electronics

MDPI

Review

Blockchain Applications to Improve Operation and Security of Transportation Systems: A Survey †

Navid Khoshavi [1,2,*], Gabrielle Tristani [2] and Arman Sargolzaei [3]

[1] Department of Computer Science, Florida Polytechnic University, Lakeland, FL 33805, USA
[2] Department of Electrical and Computer Engineering, Florida Polytechnic University, Lakeland, FL 33805, USA; gtristani8152@floridapoly.edu
[3] Mechanical Engineering Department, Tennessee Technological University, Cookeville, TN 38505, USA; asargolzaei@tntech.edu
* Correspondence: nkhoshavinajafabadi@floridapoly.edu

† Partial support of this research was provided by the National Science Foundation under Grant No. CNS-1919855. Any opinions, findings, and conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the sponsoring agency.

Abstract: Blockchain technology continues to grow and extend into more areas with great success, which highlights the importance of studying the fields that have been, and have yet to be, fundamentally changed by its entrance. In particular, blockchain technology has been shown to be increasingly relevant in the field of transportation systems. More studies continue to be conducted relating to both fields of study and their integration. It is anticipated that their existing relationships will be greatly improved in the near future, as more research is conducted and applications are better understood. Because blockchain technology is still relatively new as compared to older, more well-used methods, many of its future capabilities are still very much unknown. However, before they can be discovered, we need to fully understand past and current developments, as well as expert observations, in applying blockchain technology to the autonomous vehicle field. From an understanding and discussion of the current and potential future capabilities of blockchain technology, as provided through this survey, advancements can be made to create solutions to problems that are inherent in autonomous vehicle systems today. The focus of this paper is mainly on the potential applications of blockchain in the future of transportation systems to be integrated with connected and autonomous vehicles (CAVs) to provide a broad overview on the current related literature and research studies in this field.

Keywords: blockchain; security; privacy; financial transactions; transportation systems; autonomous vehicles

check for updates

Citation: Khoshavi, N.; Tristani, G.; Sargolzaei, A. Blockchain Applications to Improve Operation and Security of Transportation Systems: A Survey. *Electronics* **2021**, *10*, 629. https://doi.org/10.3390/electronics10050629

Academic Editor: Giuseppe Prencipe

Received: 3 January 2021
Accepted: 26 February 2021
Published: 9 March 2021

1. Introduction

Despite being widely anticipated and celebrated by many today, the field of connected and autonomous vehicles (CAVs) has also faced scathing criticism, disadvantage analysis, and distrust from wary organizations and people [1–7]. Security, safety, and privacy concerns have all been brought up and, as a result, there is a great deal of uncertainty surrounding just how beneficial CAVs can truly be to our society and overall health. A major force in this skepticism is that CAVs systems rely on online networks and, as connected devices, they may be susceptible to numerous software and hardware faults that can be exposed and exploited by attackers [8–11]. Attackers are known for using any means possible to compromise user data, overwhelm networks, and potentially cause dangerous situations for users. In the case of AVs, any form of lax security and safety measures can prove to be fatal due to the inherent hazards that are involved in driving and managing past and present location-sensitive information of users [12,13].

A centralized system is viewed by many to be incredibly ineffective, as well as dangerous, due to the constantly changing nature and wide-scale data management required in CAV operations [14]. Retrieving data in a timely manner is an absolute necessity in ensuring prompt response time, which may be difficult in the case of a single central system managing all user data. Another concern with this setup is the potential for attackers to take advantage of the single failure point for all CAVs by overwhelming the centralized system with requests or manipulating certain user data, at which point they would be able to potentially devastate the entire CAV network [15].

Over time, inherent flaws in totally centralized networks led to the search for alternative models, such as those that are depicted in Figure 1. The proposed model relies on a variety of interconnections between users and other entities instead of using a single, central node. Among the many possibilities, the most promising one was blockchain, proposed by a person or group of people using the name Satoshi Nakamoto in 2008 [16]. Blockchain has the potential to realize a large system, with its size being supported by a variety of peers, equipped with measures to validate, begin, and end transactions through its consensus and validation protocols. No longer restricted to the performance and security challenges of centralized network, blockchain provides all the same necessary features that are present in centralized networks, but, under a high throughput, scalable peer-to-peer based architecture. Despite its creation being fueled primarily by a desire to allow bitcoin technology to function, it has gained a lot of traction with researchers and the public in a wide variety of fields due to its benefits in providing secure, reliable transactions without the use of a single central entity in managing them.

As of now, the blockchain solution has already been incorporated across varying areas of study with great success, which has led many to wonder whether it can be applied similarly to other emerging fields [8]. Among these fields, the applications of blockchain in CAVs have been extensively studied [12–14]. Through these studies, a wide spectrum of methods have been proposed on how blockchain can be incorporated to add and expand on existing CAV functionality, coupled with a number of tests indicating the feasibility of implementations [17,18].

While not designed with a CAV system use in mind, blockchain has proven itself to have a number of benefits that could be successfully carried over to CAVs [19]. Its application could lend itself to use in enhancing the security of CAVs as well as improving the privacy of the users [20], increasing passengers' safety, and maintaining records on vehicle actions in the case of accidents to provide more accurate information for insurance and compensation purposes, as has been noted by a variety of researchers [21], allowing financial transactions to occur directly between a vehicle and a user or other device without the involvement of unnecessary parties [22,23], and providing CAVs with the ability to interact with other devices to offer additional relevant services to users. With its high level of use in various industries and noted security and operation-based benefits, its integration into CAVs could completely eliminate former concerns and provide a framework for entirely new capabilities.

Current blockchain faults in terms of energy and resource consumption, as well as financial cost and increased delay, when several users that are connected to a network have caused some researchers to view it as too inherently flawed to scale to such a large and time-sensitive system, but such concerns may soon prove to be unfounded. Blockchain is, when compared to a variety of other technologies today, relatively new, which means that there is still plenty of ability for improvement. In addition, there have been several proposals on how to resolve such issues, including the use of more lightweight approaches, coupled with the revision of the current Proof of Work algorithm that is responsible for many of the issues discussed [24,25]. With more time to study and improve on blockchain and the algorithms that it tends to use, it will likely prove to be fully capable to support the decentralized network discussed, with its production cost lowering in turn due to an increase in blockchain understanding between companies and develop.

The stride to achieve a safe and secure ecosystem where all-inclusive CAVs operate without a human input has been aligned with our motivation to demonstrate the potential benefits of leveraging blockchain to address the previous transportation-related threats.

Because the current literature is lacking a comprehensive study on the application of blockchain in operation and security of Transportation Systems, this paper surveys the most recent studies in this domain. In this survey, we briefly describe the structure of blockchain as well as highlighting the advantages of utilizing blockchain in CAVs. Furthermore, we thoroughly demonstrate how blockchain can be, and has already been, applied to CAV technology. More specifically, this study aims to discuss the following concerns relating to CAVs:

- The importance of future CAV applications in our day-to-day convenience, safety, security, and growth is illustrated.
- The current obstacles that hinder the public acceptance and development of CAVs, like safety, security, and speed concerns, are discussed.
- The common applications and attributes of blockchain technology and how they have been used for numerous projects in the past are included.
- The benefits for the implementation of blockchain technology in the transportation system's development are presented.

The remainder of this article is organized, as follows: Section 2 of the paper discusses the basic background information surrounding the history of blockchain and how it functions, Section 3 elaborates on how common blockchain applications and features could benefit CAVs if implemented effectively. Section 4 describes the application of Blockchain in collective decision. Section 5 presents the future research direction and challenges. Section 6 serves as the conclusion.

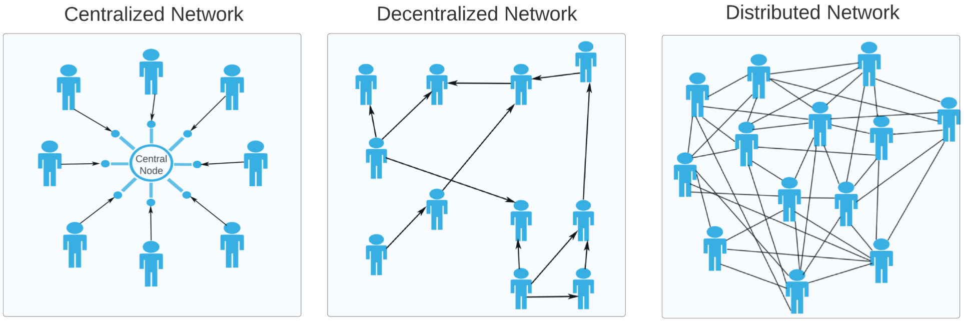


Figure 1. The different types of networks. Centralized networks have a central node that provides connection capabilities for the entire network. Decentralized networks have multiple connection paths between nodes, but some nodes can still lose connection with the network. Distributed networks have several communication paths between nodes, which drastically reduces the probability of a node disconnecting. Centralized is the most common, but decentralized and distributed are increasing in popularity.

2. Background

Before discussing specific blockchain applications, we need to briefly explain the terminologies, concepts, and algorithms that construct the blockchain methodology.

2.1. Ledger

The blockchain is best described as a distributed ledger, maintaining information regarding the transactions carried out and providing its services to all blockchain users. Under this system, every party maintains its own ledger copy, which allows them to check any past or present transaction record sent to them for security and validity. The network bundles transactions into blocks to facilitate the distribution of data across the nodes. Those blocks are then checked for authenticity and appended to the chain.

2.2. Block

A block is comprised of a number of different data-bearing segments, with each being necessary for upholding transactions. In the most general view, a block is composed of its header and its body. Its header contains important information regarding the specifics of the version, hash, and other relevant protocol details for the validation, while its body includes the actual transaction taking place, as well as its counters. One block can contain multiple transactions, with the total number of transactions being dependent on its size.

2.3. *Proof-of-Work (PoW) and Hashes*

Each block connects to the previous block by using hashes, as shown in Figure 2. Each hash is a set value, which is computed by assessing block contents and used to detect errors. As an extra mechanism to detect the alteration of previous blocks in the chain, the hash value of the prior block is included. Any entity that wants to send a block over the network needs first to compute an algorithm we will call a puzzle, Power-of-Work (PoW), and then send the solution to the network for approval. This requirement accomplishes two key goals: stopping attackers from generating and sending incorrect transaction data to the ledger and similarly limiting the number of concurrent transactions that a ledger can receive to prevent it from being overloaded.

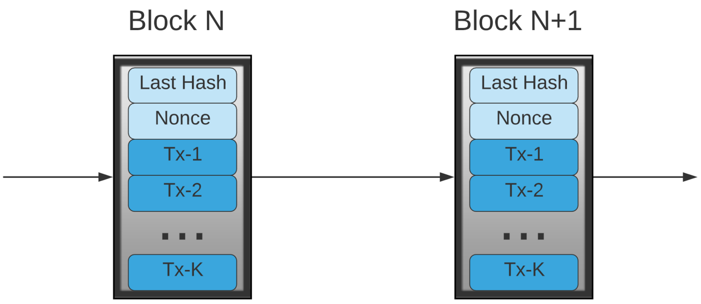


Figure 2. A diagram showing connections between blocks in blockchain technology, providing these connections through hashes.

2.4. *Scalability*

Scalability is one of the most highly desired features for any system that expects to expand over time or needs to be able to remain stable in the face of targeted attacks on its infrastructure as a whole. Centralized networks, while simple to set up and understand, are severely limited in this regard, since they rely on a single entity for all network operation, which provides a clear target for attackers, as well as allowing for the potential overload of the central node as more users join the network since these nodes do not come with their own resources to manage increased network traffic. This is demonstrated in Figure 3.

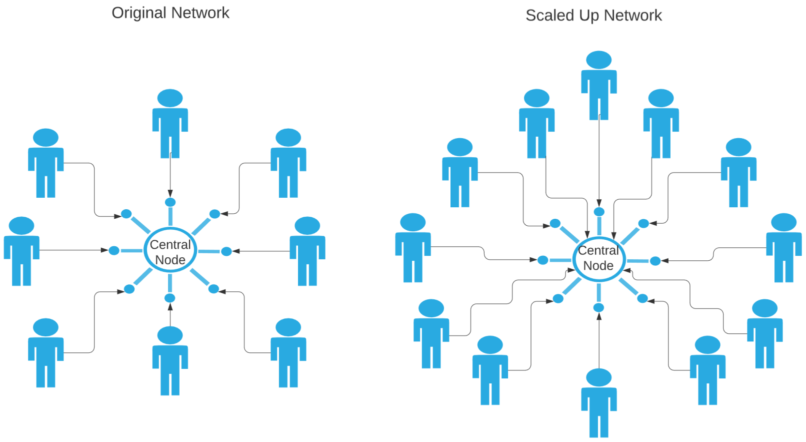


Figure 3. In a centralized network, a small percentage of the nodes handle a bulk of the work. To scale such a network, the primary nodes need to increase their ability to handle more traffic.

However, with blockchains, when a user is added to a blockchain, like in Figure 4, they come with their own set of resources. Besides the resource requirements, the complexity and run time of the consensus algorithms running on the network should also scale (either linearly or sublinearly) with the size of the network. This contribution of resources and the scalability of the consensus algorithm allows for enhanced network operation, since users will primarily take care of themselves and their own role in the chain, letting the blockchain scale easily when new users are added without straining a central server. The peer-to-peer-based architecture means that there is no single point in the network that is responsible for all normal operation of other nodes, meaning that the system lacks a single failure point, and is thus much more resilient. All of the nodes can rely on its interconnections between a variety of other nodes instead of choosing just one, providing a backup for all users over a network. This allows for the blockchain to retain overall connection and operation, even when several nodes are compromised.

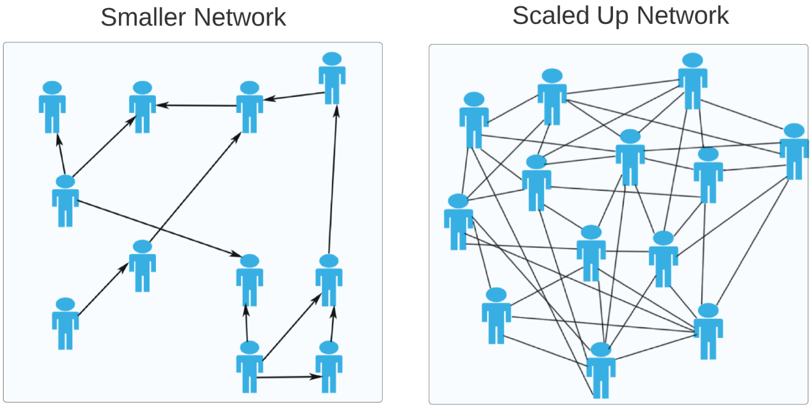


Figure 4. Scaling in a distributed network is simpler because new nodes contribute their own resources.

2.5. Privacy, Anonymity, and Keys

Instead of associating transactions with a fully-fledged identity, as is the case in fully centralized institutions, blockchain uses a pseudo-identifier. Commonly, this pseudo-identifier is just a cryptographic key. All of the transactions that would typically need a name, social security number, ID, and other associated information, now only require the key. This increases both privacy and risk proportionally, since, now, if an entity loses its key, it loses access to all of its information. Even worse, if a malicious party compromises an entity's key, it can then use that to either pretend to be the entity or access all the entities' records, credentials, and resources.

The cryptographic key is based on the famous public-private key architecture. In this architecture, a user generates two keys: the public key and private key. Private keys they keep to themselves, while public keys are broadcasted over the network whenever requested. In this system, private keys are used to encrypt the information, while public keys are utilized to decrypt encrypted messages. This allows the identity of the user to be easily verifiable. If the user encrypts a file and that file later comes into question, its authenticity can be verified, since the system trusts that a user will keep their private key secure.

2.6. Re-Purposing

Currently, the primary and most notable application of the blockchain protocol is Bitcoin. For processing transactions, users, referred to as miners, gain a digital monetary reward that is known as Bitcoin. As the number of miners on the network increase, the PoW increases proportionally. The appeal of a decentralized financial system that is unregulated by any government has led to its widespread popularity among the public.

Although blockchain was designed with application to bitcoin alone in mind, it is a very flexible system that can be applied to countless industries. Currently, blockchain technology is used in healthcare, online transaction security, and several other fields. Because blockchain is new, many researchers are eager to find new ways to apply this quickly growing and changing technology to other systems and areas.

Table 1 briefly demonstrates how blockchain can overcome the challenges of centralized systems.

Table 1. Blockchain solutions for centralized system flaws.

Centralized Problems	Blockchain Solutions
Requires Trusted Authority	Trustless System
Scalability Issues	System Scales with New Users
Information is Modifiable	Immutable Blocks Using Hashes
Identities are not Anonymous	Cryptographic Keys as Pseudo-Identifiers

3. Blockchain and Transportation

One of the main reasons CAV technology has not been fully embraced is an underlying safety concern. However, at the same time, many would agree that the most dangerous and unstable elements of transportation are the human drivers [26]. While not yet perfect, CAVs have the potential to compensate for the shortcomings of humans and fully prevent accidents. When discussing CAVs, there are several levels to consider: *level 0*, which has no automation, *level 1*, which has certain automation when needed for certain very specific and isolated functions, *level 2*, which has automation in the case of several different communicating functions, *level 3*, which has significantly limited, but still functional, self-driving capabilities that may require some user input, and *level 4*, which has the complete ability to operate and drive by itself. In the end, it is expected and desired that *level 4* CAVs will be developed, but, until then, the focus has been on enhancing the capabilities of previous levels, with the exception of level 0. Several companies, including Google, Uber, and Telsa, have recently made great strides in self-driving vehicles, and Tesla has recently announced that its shared autonomy fleet will go live within 2020.

Despite an overall reduction in accidents, there have still been many noted driving failures involving CAVs. Currently, CAVs are known to make incorrect decisions at times for two reasons: (1) because the technology is far from perfect, as it is challenging to meet the mandatory requirements, and (2) because the vehicles do not yet have enough information to process to avoid certain incidents.

Though many of the factors that cause such flaws and potential areas of improvement are well known, methods that outline how solutions can be implemented may not be as clear. Some examples of well studied problems in CAV technology are ensuring the abilities to both maintain and secure certain data, like physical and geographic location of vehicles [27–30], allow sufficient operation space for vehicles and control traffic flow [31–34], allowing and securing communication between vehicles and each other as well as other network-connected devices [35–39], providing collision warning and evasion techniques [40–44], providing security against attacks from malicious entities and faulty software or hardware [45–49], and offering safe and reliable availability of updates when needed [50]. The possibilities that are opened by CAV technology are too vast to be ignored, with broad applications to various fields to improve operation and user convenience. As noted, CAV technology lends itself to use in transport-based financial transactions, like public transportation systems [51].

CAVs are still relatively new, which leads them to suffer from a number of flaws that have lessened public support in the name of security and safety concerns for drivers and pedestrians. However, while CAVs have yet to gain full public trust, blockchain technology is viewed as one of the most secure methods used to maintain transactions and enable users to perform common operations as simply and safely as possible. In order to promote trust in CAVs and more fully demonstrate the full capabilities and possible extension of blockchain technology, the integration of blockchain technology and CAV systems is an idea that could prove advantageous to both fields. Figure 5 illustrates a summary of the leading research activities in each aspect of applications of blockchain. We explain the technical contribution of each work in the rest of the manuscript.

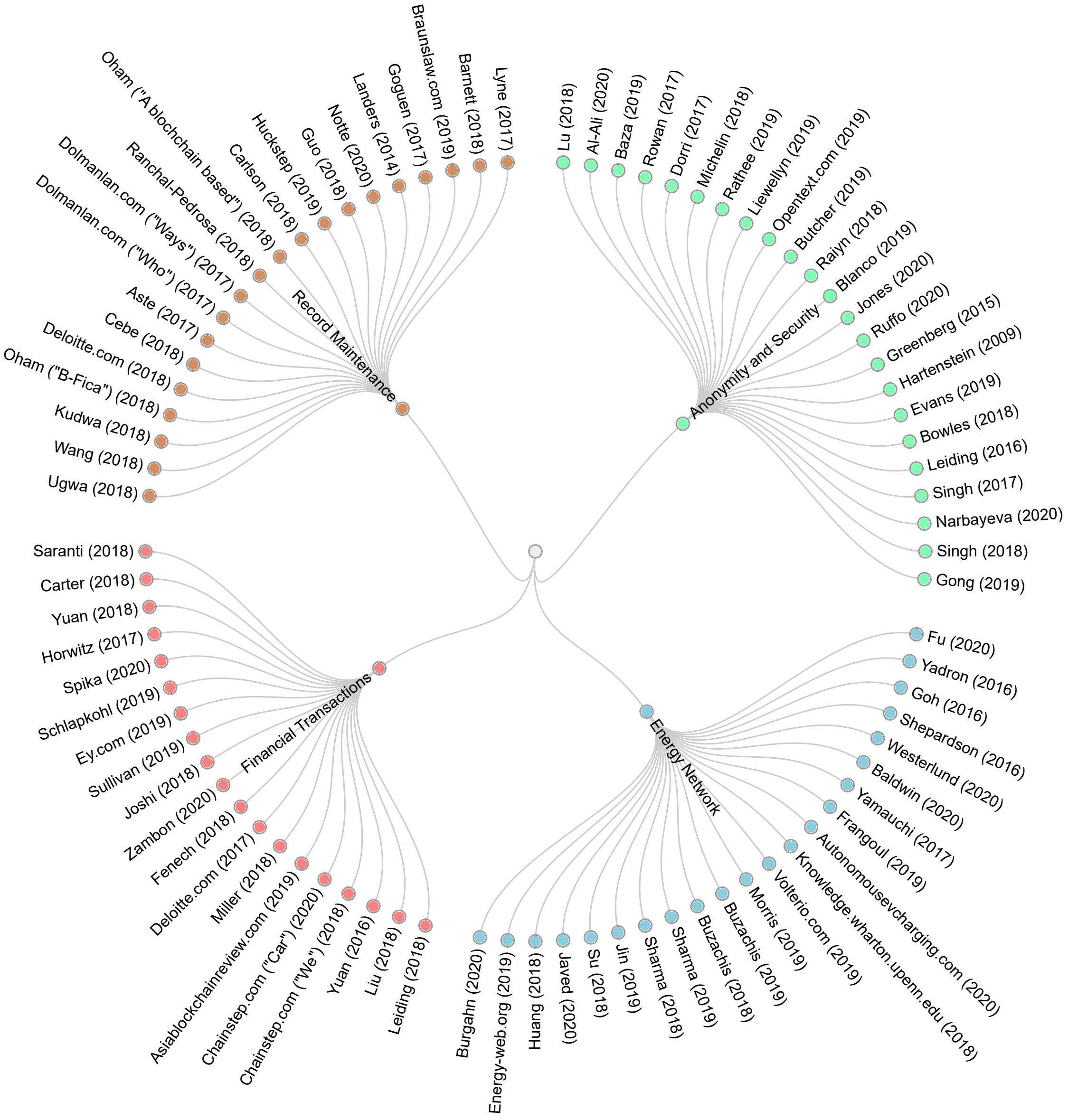


Figure 5. A circular dendrogram demonstrating the leading research activities in each domain.

3.1. *Anonymity and Security*

Figure 6 shows the attribute graph of the security concerns of CAVs that blockchain technology can address. In the case of CAVs, data and device security and anonymity are some of the largest places of failure, as well as the largest places that must be secured in vehicle operation, as brought up by a variety of researchers and wary consumers [52–56]. Because blockchain was built entirely to provide security in transactions, its role in providing security for CAV users is by far the most well studied and desired. Thus, the majority of this study will discuss this aspect, as well as the several approaches that utilize the blockchain to ensure security and user anonymity in CAV systems.

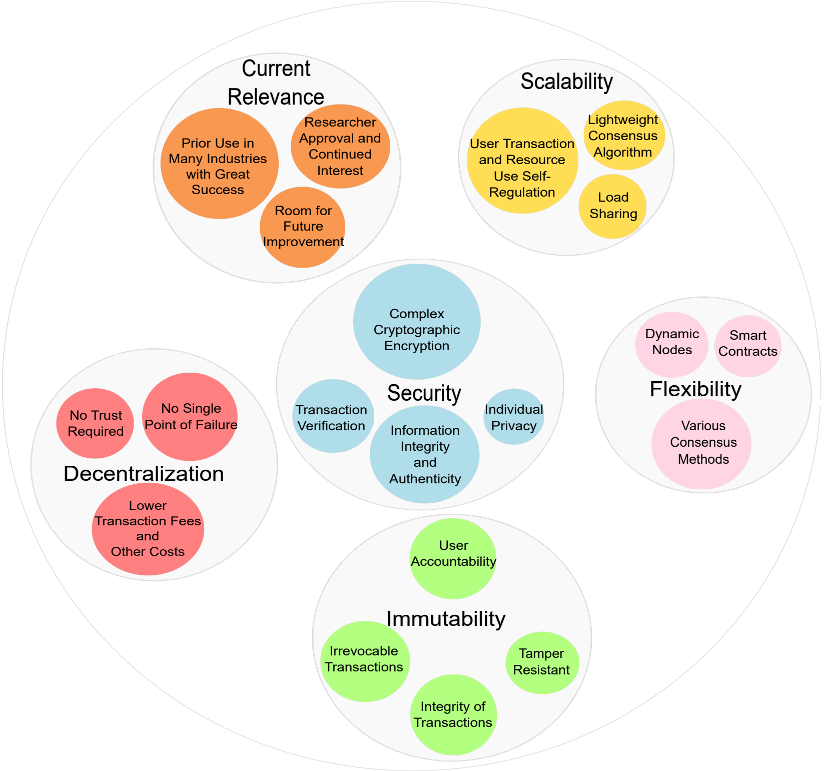

Current Relevance
Prior Use in Many Industries with Great Success
Researcher Approval and Continued Interest
Room for Future Improvement
Scalability
User Transaction and Resource Use Self-Regulation
Lightweight Consensus Algorithm
Load Sharing
Security
Complex Cryptographic Encryption
Transaction Verification
Information Integrity and Authenticity
Individual Privacy
Flexibility
Dynamic Nodes
Smart Contracts
Various Consensus Methods
Decentralization
No Trust Required
No Single Point of Failure
Lower Transaction Fees and Other Costs
Immutability
User Accountability
Irrevocable Transactions
Tamper Resistant
Integrity of Transactions

Figure 6. The attribute graph of the security concerns of connected and autonomous vehicles (CAVs) that blockchain technology can address.

Although data security and user anonymity are both highly prized features of any vehicle or device in use today, they tend to be ignored in favor of physical driver safety and more technically accurate operation. Recently, this has been extremely noticeable in CAV development, leading to user outrage from the fact that their personal data and vehicles' safety from attackers is not given necessary protection [57–61]. As an example, VANETs [62] seek to remedy the issue of numerous drivers, and the risk that is associated with them, by creating a network for cars to directly communicate with each other, sharing information on road safety issues, upcoming traffic stops, and general information to improve the efficiency of the whole vehicular system. However, while this sounds promising to many researchers and drivers, some users worry about the inherent risks involved, with concerns being based around the exposure of car, driver, and location information in these communications.

VANETs were not designed with the current developments of CAVs in mind, but could prove incredibly beneficial to an CAV network, possibly even more beneficial than it is to regular vehicle systems with the removal of human unpredictability. The use of consistent and constant communication between adjacent vehicles to help them prepare for future traffic events and situations would provide CAVs with all of the needed information to make decisions in a timely and accurate manner, which is why their incorporation is so essential. However, before they can be safely added, the previously mentioned risks to user privacy and security must be overcome.

Le et al. have outlined a system, called a Blockchain-based Anonymous Reputation System (BARS), which works using guidelines and defined operations to ensure trust throughout the network [10]. With this, Ref. [10] believe they have found a way to mitigate known security and privacy flaws in CAV systems. This BAR system works under its defined development in a number of connected phases, called steps, all of which were created to secure user privacy. The first step is to adjust blockchain features, so the preexisting, commonly used Public Key Infrastructure (PKI) can be extended to provide for a new authentication procedure that guarantees user data privacy. At this point, there is a distinct link from the communicating vehicle to its private key, which presents a huge security risk in allowing attackers to find the private key for a given user, and, in turn, gain access to their transaction information. This risk is accounted for and prevented with the addition of a Certificate Authority (CA), which serves to provide a new abstraction layer to protect the anonymity of all users, letting the whole network continue to function securely [10].

The next development step is in the researcher's design of a new algorithm to assess vehicle reputation and its level of trustworthiness based on its prior actions and broadcasts over the network, as well as nearby vehicles viewpoints [10]. Adversaries may attempt to spoof vehicles or manipulate vehicle data in such a way as to disturb the functionality of the network or the records of the victim vehicles. This can be incredibly dangerous to both the driver and the network relying on that vehicle's information. Table 2 lists the parameters that need to be considered in the design of a reliable consensus protocol in CAVs.

Currently, different trust models can be, and have been, applied to VANET systems, including entity-centric, data-centric, and combined trust models. The model used in [10] is entity-centric, meaning that it is concerned primarily with the vehicles themselves. Some potential assessment measures include a reputation-based system, as depicted in Figure 7, where every vehicle's weight is judged based on its past behavior in the network. The reputation of each vehicle transmitting data determines the validity of the transmission. There are three main message types in the network, including the following: beacon messages, which are sent periodically with simple driving status information, alert messages that are sent for emergencies and come in three levels, and disclosure messages, which are sent by witnessing vehicles and those with conflicting information [10]. By this model, underlying blockchain technology is the backbone of the system in regards to the security and stability of the system underlying vehicle operation in this model. Its inherent security, flexibility, and trust among users make it a natural choice, and one that could serve to solve many more common issues with current CAV technology.

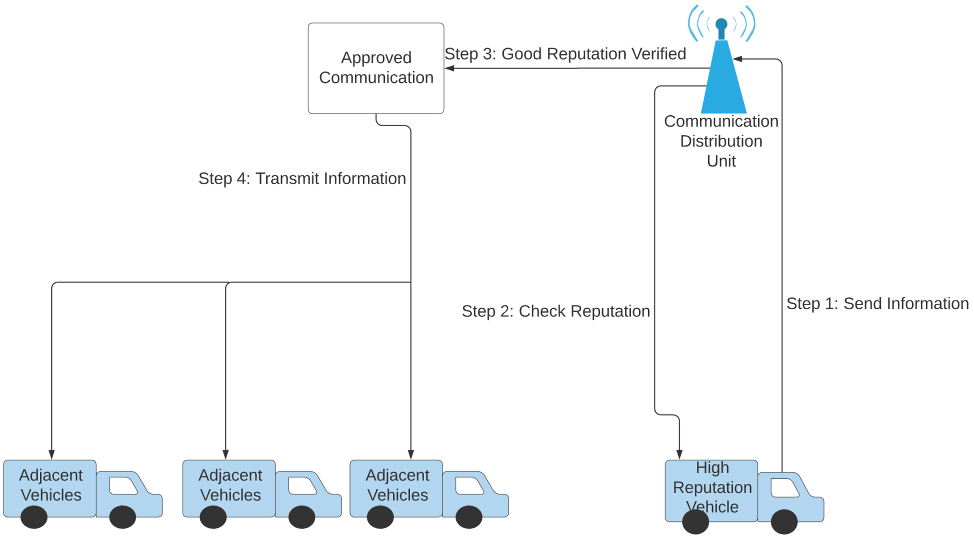


Figure 7. Reputation-based system for judging the validity of vehicles and their provided information on a network. This system is based on the past and present behavior of the vehicle and culminates in a score that is attributed to that vehicle.

Table 2. Considerations for consensus protocol involving CAVs.

Security against Known Exploits	Focused Validation Protocols
Low Communication Complexity	Vehicle Integrity Checks
Minimal Latency	Dynamic Node Tolerance
Resistant to DoS Attacks	Faulty Node Tolerance
Low Energy Cost	High Scalability
Consensus Finality	Fast Error Handling

The possibility of using blockchain in VANETs has also been noted by Leiding et al. [63], with them offering an approach based around peer-to-peer networks instead of the traditional centralized client-server architectural approach. Because blockchain inherently lends itself to decentralized approaches, it was noted as being a very promising potential choice. Decentralization is assured through the implementation of smart contracts, which function using an Ethereum blockchain implementation, with these smart contracts providing applications that make user vehicles perform operations that contribute to overall network decentralization by relying on several RSUs (road-side units) instead of a single entity [63]. Operations that are carried out may entail forcing vehicles to follow traffic rules or regulations, or presenting useful roadway condition information to drivers [63]. This heightened level of consistent control without reliance on a single party in operation ensures both the proper function of the system and connected vehicles and the stability and reliability of the underlying system, which makes this approach a very promising one to consider for future CAV use [63].

Any given VANET is heavily reliant on the reliable interaction between vehicles and, as a result, any malicious adversary interference could prove dangerous to the driver in question and other drivers in the system. To combat this risk, Singh and Kim [64] suggested implementing IV-TP into messages that are sent over the network, with their focus being to add needed security elements and data reliability. This element is represented as a singular, unpredictable number, which is chosen randomly and appended to any message sent in a particular communication. The researchers propose using a cloud storage solution that is based on blockchain to handle IV-TP communications. The authors note that the necessity for such a system derives from the fact that current vehicular ad-hoc networks use less secure forms of communication that can be accessed or manipulated by malicious adversaries, and that the proposed blockchain solution will provide a freely available and accessible ledger, secured via a Merkle tree and SHA-256 Hash with a consensus mechanism (PoW).

The new proposed system involves the use of blockchain technology, vehicular cloud computing (VCC), and a network-connected device (the vehicle). VCC operates as a form of hybrid technology, utilizing the resources that are owned by user-controlled vehicles, like their data maintenance and storage, computing power, and Internet-aided decision-making skills. In this case, the blockchain makes up much of the system and it has been divided into seven layers, similar to the popular OSI model that was used in the Internet.

An article written by Rathee et al. proposed a security method that made extensive use of blockchain technology in order to protect CAVs from exploitation [20]. Following this proposed method, blockchain technology would be used to protect user data security, as well as maintain a history of vehicle movement, decisions, and external conditions. By this implementation, blockchain technology is the main method of data protection, a job that has been noted to be extremely geared towards [20]. Similarly, Narbayeva et al. noted the applicability of blockchain technology to CAV systems [65]. The reasons for incorporating blockchain technology were supported in full with an analysis of past trends in technology to make predictions for currently developing CAV technology, as well as how many new technologies, like the Internet of Things and bitcoin, have made use of blockchain for data protection [65]. In addition to its user and producer trust, its ease of application and flexibility can be seen through its widespread use in a variety of fields to secure data and anonymity in transactions [65]. This flexibility, as discussed, makes it not only a safe and reliable, but a relatively easy and inexpensive to implement, technology [65].

In the past, blockchain technology has been applied with great success in security and it has been shown to be an effective means of facilitating the spread of information between several connected systems. Because of these traits, a study that was conducted by authors of [12] attempted to integrate blockchain technology with existing CAV traffic event validation systems to quickly and effectively secure vehicle information and eliminate misleading information exchanged by malicious vehicles [12]. To test the proposed system, the team tracked the number of attackers and the ability of the blockchain-based system to detect when users were generating malicious information, with the blockchain technology using a reputation-based system to track the trustworthiness of certain users based on their past actions [12]. The results gathered indicated that this system was very effective in distinguishing normal from attacker-generated data [12]. Its success heightens an area of particular importance for the use of blockchain technology in CAVs: attack mitigation and user safety. Based on these results, it can be said that blockchain technology has the potential to build greatly upon many previously concerning aspects of CAV operation and reliability.

Objects that are connected to a large-scale network are frequently subject to attacks, old and new, by malicious users, and CAVs have never been immune. Software vulnerabilities that are present in a given product are generally remedied through updates to fix known flaws, so the existence of a readily available system to provide such updates quickly and completely to all users is necessary. However, these updates must also be provided securely, with no chance of an attacker taking advantage of this system to infect CAVs. To meet security needs while ensuring that no vehicle is missed, Baza et al. [14] highlighted traits of blockchain technology that lend it to be used in such an application.

To explain the use of blockchain in finding a solution, the group outlined a firmware update scheme that uses blockchain technology to provide security in their releases and ensure that certain vehicles are not overlooked due to geographical location [14]. This system would use several distributors, vehicles that are rated highly based on their reputation in regards to its trustworthiness and driving history, to deliver new updates [14]. The reputation of vehicles would be recorded via the implementation of blockchain technology, ensuring availability and security to avoid the targeting of high reputation vehicles in attacks. The encryption scheme used would require that CAVs be authorized to install updates, and all of the updates would be secured via the use of smart contracts. Smart contracts can only operate via the use of blockchain technology and, as such, are known to be incredibly secure and well-used by people in electronically conducted transactions today. Blockchain technology serves as the basis for the scheme as a whole, again heightening its relevance and role in the future development of CAV operation, security, and safety.

Another method of providing secure software updates via the use of blockchain technology continues to use a cloud-based structure [13]. Wireless Remote Software Updates are, instead of tasked to several deliverers to distribute, available via cloud storage of a car manufacturer or software provider. In order to ensure the security of the update, the software provider begins a transaction, using its private key and a signature constructed via the signed hash of the software binary maintained inside of the cloud structure. Using this signature, the transaction is verified by overlay nodes within, and the manufacturer then signs the transaction. Following this, the overlay block managers supervising the public blockchain broadcast the transaction by checking the signature and ensuring that the manufacturer used the set private keys. Finally, the overlay block managers send out the transaction to all members of their clusters, and all of the connected devices can verify and download the update from the cloud storage. Figure 8 illustrates this process, providing security through the use of extensive checks instead of using outside entities to deliver essential updates [13].

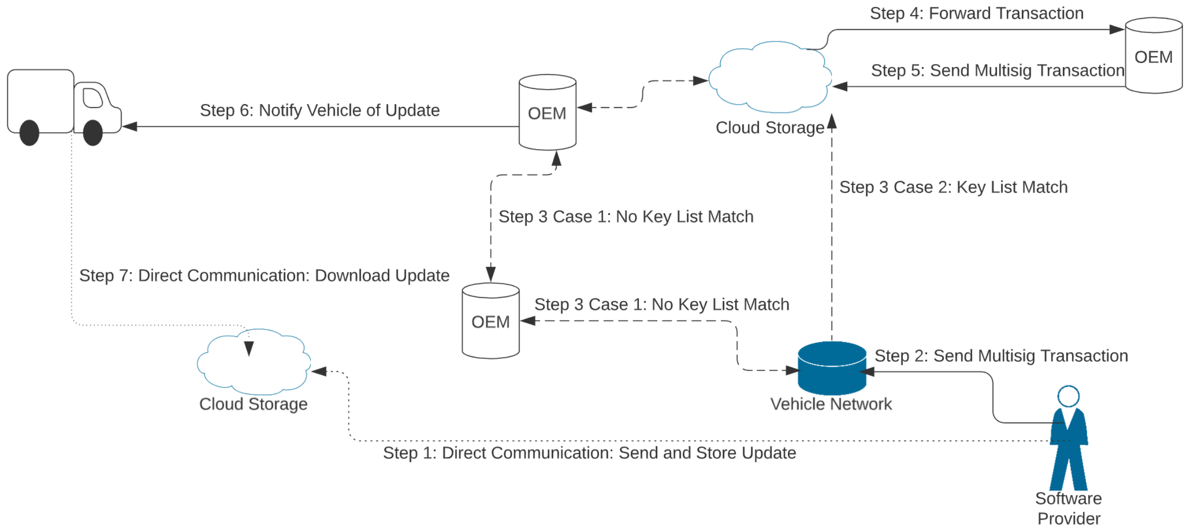

Step 4: Forward Transaction
OEM
Step 5: Send Multisig Transaction
Cloud Storage
Step 6: Notify Vehicle of Update
OEM
Step 3 Case 2: Key List Match
Step 3 Case 1: No Key List Match
Step 7: Direct Communication: Download Update
OEM
Step 3 Case 1: No Key List Match
Step 2: Send Multisig Transaction
Cloud Storage
Vehicle Network
Step 1: Direct Communication: Send and Store Update
Software Provider

Figure 8. A diagram showing how software updates are created, verified, and delivered to CAVs across the network through a cloud-based system, inspired by [13].

On top of securing user personal data, it is necessary to provide the security for the messages that is sent between vehicles. Vehicle-to-vehicle communications are necessary to keep both of the entities updated in traffic conditions and, in turn, mitigate accidents on the road. However, if these communications are compromised, so too is the network in the event of a malicious user carrying out attacks over these communication channels. Because of the huge risk that is involved in allowing vehicle-to-vehicle communication at this time and the significant benefit that this feature would provide to CAV capabilities, finding a solution that provides security while allowing these necessary interactions is a priority of many developers.

In response to this known issue, Rowan et al. [15] looked into a potential solution that incorporated many different technologies, including blockchain, to secure communication channels in CAV networks. The proposed solution outlined an advanced security system that made use of visible light and acoustic audio-based side-channel encoding to permit secure communications between two distinct vehicles, as well as using a PKI heavily based on blockchain technology to allow communication between unverified, potentially untrustworthy vehicles. In order to defend the use of blockchain, the researcher team expanded on its past capabilities in remaining secure and stable when faced with a heavy attack, as well as its proposed ability to verify information that is sent by untrusted vehicles through the use of available distributed hash tables maintained by each machine involved. Blockchain technology was incorporated for communication security and overall system stability and reliability. The implementation of the side-channels would focus primarily on the physical security of the transactions that were carried out by checking for and maintaining the identity and location information of a vehicle being communicated with. These numerous protections would allow immunity to RF channel jamming as well as physical attacks on the side channels through the double-check system, implementing blockchain on top of side channels to provide a backup if one of the systems is compromised through the use of the other one [15].

Singh and Kim [66] also brought up how the use of blockchain could serve as the solution for communication-based security vulnerabilities: citing its frequent use in similar security-based applications, as well as its high level of user trust that stems from its past reliability and flexibility between different fields. The proposed system is one that makes use of two types of blockchains: the main blockchain and a local dynamic blockchain, which each work together to store communications between vehicles. The local blockchain works in maintaining communications that are sent to it, sending any that it deems to be strange or out of the ordinary to the main blockchain, which will hold onto the strange data for longer than the local one is able to. This way, the local blockchain can continue quickly storing and maintaining understood data, while the rest is held for a longer analysis period by the main blockchain. By this method, the high power use concerns of blockchain technology are mitigated, allowing for proper network function and the security benefits provided by the blockchain. Overall, the proposed communication network would stay secure and reliable without consuming excessive data or compromising network operation.

Michelin et al. [17] suggested the use of blockchain architecture based on smart city operation, whose infrastructure connects through electronic means, allowing the city and entities operating within it to act in a more efficient, beneficial way. Smart cities need to account for all aspects of traditional cities and, thus, have to heavily consider how roadways and traffic will be controlled and maintained. Today, this is generally done through the use of advanced sensors that routinely monitor traffic conditions and let vehicles make fast, consistent, and correct decisions, helping all the parties operating in, around, or with vehicles [17].

However, the amount of data generated and analyzed by vehicles and the systems they operate over may have some unintended drawbacks. In fact, Michelin et al. noted that in the future, it would likely be possible for vehicles to create around 4000 GB of data per day [17]. Clearly, this much data requires an extensive, reliable system that is well-structured and built to expand easily when faced with greater content production, while still providing for expected security and privacy features that users need. While many systems have been considered to provide for this, there still fails to be one that provides for all necessary qualities of such a system. Eventually, blockchain technology was viewed more extensively in regards to this problem, and it was decided that it would be the best technology to use for system implementation.

Currently, SpeedyChain is a system under heavy consideration, providing measures for intelligent vehicles, elements that are present in smart cities in regards to traffic control (such as traffic lights), Service Providers (SPs), and Roadside Infrastructure Units (RSIs). Common blockchain activities, including transaction and block verification, are all controlled by system users that have significantly higher available computing power and resources than other entities, as well as those that work directly with the smart city to ensure proper operation [17]. The process of introducing new entities, like vehicles and similar network-oriented devices, as depicted in Figures 9 and 10, is well-outlined and customized, especially for blockchain-aided implementation to prevent any coordination problems. When vehicles are first added, they need to undergo a validation process conducted by an RSI, with the validation methods being performed by both the new vehicle and the city-based node [17]. In exchange, the vehicle gets its own block, which has its creation dictated by the blockchain itself. Following the block's creation, the vehicle can use it to request and respond to transactions, with all of the transactions being visible to the system.

Under the system defined, vehicles are able to create data for control or service-based operations. Vehicle control data are uploaded for the use of concerned parties, like traffic management or other vehicles, who wish to minimize the level of traffic in a certain area of the city. However, service data are used instead by certain verified parties who want to sell certain vehicle-related services to users, as well as letting users view statistics on their vehicles to ensure their proper operation maintenance [17]. However, as it stands, there are still numerous problems with vehicle-oriented blockchain technology, with a major problem being the concept of dynamism. To explain, when a vehicle is active, it is moving nearly constantly, so they hardly ever stay in the same exact place over a certain time period. Because location-based data are needed for the system to work, the researcher team came up with a possible solution: the system RSIs and SPs would both take on the role of providing for blockchain implementation, a role that suits them well due to their inherent rigidity and known reliability [17]. Whenever a node is first added to the vehicle system, the RSI, as well as all surrounding vehicles, need to guarantee that the node is valid. This process is called location-based trust establishment [17]. When performed, the process serves to validate the node's operation, which prevents the possible infiltration of malicious vehicles.

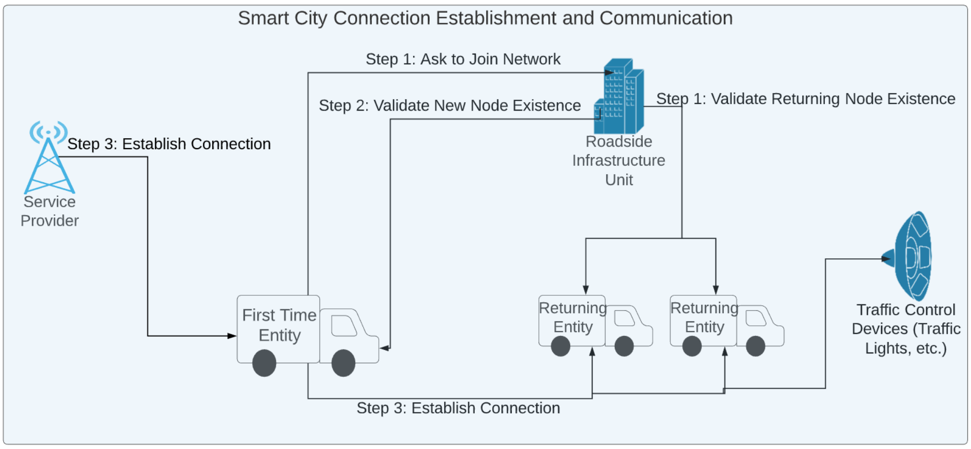

Smart City Connection Establishment and Communication
Step 1: Ask to Join Network
Step 2: Validate New Node Existence
Step 1: Validate Returning Node Existence
Step 3: Establish Connection
Service Provider
Roadside Infrastructure Unit
First Time Entity
Returning Entity
Returning Entity
Traffic Control Devices (Traffic Lights, etc.)
Step 3: Establish Connection

Figure 9. An example of a smart city infrastructure where all nodes, or entities, are capable of processing information and contributing resources to the overall network.

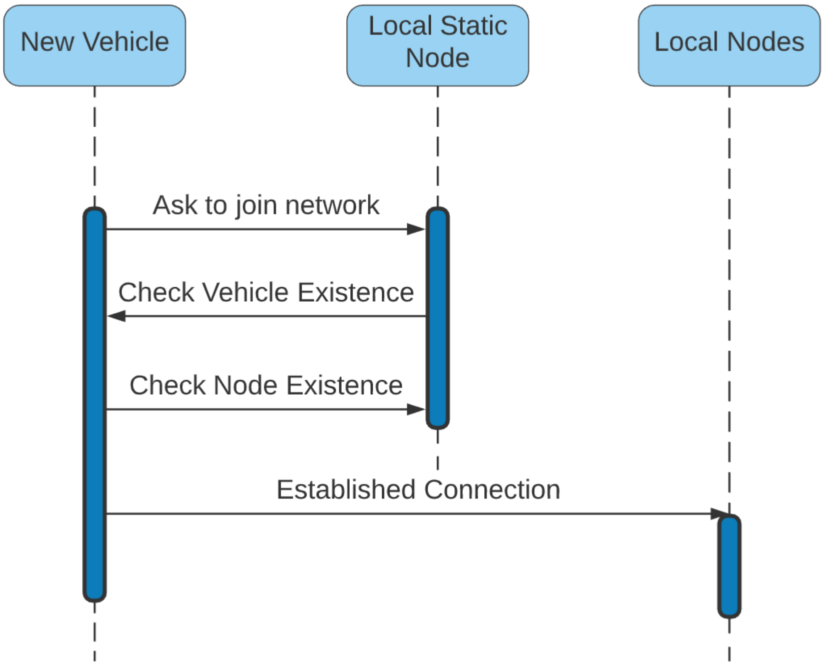


Figure 10. An example UML of a new vehicle entering a Smart City such as the one shown in Figure 9.

Smart cities have been noted to have great potential in improving their security through the use of blockchain technology in their device management system by Gong et al. [67]. Under this method, all devices, including CAVs, within the smart city network are managed under a blockchain-based system that facilitates safe and reliable updates, device control, and access only by approved parties that oversee smart city function and, overall, a secure and trusted network. Additionally, the blockchain implementation ensures the use of a peer-to-peer based system as opposed to one that is based on a single device, both aiding the reliability and protecting against data overflow and the security concerns that it could bring. Different protocols for use allow this system to communicate between any of the device types that are present within the smart city, which aids in communication, as well as device security and maintenance. In securing the network that oversees CAV operation via blockchain, the security and operation of CAVs are maintained by extension, showing that blockchain has a number of potential uses that can directly or indirectly help them function.

Through the previous discussion, it is evident that blockchain has extensive application to CAV security, as noted by several researcher teams and companies. However, all of these implementations differ tremendously, each with their own specific benefits and drawbacks. Table 3 shows a more complete discussion of each method of implementation discussed.

3.2. Financial Transactions and Enhanced Services

With many well-known uses of blockchain centering around securing financial transaction-related data [68–72], it is not surprising that researchers are already looking ahead at how this can benefit CAVs. Beyond proposed use in strictly driving and user safety security measures, blockchain technology has been identified as having immense potential in conducting financial transactions between users driving a vehicle and another entity offering a service to the user [23,73–76]. While it seems like a somewhat outlandish use upon first glance, after considering the number of transportation-related payments that need to be made by people on a day-to-day basis, it is clear that the extension of blockchain technology to this area could provide users with a number of new benefits that could save them time, as well as provide further accessibility for such features to users who may not have access to the type of payment that is required while using more traditional methods on hand [23]. Parking payments, insurance, tolls, and car rentals are just a few examples of common transactions that could be simplified and secured with less time, effort, and user confusion via the implementation of common blockchain technologies [23].

Because CAVs are an emerging technology, they will likely cost too much for average users. Similar to previous emerging technologies, commercial entities will probably be among the first to use CAVs, with prices dropping enough for general consumer use much later. Interested parties that first use this technology will likely offer services, like ride-sharing, to customers that are interested in seeing which industries the technology will head to first; Saranti et al. [18] studied the previous uses of blockchain in CAV systems, taking note of affected areas and those that might be next.

As mentioned, there is a lot of promise for CAVs in ride-sharing, in which companies save time and money by offering unmanned transport to customers. Saranti et al. then moved on to investigate another blockchain-oriented application, in which the technology was used to handle transactions between vehicles, facilitating communication through the system.

The system network is composed of several CAVs, all of which can send messages to a user directly through their phone. A user can access certain information through a mobile application, more specifically, the locations of nearby cars, as well as relevant information on the vehicle currently being driven. This consistent access to accurate information promotes user safety, with the added benefit of building trust between the user and their vehicle's security. In a case where a user wants to use the application to carry out financial transactions, users are also required to enter their own data and, if desired, make a coin ledger.

This coin ledger handles payments between the passenger and CAVs. The vehicle will be able to withdraw the required amount throughout the trip, cost per kilometer, or all at once at the end. When completed, the blockchain-aided transaction is transmitted to the network.

Viewing previous blockchain applications, like its earliest use in Bitcoin, its extension into the financial field surrounding vehicle-based transactions would be relatively easy to apply. As an added benefit, blockchain is most well-known for its widespread influence in securing payments between network-connected entities, and it already has a solid reputation among millions of satisfied users. As such, its implementation could also promote user acceptance of CAVs, allowing for further development in the field and a greater number of studies and system outlines focusing on its future applications.

Table 3. A comparison of selected security methods in terms of advantages, drawbacks, and type of blockchain used.

Model Proposed	Blockchain Type	Advantages	Drawbacks
BARS [10]	Certificate-based blockchain (CerBC) and revoked public key blockchain (RevBC)	Security and trust, authentication, low time/space overhead, anonymity and privacy.	Few results and performance analysis from few experiments and no large implementation.
Self-managed VANET [63]	Ethereum	Decentralized network, fast and reliable operation, no single failure point, secure communications, allowed user applica-tion use.	Customers charged fees for commu-nication and app use in Ethereum-gas, they pay for network.
Intelligent Vehicle Framework Model using Blockchain [64]	-	Security and privacy, IV-TP for speed. Records of communication, tamper-resistant, well-defined layering system for model.	No tests carried out, beyond system analysis, no results or space or time analysis.
Blockchain-based Connected CAV Framework [20]	-	Appropriate data hiding, transparency, data verification. Improvement in attack mitigation from previous methods due to blockchain.	Results from simulations only. No time/space analysis. Approach works well only after certain time interval. Many attackers can still compromise network.
Elliptic Curve Digital Signature Algorithm Based Approach [65]	Exonum	ECDSA securely inputs and validates information, blockchain secures vehicle state data.	No testable system, vague imple-mentation. ECDSA relies on users, but users can be unreliable.
Proof-of-Event VANET [12]	-	Higher success rate in attack detection and decision speed. Secured and pri-vate communications, but verifiable from transparency.	Performance is compromised when few vehicles are in an area. Physical tests not done.
Blockchain-Based Firmware Update Scheme [14]	Ethereum	Update scheme is peer-to-peer and hard to attack, many sources for fast updates, users are rewarded to maintain network. Effective and fast security, validity. Over- load prevented through peer-to-peer ar-chitecture.	No working model, so no tests done to see performance in real world. Users may not have update soon: some far from distributors.
Blockchain-Based Cloud Update Scheme [13]	Lightweight Scalable Blockchain (LSB)	Access to updates through cloud storage, updates verified for security and integrity, providers safely send updates to users, privacy, hash function prevents malicious node access. DDoS attacks are impossible.	Large overhead through various operations to check update security before download, cloud provides all software, which may compromise. No tests or implementation.

Table 3. *Cont.*

Model Proposed	Blockchain Type	Advantages	Drawbacks
Side-Channel Blockchain- Based Security [15]	Bitcoin	Side-channels with blockchain have many protections, if one is compromised, other is used. Physical security allows direct communications with nearby vehicles, can be applied to ensure features between vehicles, like proper spacing. Side-channel protects against wireless transmission interception.	Side-channels lost from outside conditions, causes insecurity. Low performance and speed. No extensive system testing. Vague implementation details.
Blockchain-Based Vehicle to Vehicle and Vehicle to Infrastructure Communications [66]	Branch-Based (Local dynamic and main blockchain combination)	Security in communications, user trust promotion by blockchain use. Branching is more lightweight than most blockchain, vehicles operate in real-time.	Test results are simulated. Vague implementation structure.
SpeedyChain [17]	SpeedyChain	Security with blockchain, integrity through hash functions and condition records. User privacy through timed key changes. System is immune to Sybil attacks and data tampering with SpeedyChain. Performance higher than that in Bitcoin blockchains, and others reliant on PoW.	Limited testing, no space and time analysis. Speed increases a lot with transactions when many vehicles are in a system.
Blockchain-Based Device Management Framework for Smart Cities [67]	Private Blockchain, similar to Ethereum	Data integrity and scalability through blockchain. Management system is applicable to any device type so each is secured. Energy use lowered with proof-of-stake to manage smart contracts. Outline detailed and accounts for many attacks.	No testing or estimated performance in real-world.

As Miller explained in an article that focused on the future adoption of blockchain into several different fields, blockchain technology, with its ability to allow and manage transactions securely and their details as permanent records, directly encourages the possibility of allowing CAVs to carry out transport-related financial transactions [77]. Miller went on to add that different transaction types, such as refueling or vehicle repairs, would be treated differently, with transaction rules differing depending on the exact type of service that is being provided to the user. Figure 11 shows a basic diagram of the model, which indicates the specialization of each individual process to make all transactions as simple as possible [77].

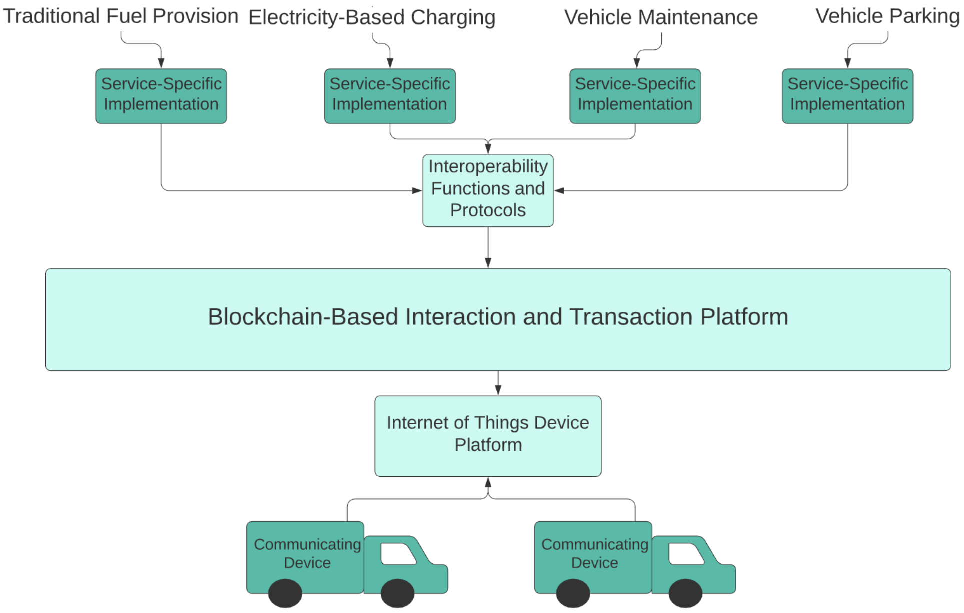
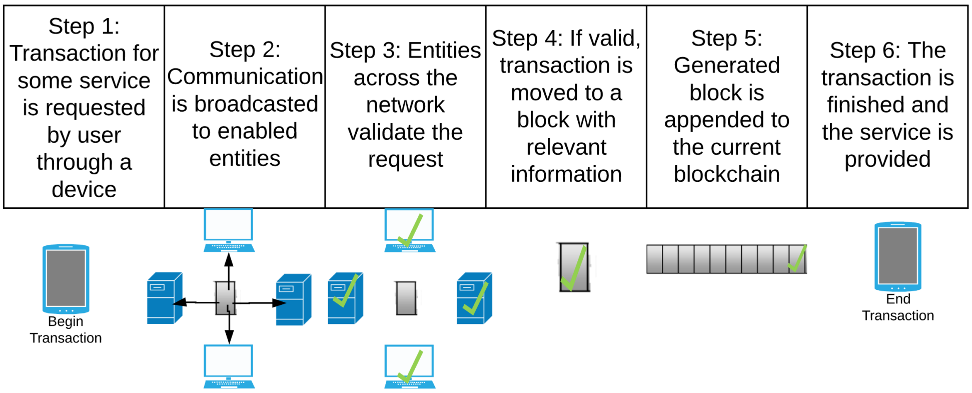

Traditional Fuel Provision
Electricity-Based Charging
Vehicle Maintenance
Vehicle Parking
Service-Specific Implementation
Service-Specific Implementation
Service-Specific Implementation
Service-Specific Implementation
Interoperability Functions and Protocols
Blockchain-Based Interaction and Transaction Platform
Internet of Things Device Platform
Communicating Device
Communicating Device

Figure 11. A model showing how transactions can be carried out and recorded through the use of blockchain in CAVs, inspired by [77].

A similar approach is brought up by Yuan and Wang, which also makes use of blockchain in meeting its goal [78]. In their paper, the potential of CAVs acting with the ability to get certain goods or services, like wi-fi or timed parking spots, through the use of stored cryptocurrency powered by blockchain is discussed in detail [78]. Via this method, it may be possible for people to make payments through the use of intelligent agents that act on their behalf, with these agents having all the specific information, like rules and algorithms, to actually carry out requested user transactions. This would greatly ease the process of making transport-related purchases, ensuring that users are never at a loss in how to carry them out, and CAVs are always equipped with the ability to facilitate financial transactions when desired. Because of this, the integration of blockchain-based cryptocurrency is certainly a promising concept and one that could serve to expand on the capabilities of CAVs greatly.

Companies have not ignored the potential for financial applications of CAVs using an underlying blockchain framework. In fact, IBM has begun contributing its own current blockchain-based architecture to promote the development of a system to access such applications [79]. Through this addition, the main goal is to provide security to the system, as well as the ability to create, end, and manage financial transactions with as much user ease of access as possible, as well as allow users to see statistics on their own vehicles in order to guarantee that everything is functioning properly [79]. The Car eWallet system, initially developed by ZF Friedrichshafen AG, is one that cites a huge number of benefits as the reason for the addition of blockchain, including its security, low processing power needs, validation of transactions, the constant and secured maintenance of transaction records, and the consistent availability of such information to only verified parties [80].

Easy user access to beneficial driving-related services, as well as ease of deploying such services to users, are both major reasons for more companies and users to use this network, and, with its broad applications to CAV technology, it could very well be a primary driving force towards user acceptance of CAVs as a whole [80]. Figure 12 presents a visual model of the transaction process carried out by this Car eWallet system.



Step 1: Transaction for some service is requested by user through a device	Step 2: Communication is broadcasted to enabled entities	Step 3: Entities across the network validate the request	Step 4: If valid, transaction is moved to a block with relevant information	Step 5: Generated block is appended to the current blockchain	Step 6: The transaction is finished and the service is provided

Figure 12. A diagram of the transaction-establishment and completion process, inspired by [81].

Transportation, while used on a day-to-day basis by most people, has a number of implementation-based flaws that limit its range of accessibility. In areas where public transportation is not an option, anyone who is unable to afford or drive their own vehicle is forced to rely on person-based transport, such as Uber or Lyft, which may not be desired due to concerns of safety in trusting complete strangers to drive them to their destination, or impossible in cases where no drivers live nearby. With the high level of activity that is required in the lives of many people today to go to work, run errands, and access certain services, consistently available and accessible transportation is an inviting concept. While working towards this goal, CAVs may face many challenges in moving forward, depending on their exact implementation. As companies jump on new CAV technology to provide their own businesses in on-demand autonomous transport, there is an inherent risk in this promoting a single transport platform, as has been seen in a number of other industries that are controlled by a few well-known giants that limit competition and promote centralization of the network and its data [21]. In such a case, if one of the major few platforms is compromised, an unacceptably large number of users will be affected, so a major goal of CAV system applications must be to promote many different transport options to discourage single points of failure.

Though many may argue that such a centralized setup is unavoidable in business, measures have been discussed further to promote decentralization, including the adaptation of blockchain technology. A concept that was presented by Catapult Transport Systems alongside the University of Sheffield elaborating on the benefits of decentralizing the transportation industry focused on how blockchain lends itself to use as a factor promoting this push on the industry [21]. Unlike many other systems that promote client-server network architecture, blockchain uses an architecture much more similar to peer-to-peer systems in enabling communication between entities. Making use of this system in transport-as-a-service applications would remove controlling entities, allowing for a collection of transport operators to moderate its use instead of putting all public trust in single entities [21]. This necessary application of CAV technology could be made more robust and reliable through these methods, allowing for its enhanced growth and development without compromising the desired decentralization of the CAV system and its use. In particular, blockchain has already shown itself to be well-trusted and used to promote decentralized networks in a number of other industries with great success across fields, so its use in more specific CAV applications would likely be met with approval from the public as well as researchers.

Similarly, Yuan et al. [82] emphasize the importance of having a decentralized Intelligent Transportation System, as well as the role of blockchain technology in ensuring it. The team also presents an outline for how such an architectural design would work, proposing a seven-layer model covering all aspects of the blockchain implementation that would be used. Unlike basic blockchain, this design is especially oriented towards an Intelligent Transportation System approach, which it accomplishes by providing a number of distinct layers. The physical layer is the first of these layers, which includes and secures IoT-enabled entities. Following it is the data layer, providing data blockchains and the ability to operate with or on them. Next is the network layer, which outlines the procedures in forwarding and verifying data and participating on the network. After the network layer is the consensus layer, which keeps track of and provides all necessary consensus algorithms and decides on the most appropriate one for any interaction. Layer five is the incentive layer, which works by motivating the network to keep up data verification efforts through the use of money-based rewarding blockchains that are granted to contributing nodes. The contract layer is used to maintain activating entities for specific blockchains, like algorithms and smart contracts. The final layer, the application layer, keeps track of different scenarios and use cases in the system. When combined, these layers form a comprehensive blockchain structure that allows for the construction and maintenance of an Intelligent Transportation System, aiding in the decentralization of CAV technology and applications [82].

When blockchain technology is considered in terms of CAV services, there are a number of different approaches that are opened up by its addition. For example, Liu et al. [83] has proposed the use of blockchain in enabling EVCE, electric vehicles cloud, and edge networks. This architectural model focuses on allowing the needed, easily opened and ended, communications between network-connected entities, while also allowing for certain other exchanges to occur. When vehicles communicate amongst each other across the network, they cannot only share information, but unused resources from a shared pool that can aid in the speed of operation and provide energy to vehicles that need it. In turn, providing vehicles are rewarded with energy or data coins, depending on what they have provided for other vehicles. These coins allow certain benefits, like greater access to the resource pool between vehicles, or lower prices for energy, which encourages users to contribute their unused resources more often. Roadside units serve as communication providers for the system, working in information exchange, and they serve to validate the information and enable transactions, as shown in Figure 13. Local aggregators have slightly different roles, both facilitating information exchange and serving as an intermediate body between an energy-providing power grid and the requesting vehicles to provide access to energy-exchange features, using available batteries to accomplish the latter [83].

The VANETs previously discussed have been noted to be particularly oriented towards the adoption of a financial transaction method, as they primarily act as huge networks of different user-owned vehicles, all of which may have different needs that can be met by suppliers. In their research paper, Benjamin Leiding and William V. Vorobev build on this, outlining a potential transaction-focused network architecture for use in VANETs, citing the number of areas in such networks that goods and services would be desired by users [84]. While similar networks are already in place after implementation by specific companies, they noted that these networks all have different requirements, standards, and methods of operation, which makes interoperability extremely difficult [84]. In order to remedy this problem, they proposed a single unified platform that allows interactions between vehicles and any other enabled devices, which makes the process of carrying out transactions much easier for users [84]. In addition, the proposed platform outlined the foundations of a system for auctioning such goods and services in cases where an agreement needs to be made on a price between a user and seller, providing greater flexibility in the types of purchases that can be made through CAVs [84]. The proposed method was also built on blockchain technology, culminating in a final outline for a network that is able to support full interaction between user vehicles and service-providing devices, letting them interact to their fullest potential by making purchases whenever necessary, regardless of manufacturer or exact object or service being bought [84]. Figure 14 shows a diagram of this system.

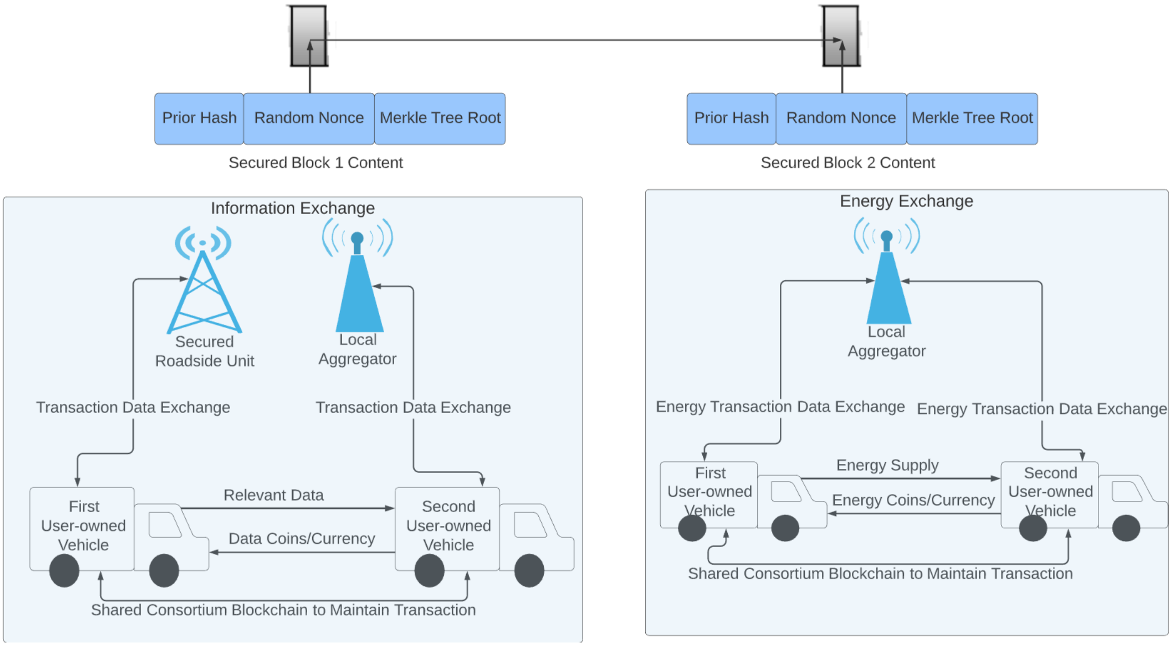


Figure 13. A model showing how energy and information is exchanged over the network using blockchain, inspired by [83].

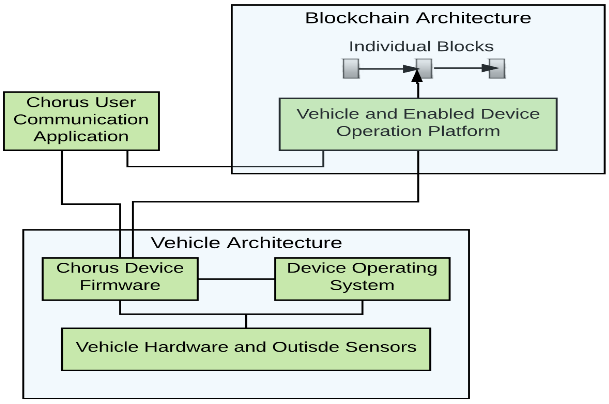

Blockchain Architecture
Individual Blocks
Vehicle and Enabled Device Operation Platform
Chorus User Communication Application
Vehicle Architecture
Chorus Device Firmware
Device Operating System
Vehicle Hardware and Outisde Sensors

Figure 14. VANETs setup via blockchain, inspired by [84].

Blockchain has been noted as being particularly useful in carrying out financial transactions, which has led to this described influx of different proposed models for how exactly it can be applied to allow for CAV transactions. While they all seek to accomplish similar goals, they all differ in the manner of implementation, and the exact provisions offered, which makes them all unique. Table 4 shows a comprehensive discussion of each method of implementation discussed.

Table 4. Comparison of selected financial transaction methods in terms of advantages, drawbacks, and type of blockchain used.

Model Proposed	Blockchain Type	Advantages	Drawbacks
Blockchain-Aided Transport Transaction System [18]	-	Public, accessible transport via CAV through an app, high availability in any location. Blockchain eases transactions, and can be applied to parking and tolls. Blockchain can also add security to transactions, peer-to-peer based.	Vague description, no real system details. Mentioned privacy, security, and ethical concerns with no exact solution. No time/space analysis.
Autonomous Transaction System [77]	-	A structure outlining a unique approach for each feature integration, ensuring no lax measures in optimizing each. Features contribute to ease of operating vehicles and increased accessibility to users who are not confident driving or performing actions relating to vehicles.	Very vague outline, no implementation detail. No time/space analysis, only base features.
Vehicle Transaction System [78]	-	Defined, comprehensive layered blockchain to cover all functions, blockchain allows new functions, like financial transactions for parking or wi-fi.	Vague outline, no implementation detail. No time/space analysis, just potential.
Car eWallet [79,80]	Hyperledger	Transactions are possible, service and good detection by vehicle, actions can be performed with little user effort, present use, testing, and implementation with great success. Security and records through blockchain.	The technology has not been very widely implemented yet, and many of its promised features have yet to be incorporated.
Decentralized Transport Network [21]	-	Comprehensive discussion of past implementation, different types of blockchain, and use in securing and allowing transport-based transactions. Predictions for future use and how it could be implemented, focus on decentralization.	Vague implementation detail, more a list of desired features, future growth, and potential based on past use.
Blockchain-Based ITS [82]	Ethereum	Intensive model to handle all operation of blockchain, discussion of past blockchain use and application, like decentralization, trust, and network device security. Decentralization greatly benefits potential services offered.	No actual implementation of model, no tests, and no time/space analysis. More focus on potential and under-lying blockchain than how it will be implemented with CAVs.
Blockchain-Aided EVCE [83]	Consortium	Defined resource-sharing models to further peer-to-peer transaction availability between cars. Encouragement of user contribution of data and energy. Decentralized, enhanced services, multiple security outlines.	No tests or implementation, and no time/ space analysis.
Chorus V2X Model [84]	Ethereum	Prototype implementation and testing. Blockchain use for security, blockchain enables service and good transactions, like transport or maintenance. Unified platform insures compatibility between networks. Flexibility in transaction details and execution. Requirement analysis.	No full system implementation, no time/space analysis, no testing carried out.

3.3. Driving Record Maintenance

In most areas of the world today, records of actions performed and their results are maintained and analyzed to come to important conclusions, such as how much damage was done in an accident, how much money is owed, and what must be done in reaction to certain events. In driving, this no different: traffic accidents are both extremely common and, in many cases, remarkably lengthy and challenging to document [85–89]. The introduction of CAVs with no event-recording measures will not necessarily help to remedy this flaw and, as such, many researchers have come to blockchain technology and similar technologies as a possible mechanism to overcome it instead. Providing evidence through accurate and secured records maintained in a database could greatly ease the current accident documentation process and issue insurance claims, determine who is responsible, and outline how reparations should be made [90–94].

With growing concern over the accountability assigned in traffic accidents involving one or more CAVs, there must be measures to avoid collisions and measures of tracking and securely maintaining information on crashes in the case that one still occurs. Accidents are not always recorded and documented effectively and, even when they are, it can be difficult to determine which parties were at fault. However, in the case of traffic incidents, this information is needed to determine what actions need to be taken to resolve the situation. From these needs, a system description from the authors of [95] emerged, focusing on the application of an approach that is based heavily on blockchain technology in maintaining records of vehicle statistics and decisions made to get a clearer view of events leading up to and following accidents to determine which party was at fault.

While not involving blockchain directly, it was the inspiration for a proposed method to take records of data, maintain these records securely, and promote the safety of CAVs and the people surrounding them [95].

Aste et al. noticed the same potential, saying that the use of unified databases to hold information are inefficient and ineffective when these databases have different information relating to the same case [96]. With the peer-to-peer based model, in which all vehicles present share gathered information, such concerns are mitigated, and the proof is ensured to be provided in a faster, more accurate, and reliable manner. Blockchain was chosen by them to be an incredibly effective method to underly such a system as well, citing its high security, ability to provide proof of existence, and maintained, up-to-date, and readily available information on transactions to verified parties. Data transparency, a decentralized network layout, and the adaption of blockchain technology to a storage facility for the information provided by a number of different relevant devices were all also reasons for its incorporation. Extensive prior use of blockchain in verifying and validating different entities before allowing them to interact is another benefit of the technology. This approach needs further consideration in the adaption of such record-maintaining structures to CAV systems [96].

Oham et al. outlined a similar approach to analyzing accident data for blame attribution [97]. This system manages to avoid several common errors in ensuring that parties are not wrongfully accused or let off for roles in accidents. The model described is resilient, relying on not one, but several parties, and it makes use of blockchain to validate provided evidence and enable only parties directly involved to present information. When accidents occur on the road, parties that are close to or involved in the accident can present evidence, information that they witnessed regarding the accident, including information that is related to time and location, and other factors gathered through visual and auditory sensors in vehicles. Blockchain, they explained, is a natural choice due to its inherent security and heavy use in data validation and decentralized networks. The peer-to-peer based system, in which all entities are able to present, agree on, and invalidate evidence presented makes it harder to miss specific crash details and, in turn, greatly eases the process of determining exactly what happened, who should be blamed, and who must be compensated. Figure 15 shows a basic model for this approach.

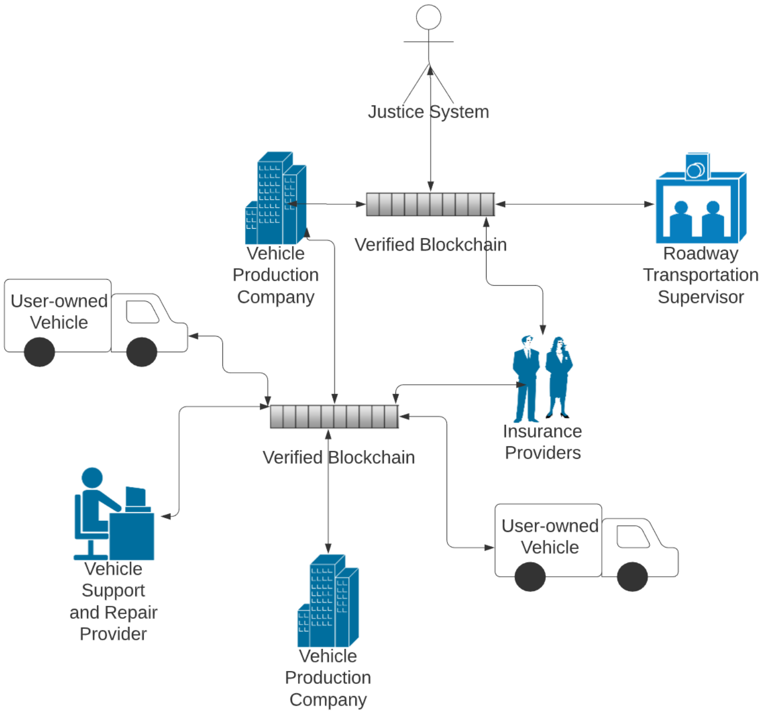

Justice System
Vehicle Production Company
Verified Blockchain
Roadway Transportation Supervisor
User-owned Vehicle
Insurance Providers
Verified Blockchain
Vehicle Support and Repair Provider
User-owned Vehicle
Vehicle Production Company

Figure 15. A model outlining the basic proposed operation of a blockchain-based information-gathering system to validate and collect accident details, inspired by [97].

Cebe et al. [98] also outlined a method of using blockchain to record events and information in the event of accidents, with this approach making use of a type of permission-oriented blockchain-based architecture, which guarantees the access to and use of vehicle-collected data only when necessary to analyze accidents, and only by parties with certain permissions. To continue providing the anonymity and security necessary in information sharing, aliases are assigned to any users participating in the blockchain, so their information will not be compromised. Information gathered can then be used to assess the entire event and, eventually, assign blame to guilty parties and offer reparations to those harmed. Because of heightened overhead in a variety of similar applications, the method accounts for preserving speed and processing capabilities by only requiring the hash values of data provided to be stored and shared in favor of the entire ledger. Figure 16 [98] outlines parties assigned permission to add, analyze, and access accident-based information.

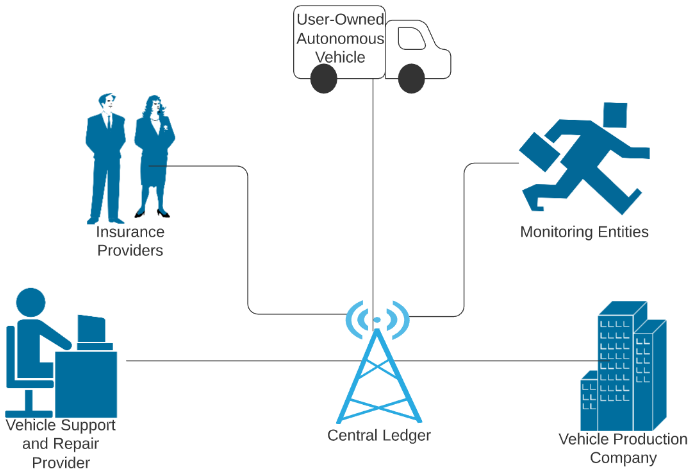

User-Owned Autonomous Vehicle
Insurance Providers
Monitoring Entities
Vehicle Support and Repair Provider
Central Ledger
Vehicle Production Company

Figure 16. Different types of users who may have permission to operate on or with accident-related data, inspired by [98].

In terms of event-recording in piecing together accident-based information, the method used must be both understandable and efficient in determining case-sensitive details. As mentioned, it can be difficult to prove what has happened in the case of traffic incidents, which is why blockchain has been viewed as a potential solution due to its extensive background in maintaining and validating records. However, when CAVs are involved, considerations need to be made for both the user and their vehicle in accident assessment. In other words, how much of the accident was due to the user, and how much was due to flaws inherent in the CAV itself?

M. Ugwu et al. proposed a new type of permissioned blockchain-based system to address concerns on how accidents can be assessed in such a model, with this system operating in a series of two tiers to promote the separation of different data types to their respective tiers [99]. As in permissioned blockchain networks, each entity involved in the accident assessment and recovery process has its own distinct permissions to add, edit, and view data, being allowed and restricted based on their defined roles. Each tier is made up of three classes of objects: those who send data, those who validate sent data, and those who monitor overall functionality and activity on their tier. Tier one deals primarily in exactly how responsible each party is for the crash, determined through communications occurring at this level. Following the full assessment at this level, each party's distinct roles are known, and the known information is moved to the second tier. Next, at tier two, the presented information is viewed and used in determining how exactly each party should be held responsible for their roles. This two-tiered approach is extremely organized and easy to view due to the clear roles, players involved, and task isolation in each area, improving the overall system's efficiency and activity. Figure 17 shows a model of behaving entities in the system [99].

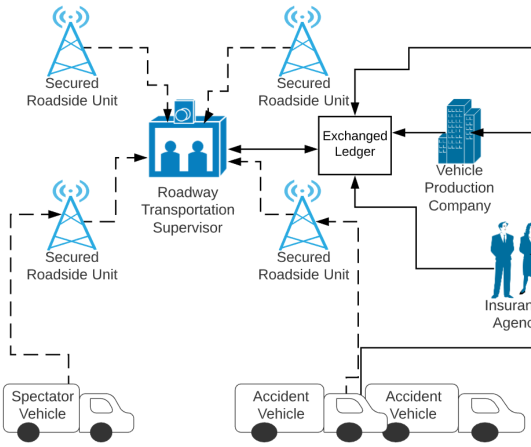


Figure 17. Different types of users who may have permission to operate on or with accident-related data under a tiered model, inspired by [99].

The implementation of a tiered system has shown promising results through its many benefits. In fact, it has shown numerous benefits over similarly proposed systems, like Block4Forensics, in its enhanced abilities in proving the existence of participating entities and their behaviors, entity involvement, and the ongoing activities of the blockchain underlying transaction control and validation. By these new capabilities, it is clear that blockchain is even more applicable to event-recording and validation in CAV systems than previously thought. If more thought is put into how exactly CAVs and the entities they work with specifically can benefit from various applications of blockchain technology, they can reach greater capabilities than ever before. Blockchain is applicable to CAV systems and outside systems that regularly interact with CAVs, so it must be thought of in terms of how it can be applied to both, not simply how it can be directly used in CAVs.

Insurance is often difficult for people to manage, and companies tend to have great difficulty in maintaining accurate information that is related to the driving history of an individual, especially in the case of undocumented traffic incidents and history of reckless driving. Claims that a driver has suffered some form of personal or property damage must be backed by extensive evidence, which is not always readily available due to the absence of constant surveillance among all roadways. Even today, when technology and electronic record keeping exists all around us, driving records do not necessarily have every single instance of traffic-related wrongdoing committed by an individual, but such information can prove itself to be extremely valuable in the case of damaging traffic accidents in assigning blame and determining future insurance rates for individuals responsible, as well as how individuals that are hurt can be properly helped by their insurance plan.

The use of blockchain in CAV insurance cannot be overlooked to remedy these flaws. To understand why, consider the primary function of blockchain: maintaining, securing, and allowing transactions. These transactions are maintained and they can be extended to recording specific conditions, like those that are internal or external to the vehicle in question in the event of a traffic accident. Automobile insurance, including that for future CAVs, is an area that could face great improvement from the addition of blockchain technology, as mentioned by Wang [100]. A consistent history of records with up to date information on vehicle actions, conditions, and location that is secured and accessible only by verified insurance-providing parties means that users can rest assured that they will be able to quickly and effectively claim benefits if they suffer harm or damages in an incident, and those insurance providers will have a simpler time accessing reliable user vehicle data and shifting prices based on user reliability. Kudwa has also assessed the future of blockchain in CAV insurance, who elaborates on just how far blockchain technology can be extended to such an approach [101]. His focus is primarily on the simplification of several auto insurance-related processes, including the ease of users in issuing claims, including those that are based on vehicle and personal injuries or damages. Figure 18 shows a proposed model of how blockchain would be used to assist in general claims [101]. As shown, the prior issue of gathering, verifying, and analyzing extensive proof is made significantly less taxing on all parties that are involved by the addition of blockchain technology due to its known accuracy, tamper-resistant nature, and overall security in the information recorded.

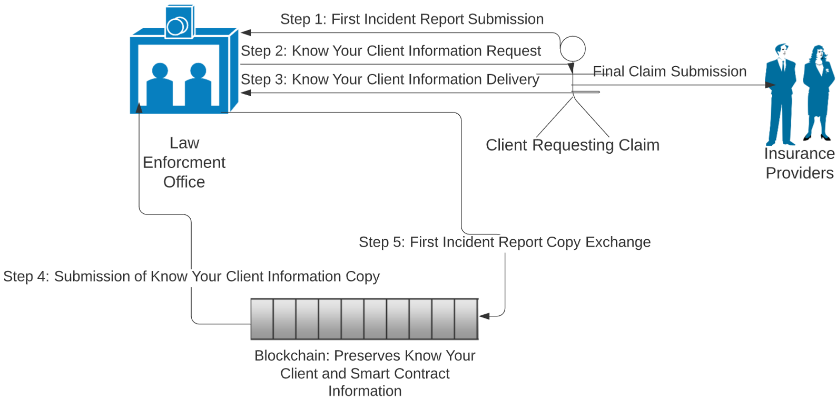

Step 1: First Incident Report Submission
Step 2: Know Your Client Information Request
Step 3: Know Your Client Information Delivery
Final Claim Submission
Law Enforcment Office
Client Requesting Claim
Insurance Providers
Step 5: First Incident Report Copy Exchange
Step 4: Submission of Know Your Client Information Copy
Blockchain: Preserves Know Your Client and Smart Contract Information

Figure 18. Information on how insurance claim processing and analysis can be benefited through blockchain, inspired by [101].

The potential use of blockchain in CAVs record-maintenance to resolve known problems in providing accurate insurance provisions is also noted in [102]. The constant maintenance of internal and external vehicle conditions and operations that are used by blockchain technology would be able to keep a collection of records, with these records being accessible if needed to present evidence of wrongdoing or traffic violation. In addition, this would greatly shorten the amount of time that is required to file claims and appropriately charge individuals responsible. Blockchain, above other existing means of maintaining such information, has shown great success in maintaining security and resistance to tampering of information, which would allow for access as needed as well as absolutely ensuring that no change has been made to the data recorded.

Consistent driving records that are reliable and accessible to verified parties is also essential in more specific operations. For example, as discussed in an article presented by Deloitte, blockchain-aided recording of delivery vehicles can provide companies or individuals with up to date information on when they can expect shipments to be delivered, as well as the current and prior states of this vehicle to inform them if something is amiss [103]. Additionally, in the case that a product is harmed through transport, internal vehicle conditions can be analyzed to determine so, proving that the customer had no responsibility for the poor state of the product and guaranteeing that they will be compensated instead of blamed for the damages. Similarly, customers will not be able to claim that a product that was damaged wholly by themselves was faulty upon arrival, as the internal conditions of the vehicle will prove that the package was secure for the duration of the trip. This allows for transparency in product condition, delivery status, and accountability in regard to damages, greatly aiding in the return process, as well as maintaining user satisfaction and company reliability.

Continuous vehicle status records also provide for a number of new features regarding vehicle rentals. In terms of leasing company benefits, the company can be sure of the past actions and track records of users prior to setting a rental price and allowing them to request certain vehicles. This setup also directly provides for the protection of safe CAVs operators in the case that a vehicle they were renting was damaged by an outside entity, which ensures that they will not receive full blame for the event in question. In such a way, responsible users and the companies that serve them benefit from this system.

The use of blockchain in transactions has already been noted as a primary reason for the technology by many, and this known benefit can be applied across most industries, including CAVs in the case of enabling and securing the generation and acceptance of contracts. The system that was outlined by [19] demonstrates the potential use of blockchain technology for allowing users to easily and securely make transportation-related agreements, letting them carpool, call autonomous taxis, and charge their vehicles without needing to perform such operations by more traditional, time-consuming means. This system is designed as a full-scale charging system, securing transactions and providing services directly between an CAVs and charging station, gathering essential user input with as little difficulty as possible.

Many people are still skeptical of the use of autonomous technology and so-called smart vehicles in maintaining user security, trust, and immunity to attackers. However, the adoption of such technology could meet these criteria and improve on existing measures in place in terms of availability and ease of access and use. Blockchain technology maintains records of all the transactions that take place, and its adoption in Bitcoin has already proven its safety and security measures. By traditional means, there is often a concern of what kind of currency a given service will require, with carpooling services ranging in whether or not they will accept electronically-made payments and, for some users, entering and exiting a vehicle to refuel or charge it can be a difficult or time-consuming task. Through the implementation of blockchain technology in allowing traditional transportation-based financial transactions to take place between machines with less direct user input, such actions can be simplified, allowing for user ease of use, access, and overall support of CAVs technology.

With the amount of attention blockchain has received in keeping secure and well-documented records of important data for later use, the focus on how this function can be applied to CAVs is not surprising. As a result, many different system outlines are available to study, test, and consider for further use, each differing in their exact specifications. Table 5 shows a table providing an overview of each of the outlines discussed previously in terms of advantages and disadvantages.

Table 5. Comparison of selected record-keeping and maintenance methods in terms of advantages, drawbacks, and type of blockchain used.

Model Proposed	Blockchain Type	Advantages	Drawbacks
Event Record System [95]	N/A	Invulnerability to many common attacks, detailed outline of system to maintain driving record information, accessible in case of accidents or calculating insurance information. Data can not be altered and is accurate based on information from several parties.	No simulated or real-world testing done. When no witness or verifier is present, the system does not record accidents. No time/space analysis.
Crash Data Record System [97]	Permissioned	High security, tamper-resistant, crash data collected and verified by several parties. Extensive security analysis and model outline. Accurate records for use by authorized parties.	No simulated or real-world testing done. No time/space analysis.
Vehicular Digital Forensics System [98]	Permissioned	High security and privacy. Mitigates space concerns by storing hash data. Maintains driving records for authorized parties in case of accident or insurance, which are accurate and assured by vehicle systems.	No simulated or real-world testing done. No time analysis, and hash value use means records are deleted after a time depending on storage in devices.
Layered Vehicular Crash Data System [99]	Permissioned	Well-defined, layered blockchain system to manage crash information, several vehicle reports used to figure out event, class separation of parties improves organization and efficiency of system. High security and reliability of data, conversation records kept between devices.	No simulated or real-world testing done, no time or space analysis.
Several Insurance-Based Blockchain Systems [101]	-	There are several different future applications discussed, like vehicle insurance claims submission and damage reports, with step-based outlines of how they work.	No actual full outline, more loose concepts on potential applications and a basic outline of how they work. Very few specific details.
Autonomous Insurance Claim Management System [102]	Permissioned	High security, tamper-resistant data, improved operation time, high data reliability. Working simulation with promising results.	Results gained from simulation only, no real-world testing. No space analysis or consideration.
Delivery Recording System [103]	-	Several different applications of blockchain in autonomous vehicle systems discussed, particularly in event record keeping. Extensive information on future uses and how blockchain helps.	No full system outline, more ideas on how blockchain can expand with vague application details.
Transport-Based Transaction System [19]	Ethereum	Architectural outline for full transport-based service providing network. Secure communication, fast execution time, method for privacy of users, and availability of communications that can be applied to let users buy transport-related services.	No simulated or real-life testing done. There are attacks it can be hit by, like overwhelming state channels by having a large user close all of its channels simultaneously or mass ignorance of certain communications by users.

3.4. Improved CAVs Operation and Energy Network Functionality

The arrival of CAVs, while widely anticipated by a number of consumers, has also been met with skepticism. Although they have shown a great deal of promise, it is difficult to ask users to put complete faith in their vehicle safely, especially following several noted failures to traverse roadways without endangering drivers or bystanders involved [104–108]. In addition, with the expected future automation of certain driving-related features, like recharging vehicles on the road, there are growing concerns regarding how these features can be handled safely and effectively with as little driver inconvenience and as much optimization as possible, with a number of existing system outlines and potential implementations [109–113]. To resolve such issues, many have started to look to blockchain technology for new solutions.

While CAVs have shown lots of promise in many areas of driving, they have also been shown to come into trouble when approaching and entering intersections [114] consistently. Intersections rely on a variety of complex rules that are easy for humans to process, understand, and quickly react to, but computer systems have difficulty in operating with the same speed and accuracy. Another factor making intersection navigation difficult to implement in CAVs is the amount of personal data that need to be analyzed in order to make important decisions regarding how to proceed, which raises numerous privacy and safety concerns from users. Of these issues, the latter relates closely to blockchain technology applications today and as such, a study that was conducted by Buzachis et al. [114] investigated how it could be implemented to aid CAVs operation.

Upon testing the discussed blockchain-based implementation of an CAVs system, the team found that the flow of information between CAVs was still too slow to provide reliable real-time decisions regarding what should be done. Latency faced a noticeable increase when met with greater send rates and user interaction, with it eventually increasing delay to the point of being unacceptable for real-time use in potentially hazardous driving scenarios. However, this does not necessarily mean that blockchain technology has no potential for future use in the area. As was discussed at several points throughout the experiment, blockchain technology is not unacceptable for priority-based decision making in complex roadway situations due to its own inherent flaws and incapabilities: the software and hardware limitations today prevent it from making these decisions in a reasonable period. With the constant and consistent evolution in software and hardware capabilities today, it is still completely possible that blockchain-based approaches will prove to be successful in meeting this currently unachievable goal.

Buzachis et al. [115] presented another proposed method to guarantee better CAVs operation, dealing with CAVs navigation of intersections. This one focused on the use of smart contracts to oversee the security and privacy of communications, relying on the underlying blockchain technology. Here, CAVs are overseen by a multi-agent autonomous intersection management system, known as an MA-AIM system, which requires the use of a specific entity, an intersection manager agent, assigned to a given intersection, in order to provide direction to each vehicle operating within its range. Of course, if not secured and protected from alteration, these communications could easily be compromised by malicious users, with potentially fatal results. The communications between adjacent vehicles, as well as those between vehicles and the intersections they operate across, are essential to this approach. Thus, blockchain technology, as well as smart contracts that are based on them, are utilized to provide security.

Similarly to real-life traffic situations today, there has been some trouble in ensuring that vehicles on the road are placed with enough space to ensure safety in the case of sudden braking to avoid obstacles. Humans are not always as responsive as necessary to avoid collisions that occur in crowded roadways, so the possibility of using CAVs technology to ensure that sufficient space is always allotted between adjacent vehicles could result in a significant decline in the number of accidents that occur. In response to such concerns, Robin Westerlund made use of an Ethereum blockchain-based system to keep track of where vehicles are in relation to each other and ensure that no boundaries are crossed during operation [31]. Through the tests conducted, Westerlund was able to demonstrate the high level of security, reliable and correct operation, and acceptable time and space use provided by the proposed system [31].

Another major source of error for CAVs today is the logic surrounding their lane change operation, as the act of switching between lanes is an inherently complex operation due to its dependence on a variety of internal and external factors [26]. Information transfer is greatly hindered by this, as the sheer amount of information that a system needs to track can be overwhelming, and even the slightest mistake or delay can lead to a collision. The data collected can also be excessive and even dangerous in the eyes of users who do not want information on their location and driving habits made known to hackers or other malicious parties.

While blockchain technology has certainly been very promising, it also relies on the use of extensive record maintenance and ledger updates to operating effectively, which presents problems in the energy use and response delay of CAVs [116]. Energy use is a huge hindrance for many vehicles and other devices today, so it cannot be ignored when present on such a major scale in an entire class of developing technology. It is not enough for CAVs to be secure and safe for users: their energy consumption must also be a factor that is considered before their full implementation. In addition, the significant number of transactions occurring at any given time over the network has dangerous implications for the network as a whole. The potential for network overload contributes to overall instability, as well as providing an opening for attackers to misdirect drivers and compromise user information. In such a case, regardless of the security and safety benefits provided by the implementation of blockchain technology into CAVs systems, it would be far too risky to use. However, at the same time, the number of transactions cannot simply be reduced without further thought. This would risk eliminating any of the beneficial aspects that are provided by blockchain technology, which makes its use pointless. Because it is not possible to prioritize either of these aspects without drastically compromising the network and devices on it, there is no truly secure way to implement blockchain technology into CAVs systems until its excessive energy-consumption and rate of transactions can be resolved.

Responding to energy-use concerns, Sharma came up with a method of drastically reducing the number of transactions that are carried out over blockchain without compromising its many benefits. Figure 19 shows a model of the approach, labeling several points where energy can be further conserved to allow improved efficiency. By his method, the number of transactions and overall energy-use would be reduced via the use of his designed distributed clustering model, with calculated 40.16% energy conservation on average and an 82.06% reduction in the number of transactions. The model does this by utilizing the optimal slots to update blockchain ledgers instead of choosing any slot indiscriminately, which is found via the use of an optimal transaction model selected from Cluster Heads. As noted, this potential reduction in energy use and the number of transactions carried out across the CAVs network would greatly increase the efficiency, speed, and overall operation of these devices, which makes it an extremely promising method to consider for blockchain implementation.

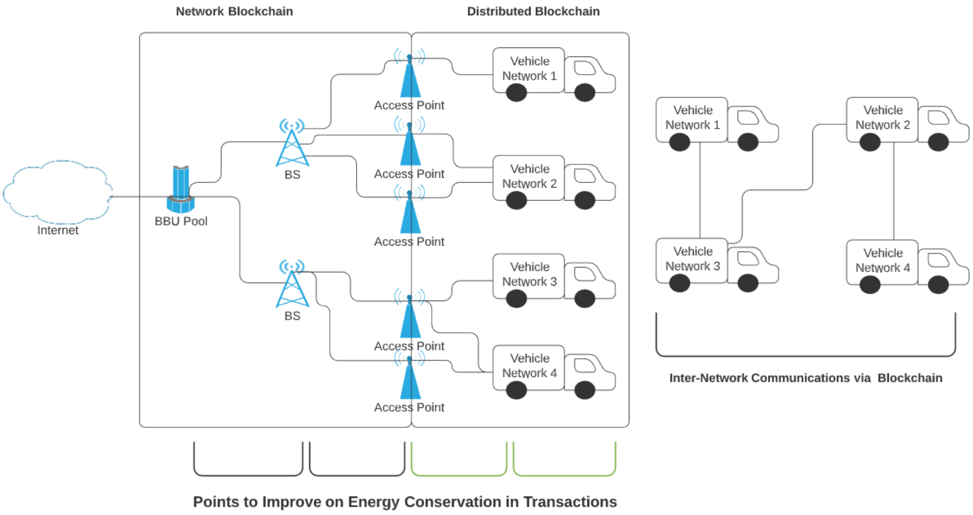


Figure 19. A model showing the structure of the areas of the CAVs network where energy use can be improved, inspired by [116].

Charging systems put in place to provide for consistent and reliable energy provisions in the case of requested transactions must also be assessed before CAVs systems as a whole can function effectively. In order to understand why, keep in mind how many vehicles may be completely autonomous in the future, and how this may open opportunities for the overload of charging stations and their resources. In such a case, the network itself may become compromised, and vehicles in need of energy may be unable to access it, compromising the operation of vehicles across the network. Energy-allocating transactions need to be readily available, presented via a scalable and resilient system, and immune to overload.

Looking to find a way to ensure this functionality, Jin et al. noted that blockchain technology is not only useful in CAVs themselves: it has a variety of traits that would benefit the operation of charging stations. Using it, energy can be provided to vehicles via a decentralized network, with ensured security and operation, very closely mirroring the architectural layout of CAVs systems as a whole. Inherent scalability, flexibility, and security present in blockchain technology have made it very well suited for such use, so it is certainly worth further consideration in terms of this application.

Charging system optimization is, as mentioned, a strong factor in determining the optimization of CAVs systems as a whole, since by improving their efficiency, CAVs will be able to operate more efficiently while still providing for the safety and health of our world in terms of environmental impact. To address concerns about the current capabilities of energy-providing units, Su et al. [117] designed a comprehensive system that works to provide a charge in a specialized, user-specific way, which guarantees that any given car will receive the optimal treatment and that charge-distributors can function with greater effect and efficiency. With the incorporation of blockchain in the system, the security level is guaranteed to carry out needed transactions, mitigating energy use concerns by implementing a permission-based model that avoids the use of an outside entity to overlook transactions. In addition, the authors discussed the possibility of using a consensus algorithm, called a delegated Byzantine fault tolerance algorithm, which heavily cuts the amount of energy that is used in carrying out transactions. Transactions are similarly carried out via blockchain to ensure the reliable, secure, and decentralized approach that is desired, with records of transactions being secured and always maintained. Figure 20 shows the results from analyzing the proposed model and previous methods for utility relative to the cleanness and environmental-consciousness of energy in use [117].

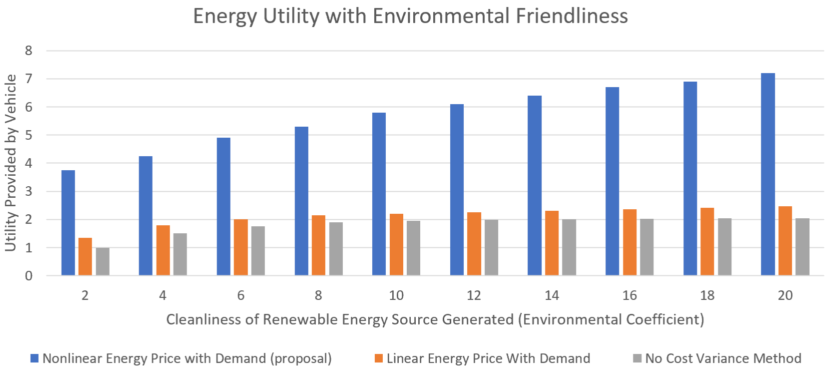


Figure 20. A model showing the environmental impact and utility of charging stations behaving under different methods, adopted from [117].

The concept of energy exchange between distinct CAVs and defined charging units or other charge providers has faced significant improvement from blockchain technology use. In an article that was presented by Javed et al. [118], an entirely new framework to charge vehicles, called a Mobile-Vehicle-to-Vehicle method, was outlined, which facilitates decentralized charging between network entities, and showed marked improvement in data security, transaction speed, energy cost, and ease in locating and accessing charge providing units for users. THe benefits listed are accomplished through, among other factors like improved algorithms, the incorporation of blockchain technology. An example of its benefits in relation to the costs of vehicles traveling overall based on the number of vehicles moving is shown in Figure 21 [118]. Underlying blockchain was used primarily in security, but also ensured user trust and approval through its extensive past use in known technologies and marked reliability, as well as its transparency in letting users view ongoing transactions in terms of who is sending and receiving information. Its implementation is an absolute necessity in this case, as, without the stability and security it provides, this charging system would be dangerous for its users, and, thus, not a feasible option for implementation [118].

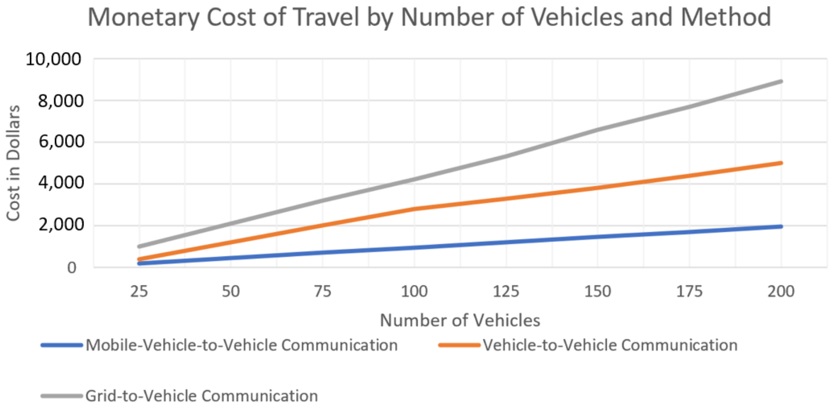


Figure 21. A graph showing the cost to transport CAVs based on method, adopted from [118].

Another example of the use of blockchain-based scheduling optimization in benefiting the energy-exchange process is shown in an article that was presented by Huang et al. [119]. In this case, a consortium blockchain-based architecture is used to define the presented charge schedule, which aims to optimize the efficiency and utility of charge stations and their users. Similar to the method that is discussed above, blockchain is used primarily in its decentralized network promotion, as well as its inherent security and promotion of user trust and transparency. Figure 22 shows a base outline of the discussed approach to charging hybrid EVs, and, as pictured, involves a number of different entities that behave in distinctly specified ways. Under the hybrid-based system, many different charging methods can be used, such as vehicle-to-vehicle and mobile charging vehicle-to-vehicle style transactions. By this method, the charge would be available to vehicles, regardless of type, model, and individual vehicle capabilities through the offer of a variety of charging methods instead of expecting all to follow a singular style best.

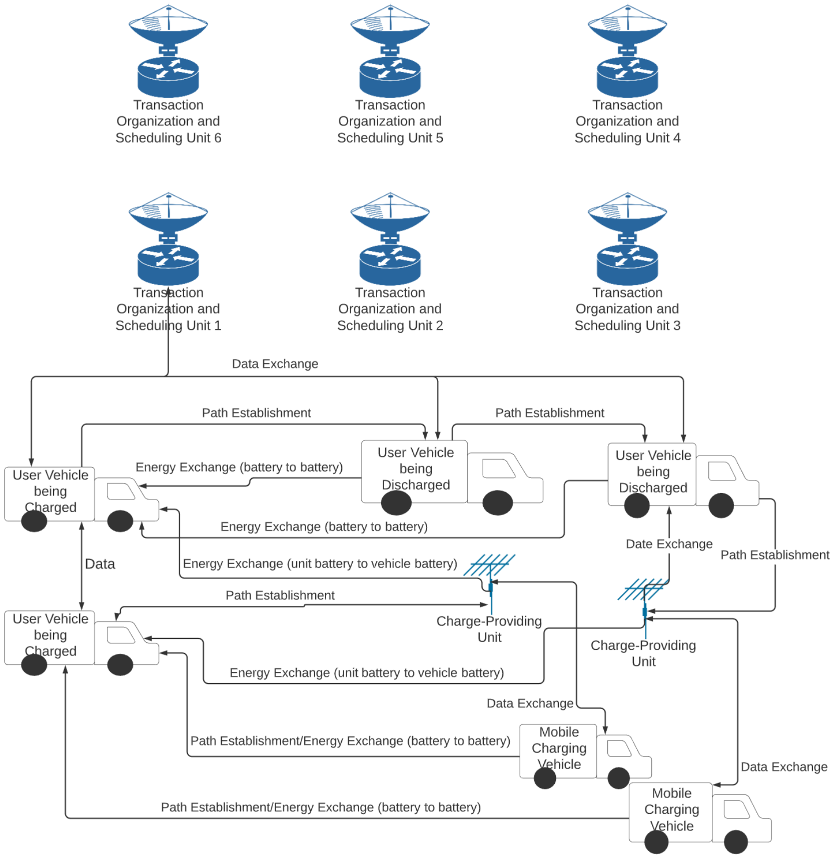

Transaction Organization and Scheduling Unit 6
Transaction Organization and Scheduling Unit 5
Transaction Organization and Scheduling Unit 4
Transaction Organization and Scheduling Unit 1
Transaction Organization and Scheduling Unit 2
Transaction Organization and Scheduling Unit 3
Data Exchange
Path Establishment
Path Establishment
User Vehicle being Discharged
User Vehicle being Discharged
Energy Exchange (battery to battery)
User Vehicle being Charged
Energy Exchange (battery to battery)
Date Exchange
Path Establishment
Data
Energy Exchange (unit battery to vehicle battery)
Path Establishment
Charge-Providing Unit
Charge-Providing Unit
User Vehicle being Charged
Energy Exchange (unit battery to vehicle battery)
Data Exchange
Mobile Charging Vehicle
Path Establishment/Energy Exchange (battery to battery)
Data Exchange
Mobile Charging Vehicle
Path Establishment/Energy Exchange (battery to battery)

Figure 22. A diagram presenting the overall layout of the hybrid-based vehicle system, inspired by [119].

Open-source, usable networks for charging electrically-powered vehicles have not only been proposed; some have already been put into place. The first example of such a network was provided by the Energy Web Foundation (EWF), which put forward the energy-based blockchain system, called the Energy Web Chain [120]. With its network, the EWF hopes that energy can be provided to vehicles via an efficient, cost-effective, and overall accessible and optimized process that, in turn, contributes to the efficiency of the vehicles in using themselves. German-based company Share&Charge has also implemented its own network, which is called the Open Charging Network (OCN), to provide electric vehicles with fuel via the use of an expansive, mobile network [121]. Among other methods and technologies, blockchain technology was a huge basis for the design of the OCN, its security, mobility, and broad scope of applications causing it to have significant attention in such areas.

With its heavy recent growth and success, it is extremely likely that this technology will soon also be applied to CAVs. In this case, the optimization of the charging system needs to be given just as much thought as that of the CAVs system, since charging will be a central part of the proper operation of CAVs. Open, decentralized networks to provide energy must be available, reliable, and presented in a user-friendly manner, while not compromising the speed expected in carrying out energy-based transactions.

The difficulty faced by CAVs attempting to change lanes safely has already been noted and studied by a number of individuals and organizations, all rushing to find a way to combat this flaw. In response, one study, which was conducted by Fu et al., decided to implement blockchain technology into a more generally used machine-learning approach in an attempt to expedite the process [26]. In this implementation, they made use of vehicular blockchain in tandem with a deep reinforcement learning model, which acted to secure and protect data collected as it related to the user. This information gathering style allowed for users to remain anonymous and completely secure without sacrificing the educational benefits offered by having access to numerous sources of information relating to CAVs progress and behavior. Using this method, it was expected that users would have fewer privacy and security concerns about CAVs, be more willing to participate in data collection on their vehicles for research purposes, and that the information gathered would be shared between CAVs more quickly and effectively, all of which would lead to a shorter learning period for CAVs, and in turn, fewer accidents.

In order to test this idea, the group assessed the security of two separate groups: one using a collective learning approach without blockchain technology, and the other implementing blockchain technology to aid privacy and security. From the security tests conducted, it was shown that, when compared to the collective learning approach, the CAVs following the blockchain-based approach had a notably higher success ratio in changing lanes as malicious nodes were added to produce faulty and harmful data. The results showed that blockchain technology improved the safety and privacy of user information, supporting the use of blockchain in further development in the lane-changing capabilities of CAVs [26].

The use of blockchain has been applied and proposed for use in a variety of systems aiming to benefit its potential applications, as well as how well resources that are involved in such operations are maintained and utilized. As discussed above, these system and method outlines, while often similar, are never the exact same in how they are applied or what problem they aim to solve, and each has its own specific strengths and weaknesses. Table 6 shows a comprehensive discussion of each method mentioned above and how they relate to each other.

Table 6. A comparison of the selected previously discussed blockchain-based improvement and energy use outlines in terms of advantages, drawbacks, and type of blockchain used.

Model Proposed	**Blockchain Type**	**Advantages**	**Drawbacks**
Hyperledger-Based Intersection-Traversal Algorithm [114]	Hyperledger	Working logic to determine priority and order, peer-to-peer structure to avoid overload or single failure point. Secure transactions and communications.	Operation time is too slow for real-time response, and unusable as a result.
Multi-Agent Autonomous Intersection Management System [115]	Private Hyperledger	Secured communications between vehicles and other vehicles or infrastructure-governing devices, in-depth explanation of how intersections are controlled to avoid collisions.	No tests or working implementation yet, no time/space analysis with roadway conditions.
Blockchain-Based Collision Avoidance [31]	Ethereum	Extensive testing and traffic reduction, and in turn, greater safety for drivers. Relatively high security and acceptable time and space use.	No real-life testing, only results are from simulations. Plaintext private keys, and anonymity is not ensured.
Blockchain-Based Collective Learning for Lane Changing [26]	-	Secure communications and group-based information retrieval, high malicious node detection and information reliability, higher lane change success rate, improved execution time and space.	There is greater difficulty in finding malicious nodes when they comprise a larger part of the network, so performance slightly degrades. All tests are simulated, there have been no real-world tests. No full execution time/space analysis.
Energy-Optimized Blockchain System [116]	-	Improved energy use, and reduced transaction number with no performance loss. Less network strain and high security in transactions. Extensive resource-use and performance consideration.	Limited testing, all results thus far are simulated, wide-scale testing is needed.
Blockchain-Based Energy Trading Network	Ethereum	Well-outlined energy management and exchange system outline and simulation testing. Ability for several different transaction types for energy, like bidding and offering in auctions. Decentralized network to avoid overload and single failure point. High security and trust.	All testing done through simulations, no real-world condition test. No considera-tion for how full network will operate, just individual energy-providing units in it.
Permissioned Energy Blockchain [117]	-	Improved energy management through use and demand analysis, decentralized network. High security, consensus, and information reliability through reputation analysis. Optimized charge station utility, and overall optimized use in turn.	Little testing has been carried out on this model, no real-world implementation, all results are simulated so far.
Energy-Exchange System [118]	Consortium	Decentralized system, reduced cost, and improved utility of charging systems through optimized charge schedule. Blockchain ensures security and trust, rewards given for active participation in network, and lowest distance from vehicle to charging system is calculated when needed.	All tests are simulated, may be inaccurate to real-world results. The model is not optimized, and presents concerns of high resource use that may drain the network or compromise security. Security can still be improved, as mentioned.

Table 6. *Cont.*

Model Proposed	Blockchain Type	Advantages	Drawbacks
Scheduled Charge System [119]	Consortium	Improved operation of charge stations through charge schedule algorithm. High security and privacy, user benefits through demand and location considerations in determining a price, as well as hybrid architecture allowing for charge for all vehicle types.	All testing is done through simulation, no real-world analysis. No space analysis for proposed system.
Blockchain-Based Energy Network [120]	Ethereum	Implemented energy system, high security, detection of malicious nodes, energy efficiency and high scalability, accessible and cost-optimized energy for users. Open-source implementation for increased user access.	Limited implementation to a few company systems, not available to the public on a wide scale. Fairly new, so there is limited testing and performance analysis.
Blockchain-Based Open Charge Network [121]	Ethereum	Implemented network to charge user vehicles, open-source and highly available to users. High security, scalability, and lack of unnecessary additional middle parties in carrying out transactions. Fairly large-scale public implementation.	Limited use and test results due to it being a relatively new technology.

4. Application of Blockchain in Collective Decision

Before their full deployment, autonomous vehicles must have both individual and group operations that are assured to be secure. After all, the majority of accidents that occur require more than one party, so there must be a way to allow for autonomous vehicles to decide what maneuvers to make with other parties in proximity to avoid accidents. While many solutions have been posed, all with their advantages and drawbacks, blockchain has been applied rather extensively in this area through a variety of applications, highlighting its ability to allow the safe and consistent operation of a variety of related parties within a group.

There are not many methods of ensuring well-timed, secured communication between distinct devices operating in a group, as mentioned previously. Many researchers have noted that while devices may work adequately when operating alone, incorporating a group is a much more difficult topic, as a great deal of the rules underlying their operation are based upon human cues that are not readily understood by machines. As a potential solution to such group-based operation problems, blockchain has emerged and been employed in common group-based exercises to test its ability to govern such interactions. For example, an experiment that was conducted by Moran Cerf, Sandra Matz, and Aviram Berg, which incorporated its use into a Public Goods game, showed that its use of Smart Contracts allowed operating entities to understand and take opportunities that yielded better results [122]. Under different rule sets, this logical operation could be applied to vehicle systems as well, allowing them to avoid collisions and operate optimally on the road, securing the safety of all group entities and their passengers.

Cooperative decision making is essential to a variety of different systems, including swarm robotics, in which blockchain has already been extremely successfully applied [123]. The secure and consistent control of these autonomous devices was one of the main features keeping it back, but, with the application of blockchain technology in the field, many of the underlying problems were overcome due largely to the security, flexibility, and scalability of blockchain, as well as its low resource use when using its Proof-of-Authority algorithm [123–125]. Through an experiment implementing it into the decision-making process, it was shown to excel in this area, allowing for different parties in the swarm to communicate seamlessly, and thus avoid colliding and allow work in an intelligent manner [123].

Similarly, this use of blockchain to encourage cooperation within a system is maintained by studies conducted by Malavika Nair, and Daniel Sutter [126]. Starting by outlining the history of blockchain, its more common uses today, and its predicted growth, their paper discusses the potential impact it will have on other group-oriented applications [126]. Through past uses of blockchain, it is evident that, as it continues to be implemented into such problems, it will greatly contribute to entities' ability to communicate quickly and securely over a network, making it a promising choice in future studies regarding AV group operation. This expectation is due to its strengths in allowing crowd-based applications to thrive, in addition to it consistently providing users with expected security and privacy needs [126].

Blockchain, by its very nature, lends itself to use in ensuring the cooperation of autonomous entities, as emphasized by researchers in [127]. Their study, which begun with the goal of finding an efficient, scalable, and effective way to allow the control of large groups of robotic entities, arrived at the conclusion that blockchain would serve as an effective means [127]. This conclusion was reached due to the known benefits blockchain has above similar methods in privacy, security, and decentralized network incorporation [127]. Through its incorporation, it is reasonable to expect that its incorporation may also gain such benefits into AVs, which would be a significant step forward towards their wide-scale implementation and acceptance.

Even more specifically, blockchain has had its use proposed in ensuring the safety of vehicles operating in a platoon, a group of closely positioned operating vehicles. One project involved its use in maintaining these platoon vehicles' safety needs while simultaneously making them secure from information-stealing and attacks [128]. Both of these traits, while being necessary to AV operation, are often viewed as mutually exclusive, since the increase of one tends to imply the relapse of the other, but, through the use of blockchain, it is expected that both of the requirements may be met [128]. Such advanced operation would allow for the hastened and safer deployment of large-scale AV structures, making blockchain incredibly desirable incorporation.

LIPS (Leadership Incentives for Platoons) is another such method that is built around blockchain to ensure the appropriate operation of connected AVs across a network [129]. Similarly, the method proposed is primarily put forth to aid AV platoons, this time increasing their ability to form dynamically by providing certain benefits, often in the form of payment, to vehicles willing to lead [129]. As proposed, this payment method would be carried out over blockchain architecture, a natural choice due to its origin in Bitcoin, ensuring secure and consistently available payment between entities [129]. In tests carried out to test this proposal, it was shown to be effective in fulfilling its goals, with a number of future areas for improvement in platoon operation and capabilities [129].

Studies of how blockchain can be applied to help AV platoons have extended far beyond simply ensuring their security; however, such technology has been extended to allow for the enhanced operation of such platoons in automated group toll payment for charging. In fact, such an application was tested in an experiment conducted by Zuobin Ying, Longyang Yi, and Maode Ma [130]. In the case of platoon operation, while it allows for the eased navigation of a group to retrieve fuel with as little wasted time as possible, there is the possibility of vehicles trying to sneak through without paying or providing incorrect information to lie to a governing distribution authority [130]. For a time, this was a pressing issue, significantly delaying its full implementation. However, it was discovered, through the test that was carried out, that blockchain could provide the perfect mechanism to allow such operation through its smart contract feature and noted security prowess [130].

In addition to approaches that are entirely reliant on the blockchain, its flexibility has allowed it to be considered an option to complement others based on differing technology. For example, it is highlighted as an excellent choice of architecture to support platoons' intelligence while navigating difficult intersections, as mentioned by a team of researchers proposing potential solutions to such problems [131]. Blockchain is viewed as a natural choice to support platoon navigational and operative techniques has also been mentioned by Emanuel Regnath and Sebastian Steinhorst, who, in their research on how to supervise platoons of AVs, noted the applicability of blockchain to verify parties that are involved in the group [132].

Based on increased interest and study and growing capabilities, blockchain is expected to provide numerous benefits in the area of group supervision, in which case its application to AVs to benefit platoon operation would be a natural next step. Prior results in implementation testing have shown to allow great strides forward already, providing a promising look at AVs' future capabilities if blockchain is to be utilized.

5. Future Research Directions, Challenges and Barriers

Bockchain has a lot of potential to be used in different areas, particularly in the field of Autonomous Vehicles, as discussed through this paper. However, before this can be deployed on a large scale, several problems surrounding the technology must be examined and repaired to ensure that it meets necessary requirements for energy consumption, resource use, and response time [24,25].

Nevertheless, the general form of Blockchain is quite inefficient in terms of consuming computation resource. Lightweight applications of Blockchain have shown a great deal of progress in reducing computational resource strain, and, even now, research is ongoing to improve on this current drawback. Blockchain technology itself also does not have an inherent flaw in computational resource consumption: this is instead linked directly to its PoW algorithm, which has been studied, with some proposals being put forth to reduce resource consumption [24,133]. As alternative algorithms to PoW are studied, Blockchain will likely be able to overcome its current high degree of resource use.

The high cost of implementation for Blockchain is the next challenge, which could be expensive in applications, such as CAVs. There are not many works discussing the expected cost for a large implementation, but examples of costs to develop other common blockchain applications are discussed across several papers [134,135]. However, as with many technologies, this cost can be expected to reduce significantly over time as more people study it, improve its efficiency, and become familiar with its structure and implementation enough to increase the number of workers who are able to work on implementing large-scale networks as needed.

Another challenge with using Blockchain in CAVs application is the fact that it requires high energy consumption. However, that depends on the exact type of blockchain type, there may be a much lower drain on energy use, as in non PoW models in use today [136]. While a good deal of blockchain applications today are fairly energy-intensive, a number of papers have also thought of how to resolve this issue, coming to a variety of possible solutions depending on the type of application desired [25]. In addition, Blockchain has shown that it provides a platform for users to interact more directly with their energy use and obtainment, as in proposed energy exchanging mechanisms between vehicles, as discussed by papers in the past, which could make up for higher rates of consumption in allowing more user control of how much energy they obtain at a time and from where they can access it [137].

Another main drawback of Blockchain is the responding time when more users are connected to the network, which makes them no suitable for safety applications. Delays are a known problem for Blockchain today, and as such, there is currently a lot of discussion on how to proceed when working to resolve the issue, as discussed in several papers [138]. Although there is not currently an agreed-upon solution to be used in all blockchain implementations, many incorporations of blockchain technology today still use their own methods to account for the issue of delay when under use by many people. For example, proposed methods like parallel proof of work [139] have shown to allow significant improvement in this area already. More lightweight blockchain applications have also been implemented, as with Block4Forensic, to improve the speeds of Blockchain when several users are in a network. With these examples, it's clear that these flaws are already noted and are currently being examined in a variety of ways to come to a resolution. In time, this flaw will most likely be mitigated, at which point blockchain technology will be closer to being ready for full use.

6. Conclusions

The blockchain technology contributes many advantages to network architecture such as scalability, security, and user safety which results in heavily being considered for future applications in CAVs systems. From its conception, blockchain technology was designed with several key features in mind: secured and maintained transactions, the use of a decentralized network, and user data protection, all of which could be extremely beneficial to future CAVs growth in a variety of ways. CAVs systems may not adequately protect against malicious user interference, leading to numerous accidents that may result in the loss of life. Thus, it still takes time to completely embrace the CAVs technology by public communities, such as engineers, mankind's scholars, legal intellectuals, social scientists, and moral philosophers. We need to take step forward to incorporate novel technologies, such as blockchain, to alleviate these concerns, as shown through experiments, outlines, and increased researcher interest in the idea. For the reasons that are discussed above, it is clear that the potential relationships between blockchain and CAVs technology need to be studied further in order to promote further development in both fields. By making use of a reliable, trusted technology to serve as a backbone for future CAVs systems, developers could be more certain in the safety and security of their products, as could users. In this way, the full potential of CAVs technology would be realized, which would contribute to a safer, more secure, and more accessible world through the mitigation of traffic accidents.

Author Contributions: Conceptualization, N.K. and G.T.; methodology, N.K. and G.T.; validation, A.S.; writing—review and editing, N.K., G.T., and A.S.; visualization, G.T. and N.K.; supervision, N.K. and A.S.; project administration, N.K. and A.S.; funding acquisition, A.S. All authors have read and agreed to the published version of the manuscript.

Funding: Partial support of this research was provided by the National Science Foundation under Grant No. CNS-1919855. Any opinions, findings, and conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the sponsoring agency.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Madrigal, A.C. 7 Arguments Against the Autonomous-Vehicle Utopia. 2018. Available online: theatlantic.com (accessed on 1 September 2020).
2. Siddiqui, F. Silicon Valley Pioneered Self-Driving Cars. But Some of Its Tech-Savvy Residents Don't Want Them Tested in Their Neighborhoods. 2019. Available online: washingtonpost.com (accessed on 1 September 2020).
3. Top 5 Dangers of Self-Driving Cars. 2019 Available online: technology.org (accessed on 1 September 2020).
4. Top 3 Possible Dangers of Self-Driving Cars. Available online: vesttech.com (accessed on 1 September 2020).
5. Deign, J. Why Self-Driving Cars Might Make Traffic Worse. 2020. Available online: https://www.greentechmedia.com/articles/read/why-a-world-with-self-driving-cars-might-not-be-such-a-great-idea (accessed on 1 September 2020).
6. Ahram, T.; Sargolzaei, A.; Sargolzaei, S.; Daniels, J.; Amaba, B. Blockchain technology innovations. In Proceedings of the 2017 IEEE Technology & Engineering Management Conference (TEMSCON), Santa Clara, CA, USA, 8–10 June 2017; pp. 137–141.
7. Daniel, J.; Sargolzaei, A.; Abdelghani, M.; Sargolzaei, S.; Amaba, B. Blockchain Technology, Cognitive Computing, and Healthcare Innovations. *J. Adv. Inf. Technol.* **2017**, *8*, 194–198. [CrossRef]
8. Zheng, Z.; Xie, S.; Dai, H.N.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
9. Kyriakidis, M.; Happee, R.; de Winter, J.C. Public opinion on automated driving: Results of an international questionnaire among 5000 respondents. *Transp. Res. Part F Traffic Psychol. Behav.* **2015**, *32*, 127–140. [CrossRef]
10. Lu, Z.; Wang, Q.; Qu, G.; Liu, Z. Bars: A blockchain-based anonymous reputation system for trust management in vanets. In Proceedings of the 2018 17th IEEE International Conference On Trust, Security And Privacy in Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp.98–103.
11. Cao, Y.; Morley Mao, Z. Autonomous Vehicles can be Fooled to 'See' Nonexistent Obstacles. Available online: https://theconversation.com/autonomous-vehicles-can-be-fooled-to-see-nonexistent-obstacles-129427#:~:text=BystrategicallyspoofingtheLiDAR,blockingtrafficorbrakingabruptly (accessed on 1 September 2020).
12. Al-Ali, M.S.; Al-Mohammed, H.A.; Alkaeed, M. Reputation Based Traffic Event Validation and Vehicle Authentication using Blockchain Technology. In Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, 2–5 February 2020; pp. 451–456.
13. Dorri, A.; Steger, M.; Kanhere, S.S.; Jurdak, R. Blockchain: A distributed solution to automotive security and privacy. *IEEE Commun. Mag.* **2017**, *55*, 119–125. [CrossRef]
14. Baza, M.; Nabil, M.; Lasla, N.; Fidan, K.; Mahmoud, M.; Abdallah, M. Blockchain-based Firmware Update Scheme Tailored for Autonomous Vehicles. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 15–18 April 2019; pp. 1–7.
15. Rowan, S.; Clear, M.; Gerla, M.; Huggard, M.; Goldrick, C.M. Securing Vehicle to Vehicle Communications using Blockchain through Visible Light and Acoustic Side-Channels. *arXiv* **2017**, arXiv:1704.02553.
16. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. Available online: https://bitcoin.org/en/bitcoin-paper (accessed on 1 September 2020).
17. Michelin, R.A.; Dorri, A.; Lunardi, R.C.; Steger, M.; Kanhere, S.S.; Jurdak, R.; Zorzo, A.F. SpeedyChain: A framework for decoupling data from blockchain for smart cities. *arXiv* **2018**, arXiv:1807.01980.
18. Saranti, P.G.; Chondrogianni, D.; Karatzas, S. Autonomous Vehicles and Blockchain Technology Are Shaping the Future of Transportation. In *The 4th Conference on Sustainable Urban Mobility*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 797–803.
19. Ranchal-Pedrosa, A.; Pau, G. ChargeltUp: On Blockchain-based technologies for Autonomous Vehicles. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, Munich, Germany, 15 June 2018; pp. 87–92. [CrossRef]
20. Rathee, G.; Sharma, A.; Iqbal, R.; Alogaily, M.; Jablan, N.; Kumar, R. A Blockchain Framework for Securing Connected and Autonomous Vehicles. *Sensors* **2019**, *19*, 3165. [CrossRef] [PubMed]

21. Carter, C.; Koh, L.D. Blockchain Disruption in Transport: Are You Decentralised Yet? Available online: https://trid.trb.org/view/1527923 (accessed on 1 September 2020).
22. Fadhil, M.; Owenson, G.; Adda, M. A Bitcoin Model for Evaluation of Clustering to Improve Propagation Delay in Bitcoin Network. In Proceedings of the 2016 IEEE Intl Conference on Computational Science and Engineering (CSE) and IEEE Intl Conference on Embedded and Ubiquitous Computing (EUC) and 15th Intl Symposium on Distributed Computing and Applications for Business Engineering (DCABES), Paris, France, 24–26 August 2016; pp. 468–475. [CrossRef]
23. Horwitz, L. Data Center-Impact of Driverless Cars Could Broaden with Blockchain. Available online: https://www.cisco.com/c/en/us/solutions/data-center/blockchain-driverless-cars.html (accessed on 1 September 2020).
24. Juričić, V.; Radošević, M.; Fuzul, E. Optimizing the Resource Consumption of Blockchain Technology in Business Systems. *Bus. Syst. Res. J.* **2020**, *11*, 78–92. [CrossRef]
25. Ghosh, E.; Das, B. A Study on the Issue of Blockchain's Energy Consumption, In *Proceedings of International Ethical Hacking Conference 2019, eHaCON 2019, Kolkata, India, 2020*; Springer: Singapore, Singapore; pp. 63–75. [CrossRef]
26. Fu, Y.; Li, C.; Yu, F.R.; Luan, T.H.; Zhang, Y. An Autonomous Lane Changing System with Knowledge Accumulation and Transfer Assisted by Vehicular Blockchain. *IEEE Internet Things J.* **2020**, *7*, 1–14. [CrossRef]
27. Choncholas, J.; Bhardwaj, K.; Gavrilovska, A. GeoENS: Blockchain-based Infrastructure for Service Discovery at the Edge. Available online: https://www.usenix.org/conference/hotedge20/presentation/choncholas (accessed on 1 September 2020).
28. Anatomy of Autonomous Vehicles: Is GIS Really Under the Hood of Self-Driving Cars? Available online: https://gisgeography.com/autonomous-vehicles-gis-self-driving-cars/ (accessed on 1 September 2020).
29. Petrovskaya, A.; Thrun, S. *Model Based Vehicle Tracking for Autonomous Driving in Urban Environments*; MIT Press: Cambridge, MA, USA, 2008. [CrossRef]
30. Sharp, C.; Schaffert, S.; Woo, A.; Sastry, N.; Karlof, C.; Sastry, S.; Culler, D. Design and Implementation of a Sensor Network System for Vehicle Tracking and Autonomous Interception. In Proceeedings of the Second European Workshop on Wireless Sensor Networks, Istanbul, Turkey, 31 January–2 February 2005; pp. 93–107.
31. Westerlund, R. Decentralized Reservation of Spatial Volumes by Autonomous Vehicles: Investigating the Applicability of Blockchain and Smart Contracts. Available online: https://www.diva-portal.org/smash/get/diva2:1437488/FULLTEXT01.pdf (accessed on 1 September 2020).
32. Zadobrischi, E.; Cosovanu, L.M.; Dimian, M. Traffic Flow Density Model and Dynamic Traffic Congestion Model Simulation Based on Practice Case with Vehicle Network and System Traffic Intelligent Communication. Available online: https://www.mdpi.com/2073-8994/12/7/1172 (accessed on 1 September 2020).
33. Van Arem, B.; Van Driel, C.J.; Visser, R. The Impact of Cooperative Adaptive Cruise Control on Traffic-Flow Characteristics. *IEEE Trans. Intell. Transp. Syst.* **2006**, *7*, 429–436. [CrossRef]
34. Yakub Abualhoul, M. Visible Light and Radio Communication for Cooperative Autonomous Driving: Applied to Vehicle Convoy. Ph.D. Thesis, Mines ParisTech, Paris, France, 2016. [CrossRef]
35. Kent, T.; Pipe, A.; Richards, A.; Hutchinson, J.; Schuster, W. A Connected Autonomous Vehicle Testbed: Capabilities, Experimental Processes and Lessons Learned. *Automation* **2020**, *1*, 17–32. [CrossRef]
36. Sichitiu, M.; Kihl, M. Inter-vehicle communication systems: A survey. *IEEE Commun. Surv. Tutorials* **2008**, *10*, 88–105. [CrossRef]
37. Luo, J.; Hubaux, J.P. A Survey of Inter-Vehicle Communication. 2004. Available online: core.ac.uk (accessed on 1 September 2020).
38. Jameel, F.; Awais Javed, M.; Zeadally, S.; Jantti, R. Efficient Mining Cluster Selection for Blockchain-based Cellular V2X Communications. *IEEE Trans. Intell. Transp. Syst.* **2020**, 1–9. . [CrossRef]
39. Jawhar, I.; Mohamed, N.; Zhang, L. Inter-vehicular Communication Systems, Protocols and Middleware. In Proceedings of the 2010 IEEE Fifth International Conference on Networking, Architecture, and Storage, Macau, China, 15–17 July 2010; pp. 282–287.
40. Takatori, Y.; Hasegawa, T. Quantitative Performance Evaluation of Predictive Collision Warning System based on Inter-Vehicle Communication. *Int. J. ITS Res.* **2007**, *4*, 13–20.
41. Lin, F.; Wang, K.; Zhao, Y.; Wang, S. Integrated Avoid Collision Control of Autonomous Vehicle Based on Trajectory Re-Planning and V2V Information Interaction. *Sensors* **2020**, *20*, 1079. [CrossRef]
42. Reichardt, D.; Shick, J. Collision Avoidance in Dynamic Environments Applied to Autonomous Vehicle Guidance on the Motorway. In Proceedings of the Intelligent Vehicles '94 Symposium, Paris, France, 24–26 October 1994; pp. 74–78. [CrossRef]
43. Funke, J.; Brown, M.; Erlien, S.M.; Gerdes, J.C. Collision Avoidance and Stabilization for Autonomous Vehicles in Emergency Scenarios. *IEEE Trans. Control. Syst. Technol.* **2017**, *25*, 1204–1216. [CrossRef]
44. Wang, P.; Gao, S.; Li, L.; Sun, B.; Cheng, S. Obstacle Avoidance Path Planning Design for Autonomous Driving Vehicles Based on an Improved Artificial Potential Field Algorithm. *Energies* **2019**, *12*, 2342. [CrossRef]
45. Gupta, R.; Tanwar, S.; Kumar, N.; Tyagi, S. Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review. *Comput. Electr. Eng.* **2020**, *86*, 106717. [CrossRef]
46. Chattopadhyay, A.; Lam, K.Y.; Tavva, Y. Autonomous Vehicle: Security by Design. *IEEE Trans. Intell. Transp. Syst.* **2020**, 1–15. [CrossRef]

47. Zelle, D.; Rieke, R.; Plappert, C.; Kraus, C.; Levshun, D.; Chechulin, A. SEPAD-Security Evaluation Platform for Autonomous Driving. In Proceedings of the 2020 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), Västerås, Sweden, 11–13 March 2020; IEEE Computer Society: Los Alamitos, CA, USA, 2020; pp. 413–420. [CrossRef]
48. Ferdowsi, A.; Challita, U.; Saad, W.; Mandayam, N.B. Robust Deep Reinforcement Learning for Security and Safety in Autonomous Vehicle Systems. In Proceedings of the 2018 21st International Conference on Intelligent Transportation Systems (ITSC), Maui, HI, USA, 4–7 November 2018; pp. 307–312.
49. Amoozadeh, M.; Raghuramu, A.; Chuah, C.N.; Ghosal, D.; Michael Zhang, H.; Rowe, J.; Levitt, K. Security Vulnerabilities of Connected Vehicle Streams and Their Impact on Cooperative Driving. *IEEE Commun. Mag.* **2015**, *53*, 126–132. [CrossRef]
50. Pokhrel, S.; Choi, J. A Decentralized Federated Learning Approach For Connected Autonomous Vehicles. In Proceedings of the IEEE Wireless Communications and Networking Conference Workshops (WCNCW), Seoul, Korea, 6–9 April 2020. [CrossRef]
51. Lam, A.Y.; Leung, Y.W.; Chu, X. Autonomous-Vehicle Public Transportation System: Scheduling and Admission Control. *IEEE Trans. Intell. Transp. Syst.* **2016**, *17*, 1210–1226. [CrossRef]
52. Llewellyn, P. Cybersecurity and Autonomous Vehicle Technology. Available online: aertech.com (accessed on1 September 2020).
53. Autonomous Vehicles: What Are the Security Risks? Available online: opentext.com (accessed on 1 September 2020).
54. Butcher, L. Increased Security for Autonomous and Connected Vehicles. Available online: autonomousvehicleinternational.com (accessed on 1 September 2020).
55. Raiyn, J. Data and Cyber Security in Autonomous Vehicle Networks. *Transp. Telecommun. J.* **2018**, *19*, 325–334. [CrossRef]
56. Blanco, S. Data Security For Autonomous Vehicles Can And Should Be Treated With Respect. Available online: forbes.com (accessed on 1 September 2020).
57. Jones, M. Tesla Personal Data Oversight Highlights Autonomous Vehicle Data Privacy Issue. Available online: techhq.com (accessed on 1 September 2020).
58. Henrique Ruffo, G. Tesla Data Leak: Components With Personal Info Find Their Way On eBay. Available online: insideevs.com (accessed on 1 September 2020).
59. Greenberg, A. Hackers Remotely Kill a Jeep on the Highway-With Me in It. Available online: wired.com (accessed on 1 September 2020).
60. Evans, S. Unsafe at Any Connection: Autonomous Vehicles Lacking in Privacy, Security Protections. Available online: sharaevans.com (accessed on 1 September 2020).
61. Bowles, J. Autonomous Vehicles and the Threat of Hacking. Available online: cpomagazine.com (accessed on 1 September 2020).
62. Hartenstein, H.; Laberteaux, K. *VANET: Vehicular Applications and Inter-Networking Technologies*; John Wiley & Sons: Hoboken, NJ, USA, 2009; Volume 1.
63. Leiding, B.; Memarmoshrefi, P.; Hogrefe, D. Self-managed and blockchain-based vehicular ad-hoc networks. In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Heidelberg, Germany, 12–16 September 2016; pp. 137–140. [CrossRef]
64. Singh, M.; Kim, S. Blockchain Based Intelligent Vehicle Data sharing Framework. *arXiv* **2017**, arXiv:1708.09721.
65. Narbayeva, S.; Bakibayev, T.; Abeshev, K.; Makarova, I.; Shubenkova, K.; Pashkevich, A. Blockchain Technology on the Way of Autonomous Vehicles Development. *Transp. Res. Procedia* **2020**, *44*, 168–175. [CrossRef]
66. Singh, M.; Kim, S. Branch Based Blockchain Technology in Intelligent Vehicle. *Comput. Netw.* **2018**, *145*, 219–231. [CrossRef]
67. Gong, S.; Tcydenova, E.; Jo, J.; Lee, Y.; Park, J. Blockchain-Based Secure Device Management Framework for an Internet of Things Network in a Smart City. *Sustainability* **2019**, *11*, 3889. [CrossRef]
68. The Impact of Blockchain on Banks & Financial Institution. Available online: asiablockchainreview.com (accessed on 1 September 2020).
69. Spilka, D. Blockchain and the Unbanked: Changes Coming to Global Finance. Available online: ibm.com (accessed on 1 September 2020).
70. Schlapkohl, K. Central Bank Digital Currency Explained. Available online: ibm.com (accessed on 1 September 2020).
71. Blockchain in Financial Services. Available online: ey.com (accessed on 1 September 2020).
72. Sullivan, M. The Future of Blockchain in Financial Services. Available online: blocktelegraph.io (accessed on 1 September 2020).
73. Joshi, N. Autonomous Vehicles and Blockchain. Available online: bbntimes.com (accessed on 1 September 2020).
74. Zambon, A. Autonomous Vehicles and Blockchain. Available online: octotelematics.com(accessed on 1 September 2020).
75. Fenech, G. The Link Between Autonomous Vehicles and Blockchain. Available online: forbes.com (accessed on 1 September 2020).
76. Blockchain @ Auto Finance: How Blockchain Can Enable the Future of Mobility. Available online: deloitte.com (accessed on 1 September 2020).
77. Miller, D. Blockchain and the Internet of Things in the Industrial Sector. *IT Prof.* **2018**, *20*, 15–18. [CrossRef]
78. Yuan, Y.; Wang, F.Y. Blockchain and Cryptocurrencies: Model, Techniques, and Applications. *IEEE Trans. Syst. Man Cybern. Syst.* **2018**, *48*, 1421–1428. [CrossRef]
79. Car Ewallet: Make Your Car a Wallet. Available online: chainstep.com (accessed on 1 September 2020).
80. We built Car eWallet on blockchain to securely facilitate machine-to-machine transactions. Available online: chainstep.com (accessed on 1 September 2020).
81. Mine, A. Blockchain based car wallet Car eWallet. Available online: gaiax-blockchain.com (accessed on 1 September 2020).

82. Yuan, Y.; Wang, F.Y. Towards blockchain-based intelligent transportation systems. In Proceedings of the 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Rio de Janeiro, Brazil, 1–4 November 2016; pp. 2663–2668.
83. Liu, H.; Zhang, Y.; Yang, T. Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing. *IEEE Netw.* **2018**, *32*, 78–83. [CrossRef]
84. Leiding, B.; Vorobev, W.V. Enabling the Vehicle Economy Using a Blockchain-Based Value Transaction Layer Protocol for Vehicular Ad-Hoc Networksguo. 2018. Available online: uploads-ssl.webflow.com (accessed on 1 September 2020).
85. Steps You Can Take to Correct a Mistake in the Police Report After Your Car Accident. Available online: braunslaw.com (accessed on 1 September 2020).
86. Goguen, D. Checklist of Records to Gather After a Car Accident. Available online: nolo.com (accessed on 1 September 2020).
87. Landers, D. Tips for Settling a Car Accident Claim. Available online: nolo.com (accessed on 1 September 2020).
88. Ways to Investigate the Cause of a Car Accident. Available online: dolmanlaw.com (accessed on 1 September 2020).
89. Who is Responsible for Your Car Accident. Available online: dolmanlaw.com (accessed on 1 September 2020).
90. Huckstep, R. Four Ways Autonomous Vehicles Will Change Auto Insurance. Available online: the-digital-insurer.com (accessed on 1 September 2020).
91. Carlson, D. The Autonomous Vehicle Revolution: How Insurance Must Adapt. Available online: marsh.com (accessed on 1 September 2020).
92. Lyne, A. Driverless Cars and the Insurance Industry. Available online: capsicumre.com (accessed on 1 September 2020).
93. Barnett, D. Autonomous Cars and Auto Insurance: What's Going to Happen. Available online: atlantainsurance.com (accessed on 1 September 2020).
94. Notte, J. How Do Self-Driving Safety Features Affect Your Car Insurance? Available online: thesimpledollar.com (accessed on 1 September 2020).
95. Guo, H.; Meamari, E.; Shen, C.C. Blockchain-inspired Event Recording System for Autonomous Vehicles. In Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China , 15–17 August 2018; pp. 218–222.
96. Aste, T.; Tasca, P.; Di Matteo, T. Blockchain Technologies: The Foreseeable Impact on Society and Industry. *Computer* **2017**, *50*, 18–28. [CrossRef]
97. Oham, C.; Kanhere, S.S.; Jurdak, R.; Jha, S. A Blockchain Based Liability Attribution Framework for Autonomous Vehicles. *arXiv* **2018**, arXiv:1802.05050.
98. Cebe, M.; Erdin, E.; Akkaya, K.; Aksu, H.; Uluagac, S. Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles. *arXiv* **2018**, arXiv:1802.00561.
99. Ugwu, M.C.; Okpala, I.C.; Oham, C.I.; Nwakanma, C.I. A Tiered Blockchain Framework for Vehicular Forensics. *Int. J. Netw. Secur. Its Appl. IJNSA* **2018**. [CrossRef]
100. Wang, A. The Future of Blockchain in Insurance. Available online: genre.com (accessed on 1 September 2020).
101. Kudwa, A.S. Blockchain: Life and Vehicle Insurance. Available online: mindtree.com (accessed on 1 September 2020).
102. Oham, C.; Jurdak, R.; Kanhere, S.S.; Dorri, A.; Jha, S.K. B-FICA: BlockChain based Framework for Auto- Claim and Adjudication. In Proceedings of the IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1171–1180.
103. Accelerating Techonlogy Disruption in the Automotive Market: Blockchain in the Automotive Industry. Available online: deloitte.com (accessed on 1 September 2020)
104. Autonomous Car Crashes: Who-or What-Is to Blame. Available online: knowledge.wharton.upenn.edu (accessed on 1 September 2020).
105. Goh, B.; Shirouzu, N. Chinese Man Blames Tesla Autopilot Function for Son's Crash. Available online: reuters.com (accessed on 1 September 2020).
106. Shepardson, D. Google Says it Bears 'Some Responsibility' After Self-Driving Car Hit Bus. Available online: reuters.com (accessed on 1 September 2020).
107. Yadron, D.; Tynan, D. Tesla Driver Dies in First Fatal Crash While Using Autopilot Mode. Available online: theguardian.com (accessed on 1 September 2020).
108. Baldwin, R. Driver in Fatal Tesla Model X Crash Had Complained About Autopilot. Available online: caranddriver.com (accessed on 1 September 2020).
109. Yamauchi, M. How Will Autonomous Vehicles Charge Themselves? Available online: pluglesspower.com (accessed on 1 September 2020).
110. Frangoul, A. VW Subsidiary to Help with Pilot of Robotic Charging Stations for Self-Driving Vehicles. Available online: cnbc.com (accessed on 1 September 2020).
111. EZ-Linck Beats Tesla with Its Completely Cable-Less Charging. Available online: autonomousevcharging.com (accessed on 1 September 2020).
112. Redefining Charging: Automatic Conductive Connection Device. Available online: volterio.com (accessed on 1 September 2020).
113. Morris, C. What's the Best Way to Grow Electric Vehicle Charging Infrastructure? Available online: evannex.com (accessed on 1 September 2020).

114. Buzachis, A.; Filocamo, B.; Fazio, M.; Ruiz, J.A.; Sotelo, M.; Villari, M. Distributed Priority Based Management of Road Intersections Using Blockchain. In Proceedings of the 2019 IEEE Symposium on Computers and Communications (ISCC), Barcelona, Spain, 29 June–3 July 2019; pp. 1159–1164.
115. Buzachis, A.; Celesti, A.; Galletta, A.; Fazio, M.; Villari, M. A Secure and Dependable Multi-Agent Autonomous Intersection Management (MA-AIM) System Leveraging Blockchain Facilities. In Proceedings of the IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion), Zurich, Switzerland, 17–20 December 2018; pp. 226–231. [CrossRef]
116. Sharma, V. An energy-efficient transaction model for the blockchain-enabled internet of vehicles (IoV). *IEEE Commun. Lett.* **2018**, *23*, 246–249. [CrossRef]
117. Su, Z.; Wang, Y.; Xu, Q.; Fei, M.; Tian, Y.C.; Zhang, N. A Secure Charging Scheme for Electric Vehicles With Smart Communities in Energy Blockchain. *IEEE Internet Things J.* **2018**. [CrossRef]
118. Javed, M.U.; Javaid, N.; Aldegheishem, A.; Alrajeh, N.; Tahir, M.; Ramzan, M. Scheduling Charging of Electric Vehicles in a Secured Manner by Emphasizing Cost Minimization Using Blockchain Technology and IPFS. *Sustainability* **2020**, *12*, 5151. [CrossRef]
119. Huang, X.; Zhang, Y.; Li, D.; Han, L. An optimal scheduling algorithm for hybrid EV charging scenario using consortium blockchains. *Future Gener. Comput. Syst.* **2018**, *91*. [CrossRef]
120. Energy Web Foundation Launches Worlds First Public, Open-Source, Enterprise-Grade Blockchain Tailored to the Energy Sector. Available online: energyweb.org (accessed on 1 September 2020).
121. Burgahn, C. Launch of the Open Charging Network. Available online: shareandcharge.com (accessed on 1 September 2020).
122. Cerf, M.; Matz, S.; Berg, A. Using Blockchain to Improve Decision Making That Benefits the Public Good. *Front. Blockchain* **2020**, *3*, 13. [CrossRef]
123. Singh, P.; Singh, R.; Nandi, S.; Ghafoor, K.; Rawat, D.B.; Nandi, S. An Efficient Blockchain-Based Approach for Cooperative Decision Making in Swarm Robotics. *Internet Technol. Lett.* **2019**, *3*, e140. [CrossRef]
124. Abbaspour, A.; Mokhtari, S.; Sargolzaei, A.; Yen, K.K. A Survey on Active Fault-Tolerant Control Systems. *Electronics* **2020**, *9*, 1513. [CrossRef]
125. Mokhtari, S.; Abbaspour, A.; Yen, K.K.; Sargolzaei, A. A Machine Learning Approach for Anomaly Detection in Industrial Control Systems Based on Measurement Data. *Electronics* **2021**, *10*, 407. [CrossRef]
126. Nair, M.; Sutter, D. The Blockchain and Increasing Cooperative Efficacy. *Indep. Rev.* **2018**, *22*, 529–550.
127. Khan, A.T.; Cao, X.; Li, S.; Milosevic, Z. Blockchain Technology with Applications to Distributed Control and Cooperative Robotics: A Survey. *Int. J. Robot. Control* **2019**, *2*, 36. [CrossRef]
128. Hexmoor, H.; Alsamaraee, S.; Almaghshi, M. BlockChain for Improved Platoon Security. *Int. J. Inf.* **2018**, *7*, 1–6.
129. Ledbetter, B.; Wehunt, S.; Rahman, M.A.; Manshaei, M.H. LIPs: A Protocol for Leadership Incentives for Heterogeneous and Dynamic Platoons. In Proceedings of the 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), Milwaukee, WI, USA, 15–19 July 2019; Volume 1, pp. 535–544. [CrossRef]
130. Ying, Z.; Yi, L.; Ma, M. BEHT: Blockchain-Based Efficient Highway Toll Paradigm for Opportunistic Autonomous Vehicle Platoon. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 1–13. [CrossRef]
131. Saiáns-Vázquez, J.V.; Ordóñez-Morales, E.F.; López-Nores, M.; Blanco-Fernández, Y.; Bravo-Torres, J.F.; Pazos-Arias, J.J.; Gil-Solla, A.; Ramos-Cabrer, M. Intersection Intelligence: Supporting Urban Platooning with Virtual Traffic Lights over Virtualized Intersection-Based Routing. *Sensors* **2018**, *18*. [CrossRef] [PubMed]
132. Regnath, E.; Steinhorst, S. CUBA: Chained Unanimous Byzantine Agreement for Decentralized Platoon Management. In Proceedings of the 2019 Design, Automation Test in Europe Conference Exhibition (DATE), Florence, Italy, 25–29 March 2019; pp. 426–431. [CrossRef]
133. Pashayev, I. Reducing Computational Waste : Space and Usefulness. Available online: https://crypto.stanford.edu/cs359c/17sp/projects/IskandarPashayev.pdf (accessed on 1 September 2020).
134. How to Determine the Cost of Blockchain Implementation? Available online: https://www.leewayhertz.com/cost-of-blockchain-implementation/ (accessed on 1 September 2020).
135. Blockchain Solution Implementation. Available online: https://www.tpptechnology.com/blog/blockchain-solutions-implementation-how-much-does-it-cost-in-2020/ (accessed on 1 September 2020).
136. Sedlmeir, J.; Buhl, H.; Fridgen, G.; Keller, R. The Energy Consumption of Blockchain Technology: Beyond Myth. *Bus. Inf. Syst. Eng.* **2020**, *62*. [CrossRef]
137. K, A.; Verma, P.; Southernwood, J.; Massey, B.; Corcoran, P. Blockchain in Energy Efficiency: Potential Applications and Benefits. *Energies* **2019**. [CrossRef]
138. Zhou, Q.; Huang, H.; Zheng, Z. Solutions to Scalability of Blockchain: A Survey. *IEEE Access* **2020**. [CrossRef]
139. Hazari, S.; Mahmoud, Q. Improving Transaction Speed and Scalability of Blockchain Systems via Parallel Proof of Work. *Future Internet* **2020**, *12*, 125. [CrossRef]