vehicles

*Review*

# Challenges and Solutions for Vehicular Ad-Hoc Networks Based on Lightweight Blockchains

**Edgar Bowlin [1], Mohammad S. Khan [1,*], Biju Bajracharya [1], Bhargav Appasani [2] and Nicu Bizon [3,4,5]**

[1] Department of Computing, East Tennessee State University, Johnson City, TN 37614, USA; bowline@etsu.edu (E.B.); bajracharya@etsu.edu (B.B.)
[2] School of Electronics Engineering, Kalinga Institute of Industrial Technology, Bhubaneswar 751024, India; bhargav.appasanifet@kiit.ac.in
[3] Pitești University Centre, The National University of Science and Technology POLITEHNICA Bucharest, 110040 Pitesti, Romania; nicu.bizon@icsi.ro
[4] Doctoral School, The National University of Science and Technology POLITEHNICA Bucharest, Splaiul Independentei Street No. 313, 060042 Bucharest, Romania
[5] ICSI Energy, National Research and Development Institute for Cryogenic and Isotopic Technologies, 240050 Ramnicu Valcea, Romania
* Correspondence: khanms@etsu.edu

**Abstract:** Current research with Vehicular Ad-hoc Networks (VANETs) has focused on adapting an efficient consensus mechanism and reducing the blockchain size while maintaining security. Care must be taken when implementing blockchains within VANET applications to leverage the chains' strengths while mitigating their weaknesses. These chains can serve as distributed ledgers that provide storage for more than financial transactions. The security provided by longer blockchains constitutes a nearly immutable, decentralized data structure that can store any data relevant to the applications. However, these chains must be adapted to the ad-hoc, resource-constrained environments found in VANETs. In the absence of abundant resources and reliable network connections, chain operation and maintenance must address the challenges presented by highly mobile nodes in novel ways, including situations such as emergency messaging that require real-time responses. Researchers have included different mechanisms to realize lightweight blockchains, such as adding reputation to existing consensus mechanisms, condensing the consensus committees, using geographical information, and monitoring a nodes behavior in attempts to adapt blockchains to these domains. This paper analyzes the challenges and gives solutions for these different mechanisms to realize lightweight blockchains for VANETs.

**Keywords:** blockchains; vehicular networks; consensus mechanisms; lightweight

check for updates

**Citation:** Bowlin, E.; Khan, M.S.; Bajracharya, B.; Appasani, B.; Bizon, N. Challenges and Solutions for Vehicular Ad-Hoc Networks Based on Lightweight Blockchains. *Vehicles* **2023**, *5*, 994–1012. https://doi.org/10.3390/vehicles5030054

Academic Editor: Alexey Vinel

Received: 22 March 2023
Revised: 11 August 2023
Accepted: 17 August 2023
Published: 19 August 2023

**Copyright:** © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

## 1. Introduction

The developments in computational power and communication capabilities have materialized novel technologies. Blockchain is one such application that has become extremely popular in the last decade. Blockchains provide secure, public, tamper-resistant ledgers for recording transactions among a chain's users. They operate with a centralized authority in permissioned chains and without one in permissionless chains [1]. They have found uses in a range of applications, including finance, education [2], industrial Internet of Things (IIoT) [3], etc.

The growth of urban populations makes traffic congestion, accident reduction, and environmental impact mitigation increasingly challenging. In traditional traffic management systems, these demands often lead to wasted time, increased pollution, and compromised safety. A smart city is a solution to this problem. By leveraging technology and data, smart cities can create more efficient and sustainable urban environments. Enhancing traffic management is a crucial aspect of smart city development. By utilizing real-time data,

predictive analytics, and intelligent infrastructure, cities can optimize traffic flow, reduce congestion, improve safety, and minimize the environmental footprint of transportation systems. Vehicular ad-hoc networks (VANETs) [4] can play a vital role in transforming the way vehicles interact with each other and their surroundings. Through VANETs it is possible to share data in real time, avoid collisions, optimize traffic flow, achieve quick emergency response, cooperative vehicle maneuvers, etc., contributing to more efficient traffic management in smart cities.

VANETs are networks of connected vehicles (CVs) and the devices with which they communicate as shown in Figure 1 [5]. Because CVs may freely leave and join VANETs, a VANET's inter-nodal connections are typically ephemeral and dynamic and their topologies are in constant flux. These changes in topology create additional problems for VANET routing algorithms, due in part to the need to route high-priority communications such as emergency event messages to all of a VANET's vehicles.

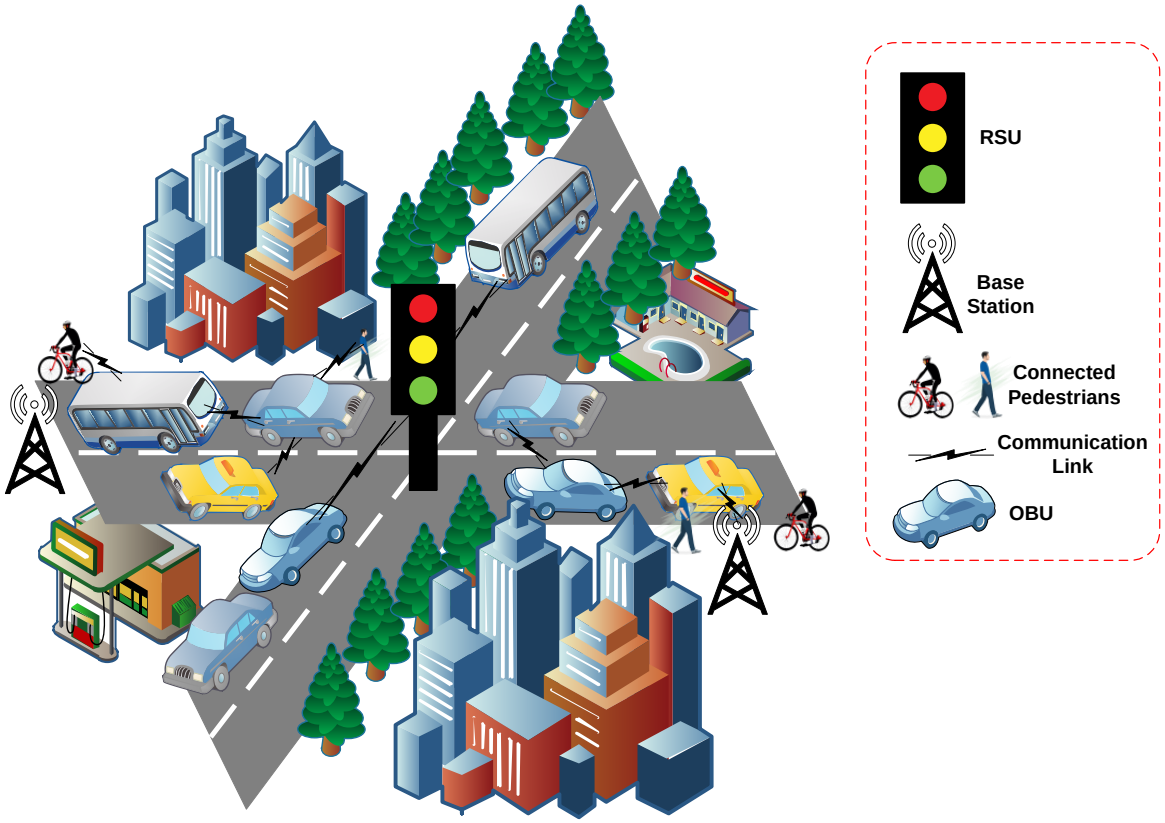



**Figure 1.** Components of a VANET.

A VANET can contain many nodes. The VANET's connected vehicles (CVs), the most dynamic of these nodes, use on-board units (OBUs) to process information and connect to networks. While CVs are highly mobile, their paths through a VANET are constrained by the host network's roadways. As roads often travel in one direction, a network can often predict a vehicle's location from its current roadway and rate of speed. To improve their manageability, VANETs commonly include roadside units (RSUs): static nodes that serve as anchor points for VANET-to-CV communications. RSUs are assumed to be more powerful than the OBUs, RSUs can provide services that OBUs cannot provide, such as traffic monitoring. RSUs send the data to the traffic management centers (TMCs) to monitor traffic.

VANET communications take one of three forms. Vehicle to Vehicle (V2V) communication, the dominant form of VANET communication, is highly ephemeral, as both vehicles could be travelling in opposite directions at high speeds. Vehicle to Infrastructure (V2I) communication occurs between RSUs and OBUs, and RSUs and TMC provides slightly

fewer routing difficulties due to the RSU acting as a stationary node. Finally, Vehicle to Everything (V2X) refers to communications between OBUs and any non-RSU/OBU device, such as pedestrians and bicyclists with connectable devices. Although many non-vehicle nodes may be mobile, their speeds do not match the connected vehicle speeds. This provides a more difficult routing problem than the V2I communication but is less difficult than V2V when vehicles are traveling in opposing lanes [6]. Traditional routing algorithms struggle to adapt to these dynamically changing configurations. The movement of the vehicles cause connectivity issues that can impact the routing decisions. Furthermore, the emergency messages are crucial for rapid emergency responses. These emergency messages have to be prioritized over other vehicular messages and communicated with high reliability and security. An adversary can capture and manipulate the information, resulting in false decisions by the TMC and the RSUs. In addition, the identity of the CVs can be known, compromising the security of the passengers. Many solutions have been proposed in recent years for enhancing the security of VANETs. Certificate-based authentication techniques that use public keys have been reported, but they are inefficient due to the large database of public keys. Group signature-based techniques are also based on keys, but the keys need to be frequently updated. Identity-based authentication schemes are too centralized to maintain secrecy of private keys; on the other hand, pseudonym-based schemes suffer from huge overhead. Certificateless schemes are more efficient but lack security. Furthermore, the OBU is resource constrained and cannot perform huge computations efficiently and quickly.

Blockchains, with their decentralized architecture, are a viable option for VANET applications. The tamper resistant nature of blockchain ensures that once the data is recorded on the blockchain it cannot be altered, making it ideal for VANETs. However, public blockchains require considerable energy and processing time, putting additional storage requirements on the network nodes. Thus, it is unsuitable for VANET applications, where the entities have limited computational power, with stringent real-time requirements. Lightweight blockchains are intended for nodes with limited resources, without compromising the security [7]. Lightweight blockchains provide mechanisms to reduce a traditional blockchain's overhead. This can take the form of making less energy-dependent consensus mechanisms or reducing network and storage overhead when transferring the chain between nodes. Lightweight blockchains can be adapted to networks where resources (computational, network, storage, etc.) are restrained due to the network's nature. These chains can bring blockchain abilities to networks traditionally not capable of traditional blockchain implementations. However, many chain adaptations are application-specific and may not easily transfer to other applications. These adaptations require additional research to generalize their operation. Lightweight chains require further research to prove their abilities match traditional chain networks where applicable. They can be of tremendous utility for VANETs, where the entities are constantly moving, have stringent real-time requirements, and with a need for strong security and authentication features. The number of published articles on blockchain is obtained from the Scopus database, illustrated in Figure 2.

The publication records in Figure 2 clearly indicate that blockchain technology is widely adopted for various applications, but not very popular for VANETs. Moreover, research on lightweight blockchains is still in nascent stages and its adoption for VANETs is miniscule. Thus, there is a need to study lightweight blockchains for VANETs, identify the challenges and propose probable solutions, which will be the subject matter of this work. A brief comparison of various survey papers on blockchains for VANETs is given in Table 1 that compare the studies based on their discussion of security, network usage, storage and computational requirements. Table 1 demonstrates various techniques intended to create a lightweight blockchain. Various aspects of using blockchains within resource-constrained networks are discussed in these studies. Chain operation within resource-restrained environments creates problems due to the overhead required in traditional chains. This overhead comes from the consensus method requirements alongside storage,

security, and network requirements. The previously mentioned works did not provide a view of creating a lightweight chain to tackle computational and network/storage issues. This study explores these works to formulate criteria to create lightweight blockchains within VANETs and to provide the foundation for generalizations within future work. This table further justifies the novelty and demonstrates the contributions of this work.

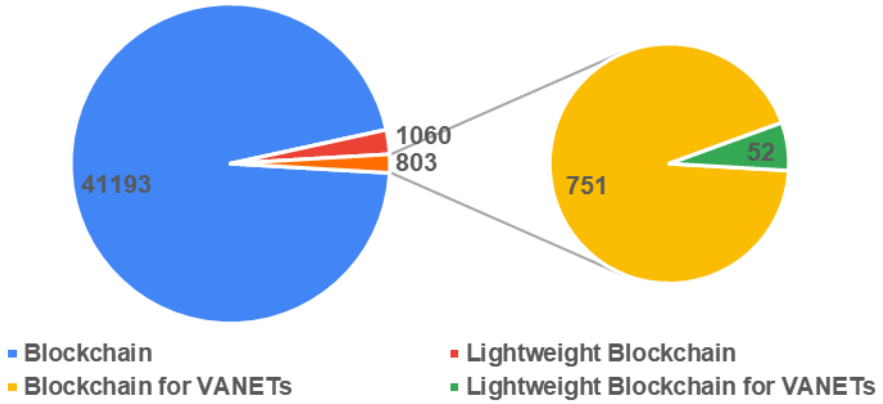



**Figure 2.** Publication statistics for blockchains and blockchains for VANETs.

**Table 1.** Existing reviews on blockchain for VANETs.

| Reference | Discussion of Security with VANET Blockchains | Discussion of Computation Reduction within VANET Blockchains | Discussion of Network Requirement Reduction within VANET Blockchains | Discussion of Storage Requirement Reduction within VANET Blockchains | Discussion of Lightweight Blockchains within VANETs and Their Effects |
|---|---|---|---|---|---|
| [8] | × | × | ✓ | ✓ | × |
| [9] | × | ✓ | × | × | × |
| [10] | ✓ | ✓ | ✓ | ✓ | × |
| [11] | ✓ | × | × | ✓ | × |
| [12] | ✓ | × | × | × | × |
| [13] | ✓ | ✓ | ✓ | ✓ | × |
| [14] | ✓ | × | × | ✓ | × |
| [15] | ✓ | ✓ | ✓ | ✓ | × |
| [16] | ✓ | ✓ | × | × | × |
| [17] | ✓ | ✓ | ✓ | ✓ | × |
| This survey | ✓ | ✓ | ✓ | ✓ | ✓ |

The existing surveys mostly focus on blockchains for VANETs, but none of them discuss the importance and use of lightweight blockchains for VANETs, which is the important contribution of this survey.

The remaining sections of the paper are organized as follows: an overview of blockchain technology is given in the second section. Additionally, a description of different consensus mechanisms is given, followed by the discussion on lightweight blockchain for VANETs in Section 3. Section 4 presents the challenges and possible solutions in the parlance of this topic. The last section presents the conclusion of the review on the prospect of a lightweight blockchain.

## 2. Overview of Blockchain

Blockchain is a decentralized ledger for recording transactions in a secure and transparent manner. It does not need any central authority for record-keeping and is maintained by a network of participants called "nodes". Each node in the blockchain network has a copy of the entire ledger or the blockchain that has the record of all the transactions. Thus, it prevents a single entity from controlling the information, thereby, providing transparency

and security. The transactions and chain-related information are stored in the blockchain in a series of blocks [18]. Every block in the chain has a reference (hash value) to the previous block forming a chain. Figure 3 illustrates a generic blockchain. The chains that bind these blocks are created by a cryptographic hash function that converts any input (data) into a fixed-size string of characters called the digest. This hash function has several important properties: it is deterministic (the same input always produces the same output), irreversible (you cannot derive the original input from the hash), and any minor change in the input produces a significantly different hash. This makes it incredibly difficult to alter data in a blockchain without detection. Blockchains commonly use the SHA-256 hashing algorithm, which outputs 32-byte digests. Users interpret the digests as 64-character hexadecimal strings that can be interpreted as integers.

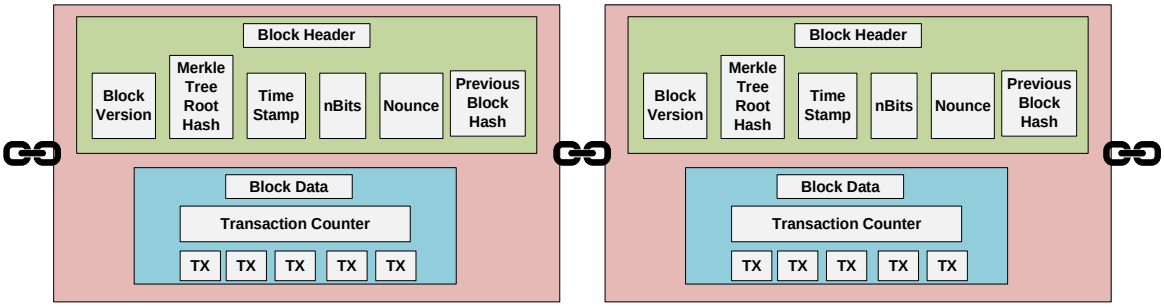



**Figure 3.** A typical blockchain.

With one exception, each of a chain's blocks contains the previous block's hash in its metadata. In place of a hash, a chain's first (genesis) block contains some preconfigured data. Because of this linkage, a block's hash affects the hash of all blocks that follow it. If any block's data changes, its hash will also change, invalidating the hashes of all blocks that follow it with a probability of close to 1, creating a need to rehash all blocks that trail it to restore the chain's integrity.

### *2.1. Transactions in a Blockchain*

Transactions' contents vary depending on the blockchain's application. In general, each transaction requires an input and an output. These parameters are often some forms of currency but can also be data. When a node in the blockchain network initiates a transaction, it is broadcasted over the network. The transaction can be financial, energy-related or consist of any other data. The other nodes in the network validate the transaction using pre-defined rules, such as verification of digital signatures, etc. To verify the identity of a transaction's creator, a transaction should be signed using asymmetric key encryption. Using two keys, a private and a public key, a node can sign-encrypt a document with their private key and distribute their public key. Then, any other node with that public key can authenticate that transaction's user by decrypting the signature.

Blockchains operate on networks of nodes—users' devices—that maintain and expand the blockchain. Two types of nodes have special status. One, a full node, stores the entire chain, ensuring its validity. The other, a publisher node, collects a network's transactions, creates blocks that document these transactions, and then attempts to publish the blocks, i.e., add them to the chain. A publisher node publishes a block by sending it to its peer nodes. Those peer nodes verify the block, then add it, if valid, to their blockchain and relay them to their peers. Eventually, a valid block will propagate to all a network's nodes. A newly added block's transactions are not immediately accepted as confirmed. For a network to confirm a block's transactions, a certain number of additional blocks must first be added to the chain. This policy is meant to minimize disruptions due to possible overwrites in the blocks that immediately precede a newly added block.

As a rule, chains have multiple publisher nodes, which compete to publish blocks. A consensus model determines a blockchain's behavior, including which nodes may publish

blocks, how conflicts related to block publication are resolved, and how often the network adds new blocks to the chain. Consensus mechanisms ensure that all nodes in the network agree on the state of the blockchain. Different mechanisms, such as proof-of-work (PoW), proof-of-stake (PoS), and delegated proof-of-stake (DPoS), use various approaches to achieve this agreement while considering factors such as security, energy efficiency, and decentralization. Whenever a block is added to the chain, its hash is linked to the previous block's hash. The result is a chain of blocks, each pointing to its predecessor. Because of the cryptographic hashing properties, it is extremely difficult to alter any past transaction without changing subsequent blocks. Therefore, the data on the blockchain is practically unchangeable.

### *2.2. Consensus Mechanisms for Blockchains*

The distributed nature of blockchain operation creates potential issues for a network's integrity. For a blockchain network to function properly, its nodes must agree on its content. One issue is trust: the ability of one node to confirm that another node acts non-maliciously. Within permissioned chains, the network must authenticate and authorize all nodes, which establishes trust, to participate with the network. Permissionless chains lack this trust-establishing step.

Another issue, bifurcation, is the concurrent addition of two different blocks to a chain by different nodes. Bifurcation creates inconsistent versions of the chain within the network. Nodes can reference either version of the chain when publishing new blocks, which leads to nodes possibly rejecting a valid block if the block does not reference the blockchain branch that node is using.

Consensus protocols assure network integrity by establishing policies for achieving agreement about the network's current, valid state. For example, a common solution to the bifurcation problem is for nodes to adopt the longest chain after a certain time. The authentication and authorization step used by permissioned chains avoids problems with trust, while permissionless chains use consensus mechanisms to inspire trust through sacrifices of non-trivial resources, e.g., time, power, or currency. A node is said to be mining when it participates in the consensus mechanism. These mechanisms are often called Proof-of-X, where X characterizes the consensus mechanism's behavior.

#### 2.2.1. Proof-of-Work

Three-fifths of all blockchains, including the Bitcoin blockchain, use the PoW consensus mechanism [19]. PoW requires publisher nodes to compete to solve a computationally intense but easily verifiable mathematical puzzle [20]. For example, for Bitcoin, this puzzle's challenge is finding a digest with more leading zeros than the current network difficulty target. In other words, if a publisher node interprets its block's digest as an integer and this integer is smaller than the difficulty target determined by the network, the node can publish that block. Nodes solve puzzles by repeatedly changing a special metadata field, known as a nonce, and recomputing their own digests until they find a value that solves the puzzle. The unpredictable nature of the SHA-256 algorithm constitutes the challenge: as the target decreases in value, nodes will require more "work" to find a suitable digest.

While every publishing node can technically publish blocks, most are published by nodes with the most processing power. In theory, the resources expended in this work should deter malicious activity. While the publication puzzle is computationally feasible, malicious users should find the puzzle financially infeasible to solve, assuming most of the network contains non-malicious nodes.

The difficulty target fluctuates due to network participation. Bitcoin's blockchain adjusts its difficulty target every 2016 blocks to ensure it adds one block to the blockchain every ten minutes. The network lowers the target value—thereby raising the difficulty—for networks with many nodes and raises it—lowering the difficulty—for networks with few nodes. Adjustments occur as nodes join and leave the network for various reasons, e.g., maintenance, power outage, and disinterest in network participation.

The "work" performed in PoW has drawbacks. Due to the amount of energy needed to solve these puzzles, PoW blockchains consume considerable power. According to Schinkus et al. [21], a single transaction can power 20 U.S. homes daily, and Bitcoin's entire network uses a similar amount of electricity annually as Austria. Ethereum, another blockchain that used a less resource-intensive PoW algorithm prior to summer 2022, required the annual energy consumption of Kenya. Users will place publisher nodes near cheap electricity due to the potential cost reduction and profit increase. As these blockchains grow, their environmental impact will continue to increase.

#### 2.2.2. Proof-of-Stake

The Proof-of-Stake (PoS) consensus model uses a probabilistic algorithm to select what node, at any given time, may act as the next publishing node. The PoS model relies on the idea that staked users are trustworthy and will be invested in the blockchain's well-being [22]. PoS assumes that a network's nodes can use cryptocurrency to buy a non-returnable heightened probability of publishing blocks. The incentive to publish a block becomes the fees charged during transactions instead of block creation-based rewards. PoS, in effect, enables users to increase their chances of publishing blocks by buying probabilities instead of better computer hardware, as in PoW. PoS systems may include voting systems. In one version, the network randomly chooses staked nodes to create blocks, then allows them to vote on which block to publish next. The network determines votes' weights through how much the node has staked, similarly to stockholders within a publicly owned company that cannot sell their shares. Yaga et al. [1] refers to these systems as Byzantine fault tolerance PoS's.

Another PoS voting system uses delegates to create blocks. This system allows staked nodes to vote on which nodes should publish. Voting occurs continuously, spawning competition between potential publishing nodes. Trust in the scenario comes from the punishment of publishing nodes. If a node behaves maliciously, the network can vote out the misbehaving node from its publishing position.

### *2.3. Smart Contracts*

In addition to descriptions of interactions involving two nodes, blocks can contain smart contracts, which are collections of code and data that a network's nodes can execute [23]. Not every blockchain can implement smart contracts. For those that can, publishing nodes attach smart contracts to blocks, similar to regular transactions. This code's output must be the same for all nodes (deterministic) and is recorded to the chain.

A smart contract's operation must depend strictly on the information that that contract receives from its user. Moreover, all nodes within the network must agree on the outcome of a smart contract's operation. These requirements limit a smart contract to one of two sources of information: that contract's host network or stable sources of outside information. If a smart contract uses information outside of the network, it is called an oracle. The oracle must assure that their information is easily obtainable so that nodes can validate outputs. Publishing a smart contract on a blockchain renders it largely immutable and tamper-resistant. These properties allow nodes to trust the contract's actions, treating it as a trusted third party. Smart contracts can provide services to a blockchain's nodes, e.g., storing data, exposing information publicly, performing calculations, and redistributing resources among a chain's users. Contracts act as functions and an output ledger of that function. Smart contracts have built-in protection mechanisms to defend against certain attacks. One, a timeout function, guards against denial-of-service attacks by stopping a smart contract's operation after a certain period of time. A second function, a fee to execute, may be required of smart contracts in permissionless blockchains. This dissuades attackers by requiring resources to stage their attack. An attack must participate within a network through honest behavior to gain these resources. This takes time that an attacker may not have. In permissioned blockchains, the risk of a malicious node is lower, due to the nodes requiring permission to operate within the network. These blockchains may forgo execution fees

entirely. However, the vulnerabilities in smart contracts are still being exploited to attack the blockchain network. Formal methods such model checking, theorem proving, symbolic verification and run-time verification can be used to minimize the vulnerabilities of smart contracts [24,25].

## 3. Lightweight Blockchain in VANETs

The architecture of a blockchain for VANETs depends on the application and on the resource constraints. Two prominent architectures are available in the literature: the use of blockchain at the RSUs, and the use of blockchain at the OBUs [26,27]. Both the architectures are depicted in Figure 4.

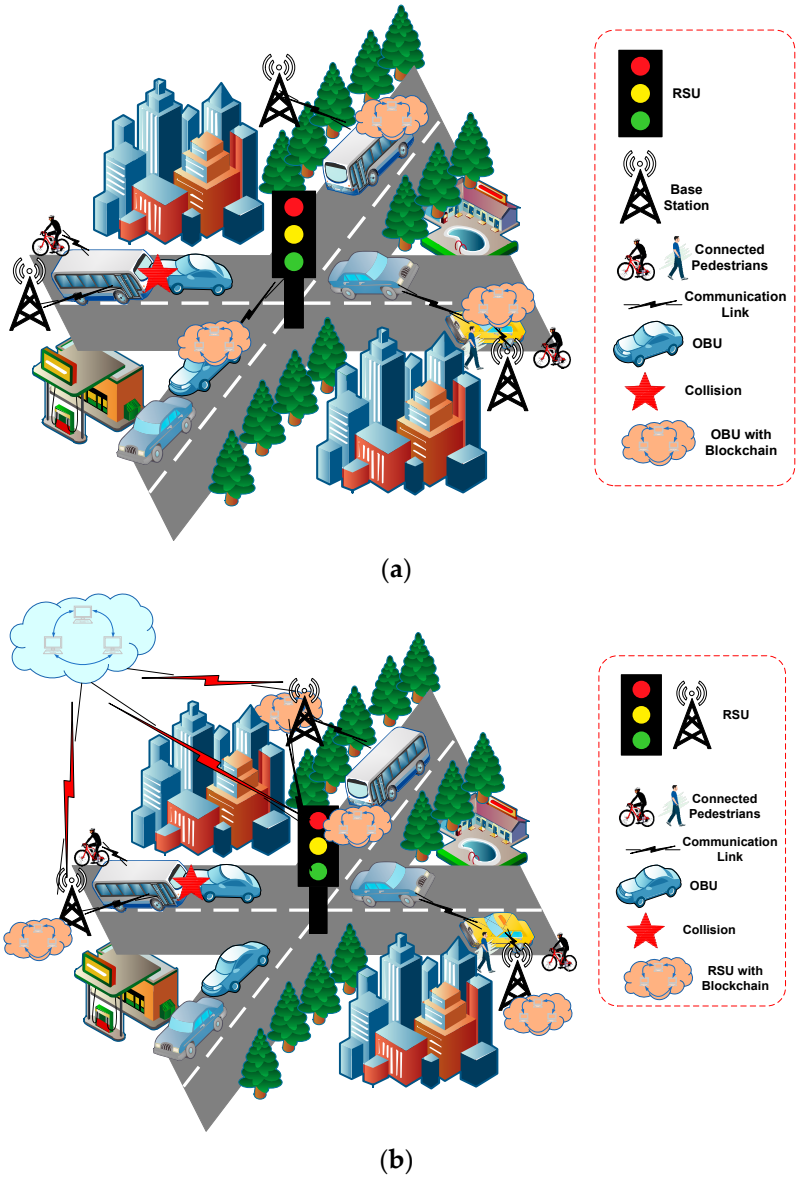



**Figure 4.** Blockchain architecture for VANETs. (**a**) Blockchain implemented at a cluster of OBUs; (**b**) blockchain implemented at RSUs.

A blockchain can run on a cluster of OBUs or RSUs, as shown in Figure 4. OBUs are more resource-constrained, and the blockchain running on OBUs must be efficiently designed compared to the blockchain implemented on RSUs. Furthermore, the mobile nature of the OBU compared to the static nature of the RSU makes blockchain implemen-

tation challenging for this architecture. There are many methods to deploy a lightweight blockchain, which are illustrated in Figure 5:

1. *Efficient Trust Evaluation*: lightweight trust evaluation schemes can reduce the computational overhead of the blockchain by identifying the malicious nodes that generate false data to overburden the target node [28]. By involving only those trusted nodes, the blockchain can be made lighter. However, the mobile nature of the nodes makes it difficult to implement these lightweight trust evaluation schemes.
2. *Lightweight Consensus Mechanism*: a lightweight blockchain can be achieved by simplifying the consensus mechanism, reducing computational costs. PoS, delegated PoS (DPoS), Direct Acyclic Graph (DAG), etc., are some of the lightweight consensus mechanisms. However, the maintenance of network synchronization, and preventing attacks can still be challenging using these lightweight mechanisms.
3. *Pruning*: pruning is the process of deleting data from the blockchain that is no longer required to validate new transactions. This technique can help reduce the size of the blockchain, making it more lightweight. In VANETs, pruning can be used to remove transaction data no longer relevant to the current traffic scenario. However, in VANETs, historical data can be important in predicting patterns and pruning may remove this data that can be important in future.
4. *Limiting the Number of Nodes*: in VANETs, it is possible to include only those nodes (OBUs) within a given geographical area, as there is a greater probability of interaction between them than in another geographical area. This can make the blockchain light. The mobile nature of the traffic makes it difficult to implement this strategy.
5. *Sharding*: sharding involves breaking up the blockchain into smaller, more manageable pieces called shards. This can help reduce the computational requirements for each node and increase the scalability of the blockchain. The dynamic nature of movement and communication constraints makes its implementation difficult.
6. *State Channels*: state channels are off-chain channels between a group of nodes (OBUs), allowing them to conduct many transactions without recording them on the main blockchain, reducing the load and making it lightweight. State channels may not be suitable for communicating emergency transactions.
7. *Data Compression*: compressing the data stored on the blockchain can help reduce the size of the blockchain. This can be achieved using compression algorithms that reduce the data size without affecting its integrity. This technique can be used in conjunction with other methods mentioned above. However, the real-time requirements of VANETs and the limited processing power of the OBUs puts constraints on the data compression techniques.

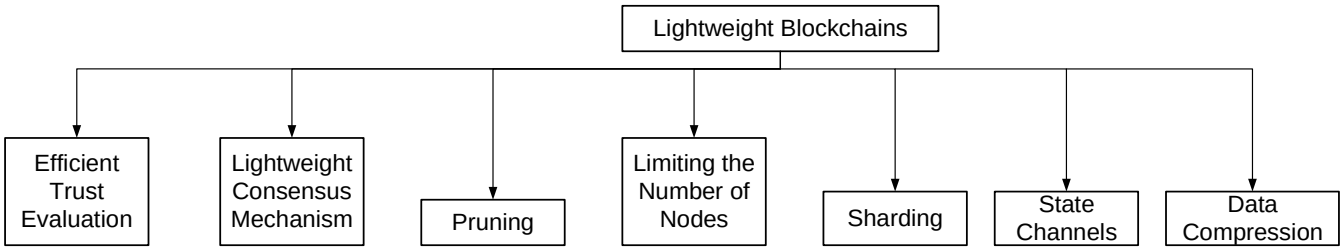



**Figure 5.** Methods for creating lightweight blockchains.

However, the literature on lightweight blockchain for VANETs has not fully explored all these various methods. Lightweight consensus mechanisms have been adopted to simplify the blockchain.

### *3.1. Efficient Trust Evaluation*

Autonomous Vehicles (AVs) have complex operating requirements due to their need for safe and secure operation. Researchers have used machine learning techniques to address some of these requirements [29], e.g., to train in-vehicle applications to identify pedestrians and detect attacks against AV software. These applications' operations can be improved by training them with more data [30]. Provided this data is representative of real conditions, its point of origin is immaterial.

Sharing data on environmental conditions can meet this need for improving AV operations. Sharing, however, poses risks to user privacy and safety. Training data may contain identifiable information, including location images, trajectory information, and credit card information. If vehicles were to share their datasets, a malicious user could identify and track a user's whereabouts or disseminate faulty data to decrease the accuracy of certain critical tasks.

In [31], the authors present a novel, private blockchain-based method to share machine learning models and datasets safely and securely. The architecture features a low-overhead, scalable consensus mechanism, which, in experiments with 16 GB of RAM and an Intel i7 8th generation processor, showed an increase in transaction verification time from 400 ms to 500 ms when the number of transactions increased from 200 to 2000.

The architecture creates a blockchain that can function effectively in a resource-constrained vehicle edge network. The chain uses a new consensus method to defend against attacks involving false models (Byzantine attacks). This method, named Proof of Vehicular Services-Byzantine Fault Tolerance (PoVS-BFT), uses a small, ratings-based, tenure-specific consensus committee to reduce the complexity of traditional consensus algorithms. Semi-trusted RSUs act as publishing nodes in this chain. Here, trustworthiness denotes how well an RSU meets its operating requirements. The network determines an RSU's trust rating by measuring how often vehicles interact with that node and how efficiently an RSU satisfies application-specific Quality of Service (QoS) requirements. An RSU that services many vehicles over time and fulfils network delivery requirements efficiently benefits the network and is treated as trustworthy.

A road network's vehicles act as nodes that make transactions and forward them to an RSU. The vehicles collectively help determine an RSU's rating by sending an evaluation of a recently used RSU to a certificate authority (CA). CAs grant pseudonyms to users to provide privacy while remaining identifiable within the network, which is a reason to trust the CA's ratings. The CA gathers these ratings and distributes them across the network.

In order to publish a block, an RSU must be on the publishing committee. PoVS-BFT's committee selection process chooses RSUs through two phases. The first elimination phase uses K-means clustering to separate potential publishing candidates into two groups. The network calculates each group's average service rating and identifies the highest-rated group as the next potential group. The validation phase removes candidates from the potential group through Euclidean distances and outlier detection. These phases decrease the committee's size while limiting membership to the most trusted and efficient RSUs. After this point, the network follows traditional BFT procedures, selecting the consensus leader round-robin style.

Another data-sharing scheme based on the Practical Byzantine False Tolerance (PBFT) consensus mechanism is proposed in [32]. This consensus mechanism is not lightweight, but is more robust to falsifying information. However, in the event of malicious attacks, the PBFT rejects some of the information based on the reputation of the nodes, thereby reducing the computational overhead. Similarly, in [33], the neuro-fuzzy machine learning method has been used to detect and filter out false requests, thereby decreasing the overall size of the blockchain. A lightweight trust evaluation scheme has been proposed in [34] to identify the malicious nodes, and it is observed that the scheme's performance matches that without any attackers.

The authors of [35] present a discussion on reputation and trust management systems within many fields, VANETs included, backed by blockchains. One of the propositions discussed was using a lightweight, scalable blockchain with lightweight consensus mechanism and throughput mechanism specifically for cyberphysical systems, such as a VANET. These mechanisms tend to be specific to the applications as these can vary in requirements.

### *3.2. Lightweight Consensus Mechanisms*

PoW is a popular blockchain consensus mechanism that can also be extended for lightweight consensus mechanisms in VANETs. Even though it is highly secure, it consumes a lot of energy and replacing PoW would be optimal for reducing a chain's network load. With PoS, even though it is more energy efficient than PoW and is suitable for lightweight consensus in VANETs, achieving fair participation of the nodes involved is challenging. DPoS and proof-of-authority (PoA) are other blockchain consensus mechanisms that can also be used for lightweight consensus, as they involve only selected nodes for participating in transaction validation. They are energy efficient and fast, but the dynamic nature of VANETs makes its implementation challenging. In the literature, researchers have reported other lightweight consensus mechanisms for VANETs. In [36], the authors made the nodes calculate matrix operations for a machine-learning algorithm. Although this is not necessarily lightweight, it matches the ideas of lightweight as the work is not reduced but made useful. If this work can help train a model used for traffic management, this can further increase the efficiency of the roadway and the network. However, this is not the case in most applications, and an alternative consensus mechanism can be used [37].

Consensus performance can be ascertained through consensus delay and block processing time. Consortium blockchains and round robin consensus methods have been used to reduce these aspects [38]. These consortium blockchains combine multiple chains from different organizations into one environment. Separating the blockchains between OBUs and RSUs allows the more powerful RSUs to handle the bulk of computation while using OBUs for less computationally difficult problems. In [38], the authors could reduce the computation cost and consensus delay more than the methods. Moreover, a modification to PBFT can be seen in the works of Vishwakarma et al. using four states when finding consensus and a new leader election scheme reduced resource usage. The experimental results show an 85% computation cost reduction, 55% storge and communication overhead, and a 90% shorter consensus delay [39].

Message dissemination within VANETs requires secure operation within environments of untrusted nodes. These nodes possess limited computing capabilities and require a non-PoW consensus method [40]. Ayaz et al. in [40] proposed a novel blockchain consensus method, Proofof-Quality-Factor (PoQF), designed for Vehicular Edge Computing (VEC)-backed VANET environments. The authors treat vehicles as VANET's mobile edge nodes and RSUs as its edge computing servers.

PoQF uses Quality Factors (QFs) to identify whether a node may publish a block in a network's operation at a given instant. When a node receives a message (transaction proposal), it calculates its own QF. This value is the product of its signal-to-noise ratio and the probability that its distance from the transaction's sender is above a certain threshold. This threshold must be chosen to ensure message delivery within the current network environment. QF ensures that a publishing node is close enough to an incident to ensure that this node can support its claims through onboard vehicle sensors.

After a node calculates its QF, it determines a message's validity and QF to a voting message to send across the network. This node then waits for a period that depends on its QF before announcing its vote to its neighbors. This random wait period reduces the likelihood of packet collision and helps to ensure fairness by assigning shorter random wait periods to trustworthy nodes. Each node tallies the votes it receives from other nodes and uses this tally in the next step.

A node can publish a block when it meets two criteria. The node must have received an arbitrary number of votes matching its vote. Many nodes may meet this criterion. The second criterion resolves publication conflicts through QFs. A node can publish its block if it has the highest QF compared to the QFs found in the voting messages. If the node votes true and the votes it received match that vote, it relays the message through the network and publishes a block about the event. Similarly, if voted false by the node and the network, the node disregards the message and still publishes a block about the event. These two criteria ensure stronger security within PoQF. Using nearby nodes to validate transactions eliminates the need to validate transactions at every node, reducing overall power usage. Moreover, nodes farther away from the incident may be unable to validate transactions due to vehicle sensors not being within range of the incident.

Ayaz et al. tested OMNet++ by integrating it into the Simulation of Urban Mobility (SUMO) simulation of a VANET; PoQS's validation time increases as the number of mining nodes increases. The number of malicious nodes within the network can affect this latency. As the malicious node percentage reaches 20% of the network and the network increases in size from 10 mining nodes to 40, validation times increase from 100 ms to about 450 ms. When that percentage reaches 60% of the network in that same situation, validation times increase from about 250 ms to 1000 ms. These messages, being emergency messages, must have a latency of at most 1 s. Otherwise, the network assumes the message is false and allows the node with the highest QF that voted false to publish a block about the event.

As more vehicles connect through VANETs, users can more efficiently use vehicular resources through sharing data. Ride sharing, the process of a driver providing transportation to a client at cost, allows access to transportation to people without a vehicle of their own. Many ride-sharing implementations use centralized servers to connect drivers to clients and process transactions. To engage in a transaction, clients and drivers must share secure data, including identifying information and credit card numbers. Peak usage times and server outages may delay these processes and reduce efficiency.

In [41], the authors modified the Proof-of-Reputation (MPoR) consensus method. Their proposed modification was to make the number of mining nodes variable to balance efficiency and accuracy through stochastic filtering and resource optimization. This was compared to Proof-of-Driving consensus and was demonstrated to resist network attacks when malicious nodes comprised less than one-third of total network nodes. This was due to Practical Byzantine Fault Tolerance used as the final consensus step. This reduces the total computation required for consensus.

Kudva et al. introduced a blockchain-based ride-sharing system to reduce fuel costs [42]. Their system uses a new consensus mechanism, Proof-of-Driving (PoD), and a method to reduce consensus committee sizes. PoD was designed to support universal accessibility, be fair to its users, support the computational economy, and resist attacks such as node collusion.

PoD is an extension of PBFT that uses PoW to limit a network's set of potential publishing nodes. Transactions contain either a passenger's request or a driver's response to a passenger. Vehicles serve as the mining nodes and collect these transactions.

Vehicles and clients can make transactions, but only vehicles can mine blocks. Driving coins earned through miles travelled serving clients determine the likelihood that a vehicle will act as a potential mining node. The network computes the average vehicle's driving coin amount to determine the difficulty of a puzzle that candidate nodes must solve. If a vehicle hashes its driving coin amount and that value is less than the average's hash value, this node becomes a potential mining node.

To further eliminate potential mining and publishing nodes, the network calculates the nodes' trustworthiness based on the number of blocks generated in the past. This metric indicates a node's willingness to participate in consensus and win publishing rights. This metric deters malicious nodes by forcing them to positively contribute to the network for an uneconomical amount of time. After the network determines the trust values, the network

chooses the highest-rated nodes to maximize the consensus committee's trustworthiness. The maximized value varies depending on the network environment.

Work has been completed on designing lightweight chains for IoT that support joining and leaving IoT nodes without large overheads for authentication using PBFT as a consensus mechanism. Using a Raspberry Pi 4B, they were able to demonstrate that encryption and decryption (both symmetric and asymmetric) times were able to reach microsecond levels. Ultimately, their work demonstrated that they were able to keep transaction generation and verification below 10 ms [43]. These may prove useful within VANET environments.

Directed Acyclical Graphs (DAGs) are another distributed ledger that works similarly to blockchains, except that they do not require storing the amount of information that traditional blockchains demand [44]. This allows DAGs to reduce the network and storage requirements of the network's nodes, as seen in the Internet of Things [45]. DAGs can also increase the transaction throughput by processing transactions in parallel [46]. In [47], the authors created a PBFT-based DAG running within an Internet of Vehicles. This consensus mechanism contained methods to reduce the number of consensus nodes by sharding the network into smaller networks and adding weights to functions to incentivize a high reputation score. These authors improved the transactions per second, consensus success rate, and time of obtaining transactions while reducing dependence on RSUs [48].

In [49], a modified DAG consensus mechanism has been adopted to achieve lightweight operation. The DAG allows reaching consensus faster by allowing the transactions to be placed in the previous transaction, thereby helping the transactions to reach consensus parallelly. This results in a faster consensus. The mechanism was compared with other approaches, such as the standard PoW, PoS, DAG, Proof-of-Driving (PoD), and DPoS. It is found that the proposed DAG approach significantly reduces the block confirmation delay to less than 100 ms, compared to the 300 ms taken by the standard PoW mechanism. Similarly, a DAG scheme has been proposed in [50], combining a historical data-pruning method, and minimizing duplicates and the storage space. The method is scalable and has reported to save the storage space by 97.13%. In [51], a DAG-based blockchain called V-Lattice has been proposed that combines pruning. Instead of storing the full blockchains, the nodes store a partial blockchain based on the storage availability.

The authors in [52] use a multilayer system, one of which involved a blockchain using a dynamic Proof-of-Work (dPoW) consensus algorithm to authenticate nodes. Their solution reduced packet flows drastically compared to their baseline solution and used reduced computational overhead compared to other solutions. Despite being PoW-based, the authors concluded that instead of using the Bitcoin model (PoW), another network such as Tron could reduce resources consumed and increase transactional throughput.

### *3.3. Limiting Geographical Reach*

A consensus mechanism's power consumption can be limited by limiting the size of a blockchain network. Fewer nodes mean less competition and communication overhead. This limit, specifically in committee sizes, often comes from an arbitrary equation. Using node location to configure blockchains provides another avenue for limiting size arbitrarily. By increasing and decreasing the size of a blockchain's local operating area, the network can increase or decrease the number of nodes operating on a chain, illustrated in Figure 6.

Shrestha et al. proposed a PoW-PoS hybrid blockchain to store safety event messages and track the participating nodes' trustworthiness [52]. The authors' network consists of vehicles, which serve as mining, transacting, and publishing nodes, and RSUs, which provide vehicle authentication services. Transactions involve sharing beacon messages, which inform other nodes of a node's presence, and safety event messages. Within this system, vehicles obtain location certificates from RSUs. Nodes send transactions with these certificates to provide proof that those nodes were near the safety event message's location. Using a trust rating and a transaction's timestamp, other nodes can verify a message's integrity and appropriately influence that node's trust rating. A node's trust rating is

a function of the ratio of the number of valid messages it sends to the total number of messages it sends.

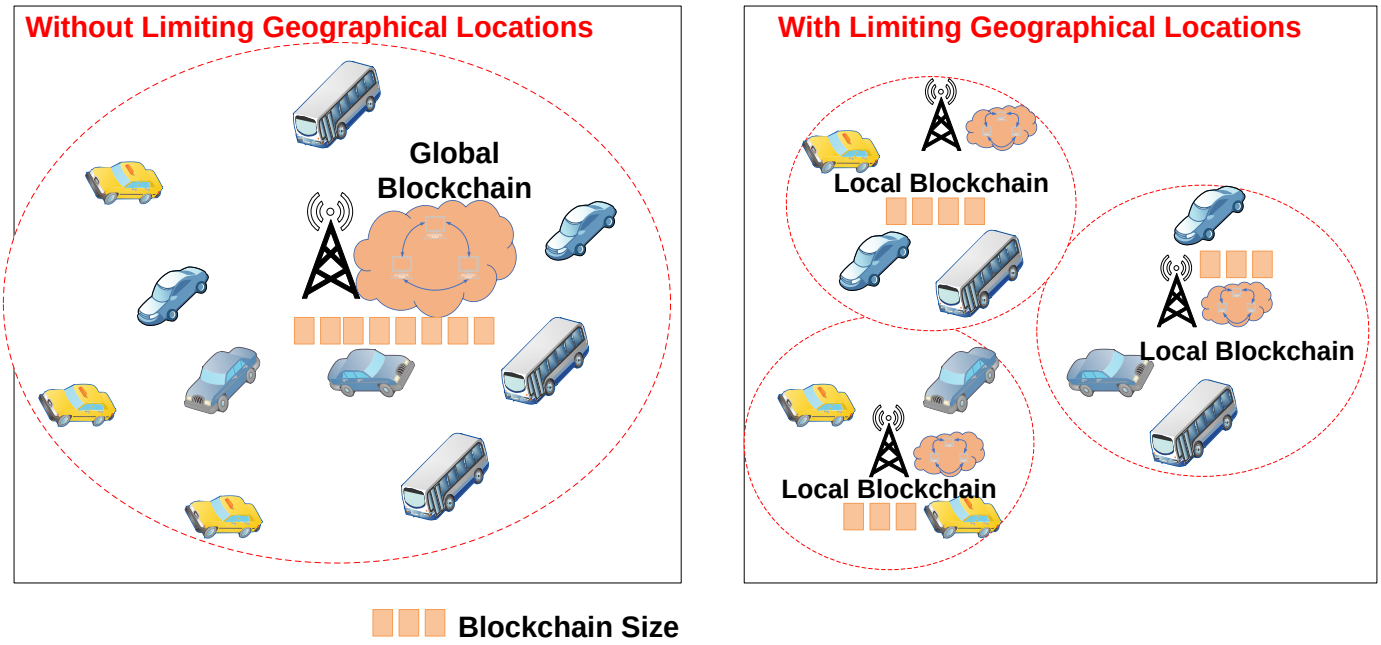



**Figure 6.** Comparing limiting geographic locations' effects on blockchain sizes.

Shreshta et al. argued that the use of location-based chains could enable the use of augmented PoW-PoS hybrid consensus mechanisms in VANETs, although the chains could grow in size, ranging from 206.51 GB to 1548.82 GB per year when transactions ranged from 200 to 1500 transactions per second. Limiting the geographical range of a blockchain would limit the network's power consumption and computational overhead while decreasing the communication overhead required for the chain to function. This approach aims to address the issue of scalability more effectively when compared to a global blockchain framework. Vehicles can accurately determine their positions by employing a location certificate system founded on the Proof of Location (PoL) principles, which can be used to create local blockchain networks. This localized blockchain infrastructure offers enhanced performance by substantially decreasing the data required for global processing and storage.

### *3.4. Pruning*

Blockchain's resource use can also be reduced through chain size reduction. The amount of blocks on the chain is proportional to the security of the chain. In resource-constrained environments, this unbounded length [53] can lead to storage and network issues, especially when nodes require a full download of the chain (bootstrapping). Pruning removes part of the chain to save resources as information becomes stale over time. Pruning can be used to shrink the size of the chain and reduce storage and network constraints. Pruned, bounded chains provide lower network and storage resources than unbounded chains [54]. The literature has embraced pruning to bound blockchain growth [55].

However, whether or not you can prune a chain depends on the data stored on the chain. Pruning becomes more complicated if the data requires all transactions to recreate the network state. If this information needs to be retained for non-sequential reasons (i.e., regulations), this data can be offloaded from the network's nodes to edge-computing resources for long-term storage [56]. This offloading must be balanced with reducing security, tamper-proofing, and data provenance, as the attributes suffer when offloading [57].

Pruning and storage issues from the unbounded growth remain under-researched. In S. BelMannoubi et al., of the works surveyed, only 34% of these blockchain applications

investigated storage issues, and only 43% addressed communication overhead [58]. Pruning provides a mechanism to manage these issues with a single technique.

## 4. Challenges and Solutions

Lightweight blockchains have the potential to bring significant benefits to VANETs; several challenges need to be addressed for their successful implementation. Some challenges in implementing lightweight blockchains for VANETs are:

1. *Scalability*: VANETs generate a large volume of data, and a blockchain that cannot handle this data efficiently may result in significant performance issues. As the number of connected vehicles increases, the blockchain's capacity to process transactions may become slower, impacting the desired transaction throughput. Solutions such as sharding or limiting the geographical area can help distribute the computational load and improve scalability.
2. *Security*: VANETs require secure vehicle communication to prevent cyberattacks and ensure safe driving. The blockchain technology used in VANETs must be secure, tamper-proof, and able to handle malicious attacks such as sybil and double-spending attacks.
3. *Decentralization*: the decentralization of the blockchain is crucial for ensuring that VANETs can operate autonomously without the need for a centralized authority. However, achieving true decentralization requires many nodes, which can be challenging to achieve in VANETs due to the high mobility of the vehicles.
4. *Interoperability*: interoperability enables different vehicles and infrastructures to communicate effectively. The blockchain technology used in VANETs must be interoperable with other communication protocols and technologies.
5. *Privacy*: VANETs generate many data, and ensuring the privacy of this data is crucial for maintaining user trust. The blockchain technology used in VANETs must provide a way to encrypt and anonymize data to ensure privacy and protect user data.
6. *Energy Efficiency*: VANETs are typically powered by energy-limited resources with limited capacity. Future research can focus on developing new energy-efficient blockchain architectures and consensus algorithms to reduce the energy consumption of blockchain-based VANETs.
7. *Real-time Applications*: VANETs are used in many real-time applications such as collision avoidance and traffic management. Future research can focus on developing new lightweight blockchain architectures and consensus algorithms that can provide real-time guarantees for these applications.
8. *Integration with AI and Machine Learning*: VANETs can generate large amounts of data, which can be analyzed using AI and machine learning algorithms to provide insights into traffic patterns and driving behavior. Future research can focus on developing new blockchain-based architectures and consensus algorithms that can support AI and machine learning applications in VANETs. AI applications are already being developed for VANET with blockchains [59] and even using AI to determine which nodes can participate in the consensus method [60].

Overall, implementing lightweight blockchains for VANETs requires addressing the above challenges effectively. Addressing these challenges requires a deep understanding of VANETs and the blockchain technology used. Developing standards and protocols that enable interoperability, scalability, and security is crucial for successful implementation.

Solutions that can potentially improve the performance and efficiency of lightweight blockchains for VANETs are:

1. *Hybrid Consensus Mechanisms*: hybrid consensus mechanisms can be used to combine the strengths of different consensus mechanisms and mitigate their weaknesses. A hybrid consensus mechanism can combine the efficiency of a lightweight consensus mechanism such as PoS or DPoS with the security of a more robust consensus mechanism such as PBFT.

2. *Network Partitioning*: network partitioning can be used to improve the scalability of lightweight blockchains for VANETs. By partitioning the network into smaller sub-networks, the overhead of the consensus mechanism can be reduced, and the scalability can be improved. Network partitioning can also increase the robustness of the network by isolating faulty or malicious nodes.
3. *Size Reduction Techniques*: size reduction techniques can be used to reduce the size of the blockchain and the amount of data that needs to be transmitted between nodes. This can be achieved by compressing transaction data or using techniques such as Merkle trees to reduce the size of the blockchain.
4. *Off-Chain Transactions*: off-chain transactions can reduce the computational overhead of the blockchain by processing transactions off-chain and only submitting the outcome to the blockchain. This can be achieved using techniques such as state channels or payment channels.
5. *Light Client Protocols*: light client protocols can be used to reduce the computational and storage requirements of nodes in the network. Using a lightweight protocol, nodes can participate in the network without downloading and storing the entire blockchain.
6. *IoT Blockchains*: another possible solution is to employ the lightweight blockchains developed for Internet of Things (IoT) applications for VANETs, such as IOTA, BlockCloud, Atonomi, etc. [61,62].

These solutions can potentially improve the performance and efficiency of lightweight blockchains for VANETs, but further research is needed to evaluate their effectiveness and suitability for VANETs.

## 5. Conclusions

Artificial intelligence (AI) and high-speed communication networks will increase the number of connected vehicles. VANETs must be reliable and secure, where blockchain will play an important role in the next few years. The real-time and dynamic nature of traffic involved in VANETs makes the adoption of blockchain for VANETs feasible. This survey focuses on the use of lightweight blockchains for VANETs. Even in nascent stages, the research can impact the adoption of lightweight blockchain for practical applications in VANETs. Researchers have focused on developing lightweight consensus mechanisms and detecting and minimizing false requests before involving them in a transaction, thereby reducing the complexity. Future research can focus on developing efficient pruning methods.

**Author Contributions:** Conceptualization, E.B. and M.S.K.; methodology, B.A. and B.B.; software, B.A. and E.B.; validation, B.A. and B.B.; formal analysis, M.S.K. and B.A.; investigation, N.B., M.S.K., and B.A.; resources, B.A., M.S.K. and N.B.; data curation, E.B. and M.S.K.; writing—original draft preparation, E.B., M.S.K. and B.A.; supervision, N.B.; project administration, N.B.; funding acquisition, N.B.; writing—review and editing: M.S.K., B.A., B.B. and N.B.; coordination, B.A. and N.B. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

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

## References

1. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. *Blockchain Technology Overview*; NIST IR 8202; National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2018. [CrossRef]
2. Zhang, C.; Wu, C.; Wang, X. Overview of Blockchain Consensus Mechanism. In Proceedings of the 2020 2nd International Conference on Big Data Engineering, Shanghai, China, 29–31 May 2020; pp. 7–12.
3. Wang, E.K.; Liang, Z.; Chen, C.-M.; Kumari, S.; Khan, M.K. PoRX: A reputation incentive scheme for blockchain consensus of IIoT. *Future Gener. Comput. Syst.* **2020**, *102*, 140–151. [CrossRef]
4. Javaid, U.; Aman, M.N.; Sikdar, B. DrivMan: Driving Trust Management and Data Sharing in VANETs with Blockchain and Smart Contracts. In Proceedings of the 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 28 April–1 May 2019; pp. 1–5.
5. Hussain, R.; Hussain, F.; Zeadally, S. Integration of VANET and 5G Security: A review of design and implementation issues. *Future Gener. Comput. Syst.* **2019**, *101*, 843–864.

6. Tappeta VS, R.; Appasani, B.; Patnaik, S.; Ustun, T.S. A Review on Emerging Communication and Computational Technologies for Increased Use of Plug-In Electric Vehicles. *Energies* **2022**, *15*, 6580. [CrossRef]
7. Cebe, M.; Erdin, E.; Akkaya, K.; Aksu, H.; Uluagac, S. Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles. *IEEE Commun. Mag.* **2018**, *56*, 50–57. [CrossRef]
8. Elagin, V.; Spirkina, A.; Buinevich, M.; Vladyko, A. Technological aspects of blockchain application for vehicle-to-network. *Information* **2020**, *11*, 465. [CrossRef]
9. Mollah, M.B.; Zhao, J.; Niyato, D.; Guan, Y.L.; Yuen, C.; Sun, S.; Koh, L.H. Blockchain for the internet of vehicles towards intelligent transportation systems: A survey. *IEEE Internet Things J.* **2020**, *8*, 4157–4185. [CrossRef]
10. Peng, C.; Wu, C.; Gao, L.; Zhang, J.; Alvin Yau, K.L.; Ji, Y. Blockchain for vehicular Internet of Things: Recent advances and open issues. *Sensors* **2020**, *20*, 5079. [CrossRef]
11. Wang, C.; Cheng, X.; Li, J.; He, Y.; Xiao, K. A survey: Applications of blockchain in the internet of vehicles. *EURASIP J. Wirel. Commun. Netw.* **2021**, *2021*, 77. [CrossRef]
12. Mikavica, B.; Kostić-Ljubisavljević, A. Blockchain-based solutions for security, privacy, and trust management in vehicular networks: A survey. *J. Supercomput.* **2021**, *77*, 9520–9575. [CrossRef]
13. Grover, J. Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review. *Veh. Commun.* **2022**, *34*, 100458. [CrossRef]
14. Saad, M.; Khan, M.K.; Ahmad, M.B. Blockchain-Enabled Vehicular Ad Hoc Networks: A Systematic Literature Review. *Sustainability* **2022**, *14*, 3919. [CrossRef]
15. Azam, F.; Yadav, S.K.; Priyadarshi, N.; Padmanaban, S.; Bansal, R.C. A comprehensive review of authentication schemes in vehicular Ad hoc network. *IEEE Access* **2021**, *9*, 31309–31321. [CrossRef]
16. Sharma, R.; Thanvi, A.; Singh, S.; Kumar, M.; Jangir, S.K. Blockchain for vehicular Ad-hoc network and intelligent transportation system: A comprehensive study. In *Machine Learning Approaches for Convergence of IoT and Blockchain*; Wiley: Hoboken, NJ, USA, 2021; pp. 145–173.
17. Dwivedi, S.K.; Amin, R.; Das, A.K.; Leung, M.T.; Choo, K.K.R.; Vollala, S. Blockchain-based vehicular Ad-hoc networks: A comprehensive survey. *Ad Hoc Netw.* **2022**, *137*, 102980. [CrossRef]
18. Appasani, B.; Mishra, S.K.; Jha, A.V.; Mishra, S.K.; Enescu, F.M.; Sorlei, I.S.; Bizon, N. Blockchain-enabled smart grid applications: Architecture, challenges, and solutions. *Sustainability* **2022**, *14*, 8801. [CrossRef]
19. Wang, W.; Hoang, D.T.; Hu, P.; Xiong, Z.; Niyato, D.; Wang, P.; Kim, D.I. A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access* **2019**, *7*, 22328–22370. [CrossRef]
20. Lashkari, B.; Musilek, P. A comprehensive review of blockchain consensus mechanisms. *IEEE Access* **2021**, *9*, 43620–43652. [CrossRef]
21. Schinckus, C. Proof-of-work based blockchain technology and Anthropocene: An undermined situation? *Renew. Sustain. Energy Rev.* **2021**, *152*, 111682. [CrossRef]
22. Nguyen, C.T.; Hoang, D.T.; Nguyen, D.N.; Niyato, D.; Nguyen, H.T.; Dutkiewicz, E. Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities. *IEEE Access* **2019**, *7*, 85727–85745. [CrossRef]
23. Hewa, T.; Ylianttila, M.; Liyanage, M. Survey on blockchain based smart contracts: Applications, opportunities and challenges. *J. Netw. Comput. Appl.* **2021**, *177*, 102857.
24. Krichen, M.; Lahami, M.; Al–Haija, Q.A. Formal methods for the verification of smart contracts: A review. In Proceedings of the 2022 15th International Conference on Security of Information and Networks (SIN), Sousse, Tunisia, 11–13 November 2022; IEEE: New York, NY, USA, 2022; pp. 1–8.
25. Abdellatif, T.; Brousmiche, K.L. Formal verification of smart contracts based on users and blockchain behaviors models. In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018; IEEE: New York, NY, USA, 2018; pp. 1–5.
26. More, S.; Sonkamble, R.; Naik, U.; Phansalkar, S.; More, P.; Saini, B.S. Secured communication in vehicular Ad-hoc networks (VANETs) using blockchain. *IOP Conf. Ser. Mater. Sci. Eng.* **2021**, *1022*, 012067. [CrossRef]
27. Liu, H.; Han, D.; Li, D. Behavior analysis and blockchain based trust management in VANETs. *J. Parallel Distrib. Comput.* **2021**, *151*, 61–69. [CrossRef]
28. Lwin, M.T.; Yim, J.; Ko, Y.B. Blockchain-based lightweight trust management in mobile ad-hoc networks. *Sensors* **2020**, *20*, 698. [CrossRef] [PubMed]
29. Hossain, M.A.; Md Noor, R.; Yau, K.-L.A.; Azzuhri, S.R.; Z'aba, M.R.; Ahmedy, I.; Jabbarpour, M.R. Machine Learning-Based Cooperative Spectrum Sensing in Dynamic Segmentation Enabled Cognitive Radio Vehicular Network. *Energies* **2021**, *14*, 1169. [CrossRef]
30. Hossain, M.A.; Md Noor, R.; Azzuhri, S.R.; Z'aba, M.R.; Ahmedy, I.; Yau, K.L.A.; Chembe, C. Spectrum sensing challenges & their solutions in cognitive radio based vehicular networks. *Int. J. Commun. Syst.* **2021**, *34*, e4748.
31. Islam, S.; Badsha, S.; Sengupta, S. A Light-weight Blockchain Architecture for V2V Knowledge Sharing at Vehicular Edges. In Proceedings of the IEEE International Smart Cities Conference (ISC2), Piscataway, NJ, USA, 28 September–1 October 2020; pp. 1–8.
32. Zhou, Y.; Cao, Z.; Dong, X.; Zhou, J. BLDSS: A Blockchain-based Lightweight Searchable Data Sharing Scheme in Vehicular Social Networks. *IEEE Internet Things J.* **2022**, *10*, 7974–7992. [CrossRef]

33. Ogundoyin, S.O.; Kamil, I.A. An efficient authentication scheme with strong privacy preservation for fog-assisted vehicular ad hoc networks based on blockchain and neuro-fuzzy. *Veh. Commun.* **2021**, *31*, 100384. [CrossRef]
34. He, J.; Chun, Y.J.; So, H.C.; Member EURASIP. Modeling and performance analysis of blockchain-aided secure TDOA localization under random internet-of-vehicle networks. *Signal Process.* **2023**, *206*, 108904. [CrossRef]
35. Putra, G.D.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R. Blockchain for Trust and Reputation Management in Cyber-Physical Systems. In *Handbook on Blockchain*; Springer Optimization and Its Applications; Tran, D.A., Thai, M.T., Krishnamachari, B., Eds.; Springer: Cham, Switzerland, 2022; Volume 194.
36. Wei, Y.; An, Z.; Leng, S.; Yang, K. Evolved PoW: Integrating the Matrix Computation in Machine Learning into Blockchain Mining. *IEEE Internet Things J.* **2023**, *10*, 6689–6702. [CrossRef]
37. Aung, N.; Kechadi, T.; Zhu, T.; Zerdoumi, S.; Guerbouz, T.; Dhelim, S. Blockchain Application on the Internet of Vehicles (IoV). In Proceedings of the 2022 IEEE 7th International Conference on Intelligent Transportation Engineering (ICITE), Beijing, China, 11–13 November 2022; pp. 586–591.
38. Vishwakarma, L.; Das, D. SmartCoin: A novel incentive mechanism for vehicles in intelligent transportation system based on consortium blockchain. *Veh. Commun.* **2022**, *33*, 100429. [CrossRef]
39. Vishwakarma, L.; Nahar, V.; Das, D. LBSV: Lightweight Blockchain Security Protocol for Secure Storage and Communication in SDN-Enabled IoV. *IEEE Trans. Veh. Technol.* **2022**, *71*, 5983–5994. [CrossRef]
40. Ayaz, F.; Sheng, Z.; Tian, D.; Guan, Y.L. A Proof-of-Quality-Factor (PoQF)-Based Blockchain and Edge Computing for Vehicular Message Dissemination. *IEEE Internet Things J.* **2021**, *8*, 2468–2482. [CrossRef]
41. Hou, B.; Zhu, H.; Xin, Y.; Wang, J.; Yang, Y. MPoR: A Modified Consensus for Blockchain-Based Internet of Vehicles. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 1644851. [CrossRef]
42. Kudva, S.; Badsha, S.; Sengupta, S.; Khalil, I.; Zomaya, A. Towards secure and practical consensus for blockchain based VANET. *Inf. Sci.* **2021**, *545*, 170–187. [CrossRef]
43. Hao, X.; Ren, W.; Fei, Y.; Zhu, T.; Choo K -KR, A. Blockchain-Based Cross-Domain and Autonomous Access Control Scheme for Internet of Things. *IEEE Trans. Serv. Comput.* **2022**, *16*, 773–786. [CrossRef]
44. Wang, X.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Niu, X.; Zheng, K. Survey on blockchain for Internet of Things. *Comput. Commun.* **2019**, *136*, 10–29. [CrossRef]
45. Kably, S.; Arioua, M.; Alaoui, N. Lightweight Direct Acyclic Graph Blockchain for Enhancing Resource-Constrained IoT Environment. *Comput. Mater. Contin.* **2022**, *71*, 5271–5291. [CrossRef]
46. Alladi, T.; Chamola, V.; Sahu, N.; Venkatesh, V.; Goyal, V.; Guizani, M. A Comprehensive Survey on the Applications of Blockchain for Securing Vehicular Networks. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 1212–1239. [CrossRef]
47. Zhang, X.; Li, R.; Zhao, H. A Parallel Consensus Mechanism Using PBFT Based on DAG-Lattice Structure in the Internet of Vehicles. *IEEE Internet Things J.* **2023**, *10*, 5418–5433. [CrossRef]
48. Chai, H.; Leng, S.; Wu, F.; He, J. Secure and Efficient Blockchain-Based Knowledge Sharing for Intelligent Connected Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 14620–14631. [CrossRef]
49. Yang, W.; Dai, X.; Xiao, J.; Jin, H. LDV: A lightweight DAG-based blockchain for vehicular social networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5749–5759. [CrossRef]
50. Zhang, X.; Li, R.; Hou, W.; Zhao, H. V-Lattice: A lightweight blockchain architecture based on DAG-lattice structure for vehicular ad hoc networks. *Secur. Commun. Netw.* **2021**, *2021*, 9942632. [CrossRef]
51. Gupta, M.; Kumar, R.; Shekhar, S.; Sharma, B.; Patel, R.B.; Jain, S.; Dhaou, I.B.; Iwendi, C. Game Theory-Based Authentication Framework to Secure Internet of Vehicles with Blockchain. *Sensors* **2022**, *22*, 5119. [CrossRef] [PubMed]
52. Shrestha, R.; Bajracharya, R.; Shrestha, A.P.; Nam, S.Y. A new type of blockchain for secure message exchange in VANET. *Digit. Commun. Netw.* **2020**, *6*, 177–186. [CrossRef]
53. Bowlin, E.W.; Khan, M.S. On Utilizing Prune-able Blockchains for Secure Message Dissemination in VANETs. In Proceedings of the 2021 IEEE 7th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 20–24 June 2021; pp. 295–300.
54. Bowlin, E.W.; Khan, M.S.; Bajracharya, B. A Blockchain Application on Bootstrapping Mobile Nodes within VANET. In Proceedings of the 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 8–11 March 2023; pp. 1011–1016.
55. Kevin, D.; David, B. HACIT2: A Privacy Preserving, Region Based and Blockchain Application for Dynamic Navigation and Forensics in VANET. In *Ad Hoc Networks*; AD-HOCNETS 2018; Zheng, J., Xiang, W., Lorenz, P., Mao, S., Yan, F., Eds.; Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; Springer: Cham, Switzerland, 2019; Volume 258.
56. Chen, X.; Chen, Y.; Wang, X.; Zhu, X.; Fang, K. DSVN: A Flexible and Secure Data-Sharing Model for VANET Based on Blockchain. *Appl. Sci.* **2023**, *13*, 217. [CrossRef]
57. Sey, C.; Lei, H.; Qian, W.; Li, X.; Fiasam, L.D.; Kodjiku, S.L.; Adjei-Mensah, I.; Agyemang, I.O. VBlock: A Blockchain-Based Tamper-Proofing Data Protection Model for Internet of Vehicle Networks. *Sensors* **2022**, *22*, 8083. [CrossRef] [PubMed]
58. BelMannoubi, S.; Touati, H.; Hadded, M.; Toumi, K.; Shagdar, O.; Kamoun, F. A comprehensive survey on blockchain-based C-ITS applications: Classification, challenges, and open issues. *Veh. Commun.* **2023**, *43*, 100607. [CrossRef]
59. Javed, A.R.; Hassan, M.A.; Shahzad, F.; Ahmed, W.; Singh, S.; Baker, T.; Gadekallu, T.R. Integration of Blockchain Technology and Federated Learning in Vehicular (IoT) Networks: A Comprehensive Survey. *Sensors* **2022**, *22*, 4394. [CrossRef] [PubMed]

60. Zalte, S.S.; Ghorpade, V.R.; Kamat, R.K. Synergizing Blockchain, IoT, and AI with VANET for Intelligent Transport Solutions. In *Emerging Computing Paradigms: Principles, Advances and Applications*; Wiley: Hoboken, NJ, USA, 2022; pp. 193–210.
61. Available online: https://www.iota.org/ (accessed on 10 February 2023).
62. Available online: https://atonomi.io/ (accessed on 10 February 2023).

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.