002, pp. 545–550 vol.2.

[21] J. B. Kenney, "Dedicated short-range commun. (dsrc) standards in the united states," *Proc. of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[22] 3GPP, "Vehicle-to-Everything (V2X) services in 5G System (5GS); Stage 3," 3rd Generation Partnership Project (3GPP), Technical specification (TS) 24.587, 12.

[23] "Applications," 5 2016. [Online]. Available: http://local.iteris.com/cvria/html/applications/applications.html

[24] Y. Gilad *et al.*, "Algorand: Scaling byzantine agreements for cryptocurrencies," in *Proc. of the 26th Symp. on Operating Syst. Principles*, 2017, pp. 51–68.

[25] L. Chen *et al.*, "On security analysis of proof-of-elapsed-time (poet)," in *Int. Symp. on Stabilization, Safety, and Security of Distributed Syst.* Springer, 2017, pp. 282–297.

[26] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. bft replication," in *Open Problems in Network Security*, J. Camenisch *et al.*, Eds., 2016, pp. 112–125.

[27] L. Lamport *et al.*, "The byzantine generals problem," in *Concurrency: the Works of Leslie Lamport*, 2019, pp. 203–226.

[28] G. Zhang *et al.*, "An efficient consensus protocol for real-time permissioned blockchains under non-byzantine conditions," in *Int. Conf. on Green, Pervasive, and Cloud Computing*. Springer, 2018, pp. 298–311.

[29] M. Castro *et al.*, "Practical byzantine fault tolerance," in *OSDI*, vol. 99, 1999, pp. 173–186.

[30] A. Bessani *et al.*, "State machine replication for the masses with bft-smart," in *44th Annual IEEE/IFIP Int. Conf. on Dependable Syst. and Networks*, 2014, pp. 355–362.

[31] E. Androulaki *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proc. of the Thirteenth EuroSys Conf.* ACM, 2018, p. 30.

[32] R. G. Brown *et al.*, "Corda: an introduction," *R3 CEV*, 2016.

[33] G. G. Gueta *et al.*, "SBFT: a scalable and decentralized trust infrastructure," in *49th Annual IEEE/IFIP international conference on dependable systems and networks (DSN)*, 2019, pp. 568–580.

[34] M. Yin *et al.*, "Hotstuff: Bft consensus with linearity and responsiveness," in *Proc. of the 2019 ACM Symp. on Principles of Distributed Computing*, 2019, pp. 347–356.

[35] G. Zhang *et al.*, "Prosecutor: An Efficient BFT Consensus Algorithm with Behavior-aware Penalization Against Byzantine Attacks," in *Middleware '21: 22st ACM/IFIP Int. Middleware Conf.*, 2021.

[36] Y. Yuan *et al.*, "Towards blockchain-based intelligent transportation systems," in *2016 IEEE 19th Int. Conf. on Intelligent Transportation Syst. (ITSC)*, 2016, pp. 2663–2668.

[37] A. Dorri *et al.*, "Blockchain: A distributed solution to automotive security and privacy," *IEEE Commun. Magazine*, vol. 55, no. 12, pp. 119–125, 2017.

[38] T. Jiang *et al.*, "Blockchain-based internet of vehicles: Distributed network architecture and performance analysis," *IEEE Internet of Things J.*, vol. 6, no. 3, pp. 4640–4649, 2019.

[39] J. Kang *et al.*, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet of Things J.*, vol. 6, no. 3, pp. 4660–4670, 2019.

[40] R. Shrestha *et al.*, "Blockchain-based message dissemination in vanet," in *2018 IEEE 3rd Int. Conf. on Computing, Communication and Security (ICCCS)*, 2018, pp. 161–166.

[41] V. Hassija *et al.*, "Dagiov: A framework for vehicle to vehicle communication using directed acyclic graph and game theory," *IEEE Trans. on Veh. Technology*, vol. 69, no. 4, pp. 4182–4191, 2020.

[42] P. Fraga-Lamas *et al.*, "A review on blockchain technologies for an advanced and cyber-resilient automotive industry," *IEEE Access*, vol. 7, pp. 17 578–17 598, 2019.

[43] M. Li *et al.*, "Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing," *IEEE Internet of Things J.*, vol. 6, no. 3, pp. 4573–4584, 2019.

[44] J. Kang *et al.*, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. on Industrial Informatics*, vol. 13, no. 6, pp. 3154–3164, 2017.

[45] F. Gao *et al.*, "A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks," *IEEE Network*, vol. 32, no. 6, pp. 184–192, 2018.

[46] Z. Yang *et al.*, "Blockchain-based decentralized trust management in veh. networks," *IEEE Internet of Things J.*, vol. 6, no. 2, pp. 1495–1505, 2019.

[47] Safety Policy & Education Branch, Ministry of Transportation, "Ontario road safety annual report 2017," 2017.

[48] J. Eckert *et al.*, "A blockchain-based user-centric emission monitoring and trading system for multi-modal mobility*," in *2020 Forum on Integrated and Sustainable Transportation Syst. (FISTS)*, 2020, pp. 328–334.

[49] Government of Canada, "Electric charging and alternative fuelling stations locator," 2018.

[50] Electric Mobility Canada, "Electric vehicle sales in canada," 2021.

[51] National Resource Canada, "Canadian vehicle survey," 2010.

[52] S. A. Adderly *et al.*, "Electric vehicles and natural disaster policy implications," *Energy Policy*, vol. 112, pp. 437–448, 2018.

[53] Coordicide Team, IOTA Foundation, "The coordicide." [Online]. Available: https://cdn0.tnwcdn.com/wp-content/blogs.dir/1/files/2019/05/Coordicide_WP.pdf

[54] "Layer 2 scaling." [Online]. Available: https://ethereum.org/en/developers/docs/layer-2-scaling/

[55] A. Veneris *et al.*, "Central bank digital loonie: Canadian cash for a new global economy," *Available at SSRN 3770024*, 2021.

[56] Z. Yang *et al.*, "A blockchain-based reputation system for data credibility assessment in vehicular networks," in *2017 IEEE 28th Annual Int. Symp. on Personal, Indoor, and Mobile Radio Commun. (PIMRC)*, 2017, pp. 1–5.