8-2023

# Lightweight Blockchains and Their Network Impact on Vehicular Ad-hoc Network-based Blockchain Applications

Edgar Bowlin
*East Tennessee State University*

## Recommended Citation

Bowlin, Edgar, "Lightweight Blockchains and Their Network Impact on Vehicular Ad-hoc Network-based Blockchain Applications" (2023). *Electronic Theses and Dissertations.* Paper 4242. https://dc.etsu.edu/etd/4242

# Lightweight Blockchains and Their Network Impact on Vehicular Ad-hoc Network-based Blockchain Applications

---

A thesis

presented to

the faculty of the Department of Computing

East Tennessee State University

In partial fulfillment

of the requirements for the degree

Master of Science in Computer and Information Sciences, Applied Computer Science

---

by

Edgar Wallace Bowlin III

August 2023

---

Mohmmad S. Khan, Ph.D, Chair

Biju Bajracharya, Ph.D

Ghaith Husari, Ph.D

Keywords: VANET, Vehicular, Blockchain, Lightweight, Pruning, Networking, Floating Genesis Blockchain

# ABSTRACT

Lightweight Blockchains and Their Network Impact on Vehicular Ad-hoc Network-based Blockchain Applications

by

Edgar Wallace Bowlin III

Vehicular Ad-hoc Networks (VANETs) provide networks for smart vehicles and will enable future systems to provide services that enhance the overall transportation experience. However, these applications require consideration to possible damage to both property and human life. Communication between vehicles requires data immutability and user privacies to provide safe operation of the system. Blockchains can provide these properties and more to create a more secure and decentralized system. However, a chain's security comes from the chain length. VANETs' ephemeral connections provide harm limits how much data can be exchanged during vehicle rendezvous. This thesis investigates lightweight blockchains that operate with lower overheads. A survey of current techniques to accomplish this are discussed in Chapter 1. Two techniques are demonstrated within two separate environments to demonstrate the network overhead reductions when using a lightweight blockchain with respect to network and storage loads within these VANET environments.

# DEDICATION

I dedicate this thesis to my family, both by blood (my parents Edgar Jr. and April Horton) and by choice (Hannah George, Elijah Franklin), and thank them for supporting me and forever pushing me to work harder while always taking time to relax. I would also like to dedicate this to Loubella and Cricket, the dogs. I would further dedicate this to Dr. Khan, Dr. Bajarachya, Dr. Husari, and the rest of the faculty and staff of the Computing Department and my bosses at Bays Mountain Planetarium, Adam Thanz and Jason Dorfman for supporting and guiding me through this experience. Finally I dedicate this to my life partner, Elaine King (soon-to-be Bowlin). Thank you for your constant love and support.

## ACKNOWLEDGEMENTS

This work would not exist without the help of Dr. Mohammad Khan, and Dr. Biju Bajracharya. Their input and guidance allowed this work to exist. I would also like to thank Dr. Bhargav Appasani and Dr. Nicu Bizon for their assistance in creating the survey found in this work. Finally, I would like to thank Dillon Buchanan for his input on artificial intelligence and machine learning for the future steps in this research.

TABLE OF CONTENTS

# LIST OF FIGURES

# 1 INTRODUCTION

## 1.1 Motivation

The growing interest within Vehicular Ad-hoc Networks (VANETs) only continues to grow as more vehicles are produced with networking capabilities. However, as a highly mobile ad-hoc network, the network topologies are dynamic with ephemeral connections between nodes. These nodes largely consist of highly mobile vehicles which force the chaotic topologies and ephemeral connections during operation.

Applications running within these networks require various characteristics depending on services provided. However, any application that requires identification, like safety event messages during vehicle accidents, must provide privacy to users as traditional vehicle identification through license plates can directly open a user's data to the wider public and possibly malicious users. These applications may also need to store data long-term for governmental usage. This data must remain tamper-resistant while simultaneously providing data integrity.

Blockchains can provide user privacy, tamper-resistance, and data integrity. This data structure has evolved from its financial abilities into a general, distributed data structure. However, traditional implementations require large investments in both hardware and electricity use due to the popular consensus mechanism Proof-of-Work. Blockchain's growth is traditionally unbounded, and this growth provides challenges when transferring the chain from one node to another in resource-constrained networks.

These challenges require modifications to blockchains for efficient operation within these environments. The chain network's overhead, particularly during bootstrapping nodes joining a network, must be lowered to operate within the tumultuous network environments of VANETs. Traditional unbounded blockchains cause both storage and, more importantly, network issues within VANETs. If a blockchain like Bitcoin, almost 500 gigabytes in size at time of writing, is used within a VANET application, the network topology complicates block transfers and would severely hinder performance.

## 1.2 Statement of Research Problem

The initial stage of this thesis involved creating a survey of blockchains within resource constrained environments and their overhead reductions with a focus on VANETs. This was undertaken to gain a better understanding of current overhead reduction strategies in literature. This understanding allowed for identification of weaknesses in current literature when considering VANETs. VANETs' network topology and its dynamic behavior alongside blockchains and their behavior within resource constrained networks were described within this survey. Current overhead reduction strategies are explained (alternate consensus mechanisms, chain pruning, limiting the network to a geographical region) in an attempt to find an unexplored avenue in overhead reduction. The survey provided evidence to pursue chain length reduction as a strategy to help adapt blockchains to the chaotic topologies of VANETs.

This missing link is exploited in this work through two separate experiments that proposed using block size variation and pruning mechanisms respectively for safety event message applications within VANETs. The proposed methods were able to reduce the overall storage and network overheads by almost 75% in terms of data sent over the network by leveraging the Floating Genesis Block pruning method to reduce the overall chain size. Several researchers are concentration on issues like a more efficient consensus method or adjusting the chain structure. However, very few authors focus on storage and network overhead reduction through chain reduction technqiues within VANETs. To add value to the current literature, this work provides a survey to highlight current overhead reductions and provide a primer for researchers to begin in this research area. As a result of the survey, two works were created investigating block size variation and pruning's network affects in two separate VANET environments.

In addressing the length issues stated above, this work focuses on three key problems and possible solutions:

1. A current literature survey was compiled to gain an understanding of VANETs, blockchains, and blockchains adapted to VANET applications. This survey describes current solutions

to reducing the overall chain overhead within resource-constrained networks. This survey focused on how these adaptations could be used within VANET applications and their implications within this environment. This survey provided insight on weaknesses and potential improvements of techniques within current literature. The survey provides the grounds on which the other two works in this thesis are built.

2. A block size variation technique was investigated within a platoon VANET environment. A platooning environment was coded and a blockchain application was created to run within this environment to better analysis the chain's network overhead. From this, an analysis was created between chains with varying block size limits within a platoon environment of vehicles traveling at the same speed and direction for long time periods with new vehicles joining at fixed time intervals. These vehicles traveled at fixed distances relative to each other. This block size variation allows for a network overhead reduction as the smaller blocks required less data to transmit to vehicles newly joining the platoon.

3. A pruning mechanism was studied within a more realistic VANET scenario. This environment consisted of a two-lane, opposite direction highway that spanned a straight line of length 25 miles. Vehicles would randomly travel between 55 and 75 miles an hour and spawn at random intervals to simulate a suburban highway environment. This environment also contained Road-Side Units to act as stationary nodes within the network. The vehicles in this case did not stay at fixed distances and thus increased the network complexity. An analysis of this environment with respect to network overhead was conducted with pruned and unpruned blockchains demonstrating that a shorter chain would lead to fewer dropped packets and an overall reduction to the data sent over the network.

## 1.3 Results

This in-depth research of optimizing blockchains for VANETs and pruning blockchains within VANETs provide 3 novel results.

1. Affirmation of Lightweight blockchains existence and confirmation of a lack of research concerning Lightweight VANET-based blockchains. Although optimizations are being made to blockchains specifically for VANETs, this research concerned itself largely with consensus methods. A survey of current techniques was created to provide researchers a starting point for VANET blockchain optimization.

2. Affirmation through simulation that varying block size limits of a blockchain within a platooning environment reduces network overhead and helps to optimize network use depending on the size chosen for that application. This block size limit allows for a chain's network impact on bootstrapping nodes to be lessened.

3. Affirmation through simulation that pruning a blockchain within a highly mobile VANET environment reduces network overhead and reduces the chance of dropping packets. A pruned blockchain is more efficient for this chaotic network to successfully transfer the chain to bootstrapping nodes.

The results stated above and detailed descriptions of the survey and pruning experiments, including the future research of this thesis, are discussed in detail in the remainder of this work.

# 2 CHALLENGES AND SOLUTIONS FOR VEHICULAR AD-HOC NETWORKS BASED ON LIGHTWEIGHT BLOCKCHAINS

*Edgar Bowlin, Mohammad S. Khan, Biju Bajracharya, Bhargav Appasani, Nicu Bizon*

## 2.1 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 a distributed ledger that provides storage for more than financial transactions. The security provided by longer blockchains provide 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 like 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 analyses the challenges and gives solutions on these different mechanisms to realize lightweight blockchains for VANETs.

## 2.2 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]. Blockchains' application in Vehicular Ad-hoc Networks (VANETs) [4] is important owing to a growing need for efficient traffic management in smart cities.

VANETs are networks of connected vehicles (CVs) and the devices with which they communicate as shown in 2.2.1 [4]. 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.

A VANET can contain many nodes. The most dynamic of these nodes, the VANET's connected vehicles (CVs), 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

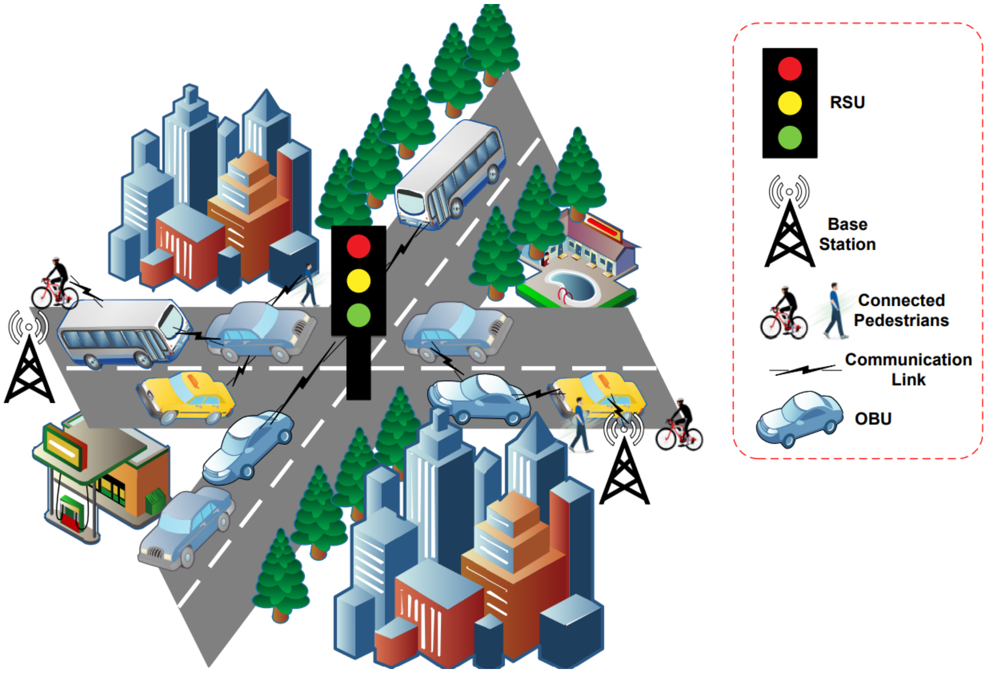


Figure 2.2.1: Components of a VANET.

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 can't provide, such as traffic monitoring. RSUs send the data to the traffic management centers (TMCs) for monitoring of 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, which takes place 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 less difficult than V2V when vehicles are traveling in opposing lanes [5]. Also, due to the dynamic nature of the entities involved, and the open nature of wireless communication in VANETs, security becomes a concern. An adversary can capture the information and manipulate it, resulting in false decisions by the TMC and the RSUs. Also, the identity of the CVs can be known compromising the security of the passengers. Many solutions have been proposed in the recent years for enhancing the security in 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, and, 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 (if only by virtue of extremely short connection times limit computational time).

Blockchains with their decentralized architecture is a viable option for VANET applications. However, public blockchains require considerable amount of energy, processing time, and also puts additional storage requirements on the network nodes. Thus, it is not suitable 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 [6]. Lightweight blockchains provide mechanisms to reduce a traditional blockchain's overhead. This can take the form of making a less energy dependent consensus mechanisms or through 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 applications 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 that of traditional chain networks where applicable. They can be of tremendous utility for VANETs, where the entities are constantly moving, having stringent real-time requirements, and with a need for strong security and authentication features. The number of published articles on blockchain are obtained from the Scopus database that is illustrated in 2.2.2.

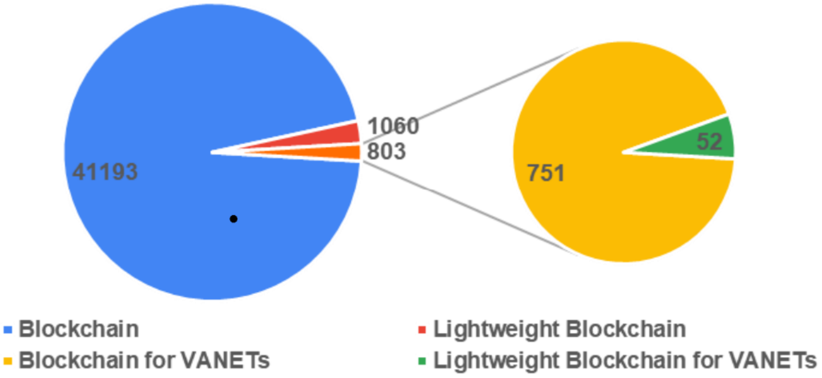


Figure 2.2.2: Publication statistics for blockchains in and out of VANETs

The publication records in 2.2.2, clearly indicate that the blockchain technology is being widely adopted for various applications, but not much popular for VANETs. Moreover, research on lightweight blockchains is still in nascent stages and its adoption for VANETs is minuscule. Thus, there is 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 2.2.1 that compare the studies based on their discussion of security, network usage, storage and computational requirements. Table 2.2.1 demonstrates various techniques intended to create a lightweight blockchain. Various aspects of using blockchains within resources 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 meant to tackle computational and network/storage issues.These works are used to formulate criteria to create lightweight blockchain within VANETs and to provide foundation for generalizations within future work. This table further justifies the novelty of this work and demonstrate the contributions of this work.

Table 2.2.1: Surveys reviewed in this work

| 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 |
|---|---|---|---|---|---|
| [7] | ✗ | ✗ | ✓ | ✓ | ✗ |
| [8] | ✗ | ✓ | ✗ | ✗ | ✗ |
| [9] | ✓ | ✓ | ✓ | ✓ | ✗ |
| [10] | ✓ | ✗ | ✗ | ✓ | ✗ |
| [11] | ✓ | ✗ | ✗ | ✗ | ✗ |
| [12] | ✓ | ✓ | ✓ | ✓ | ✗ |
| [13] | ✓ | ✗ | ✗ | ✓ | ✗ |
| [14] | ✓ | ✓ | ✓ | ✓ | ✗ |
| [15] | ✓ | ✓ | ✗ | ✗ | ✗ |
| [16] | ✓ | ✓ | ✓ | ✓ | ✗ |
| This survey | ✓ | ✓ | ✓ | ✓ | ✓ |

The existing surveys mostly focus of 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 the blockchain technology is given in the second section. Also, 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 parlance of this topic. The last section presents the conclusion of the review on lightweight blockchain.

## 2.3 Overview of Blockchain

Blockchains consist of blocks that document transactions, along with chain-related metadata [17]. 2.3.1 illustrates a generic blockchain. The chains that bind these blocks are created by hash functions: functions that map an arbitrary input to a fixed-length, characteristic value called a digest. This digest must be a function of all the input's content, must obscure the original input's content, and must be difficult to reverse-engineer: i.e., finding two inputs with the same digest must be computationally infeasible. Blockchains commonly use the SHA-256 hashing algorithm, which outputs 32-byte digests. Users interpret the digests as a 64-character hexadecimal strings that can be interpreted as integers.

With one exception, each of a chain's blocks contains the hash of the previous block in its metadata. In lieu 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.

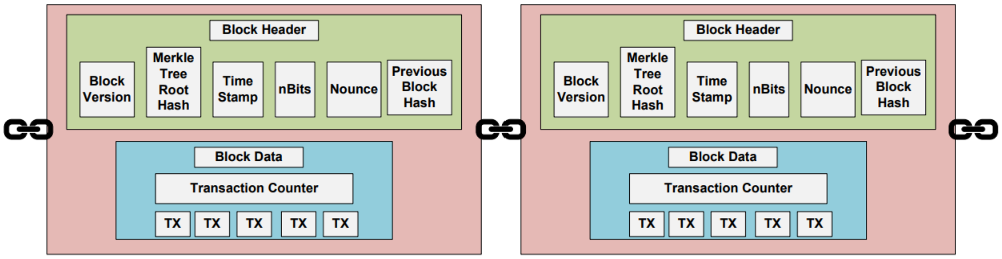


Figure 2.3.1: A typical blockchain.

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. A blockchain's user engages in a transaction by creating the transaction, then broadcasting it over the network. These transactions are collected by each user that may add to the blockchain. To protect users from counterfeit transactions, transactions must be validated and authenticated. 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 user can sign-encrypt a document with their private key and distribute their public key. Then, any user 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, 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. In order 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.

Chains, as a rule, 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.

### 2.3.1 Consensus Models 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.

### 2.3.2 Proof of Work

Three-fifths of all blockchains, including the Bitcoin blockchain, use the Proof of Work (PoW) consensus mechanism [18]. PoW requires publisher nods to compete to solve a computationally intense but easily verifiable mathematical puzzle [19]. For example, for Bitcoin, this puzzle's challenge is to find a digest that has 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 assure that it adds one block to the blockchain about 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" done 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. [20], a single transaction can power 20 U.S. homes for a day, and Bitcoin's entire network uses a similar amount of electricity annually as Austria. Etherium, another blockchain that uses a less resource-intensive PoW algorithm, requires the annual consumption of Kenya. Users will place publisher nodes near cheap electricity due to the potential cost reduction and profit increase. As these blockchains continue to grow, their environment impact will continue to increase.

### 2.3.3 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 [21]. 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, like 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.

### 2.3.4 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 [22]. 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. All nodes within the network, moreover, 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 like a trusted third party. Smart contracts can provide services to a blockchain's nodes: e.g., storing data, exposing information publicly, doing calculations, and redistributing resources among a chain's users. Contracts act as functions and an output ledger of that function.

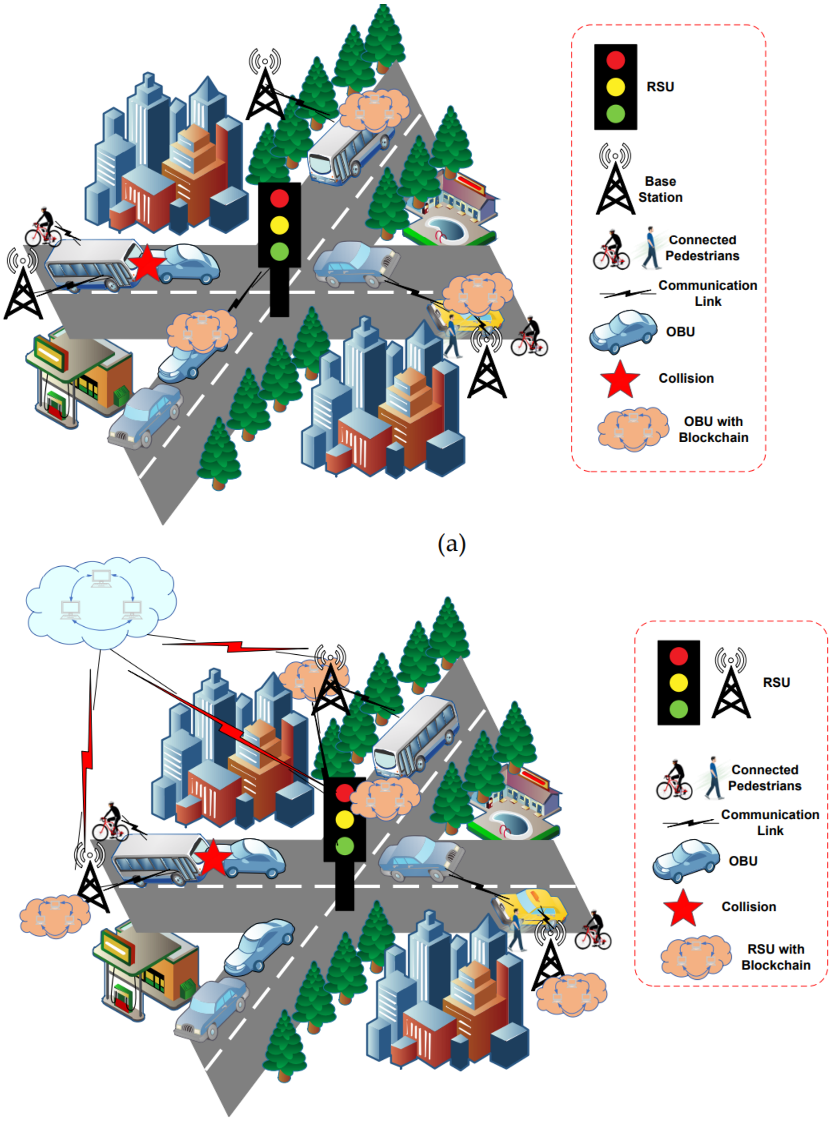
Smart contracts have built-in protections to defend against certain attacks. One, a timeout function, guards against denial of service attacks by stopping a smart contract's operation after a certain period of time. A second, a fee to execute, may be required of smart contracts in permissionless blockchains. This dissuades attackers by requiring resources to stage their attack. To gain these resources, an attack must participate within a network through honest behavior. 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.

## 2.4 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: use of blockchain at the RSUs, and the use of blockchain at the OBUs [23, 24]. Both of the architectures are depicted in 2.4.1.

Blockchain can be running on a cluster of OBUs or on the RSUs a shown in 2.4.1. OBUs are more resource constrained and the blockchain running on OBUs has to be efficiently designed compared to the the blockchain implemented on RSUs. Furthermore, the mobile nature of the OBU as compared to the static nature of the RSU, makes the implementation of blockchain challenging for this architecture. There are many methods to deploy a lightweight blockchain:

- 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 [25]. By involving only those trusted nodes, the blockchain can be made lighter.
- Lightweight Consensus Mechanism: A lightweight blockchain can be achieved by simplifying the consensus mechanism, which can also reduce the computational costs. PoS, delegated PoS (DPoS), Direct Acyclic Graph (DAG), etc., are some of the lightweight consensus mechanisms.



(a)

(b)

Figure 2.4.1: Blockchain architecture for VANETs (a) Blockchain implemented at a cluster of OBUs (b) Blockchain implemented at RSUs

- Pruning: Pruning is the process of deleting data from the blockchain that is no longer required for the validation of 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 that is no longer relevant to the current traffic scenario.

- Limiting the Number of Nodes: In VANETs, it is possible to include only those nodes (OBUs), which are within a given geographical area, as there is a greater probability of interaction between them, compared to those in another geographical area. This can make the blockchain light.

- 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.

- State Channels: State channels are off-chain channels between a group of nodes (OBUs), which allow them to conduct a large number of transactions without recording them on the main blockchain, reducing the load and making it lightweight.
- Data Compression: Compressing the data stored on the blockchain can help reduce the size of the blockchain. This can be achieved by using compression algorithms that can reduce the size of the data without affecting its integrity. This technique can be used in conjunction with other methods mentioned above.

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

### 2.4.1 Lightweight Blockchains by Efficient Trust Evaluation

Autonomous Vehicles (AVs) have complex operating requirements, due to their need for safe, secure operation. Researchers have used machine learning techniques to address some of these requirements [26]: e.g., to train in-vehicle applications to identify pedestrians and detect attacks against AV software. These applications' operation can be improved by training them with more data [27]. So long as this data is representative of real conditions, its point of origin is immaterial.

The sharing of data on environmental conditions can meet this need for improving AV operation. Sharing, however, poses risks for 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 data sets, a malicious user could identify and track the whereabouts of a user or disseminate faulty data to decrease the accuracy of certain critical tasks.

In [28], the authors present a novel, private blockchain-based method to share machine learning models and data sets safely and securely. The architecture features a low-overhead, scalable consensus mechanism, which, in experiments with 16GB of RAM and an Intel i7 8th generation processor, showed an increase in transaction verification time from 400 milliseconds to 500 milliseconds 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, the 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 by how efficiently an RSU satisfies application-specific Quality of Service (QoS) requirements. An RSU that services many vehicles over time and fulfills 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 through 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. The network follows traditional BFT procedures after this point with the network selecting the consensus leader round robin style.

Another data sharing scheme based on Practical Byzantine False Tolerance (PBFT) consensus mechanism is proposed in [29]. This consensus mechanism is not itself lightweight, but is more robust to falsification of 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 [30], 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 scheme has been proposed in [31], to identify the malicious nodes and it is observed that the performance of the scheme matches that without the presence of any attackers.

In [32], 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 that uses lightweight consensus mechanism and throughput mechanism specifically for cyberphysical systems, like a VANET. These mechanisms tend to be specific to the applications as these can vary in requirements.

### 2.4.2 Lightweight Blockchains Using Lightweight Consensus Mechanisms in VANETs

Overall, replacing PoW would be optimal to reduce a chain's network load. If PoW cannot be replaced then work can be made "useful". In [33], 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, in most applications, this is not the case and an alternative consensus mechanism can be used, like one of the variety mentioned in [34].

Consensus performance can be ascertained through consensus delay and block processing time. Consortium blockchains and a Round Robin consensus methods have been used to reduce these aspects[36]. 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 [35], the authors were able to reduce the computation cost and consensus delay more than other methods seen in that work. 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 led to a reduction of resource usage. The experimental results shows an 85% computation cost reduction, 55% storage and communication overhead, and a 90% shorter consensus delay [36].

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 [37]. Ayaz et al. in [37] proposed a novel blockchain consensus method, Proof of Quality Factor (PoQF), designed for Vehicular Edge Computing (VEC)-backed VANET environments. The authors treat vehicles as a 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 at a given instant in a network's operation. When a node receives a message (transaction proposal), the node first 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 on-board vehicle sensors.

After a node calculates its QF, the node adds its determination of a message's validity and its 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 and only if it has the highest QF when compared to the QFs found in the voting messages. If the node voted true and the votes it received match that vote, the node 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 vehicle sensors not being within range of the incident.

Ayaz et al. tested OMNet++ by integrating into a Simulation of Urban Mobility (SUMO) simulation of a VANET, PoQS's validation time increases as the number of mining nodes increase. 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 milliseconds to about 450 milliseconds. When that percentage reaches 60% of the network in that same situation, validation times increase from about 250 milliseconds to 1000 milliseconds. These messages, being emergency messages, must have a latency of at most 1 second. 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 who have none. Many current ride sharing implementations use centralized servers to connect drivers to clients and process transactions. Clients and drivers must share secure data, including identifying information and credit card numbers, to engage in a transaction. Peak usage times and server outages may delay these processes and reduce efficiency.

In [38], the authors modified the Proof of Reputation (MPoR) consensus method. Their proposed modification was to make the number of mining nodes variable as needed 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 made up less that 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 systems meant to reduce fuel costs [39]. 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 computational economy, and resist attacks such as node collusion.

PoD is as an extension of PBFT that uses PoW to limit a network's set of potential publishing nodes. Transactions contain either a request from a passenger or a response from a driver 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 vehicles' 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 total trustworthiness. The maximized value varies depending on the network environment.

Work has been completed into designing lightweight chains for IoT that support joining and leaving of 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 [40]. These may prove useful within VANET environments.

Directed Acyclic 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 [41]. This allows DAGs to reduce the network and storage requirements the network's nodes, as seen in the Internet of Things [42]. DAGs can also increase the transaction throughput by processing transactions in parallel [43]. In [44], 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 through sharding the network into smaller networks and adding weights to functions to provide incentive to have a high reputation score. These authors were able to improve the transactions per second, consensus success rate, and time of obtaining transactions while reducing dependence on RSUs.

In [45], a modified DAG consensus mechanism has been adopted to achieve lightweight operation. The DAG allows to reach consensus faster by allowing the transactions to be placed in previous transaction, thereby, helping the transactions to reach consensus in parallel. 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 [46] that also combines a historical data pruning method, minimizing duplicates and the storage space. The method is scalable and has reported to save the storage space by 97.13%. In [47], a DAG based blockchain called V-Lattice has been proposed that also combines pruning. Instead of storing the full blockchains, the nodes store a partial blockchain based on the storage availability.

The authors in [48] uses a multilayer system, one of which involved a blockchain using a dynamic Proof of Work (dPoW) to provide authentication to nodes. Their solution was able to reduce packet flows drastically compared to their baseline solution as well as using reducing computational overhead compared to other solutions. Despite being PoW based, the authors concluded that instead of using the Bitcoin model (PoW), another network like Tron could be used to reduce resources consumed and increase transactional throughput [48].

### 2.4.3 Lightweight Blockchain by Limiting Geographical Reach

A consensus mechanism's power consumption can be lowered 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 of 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 2.4.1.

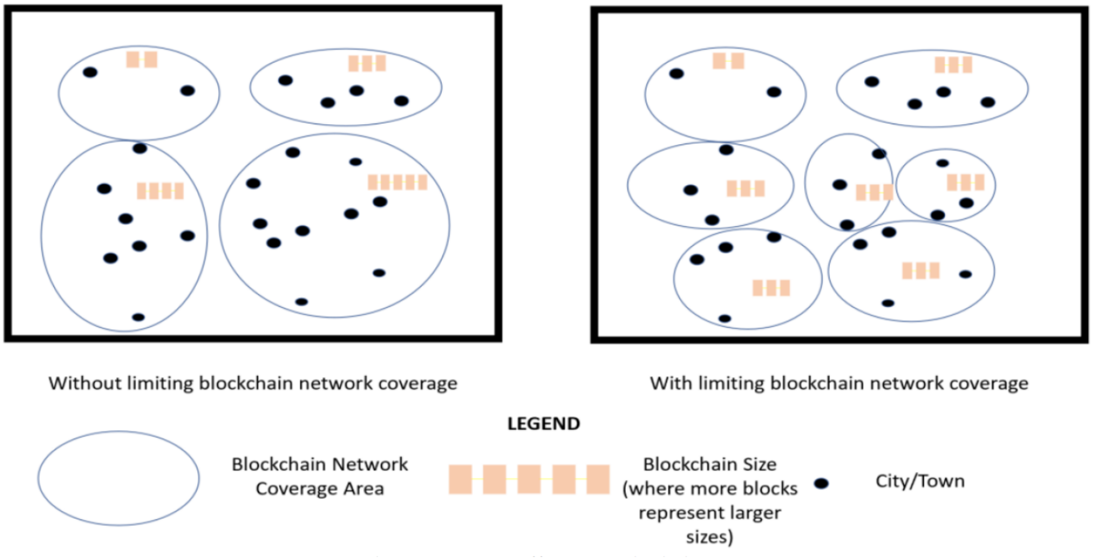

Without limiting blockchain network coverage
With limiting blockchain network coverage
LEGEND
Blockchain Network Coverage Area
Blockchain Size (where more blocks represent larger sizes)
City/Town

Figure 2.4.1: Comparing Limiting Geographic Locations' effects on Blockchain Sizes

Shrestha et al., proposed a PoW-PoS hybrid blockchain to store safety event messages and track the participating nodes' trustworthiness [49]. The authors' network consists of vehicles, which serve as mining, transacting, and publishing nodes, and RSUs, which provide authentication services to the vehicles. Transactions involve the sharing of beacon message, 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 influence that node's trust rating appropriately. A node's trust rating is a function of the ratio of number of valid messages it sends to the total number of messages it sent.

Shreshta et al. argued that 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 its computational overhead while decreasing the communication overhead required for the chain to function.

### 2.4.4 Lightweight Blockchain by Pruning

Blockchain's resource use can also be reduced through chain size reduction. The amount of blocks on the chain are proportional to the security of the chain. In resource constrained environments, this unbounded length [50] can lead to storage and network issues, especially when nodes require a full download of the chain (bootstrapping). Pruning is the process of removing part of the chain to save resources as information becomes stale over time. Pruning can be used to shrink the chains size and reduce storage and network constraints. Pruned, bounded chain provide lower network and storage resources compared to unbounded chains [51]. Pruning has been embraced in literature to bound blockchain growth [52].

However, whether or not you can prune a chain depends on the data stored on the chain. If the data requires all transactions to recreate the network state, then pruning becomes more complicated. 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 [53]. This offloading must be balanced with the reduction of security and tamper-proofing and data provenance as the attributes suffer when offloading [54].

Pruning, and storage issues from the unbounded growth, remain under researched. In S. Bel-Mannoubi et al., of the works they surveyed, only 34% of these blockchain applications investigated storage issues and only 43% address communication overhead [55]. Pruning provides a mechanism to manage these issues with a single technique.

## 2.5 Challenges and Solutions

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

- 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 may become slower, making it challenging to achieve the desired level of transaction throughput.

- Security: VANETs require secure communication among vehicles 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 attacks and double-spending attacks.
- 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 a large number of nodes, which can be challenging to achieve in VANETs due to the high mobility of the vehicles.
- Interoperability: Interoperability is essential for enabling different vehicles and infrastructure to communicate with each other effectively. The blockchain technology used in VANETs must be interoperable with other communication protocols and technologies.
- Privacy: VANETs generate a large amount of 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.
- Energy Efficiency: VANETs are typically powered by energy limited resources, which have limited capacity. Future research can focus on developing new energy-efficient blockchain architectures and consensus algorithms to reduce the energy consumption of the blockchain-based VANETs.
- 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.
- 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 [56] and even using AI to determine which nodes can participate in the consensus method [57].

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. Additionally, 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. Here are some examples:

- 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.

- 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.

- 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.

- Off-Chain Transactions: Off-chain transactions can be used to reduce the computational overhead of the blockchain by processing transactions off-chain and only submitting the final outcome to the blockchain. This can be achieved using techniques such as state channels or payment channels.

- Light Client Protocols: Light client protocols can be used to reduce the computational and storage requirements of nodes in the network. By using a lightweight protocol, nodes can participate in the network without having to download and store the entire blockchain.

- 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 [58, 59].

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.

## 2.6 Conclusion

Artificial intelligence (AI) and high speed communication networks will help mitigate the increase the number of connected vehicles with time. VANETs need to 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 difficult without direct modification. This survey focuses on the use of lightweight blockchains for VANETs. The research, even though in nascent stages, can impact the adoption of blockchain for practical applications in VANETs. Researchers have focused on developing lightweight consensus mechanisms and in detecting and minimizing the false requests before involving them in a transaction, thereby reducing the complexity. Future research can focus on developing efficient pruning methods.

## 2.7 References

[1] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," Tech. Rep. NIST IR 8202, National Institute of Standards and Technology, Gaithersburg, MD, Oct. 2018.

[2] C. Zhang, C. Wu, and X. Wang, "Overview of Blockchain Consensus Mechanism," in *Proceedings of the 2020 2nd International Conference on Big Data Engineering*, (Shanghai China), pp. 7–12, ACM, May 2020.

[3] E. K. Wang, Z. Liang, C.-M. Chen, S. Kumari, and M. K. Khan, "PoRX: A reputation incentive scheme for blockchain consensus of IIoT," *Future Generation Computer Systems*, vol. 102, pp. 140–151, Jan. 2020.

[4] U. Javaid, M. N. Aman, and B. Sikdar, "DrivMan: Driving Trust Management and Data Sharing in VANETs with Blockchain and Smart Contracts," in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, (Kuala Lumpur, Malaysia), pp. 1–5, IEEE, Apr. 2019.

[5] V. S. R. Tappeta, B. Appasani, S. Patnaik, and T. S. Ustun, "A Review on Emerging Communication and Computational Technologies for Increased Use of Plug-In Electric Vehicles," *Energies*, vol. 15, p. 6580, Sept. 2022.

[6] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles," *IEEE Communications Magazine*, vol. 56, pp. 50–57, Oct. 2018. arXiv:1802.00561 [cs].

[7] V. Elagin, A. Spirkina, M. Buinevich, and A. Vladyko, "Technological Aspects of Blockchain Application for Vehicle-to-Network," *Information*, vol. 11, p. 465, Sept. 2020.

[8] M. B. Mollah, J. Zhao, D. Niyato, Y. L. Guan, C. Yuen, S. Sun, K.-Y. Lam, and L. H. Koh, "Blockchain for the Internet of Vehicles towards Intelligent Transportation Systems: A Survey," *IEEE Internet of Things Journal*, vol. 8, pp. 4157–4185, Mar. 2021. arXiv:2007.06022 [cs].

[9] C. Peng, C. Wu, L. Gao, J. Zhang, K.-L. Alvin Yau, and Y. Ji, "Blockchain for Vehicular Internet of Things: Recent Advances and Open Issues," *Sensors*, vol. 20, p. 5079, Sept. 2020.

[10] C. Wang, X. Cheng, J. Li, Y. He, and K. Xiao, "A survey: applications of blockchain in the Internet of Vehicles," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, p. 77, Dec. 2021.

[11] B. Mikavica and A. Kostić-Ljubisavljević, "Blockchain-based solutions for security, privacy, and trust management in vehicular networks: a survey," *The Journal of Supercomputing*, vol. 77, pp. 9520–9575, Sept. 2021.

[12] J. Grover, "Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review," *Vehicular Communications*, vol. 34, p. 100458, Apr. 2022.

[13] M. Saad, M. K. Khan, and M. B. Ahmad, "Blockchain-Enabled Vehicular Ad Hoc Networks: A Systematic Literature Review," *Sustainability*, vol. 14, p. 3919, Mar. 2022.

[14] F. Azam, S. K. Yadav, N. Priyadarshi, S. Padmanaban, and R. C. Bansal, "A Comprehensive Review of Authentication Schemes in Vehicular Ad-Hoc Network," *IEEE Access*, vol. 9, pp. 31309–31321, 2021.

[15] R. Sharma, A. Thanvi, S. Singh, M. Kumar, and S. K. Jangir, *Blockchain for Vehicular Ad Hoc Network and Intelligent Transportation System: A Comprehensive Study*, ch. 7, pp. 145–173. John Wiley  Sons, Ltd, 2021.

[16] S. K. Dwivedi, R. Amin, A. K. Das, M. T. Leung, K.-K. R. Choo, and S. Vollala, "Blockchain-based vehicular ad-hoc networks: A comprehensive survey," *Ad Hoc Networks*, vol. 137, p. 102980, Dec. 2022.

[17] B. Appasani, S. K. Mishra, A. V. Jha, S. K. Mishra, F. M. Enescu, I. S. Sorlei, F. G. Bîrleanu, N. Takorabet, P. Thounthong, and N. Bizon, "Blockchain-Enabled Smart Grid Applications: Architecture, Challenges, and Solutions," *Sustainability*, vol. 14, p. 8801, July 2022.

[18] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019.

[19] B. Lashkari and P. Musilek, "A Comprehensive Review of Blockchain Consensus Mechanisms," *IEEE Access*, vol. 9, pp. 43620–43652, 2021.

[20] C. Schinckus, "Proof-of-work based blockchain technology and Anthropocene: An undermined situation?," *Renewable and Sustainable Energy Reviews*, vol. 152, p. 111682, Dec. 2021.

[21] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, and E. Dutkiewicz, "Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities," *IEEE Access*, vol. 7, pp. 85727–85745, 2019.

[22] T. Hewa, M. Ylianttila, and M. Liyanage, "Survey on blockchain based smart contracts: Applications, opportunities and challenges," *Journal of Network and Computer Applications*, vol. 177, p. 102857, Mar. 2021.

[23] S. More, R. Sonkamble, U. Naik, S. Phansalkar, P. More, and B. S. Saini, "Secured Communication in Vehicular Adhoc Networks (VANETs) using Blockchain," *IOP Conference Series: Materials Science and Engineering*, vol. 1022, p. 012067, Jan. 2021. Publisher: IOP Publishing.

[24] H. Liu, D. Han, and D. Li, "Behavior analysis and blockchain based trust management in VANETs," *Journal of Parallel and Distributed Computing*, vol. 151, pp. 61–69, May 2021.

[25] M. T. Lwin, J. Yim, and Y.-B. Ko, "Blockchain-Based Lightweight Trust Management in Mobile Ad-Hoc Networks," *Sensors*, vol. 20, p. 698, Jan. 2020.

[26] M. A. Hossain, R. Md Noor, K.-L. A. Yau, S. R. Azzuhri, M. R. Z'aba, I. Ahmedy, and M. R. Jabbarpour, "Machine Learning-Based Cooperative Spectrum Sensing in Dynamic Segmentation Enabled Cognitive Radio Vehicular Network," *Energies*, vol. 14, p. 1169, Feb. 2021.

[27] M. A. Hossain, R. Md Noor, S. R. Azzuhri, M. R. Z'aba, I. Ahmedy, K.-L. A. Yau, and C. Chembe, "Spectrum sensing challenges & their solutions in cognitive radio based vehicular networks," *International Journal of Communication Systems*, vol. 34, p. e4748, May 2021. Publisher: John Wiley & Sons, Ltd.

[28] S. Islam, S. Badsha, and S. Sengupta, "A Light-weight Blockchain Architecture for V2V Knowledge Sharing at Vehicular Edges," in *2020 IEEE International Smart Cities Conference (ISC2)*, pp. 1–8, Oct. 2020. Journal Abbreviation: 2020 IEEE International Smart Cities Conference (ISC2).

[29] Y. Zhou, Z. Cao, X. Dong, and J. Zhou, "BLDSS: A Blockchain-Based Lightweight Searchable Data Sharing Scheme in Vehicular Social Networks," *IEEE Internet of Things Journal*, vol. 10, pp. 7974–7992, May 2023.

[30] S. O. Ogundoyin and I. A. Kamil, "An efficient authentication scheme with strong privacy preservation for fog-assisted vehicular ad hoc networks based on blockchain and neuro-fuzzy," *Vehicular Communications*, vol. 31, p. 100384, Oct. 2021.

[31] J. He, Y. J. Chun, and H. C. So, "Modeling and performance analysis of blockchain-aided secure TDOA localization under random internet-of-vehicle networks," *Signal Processing*, vol. 206, p. 108904, May 2023.

[32] G. D. Putra, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "Blockchain for Trust and Reputation Management in Cyber-Physical Systems," in *Handbook on Blockchain* (D. A. Tran, M. T. Thai, and B. Krishnamachari, eds.), pp. 339–362, Cham: Springer International Publishing, 2022.

[33] Y. Wei, Z. An, S. Leng, and K. Yang, "Evolved PoW: Integrating the Matrix Computation in Machine Learning Into Blockchain Mining," *IEEE Internet of Things Journal*, vol. 10, pp. 6689–6702, Apr. 2023.

[34] N. Aung, T. Kechadi, T. Zhu, S. Zerdoumi, T. Guerbouz, and S. Dhelim, "Blockchain Application on the Internet of Vehicles (IoV)," in *2022 IEEE 7th International Conference on Intelligent Transportation Engineering (ICITE)*, pp. 586–591, Nov. 2022. Journal Abbreviation: 2022 IEEE 7th International Conference on Intelligent Transportation Engineering (ICITE).

[35] L. Vishwakarma and D. Das, "SmartCoin: A novel incentive mechanism for vehicles in intelligent transportation system based on consortium blockchain," *Vehicular Communications*, vol. 33, p. 100429, Jan. 2022.

[36] L. Vishwakarma, A. Nahar, and D. Das, "Lbsv: Lightweight blockchain security protocol for secure storage and communication in sdn-enabled iov," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 6, pp. 5983–5994, 2022.

[37] F. Ayaz, Z. Sheng, D. Tian, and Y. L. Guan, "A proof-of-quality-factor (poqf)-based blockchain and edge computing for vehicular message dissemination," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2468–2482, 2021.

[38] B. Hou, H. Zhu, Y. Xin, J. Wang, and Y. Yang, "MPoR: A Modified Consensus for Blockchain-Based Internet of Vehicles," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–17, Aug. 2022.

[39] S. Kudva, S. Badsha, S. Sengupta, I. Khalil, and A. Zomaya, "Towards secure and practical consensus for blockchain based VANET," *Information Sciences*, vol. 545, pp. 170–187, Feb. 2021.

[40] X. Hao, W. Ren, Y. Fei, T. Zhu, and K. -K. R. Choo, "A Blockchain-Based Cross-Domain and Autonomous Access Control Scheme for Internet of Things," *IEEE Transactions on Services Computing*, vol. 16, pp. 773–786, Apr. 2023.

[41] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Survey on blockchain for Internet of Things," *Computer Communications*, vol. 136, pp. 10–29, Feb. 2019.

[42] S. Kably, M. Arioua, and N. Alaoui, "Lightweight Direct Acyclic Graph Blockchain for Enhancing Resource-Constrained IoT Environment," *Computers, Materials & Continua*, vol. 71, no. 3, pp. 5271–5291, 2022.

[43] T. Alladi, V. Chamola, N. Sahu, V. Venkatesh, A. Goyal, and M. Guizani, "A Comprehensive Survey on the Applications of Blockchain for Securing Vehicular Networks," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 1212–1239, 2022.

[44] X. Zhang, R. Li, and H. Zhao, "A Parallel Consensus Mechanism Using PBFT Based on DAG-Lattice Structure in the Internet of Vehicles," *IEEE Internet of Things Journal*, vol. 10, pp. 5418–5433, Mar. 2023.

[45] H. Chai, S. Leng, F. Wu, and J. He, "Secure and efficient blockchain-based knowledge sharing for intelligent connected vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 14620–14631, 2022.

[46] W. Yang, X. Dai, J. Xiao, and H. Jin, "LDV: A Lightweight DAG-Based Blockchain for Vehicular Social Networks," *IEEE Transactions on Vehicular Technology*, vol. 69, pp. 5749–5759, June 2020.

[47] X. Zhang, R. Li, W. Hou, and H. Zhao, "V-Lattice: A Lightweight Blockchain Architecture Based on DAG-Lattice Structure for Vehicular Ad Hoc Networks," *Security and Communication Networks*, vol. 2021, pp. 1–17, May 2021.

[48] M. Gupta, R. Kumar, S. Shekhar, B. Sharma, R. B. Patel, S. Jain, I. B. Dhaou, and C. Iwendi, "Game Theory-Based Authentication Framework to Secure Internet of Vehicles with Blockchain," *Sensors*, vol. 22, p. 5119, July 2022.

[49] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, “A new type of blockchain for secure message exchange in VANET,” *Digital Communications and Networks*, vol. 6, pp. 177–186, May 2020.

[50] E. W. Bowlin and M. S. Khan, “On Utilizing Prune-able Blockchains for Secure Message Dissemination in VANETs,” in *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*, pp. 295–300, July 2021. Journal Abbreviation: 2021 IEEE 7th World Forum on Internet of Things (WF-IoT).

[51] E. W. Bowlin, M. S. Khan, and B. Bajracharya, “A Blockchain Application on Bootstrapping Mobile Nodes within VANET,” in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 1011–1016, Mar. 2023. Journal Abbreviation: 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC).

[52] D. Kevin and B. David, “HACIT2: A Privacy Preserving, Region Based and Blockchain Application for Dynamic Navigation and Forensics in VANET,” in *Ad Hoc Networks* (J. Zheng, W. Xiang, P. Lorenz, S. Mao, and F. Yan, eds.), (Cham), pp. 225–236, Springer International Publishing, 2019.

[53] X. Chen, Y. Chen, X. Wang, X. Zhu, and K. Fang, “DSVN: A Flexible and Secure Data-Sharing Model for VANET Based on Blockchain,” *Applied Sciences*, vol. 13, p. 217, Dec. 2022.

[54] C. Sey, H. Lei, W. Qian, X. Li, L. D. Fiasam, S. L. Kodjiku, I. Adjei-Mensah, and I. O. Agyemang, “VBlock: A Blockchain-Based Tamper-Proofing Data Protection Model for Internet of Vehicle Networks,” *Sensors*, vol. 22, p. 8083, Oct. 2022.

[55] S. BelMannoubi, H. Touati, M. Hadded, K. Toumi, O. Shagdar, and F. Kamoun, “A comprehensive survey on blockchain-based C-ITS applications: Classification, challenges, and open issues,” *Vehicular Communications*, p. 100607, May 2023.

[56] A. R. Javed, M. A. Hassan, F. Shahzad, W. Ahmed, S. Singh, T. Baker, and T. R. Gadekallu, “Integration of Blockchain Technology and Federated Learning in Vehicular (IoT) Networks: A Comprehensive Survey,” *Sensors*, vol. 22, p. 4394, June 2022.

[57] S. Zalte, V. Ghorpade, and R. K. Kamat, “Synergizing Blockchain, IoT, and AI with VANET for Intelligent Transport Solutions,” in *Emerging Computing Paradigms*, pp. 193–210, July 2022.

[58] *Available at: https://www.iota.org/ (Accessed: 10th February, 2023)*.

[59] *Available at: https://atonomi.io/ (Accessed: 10th February, 2023)*.

# 3 A BLOCKCHAIN APPLICATION ON BOOTSTRAPPING MOBILE NODES WITHIN VANET

*Edgar Wallace Bowlin III, Mohammad S. Khan, and Biju Bajracharya*

## 3.1 Abstract

Blockchains within Vehicular Ad-hoc Networks (VANETs) can solve issues relating to security, trust, and secure message dissemination. Platooning requires these traits to facilitate safe operation. However, traditional blockchains are not a good fit for this application. Modified blockchains are required to operate correctly within these environments. In this early work, a discussion on the packets required to operate a basic blockchain within a VANET platoon alongside a simulation are presented to demonstrate the burden of traditional blockchains in these environments and how future work can overcome these challenges.

## 3.2 Introduction

As technology improves, the creative applications of that technology multiply. The same is true for Vehicular Ad-hoc Networks (VANETs), which have matured into a into a well-researched topic and applied to real world scenarios.

Networks are used for communication, with VANETs being no exception. As more applications are designed for VANETs, requirements like security, data recoverability, and network resources are clearly defined depending on the application. For example, platooning, or the act of certain vehicles (specifically semi-trailers) cooperatively driving close together, allows for improved fuel economy. This application requires secure and trusted communication or face the risk of rogue vehicles causing harm.

Blockchains behave in such a way that provides the necessary requirements needed to operate within a VANET. However, certain challenges (which includes ephemeral connections between nodes due to their high mobility) prevent efficient blockchain operation. These connections' short life spans limit overall network throughput and may interfere with certain blockchain mechanisms like bootstrapping nodes and passing blocks between nodes.

Within this work, a discussion on the effects of block size highlights the need for implementing methods to reduce blockchains' storage requirements in VANET platoons. This work extends the discussion into packet amounts required to transfer blocks throughout a network, specifically when a new vehicle joins the network. This work is part of an on-going effort to reduce the packets required for blockchain operation and to provide a foundation for applying machine learning to this field. The rest of this work is structured in the following manner. Section 3 will discuss background information. Section 4 contains a literature review. Section 5,6,7,8 will contain the methodology, results, discussion and future work, and the conclusion.

## 3.3 Background

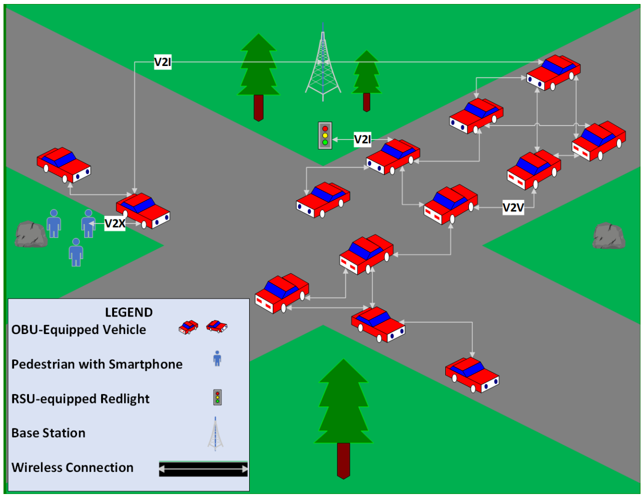


Figure 3.3.1: An example of a VANET environment.

### 3.3.1 Vehicular Ad-hoc Networks

Vehicular Ad-hoc Networks (VANETs) are networks created between vehicular nodes. These vehicles have On-Board Units (OBUs) to communicate with other devices in their environment. These nodes are highly mobile due to their vehicular nature [1]. This movement causes connections between these nodes to be ephemeral in the worst case (vehicles going opposite directions at highway speeds). Other nodes can exist within these networks, including Road Side Units (RSUs) [2] that exist on the road side and can serve as stationary edge nodes. These nodes can be used to offload computations from the mobile vehicular nodes. Depending on the wireless medium used, 5G base stations can also serve as nodes within these networks [3].

Different communication styles provide communication between different nodes within a VANET. These communication styles are largely divided by which nodes are currently communicating [3]. Vehicles communicating with other vehicles describes Vehicle-to-Vehicle (V2V) communication. Other forms of communication fall under the Vehicle-to-Everything (V2X) but can be further subdivided into Vehicle-to-Infrastructure and Vehicle-to-Pedestrian and even more divisions exist within literature [3]. These different communication styles all suffer from the high mobility of vehicular nodes. The mobile nature of these nodes creates brief connections between nodes in the worst case scenario and require special considerations from potential VANET applications. As seen in Figure 4.3.1, a VANET can commonly use each of these types at any particular moment.

VANETs exhibit certain characteristic due their nature. Within [4] several characteristics are discussed, including the following:

- Vehicular nodes have “unlimited” power compared to wireless IoT devices.
- Vehicular nodes are considered to have better storage capabilities than IoT devices.
- Vehicular nodes are highly mobile, but have predictable mobility.
- Vehicular nodes experience a non-constant topology with diverse network conditions.

These characteristics provide certain considerations that must be made when designing any application to a VANET. Of the possible requirements, privacy and security are two factors into some applications. Entertainment applications, like a video streaming service, would require less consideration into security and privacy as compared to a safety-related applications [3], such as a safety event messages and secure message dissemination [5].

Platooning, when semi-trailers travel fairly close to each to increase fuel efficiency [6] allow for shipping companies to reduce costs and their impact on the environment. This VANET application contains the considerations mentioned in this work. Semi-trailers often have to travel long distances between stops and consumes large amounts of fuel. With adaptive cruise control and V2V communication, these semis easily travel in such a way to exploit aerodynamics on these long trips and to improve road use [6]. However, if this environment is to use blockchains based on the node level as some authors have [7, 8], this creates issues related to the packet transmission. Although these semis are meant to be driving synchronously, the real-time nature of driving will necessarily force situations where vehicles may not have a clear connection to each other. Driving during rush hour in a large urban area would force these platoons to maneuver in ways that may break their connections and increase the packet drop rate throughout the network. If a blockchain must be used in this situation, a lite blockchain must be used to reduce the overhead (in this case, network overhead) as ephemeral connections will increase the packet drop percentage and further stress the network.

Within a VANET, partially due to the ad-hoc nature, nodes may not have a reason to inherently trust that a neighboring node will act in a non-malicious manner. If malicious vehicles are present, misinformation can spread or certain safety messages may not relayed through these vehicles which can lead to collateral damage [9]. If a safety-related application is to be implemented within VANETs, it must deal with the matter of trust between nodes. VANETs and the need for communication between its nodes requires a secure data structure than can help disseminate messages throughout a untrustworthy network environment.

### 3.3.2 Blockchains

Blockchains are distributed ledgers that are consensus and peer-to-peer (P2P) network based [10]. Their implementations vary depending on the application, but certain concepts are at least similar throughout these variations. Ultimately, some collection of nodes (the exact devices vary on the application) forms a P2P networks to exchange cryptographically signed data in a secure, shared, and distributed manner [11]. The blockchain itself acts as the ledger to store network relevant data and the underlying network performs its maintenance. Certain blockchain features explained later allow for nodes within these networks to overcome certain challenges [12].

- Blockchains networks provide immutability through its append only nature.
- Blockchain networks provide integrity, security, data recoverability, and distributed storage.
- Blockchain networks provide trust between nodes without a third party.

Blockchain networks can exist as one of four types (although the latter two are rarely, if ever, implemented): Private-Permissioned, Public-Permissionless, Public-Permissioned, and Private-Permissionless [10]. Public networks allow any nodes to join the network, whereas private networks only allow certain nodes to join. In contrast, permissioned networks require a node to obtain permission to publish blocks (add blocks to the chain) where a permissionless network does not [11]. Each type has their downsides and are dependent upon the application. Adding some form of permissioned access centralizes a blockchain as opposed to decentralizing it, but reduces the risk that a node will go rogue and attempt to damage the network.

Transactions form the bulk of a blockchain's storage requirements. Transactions can be viewed as traditional bank transactions [13], but can be more broadly viewed as an interaction between two parties in the network [11]. As such, the exact transaction contents will vary dependent upon application. For example, a transaction may contain the trust values of individual nodes within a network [14]. Each transaction is cryptographically signed using public key infrastructure to provide data integrity, security, and non-repudiation [11]. When a transaction is created, it is sent across the network to be stored in transaction pools found within certain nodes in the network. These can be seen as blockchain state transitions [13].

Blocks are the main data structure of the chain and contain a block header and block data [11]. A block header contains the block's metadata. What is contained in the metadata varies between implementations, but the previous block's hash remains in all implementations to form the chain.

The data portion contains transactions created within the network. These blocks are normally stored on most nodes participating within the network [13], which provides an avenue for data recovery. These blocks are immutable after a certain time and can only be appended to the chain's tail.

Storing the previous block's hash create the eponymous chain within a blockchain. Hashing algorithms take any length input and produce an unique, fixed length, output [10]. Given any input, if a new input was created that differed from the given input by a single bit, when a hash function is applied to each input, their outputs will be completely different. Moreover, in a well-designed algorithm, it Is computationally infeasible to work out a relationship between the input and output [13]. As each block contains the previous block's hash, any block's hash affects the hash of all blocks that follow it. If any data within a block is changed, its hash will be invalid and can be detected through hash checking accomplished by the individual nodes. This mechanism, along with being append-only, allows blockchains to provide data integrity and security, while providing data immutability. Blockchain networks add blocks through consensus mechanisms that allow for nodes to reach agreement on the state of the blockchain. Examples of these are Proof-of-Work found in Bitcoin and Proof-of-Stake within Ethereum.

A basic blockchain theoretically has unbounded growth [15], hardware limitations notwithstanding. Although this may be favorable in some applications, this growth affects blockchains operating within resource-constrained devices. This unbounded growth can be detrimental to network operations. A blockchain's ability to provide immutable data storage derives its strength from a chain's length. The more blocks residing on chain results in more work to be accomplished to modify a transaction found near the chain's beginning in a way that would be undetectable. However, within a VANET application, innate challenges provide difficulties to the concept of unbounded chain growth as seen in Bitcoin's chain [15]. Specifically within VANETs, OBUs storage capabilities could be upgraded to sustain this growth. This growth causes networking issues when new nodes join and must download the chain in a process called bootstrapping. The vehicle nodes' mobility creates challenges when routing packets to their destination. Nodes that require a full blockchain download also complicate this issue.

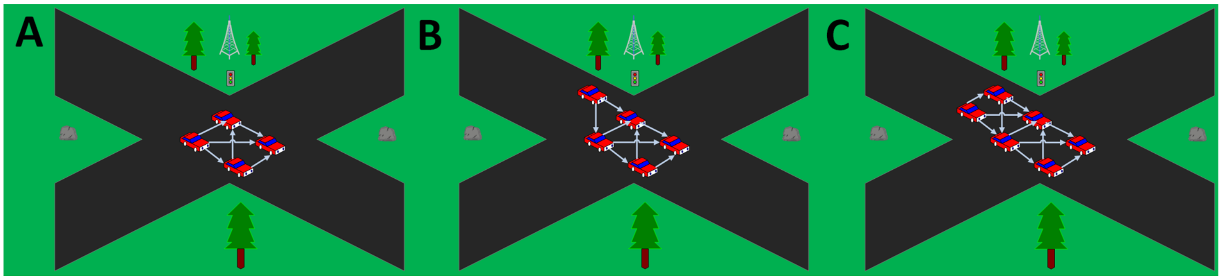


Figure 3.3.1: A) Beginning state of simulation B) Add one vehicle to state A C) Add one Vehicle to state B

### 3.3.3 Blockchain, VANET, Machine Learning, and Networking

Blockchains have been used within VANETs to ensure secure and immutable message dissemination. However, their mobility creates problems when communication between nodes is involved. To approach this issue, the authors in [16] propose separating the network into three layers, a layer that directly interacts with nodes, a layer that interacts with edge computing resources to process transactions created in the first layer, and a third layer to handle cloud services and blockchain. When designed in this manner, computational work is taken from the highly mobile nodes and placed in a more centralized location. However, data must be sent to an edge resource and may suffer from latency issues. However, for applications where the blockchain must reside on the nodes themselves, this technique may not be applicable.

Networking applications can benefit from the advantages provided by the blockchains' security and immutability and the optimization capabilities of machine learning. In [17], the authors conducted a survey of blockchain and machine learning uses within communication networks and provided key aspects as well as open challenges in this field. In particular, the authors describe advantages brought to blockchain through machine learning integration. Machine Learning can provide resource optimization to blockchain network applications [17]. Traditional Proof-of-Work consensus algorithms require large amounts of useless work for non-wining nodes, as winning could be argued as making this work useful. However, a few authors describe certain consensus mechanisms that turn this work into a useful endeavor, such as determining the winning node by choosing the best machine learning model produced by that node in a given time [17].

## 3.4 Related Works

### 3.4.1 Solana Dataset Creation

Blockchain networks contain many differently parameters that influence the network's behavior. Most blockchain networks' parameter are not easily changeable from a non-administrator role [18], but can easily be changed within test networks. Changing these parameters to optimize blockchain operation requires ML/DL to allow for learning and adapting to constantly changing network environments. [18] describes two network parameter types: observable and unobservable.

A user can easily see the exact parameter value for an observable parameter like minimum and maximum block sizes. Latency, network graphs, and bandwidth [18] cannot directly be seen within a public, permissionless blockchain network but their effects influence a blockchain's behavior. Ultimately, a blockchain can be ranked on its transactions per second, which is affected by both network parameters. [18] states that the block weight limit and difficulty adjustment result in around 2500 transactions per block or 4 transactions per second for Bitcoin's Blockchain.

The authors of [18] propose using a Machine Learning/Deep Learning (ML/DL) technique to better select the controllable observable parameters to optimize blockchain operation. Early in this endeavor, the authors focus on the creation of a data set within this paper. A Solana test net was used to gather measurements from its operation to create a data set with dimensionality of [28, 40]. The authors cleaned the data set by removing features that had an inconsequential impact using the SHAP algorithm that uses the data set and a recommender model (a 2-layer fully connected neural net) to find each feature's importance values [18] and reduced the necessary features down to six. However, the authors stopped short of using this data set with a ML/DL model but plan to pursue this action in the future.

### 3.4.2 Blockchain Enabled Deep Reinforcement Learning

Within [19], the authors combine deep reinforcement learning to optimize a blockchain's performance within an IoT Network to optimize the processing time of blocks in the network. These authors use a dynamic reinforcement learning technique to train agents to respond to their surroundings in real time [19]. Their findings found that compared to other methods, their results were able to increase system performance by 87.5%. As transactions are more quickly processed (verified by other nodes as valid), they can be sent quickly across the network. Although this optimizes blockchain performance, it also increase the amount of network traffic from transactions, and by extension through the new blocks created with those transactions. Further optimization must take place for blockchain networks to manage network resources. Without these considerations, resource-constrained nodes may perform sub-optimally or not at all.

### 3.4.3 Block Size Variation

The block size affects different aspects of blockchain networks, as seen in [20]. Using a triple layer architecture, with a VANET, application, and Blockchain layer using Hyper Ledger Fabric, the authors collected data on the impact of various block size parameters on different metrics including number of read/writes, throughput (transactions per second), and transaction latency. As the block size increased (more transactions stored within the block), throughput and transaction latency increased. As the throughput was increased, so too was the latency between a transaction's creation which causes delays for transactions to be added to the blockchain. However, after a saturation point, larger block sizes tended to reduce the transactional latency [20]. Ultimately, the authors conclude that block size affects the overall blockchain performance.

Depending on implementation, if a joining node wants to participate within the consensus mechanism, the blockchain (or at least a portion of it) must be downloaded to the node before it starts participating. However, within VANETs, the network's nodes are often moving, causing problems with routing packets. To begin analysis on this challenge, an environment, in this case, a platooning environment, must be created to understand the internal mechanisms in play.

## 3.5 Methodology

Within this paper, a basic blockchain simulator was created with Python to simulate the changes in packet counts when various block sizes when vehicles join the platoon. Within this simulation, the initial network state consists of a configuration of 4 nodes. When vehicles join the network, they join as seen in Figure 3.3.1, depending on the current configuration. For simplicity, all blocks are assumed to be the same size depending on the number of transactions stored within it (in addition to a constant 80 bytes for header information). The number of transactions within a block will vary depending on experimental settings (500, 1000, and 2000 transactions per block). All transactions are 524 bytes so that at 2000 transactions, the block size is similar to Bitcoin's blockchain for reference. The number of packets necessary was derived from dividing the total size of the block or chain being sent by the maximum size of a UDP packet (65,527 bytes without header information).

### 3.5.1 Blockchain operation

A full blockchain was not implemented for this work. However, the mechanics to create and transfer blocks through a graph of nodes to current and joining nodes is simulated to observe packet behavior. When a block is created by a randomly chosen node, it is broadcast throughout the network to all nodes. The latency of each message is set to 100ms to meet safety event message needs. To implement this functionality, nodes flood the network and use a list of hashes of previously seen messages to stop the flood through dropping any message's whose hash exists in the list. As a hybrid p2p network using a UDP-like protocol, there is not built-in mechanism to assure a packet has been sent. A simple UDP packet (10 bytes) is sent as a form of acknowledgement to assure all vehicles see all transactions eventually. If a node does not receive this message 300 milliseconds after sending a block message, it will resend the packet. Acknowledgement packets are assumed to always reach their destination as their size is inconsequential compared to the maximum UDP packet size that a blockchain download would require.

Moreover, VANETs' highly mobile vehicles will create different network conditions based on their location and traffic conditions. To simulate this, the network is assumed to have a specific packet drop percentage network-wide that varies between simulation runs. Vehicles are assumed to be travelling at a constant velocity down a straight highway to maintain inter-vehicle distances that allow for the specific packet drop percentages (0%, 25%, 50%). Vehicles are assumed to have unlimited storage in their message buffers. Assuming no packet drop, a node will receive and process a successfully sent packet 100ms (as these are meant to be emergency messages [21]) after leaving the sender. When sending multiple packets, there is a 1ms delay between each packet being sent on top of the normal processing and latency delay.

The simulation lasts for 4 hours in 1 ms steps on a trip between two urban areas. Blocks will be created every 10 minutes contain either 500,1000, or 2000 transactions to model the block creation rates as seen in Bitcoin. A new vehicle will join every ten minutes and require a full blockchain download. Each transaction amount will be tested with three network wide packet drop packages, specifically 0%, 25%, and 50%. The simulation tracks the number of successful packets sent, number of acknowledgement packets sent, number of unsuccessful packets sent, the number of vehicles that have joined, the amount of data successfully sent, the amount of data lost to packet drops, and the total data sent in the network. The network began with a blockchain that is 500 megabytes in size and increases as blocks are added. Each configuration was ran 50 times and averaged together to get the following data.

## 3.6 Results

Figure 3.6.1: Made with Matplotlib [22]

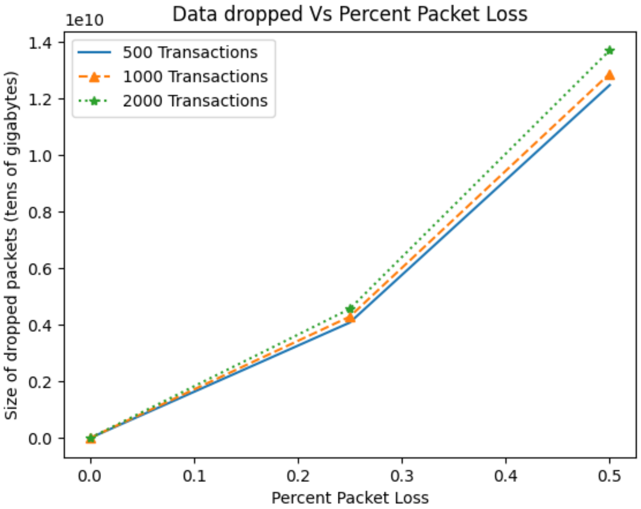
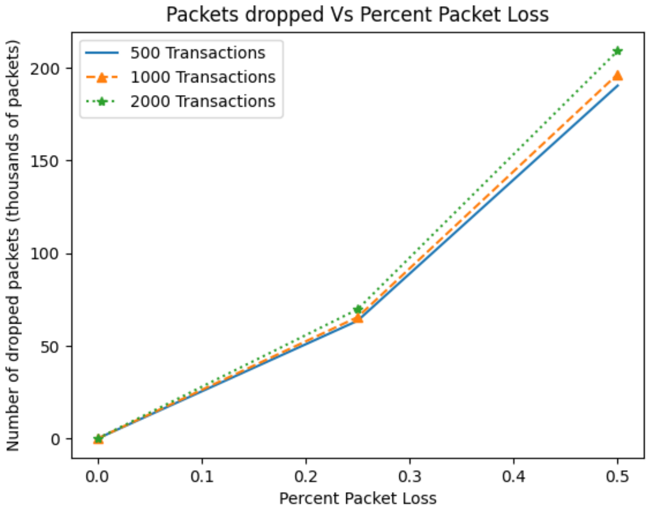


Figure 3.6.2: Made with Matplotlib [22]



As seen in Figures 3.6.1 and 3.6.2, the experimental results show that as the number of packets required to send a chain/block increases, so too does the number of dropped packets when the network is dropping packets. With more packets necessary to deliver these data structures, the higher the chance a packet will drop and degrade the quality of service for that platoon. Although larger block sizes may allow for more transactions, it also increases the chance that a packet will be dropped in poor network conditions. This relationship must be addressed depending upon an application's needs.

As vehicles joined, the number of packets sent increased greatly. The blockchain was 500 megabytes and only had 23 more blocks (of varying sizes) added to it during the simulation. The bulk of packets belonged to the chain downloads from these 23 vehicles, especially in the smaller block size simulation runs. Vehicles joining a blockchain network for the first time create an increase in the number of needed packets for proper blockchain operation. If more vehicles existed within this network for a long time, this relationship may be reversed, but would still contribute a large portion of the packets required. When designing a blockchain VANET application, this consideration allows the network to efficiently transmit data within the short rendezvous times seen within highway VANETs.

Ultimately, node bootstrapping will require a large packet commitment when a new node joins the platoon. Depending on the current size of the blockchain, this may be the bulk of sent packets. If these considerations are not considered, packet amounts will grow unbounded. These unbounded chains will create larger bottlenecks as more vehicles join the network.

## 3.7 Discussion and Future Work

Although network capacities continue to increase, any optimization on packet numbers can reduce the overall network efficiency. The results shown here demonstrate that even with a modest 25% pack drop rate, a large amount of data can be dropped within a small window of time. Twenty-three vehicles joined the network during each simulation, but in an urban environment, this number would be much larger and should be accounted for in later simulations. The packets sent when new nodes join will cause increased packet traffic. This could possibly be remedied through pre-downloading a blockchain as a vehicle is headed toward a new region or having a separate network layer handle the blockchain administration. If the blockchain must remain within the nodes, pruning the chain will be necessary for new nodes to join the network quickly and efficiently.

As a block is divided over more packets, there is a larger chance that one of them will be dropped. This action leads to a delay getting the block that could disrupt the function of the network. However, blockchains suffer from low transaction throughputs and using smaller blocks would increase this problem. A balance must be struck between security and throughput. This balance will vary from application to application but may vary even within the same application due to network conditions. Using machine learning, as seen in other VANET applications, may provide a way to determine this balance and give the network an ability to automatically adjust these settings.

## 3.8 Conclusion

The authors of this work investigated the effects block size have on packet amounts sent throughout a chain's network in a platoon-like setting. A basic simulator was created to observe how packet drops will affect the data size sent through the network to bootstrap joining nodes. As the block size increased, this network's transactions per second increased but so did the number of packets required to send it through the network. This increase demands more network resources that may not be available easily to mobile VANET nodes contributing to blockchain adoption challenges. If machine learning is leveraged to optimize this imbalance found in VANETs, blockchains could be seen as a more appealing option in these dynamic environments.

## 3.9 References

[1] K. Raheja, M. Mahajan, and A. Goel, “Implementation of GPSR protocol with various mobility models in VANET Scenario,” *Journal of Physics: Conference Series*, vol. 1950, p. 012080, Aug. 2021.

[2] P. M., S. Bourouis, A. N. Ahmed, V. M., V. K.G.S., W. Alhakami, and M. Hamdi, “A Novel Secured Multi-Access Edge Computing based VANET with Neuro fuzzy systems based Blockchain Framework,” *Computer Communications*, vol. 192, pp. 48–56, Aug. 2022.

[3] R. Hussain, F. Hussain, and S. Zeadally, “Integration of VANET and 5G Security: A review of design and implementation issues,” *Future Generation Computer Systems*, vol. 101, pp. 843–864, Dec. 2019.

[4] I. Tal and G.-M. Muntean, “Clustering and 5g-enabled smart cities: A survey of clustering schemes in vanets,” in *Research Anthology on Developing and Optimizing 5G Networks and the Impact on Society*, pp. 1012–1050, IGI Global, 2021.

[5] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, “A new type of blockchain for secure message exchange in vanet,” *Digital communications and networks*, vol. 6, no. 2, pp. 177–186, 2020.

[6] Q. Lan, D. Wen, Z. Zhang, Q. Zeng, X. Chen, P. Popovski, and K. Huang, “What is semantic communication? a view on conveying meaning in the era of machine intelligence,” *Journal of Communications and Information Networks*, vol. 6, no. 4, pp. 336–371, 2021.

[7] P. K. Singh, R. Singh, S. K. Nandi, and S. Nandi, *INTEGRATING BLOCKCHAIN WITH CACC FOR TRUST AND PLATOON MANAGEMENT*, ch. 5, pp. 77–97. John Wiley & Sons, Ltd, 2020.

[8] H. Hexmoor, S. Alsamaraee, and M. Almaghshi, “Blockchain for improved platoon security,” *International Journal of Information*, vol. 7, no. 2, pp. 1–6, 2018.

[9] S. Kudva, S. Badsha, S. Sengupta, I. Khalil, and A. Zomaya, “Towards secure and practical consensus for blockchain based VANET,” *Information Sciences*, vol. 545, pp. 170–187, Feb. 2021.

[10] H. Wan, K. Li, and Y. Huang, “Blockchain: A Review from The Perspective of Operations Researchers,” in *2020 Winter Simulation Conference (WSC)*, (Orlando, FL, USA), pp. 75–89, IEEE, Dec. 2020.

[11] D. Yaga, P. Mell, N. Roby, and K. Scarfone, “Blockchain technology overview,” Tech. Rep. NIST IR 8202, National Institute of Standards and Technology, Gaithersburg, MD, Oct. 2018.

[12] A. Z. Al-Marridi, A. Mohamed, and A. Erbad, “Reinforcement learning approaches for efficient and secure blockchain-powered smart health systems,” *Computer Networks*, vol. 197, p. 108279, Oct. 2021.

[13] D. Bryson, D. Penny, D. C. Goldenberg, and G. Serrao, “Blockchain technology for government,” tech. rep., MITRE CORP MCLEAN VA, 2017.

[14] R. Shrestha, R. Bajracharya, and S. Y. Nam, “Blockchain-based message dissemination in vanet,” in *2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS)*, pp. 161–166, 2018.

[15] E. W. Bowlin and M. S. Khan, “On Utilizing Prune-able Blockchains for Secure Message Dissemination in VANETs,” in *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*, pp. 295–300, July 2021. Journal Abbreviation: 2021 IEEE 7th World Forum on Internet of Things (WF-IoT).

[16] X. Zhang, R. Li, and B. Cui, “A security architecture of VANET based on blockchain and mobile edge computing,” in *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, (Shenzhen), pp. 258–259, IEEE, Aug. 2018.

[17] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. M. Leung, “Blockchain and Machine Learning for Communications and Networking Systems,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1392–1431, 2020.

[18] V. Amelin, N. Romanov, R. Vasilyev, R. Shvets, Y. Yanovich, and V. Zhygulin, “Machine Learning View on Blockchain Parameter Adjustment,” in *2021 3rd Blockchain and Internet of Things Conference*, (Ho Chi Minh City Vietnam), pp. 38–43, ACM, July 2021.

[19] T. Alam, “Blockchain-Enabled Deep Reinforcement Learning Approach for Performance Optimization on the Internet of Things,” *Wireless Personal Communications*, vol. 126, pp. 995–1011, Sept. 2022.

[20] P. Gaba, R. S. Raw, M. A. Mohammed, J. Nedoma, and R. Martinek, “Impact of Block Data Components on the Performance of Blockchain-Based VANET Implemented on Hyperledger Fabric,” *IEEE Access*, vol. 10, pp. 71003–71018, 2022.

[21] T. M. Mohamed, I. Z. Ahmed, and R. A. Sadek, “Efficient vanet safety message delivery and authenticity with privacy preservation,” *PeerJ Computer Science*, vol. 7, p. e519, 2021.

[22] J. D. Hunter, “Matplotlib: A 2d graphics environment,” *Computing in Science & Engineering*, vol. 9, no. 3, pp. 90–95, 2007.

# 4 REDUCING BOOTSTRAP OVERHEAD WITHIN VANET BLOCKCHAIN APPLICATIONS THROUGH PRUNING

*Edgar Wallace Bowlin III, Mohammad S. Khan, and Biju Bajracharya*

## 4.1 Abstract

Blockchains within Vehicular Ad-hoc Networks (VANETs) have enjoyed different applications within literature. Certain characteristics, like privacy and data security, are necessary to create a secure network. Blockchains provide different characteristics that can benefit VANETs. Traditional blockchains do not translate well into the highly mobile environments like VANETs. Currently, literature yields progress in adapting these data structures into these networks. However, little discussion has been created about the bootstrapping requirements when nodes join a blockchain network. Bootstrapping requires downloading a large portion of the chain and can create large network loads depending on the chain size. This work sets out to provide a pruning technique demonstrations that prunes in specific time intervals to reduce network and storage load. This method removes unnecessary blocks that are no longer need due to age and irrelevancy to the current road conditions. A discussion on the rationale of why to prune a chain is conducted. Over all, pruning provides a reduction in the overall data sent over the network, which primarily comes from bootstrapping nodes.

## 4.2 Introduction

Vehicular Ad-hoc Networks (VANETs) provide new possibilities as more connected vehicles enter the market. However, VANETs nature inherently involves human safety and property damage concerns as malicious attackers inevitably target the system. This necessitates secure data structures like blockchain, but traditional blockchains cannot be directly translated into these networks. Unbounded growth presents a problem within this network largely due to a process known as bootstrapping. VANETs are not able to handle unbounded growth and operate efficiently.

## 4.3 Vehicular Ad-hoc Networks

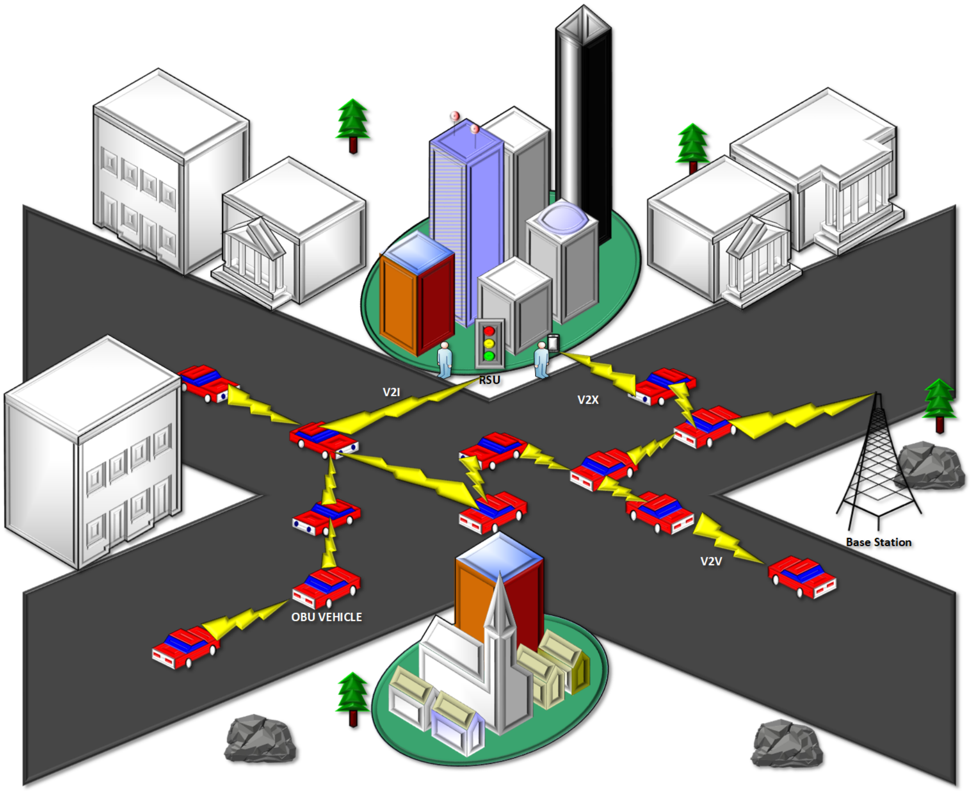


Figure 4.3.1: An example of a VANET environment.

Vehicular ad-hoc networks (VANETs) are a mobile ad-hoc network where most nodes are vehicles. VANETs consist of largely vehicular nodes but can also contain various nodes including roadside computers and user's personal devices. Vehicle nodes contain On-Board Units (OBUs) [1] that handle networking and computational needs for vehicles. Nodes designed specifically for the road-side are called Road-Side Units (RSUs) [1]. The RSUs can be assumed to be controlled by some municipality and can be assumed to be trustworthy for this work (assuming no tampering of the RSU) as these nodes can be physically protected [2].

Different communication styles exist within VANETs. Vehicle to vehicle (V2V) [1] communication has the largest variation in connection time as vehicles could be traveling in any number of directions at any number of speeds. Vehicle to Infrastructure (V2I) involves a non-moving node infrastructure node (RSU) and an OBU-equipped vehicle communicating. Vehicle to Everything (V2X) involves any device that it can wireless connect to [1], for example a pedestrian's smartphone. These can be seen in Figure 4.3.1. The wireless medium used varies depending on implementation, ranging from DSRC to 5G and may be a heterogeneous system of different mediums [3].

Vehicles provide unique challenges for wireless connectivity due to their mobile nature and the risk to property and human life. These networks require specific considerations when designing network-specific applications, as applications have clearly defined objectives to complete [4].

Applications within this type of network can be divided into three groups: road safety, road efficiency, and commercial/infotainment applications [4]. These networks encounter challenges that traditional wired networks do not. Security, privacy, and routing issues require robust solutions to assure proper network operation [4].

Routing messages through these networks requires advanced routing protocols [4]. Improving these routing mechanisms may provide a more efficient way to decrease network activity. Although ongoing works [5] are working on this issue, a simpler method to decrease network overhead would be to directly reduce the amount of data sent. Any application within VANETs must provide certain characteristics to maintain safe operation. Data must be readily available within the network and maintain its integrity. For the user's safety, there must also be some confidentiality [6].

## 4.4 Blockchains

Blockchains are a form of distributed ledger that allow for nodes to reach consensus on and store data within their shared, peer to peer network. These can be one of four network types, but only private-permissioned and public-permissionless networks are currently used [7]. The nodes can be any networked computational platform. Blockchain network operation is highly varied depending on the implementation, but these implementations all share fundamental principles that define blockchain.

Basic blockchain's data structure footprint exists through blocks that form a chain. The block is a data structure itself, but the chain forms because of metadata information within the block.

Blocks exact structure varies, but all contain a metadata section and a data (payload) section that contains transactions within the network. These transactions can simply be thought of as interactions between two or more nodes within the network [8]. Blockchain networks also use cryptography to manage signatures on transactions, among other uses [8]. Public Key Infrastructure is used to provide confidentiality to the users of the network [9]. The metadata stores various fields but the most fundamental field is the previous block's hash. This hash serves as the chain's foundation.

A well-designed hash function takes any length input and returns a unique, fixed length output. The previous blocks' hash acts as tampering detection within the blockchain. This grants a certain number of blocks maintain immutability and, assuming a network environment that is majority non-malicious, provides a secure mechanism to store data across a distributed system.

Nodes within the network serve various roles. Some nodes only contribute new transactions, whereas others take place in a consensus method to determine what data to store on the chain. Many different nodes store the chain locally and which nodes must store the chain varies. The nodes participating in consensus are often called miners [10]. These nodes often require the chain locally downloaded to be able to participate within the consensus method. Various consensus methods exist within literature and industry [10], but Proof of Work (PoW), a commonly used method, consumes large amounts of electricity. Bitcoin's blockchain uses PoW and the entire network consumed electricity equivalent to the country of Austria [11].

Blockchains provide confidentiality, integrity, and data availability to nodes within the network [6]. Blockchains within VANETs have been used for trust management within a routing protocol [12] and making security architecture along side mobile edge computers [13]. However, an issue arises in networks that serve many devices. Bootstrapping occurs when a new node joins the network [14]. This bootstrapping can add unnecessary load on the network.

This work contributes a discussion on current techniques to lighten network and storage load in literature. A simulation to provide insight and the simulation results are provided to demonstrate bootstrapping's effects on network load with a pruned and control blockchain. The final contribution comes from a discussion of the rationale on pruning and how to prune blockchains for VANET environments.

A literature review of current growth mitigation techniques is discussed to understand the current problem state in Section 2. An experiment to demonstrate pruning and other size mitigation techniques versus a control blockchain and its methodology is explained in Section 3 with a discussion of results in Section 4. Discussion and Future Work is discussed in Section 5 with a conclusion ending this work in Section 6.

## 4.5 Literature Review

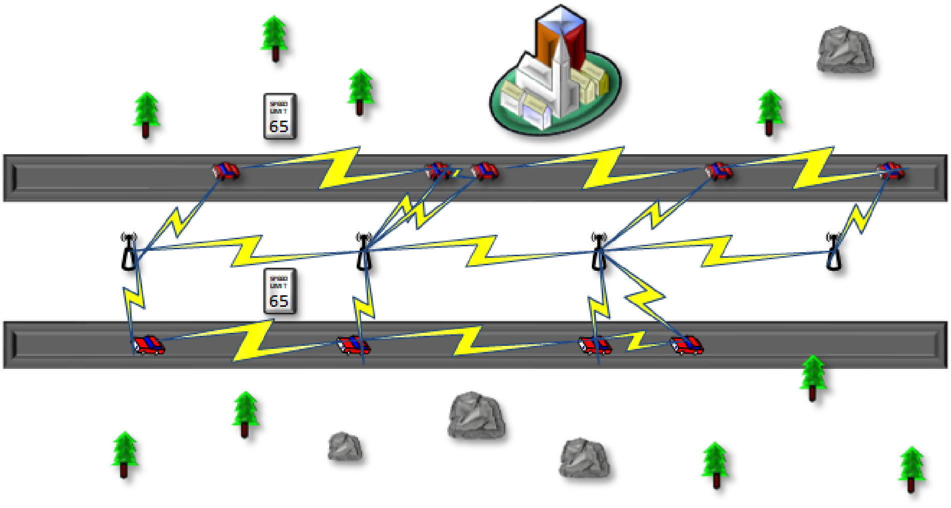


Figure 4.5.1: An example of the experiment environment.

When a blockchain is pruned, some portion of the chain is removed to reduce the overall blockchain size for some nodes [15]. How this is accomplished varies per applications' data needs but can be leveraged to reduce the chain's storage and network requirements. Traditional blockchains have unbounded growth [16], but pruning can provide a way for nodes to reduce the amount of data sent over the network. Within VANETs, data is temporally related [17] as events described in VANET environments becomes stale. Pruning within these environments have not been well studied as to how it would improve performance except through the transactions per second metric [18]. Using only this metric ignores the realities of network operation as this does not necessarily relate to other metrics like packet drop ratio.

When the blocks where pruned within [17], their metadata was retained on the RSUs so that blockchain validation could occur. As the metadata is retained, the chain retains the security of its length, but still increases without bound over a much longer period. Although within Bitcoin's blockchain, CoinPrune was proposed to prune that chain. This method was able to prune data not connected to unspent transaction data. This meant that transactions that occurred very long ago in the chain that are not relevant anymore were about to be removed. The authors saw an 85.60% reduction in size of their chain using this process [19].

A blockchain could also be sharded, or split between different groups. This allows for multiple blockchains that serve the purpose of one large blockchain. Sharding involves dividing nodes into groups (shard) that operate independently from each other [17]. Transactions within a shard are only sent and processed by the nodes within that shard. Within a VANET, sharding can be accomplished through geographic location [17]. This allows for a smaller chain per shard which would ease the network's resource use when bootstrapping nodes. The unbounded problem remains.

A Directed Acyclic Graph (DAG) [20] is a distributed ledger that functions similarly to blockchain's storage mechanism except for the main data structure. Blocks are not used within a DAG and transactions serve as the main data structure disseminated throughout the network. This allows the network to process transactions more quickly than having to wait for block generation, and it can provide parallel transaction processing. As these transactions are not linked to blocks, they can be more easily pruned allowing for a lite distributed ledger. Most nodes would only need to download a certain portion of the DAG relevant to the current time. In [21], their proposed V2V communication model, a DAG was used to avoid forking and pruning issues.

Overall, few studies have directly looked at the number of packets necessary for a highway VANET scenario. Although pruning, sharding, and DAG are attempts to increase blockchain optimization but the specific criteria would depend on the application. Focusing on network load is not as explored in current literature.

## 4.6 Methodology

Within this work, a simulation was created within Python to demonstrate chain length's effects on network performance, particularly when bootstrapping new nodes or nodes that have not been in the network for some time.

The simulation aims to compare two scenarios, a traditional blockchain and a blockchain pruned to one-fourth the size of the traditional blockchain to demonstrate the packet load created when nodes join this VANET on top of normal operation. This VANET simulates a sharded blockchain as it only covers 20 miles of highway traveling in both directions. These shards could be seen as small geographic portions of a municipality. These distributed ledgers will use the Proof-of-Work to reach consensus on the data stored in the respective data structure.

The simulation environment can be seen in Figure 4.5.1. This simulation contains a highway with lanes travelling in opposite directions with RSUs scattered throughout the highway such that all parts of the highway have wireless access to an RSU. There are no obstacles between the lanes that could block wireless connections.

Vehicles are created on each lane independently every 1 to 5 minutes with the specific time changing with each vehicle created. These vehicles travel at a constant speed between 55 and 75 miles per hour. Vehicles are traveling down a straight highway until they leave the region's blockchain shard. All messages sent by a node, even if they have left the shard region, are assumed to be eventually sent to the respective vehicle. Vehicles connect to vehicles travelling in the same direction and the closest RSU. Each RSU node connects to all vehicles within its range and is positioned so that when a vehicle leaves one RSU's service zone, it enters another.

Blocks are created every ten minutes whereas transactions are created every 500 milliseconds. Each node has a range of 3 miles. This application is assumed to use a modified UDP where the only modification is acknowledgements are sent after every message. UDP was chosen to calculate a specific size limit to packets and to know how to divide up the chain when bootstrapping another node. Three types of packets are sent during this simulation: transaction packets, blockchain packets, and bootstrapping blockchain packets. As seen in [22], for safety event applications, messages must be sent and processed within 100 milliseconds. All packets are assumed to reach this rate if they are not dropped. Packets are dropped in one of two ways, either they are dropped due to the distance from the receiver interfering with the signal, or if the message queue of the receiving node is full. If they are dropped, they are resent after another 200 milliseconds.

When a block is created, the publishing node floods its neighbors and so on until all nodes receive the message. If a vehicle receives a message it has already seen, it will be dropped as its neighbors would also have seen that message. The same mechanism is used to send transactions throughout the network. Bootstrap blockchain packets are not flooded throughout the network and only sent to the node requesting the bootstrap. Each node has a 1GB message buffer.

For this work, 40 simulations (20 per size setting) were conducted using the experimental settings described thus far. Two blockchains were used, a control chain set to 2GB in size and a pruned chain of only 500MB. These simulations were set over a 30-minute time with transaction occurring every 500ms. Vehicles entered the simulation once every 1-5 minutes, chosen randomly each time and only contained a randomly sized chain portion locally downloaded. When vehicles joined, adjacent nodes began to send the new vehicle the missing chain portions to bootstrap that vehicle. Every ten minutes, a block was created randomly from a vehicle and sent across the network. Packet counts and sizes were measured during the simulation to understand network and storage resources required. Blocks contained 1200 transactions (524 bytes each). There was a maximum of 30% packet drop chance based on a node's distance from another node. At the absolute broadcast distance, 30% of the packets would drop and that percentage would decrease until reaching 0% when nodes were adjacent.

Limitations to the simulation include the following statements. Not all packets were simulated as only the largest packets are investigated within the simulation. This simulation is assuming a best case scenario based loosely on 5G standard. Only the movement of data was simulated, so a full scale simulation of both a blockchain network and a VANET are not presented here.

## 4.7 Results

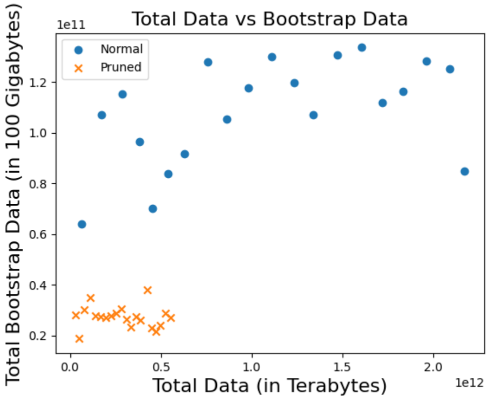


Figure 4.7.1: Comparing Total Data versus Bootstrap data

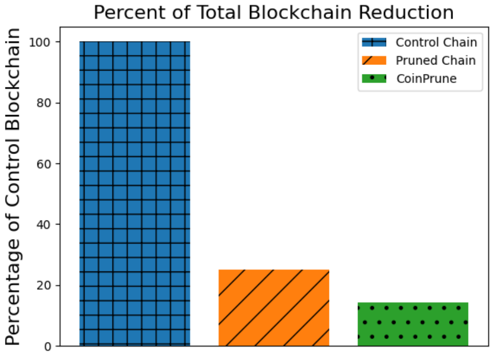


Figure 4.7.2: Comparing pruning sizes to the control chain

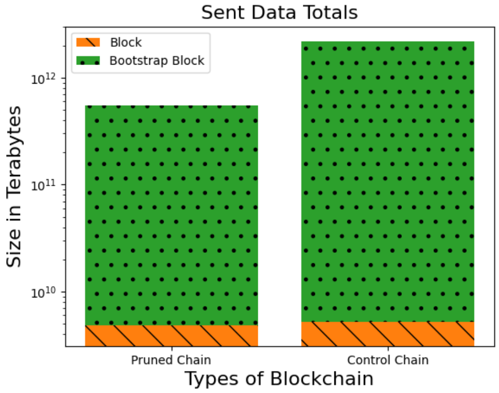


Figure 4.7.3: Comparison between Bootstrap and non-Bootstrap Data Sent

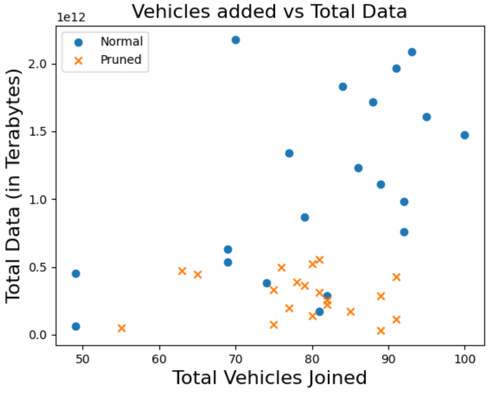


Figure 4.7.4: Vehicles Added versus Total Data

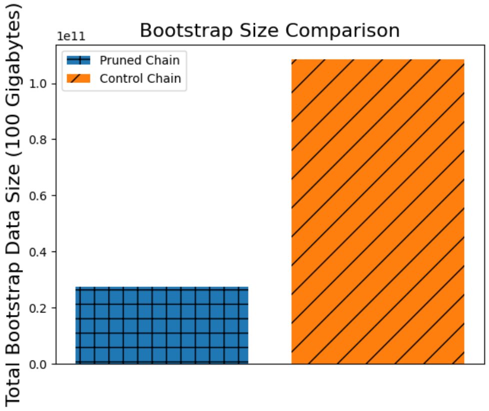


Figure 4.7.5: Bootstrap Data Size Comparison

The longer blockchains required more network traffic to bootstrap the nodes than shorter chains. The following data amounts from the tested chains can be seen in Figure 4.7.1, specifically the total data versus bootstrapping data. As more vehicles traveled the highway, the more bootstrapping had to be done to assure vehicles could actively participate in the network as seen in Figure 4.7.4. the largest portion of packets by far was from bootstrapping, but this decreased on the shorter chain.

In Figure 4.7.3, this represents the total data amounts averaged over the simulations and shows the difference between newly created blocks' overhead versus the bootstrapping processes' overhead. As seen in this experiment, the amount of bootstrapping can take up a large portion of the network's bandwidth. Depending on the amount of data most nodes are missing, bootstrapping could potentially overload a network.

The data reduction can be seen in Figure 4.7.2 in relation to the two chains simulated and a theoretical reduction if a method like CoinPrune was used. Although this reduction could be higher on the simulated chain, the chain sizes (2GB and 500MB) represent roughly an hour of history on the road and a quarter hour respectively [23]. The overall reduction of pruning can be seen in Figure 4.7.5.

## 4.8 Discussion and Future Work

When considering using distributed ledgers within VANETs, the ephemeral network topology must be considered when designing applications. Although computational and storage capabilities may not be a consideration, network resources must be considered as connections are formed and broken at rapid rates due to node movement. Although sending blocks may ultimately be trivial, bootstrapping nodes when joining the network provides a non-trivial drain on network resources. Traditional blockchain network operation allows for unbounded chain growth. As the chain grows longer, vehicles must wait longer to download what blocks they are missing. Limiting the chain size allows for growth to be bounded to an arbitrary size. This size should take into consideration the security required in the chain network and how many bootstrap-requiring nodes can be anticipated to join the network at a given time. The relationship between these considerations is the inverse. As the security needs are increased, the expected number of nodes bootstrapping needs to decrease otherwise network bandwidth would be largely dedicated to bootstrapping nodes. Machine learning has been used to various capacities within VANETs [24] and could be used here to predict these patterns. Block size should also be investigated as this can affect transaction throughput as well as network usage [25].

Iota can offer similar message dissemination without the overhead of blocks. As transactions are the only structure part of the DAG, this makes the entire structure smaller than a blockchain holding the same transactions. Another advantage for DAG is the fact nodes are only required to store transactions that they choose. RSUs could hold onto the entire graph and vehicles would only be required to store transactions relevant to it. This reduction in data structure leads to a reduction of overall network resource usage. However, as a transaction needs other transactions to affirm it, the transaction creation rate is tied to network activity. As blockchains block size can vary depending on the number of transactions stored within it, blocks can still be published at a specific rate without needing a certain number of transactions to be created. These blocks would be much smaller compared to blocks during a busy network session but allow for transactions to remain at a specific rate.

One current issue with IOTA and DAG distributed ledgers is their age. Blockchain has been around since 2009 and has been tested in various real-world applications, like Bitcoin. IOTA, on the other hand, was first mentioned in 2016 and lacks as much real-world application compared to blockchain. There may also be potential security issues revealed as this technology gains more real-world applications. Although work has been completed investigating DAG and IOTA within VANETs in literature [26], time will tell if IOTA can be as reliable as traditional blockchain systems.

Overall, the pruning action must not affect the blockchain network operation. However, this interference would vary between application to application. A safety application would not necessarily have to store data about year-old collisions long term, but a financial ledger that may handle fee enforcement would have to store data long term so that any currency within the network can be traced back through each user that interacts with it. Specific pruning heuristics are necessary per application as each application may have a unique use case when it comes to what data must be maintained and what data can either be discarded or moved to long term storage outside of the network for data analysis.

When dealing with distributed ledgers, or any other data structure, they should not have unbounded growth as the chaotic topology prevents reliable connections. Without these limitations in place, applications that require all nodes to download the entire data structure will make up the bulk of the network resource usage.

## 4.9 Conclusion

Blockchain provide opportunities for new and more advanced applications within the VANET domain. However, traditional blockchains may not translate well into dynamic topology environments like VANETs. Within this work, a discussion of why blockchains may benefit VANETs and their limitations, as well as an experiment demonstrating the reduction in network use, specifically number of packets and size of data sent, when using pruned chains. A literature review was conducted to see current methodology and to present a rational as to why to prune chains. Blockchains and other distributed ledgers should beodified to operate more efficiently in VANET network topologies in regards to bounded growth. Through a network and storage usage analysis between a control and pruned chain, this work contributed a new insight into previously used pruning systems and rationale on how to prune a chain with bootstrapping nodes within VANET environments. m

## 4.10 References

[1] N. H. Hussein, C. T. Yaw, S. P. Koh, S. K. Tiong, and K. H. Chong, "A Comprehensive Survey on Vehicular Networking: Communications, Applications, Challenges, and Upcoming Research Directions," *IEEE Access*, vol. 10, pp. 86127–86180, 2022.

[2] A. Quyoom, A. A. Mir, and D. A. Sarwar, "Security Attacks and Challenges of VANETs : A Literature Survey," *Journal of Multimedia Information System*, vol. 7, pp. 45–54, Mar. 2020.

[3] R. Hussain, F. Hussain, and S. Zeadally, "Integration of VANET and 5G Security: A review of design and implementation issues," *Future Generation Computer Systems*, vol. 101, pp. 843–864, Dec. 2019.

[4] M. Maad Hamdi, L. Audah, S. Abduljabbar Rashid, A. Hamid Mohammed, S. Alani, and A. Shamil Mustafa, "A Review of Applications, Characteristics and Challenges in Vehicular Ad Hoc Networks (VANETs)," in *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, (Ankara, Turkey), pp. 1–7, IEEE, June 2020.

[5] A. Srivastava, A. Prakash, and R. Tripathi, "Location based routing protocols in VANET: Issues and existing solutions," *Vehicular Communications*, vol. 23, p. 100231, June 2020.

[6] A. S. Mustafa, M. M. Hamdi, H. F. Mahdi, and M. S. Abood, "VANET: Towards Security Issues Review," in *2020 IEEE 5th International Symposium on Telecommunication Technologies (ISTT)*, (Shah Alam, Malaysia), pp. 151–156, IEEE, Nov. 2020.

[7] H. Wan, K. Li, and Y. Huang, "Blockchain: A Review from The Perspective of Operations Researchers," in *2020 Winter Simulation Conference (WSC)*, (Orlando, FL, USA), pp. 75–89, IEEE, Dec. 2020.

[8] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," Tech. Rep. NIST IR 8202, National Institute of Standards and Technology, Gaithersburg, MD, Oct. 2018.

[9] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *Journal of Network and Computer Applications*, vol. 126, pp. 45–58, Jan. 2019.

[10] D. P. Oyinloye, J. S. Teh, N. Jamil, and M. Alawida, "Blockchain Consensus: An Overview of Alternative Protocols," *Symmetry*, vol. 13, p. 1363, July 2021.

[11] C. Schinckus, "The good, the bad and the ugly: An overview of the sustainability of blockchain technology," *Energy Research & Social Science*, vol. 69, p. 101614, Nov. 2020.

[12] S. Kudva, S. Badsha, S. Sengupta, H. La, I. Khalil, and M. Atiquzzaman, "A scalable blockchain based trust management in VANET routing protocol," *Journal of Parallel and Distributed Computing*, vol. 152, pp. 144–156, June 2021.

[13] X. Zhang, R. Li, and B. Cui, "A security architecture of VANET based on blockchain and mobile edge computing," in *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, (Shenzhen), pp. 258–259, IEEE, Aug. 2018.

[14] E. W. Bowlin, M. S. Khan, and B. Bajracharya, "A blockchain application on bootstrapping mobile nodes within vanet," in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 1011–1016, 2023.

[15] C. P. Fernandes, C. Montez, D. D. Adriano, A. Boukerche, and M. S. Wangham, "A blockchain-based reputation system for trusted VANET nodes," *Ad Hoc Networks*, vol. 140, p. 103071, Mar. 2023.

[16] E. W. Bowlin and M. S. Khan, "On utilizing prune-able blockchains for secure message dissemination in vanets," in *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*, pp. 295–300, 2021.

[17] J. Huang, L. Kong, J. Wang, G. Chen, J. Gao, G. Huang, and M. K. Khan, “Secure Data Sharing over Vehicular Networks Based on Multi-Sharding Blockchain,” *ACM Transactions on Sensor Networks*, p. 3579035, Jan. 2023.

[18] E. Bellini, Y. Iraqi, and E. Damiani, “Blockchain-Based Distributed Trust and Reputation Management Systems: A Survey,” *IEEE Access*, vol. 8, pp. 21127–21151, 2020.

[19] R. Matzutt, B. Kalde, J. Pennekamp, A. Drichel, M. Henze, and K. Wehrle, “Coinprune: Shrinking bitcoin’s blockchain retrospectively,” *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 3064–3078, 2021.

[20] X. Zhang, R. Li, W. Hou, and H. Zhao, “V-Lattice: A Lightweight Blockchain Architecture Based on DAG-Lattice Structure for Vehicular Ad Hoc Networks,” *Security and Communication Networks*, vol. 2021, pp. 1–17, May 2021.

[21] V. Hassija, V. Chamola, V. Gupta, and G. S. S. Chalapathi, “A Framework for Secure Vehicular Network using Advanced Blockchain,” in *2020 International Wireless Communications and Mobile Computing (IWCMC)*, (Limassol, Cyprus), pp. 1260–1265, IEEE, June 2020.

[22] T. M. Mohamed, I. Z. Ahmed, and R. A. Sadek, “Efficient vanet safety message delivery and authenticity with privacy preservation,” *PeerJ Computer Science*, vol. 7, p. e519, 2021.

[23] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, “A new type of blockchain for secure message exchange in VANET,” *Digital Communications and Networks*, vol. 6, pp. 177–186, May 2020.

[24] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. M. Leung, “Blockchain and Machine Learning for Communications and Networking Systems,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1392–1431, 2020.

[25] P. Gaba, R. S. Raw, M. A. Mohammed, J. Nedoma, and R. Martinek, “Impact of Block Data Components on the Performance of Blockchain-Based VANET Implemented on Hyperledger Fabric,” *IEEE Access*, vol. 10, pp. 71003–71018, 2022.

[26] V. S. Naresh, V. V. L. D. Allavarpu, and S. Reddi, “Blockchain iota sharding-based scalable secure group communication in large vanets,” *IEEE Internet of Things Journal*, vol. 10, no. 6, pp. 5205–5213, 2023.

# 5 CONCLUSION AND FUTURE RESEARCH WORK

## 5.1 Conclusion

Although Blockchains provide certain characteristics required within a VANET, the traditional implementations do not work efficiently, or at all, within a resource constrained environment. A lightweight blockchain which takes advantage of multiple aspects including, but not limited to the following: less resource-intensive consensus methods, limiting a chain network's geographic reach, determining maximum block size, and pruning blockchains. Ultimately, for a chain network to operate efficiently, they must incorporate each of these, and possibly more.

From a network and storage perspective, pruning provides an advantage to reducing overhead and was the focus of this work. The methods proposed and investigated within this work demonstrate through a combination of geographic network limitations, block size limits, and pruning methods that the total network bandwidth can be reduced, especially when considering nodes joining the network (especially for the first time as they require bootstrapping). This pruning technique would have an a specific limit to the chain size and force a static size for the chain. To the best of these author's knowledge, this is the first demonstration of pruning chains compared to control chains with a VANET that focuses on bandwidth and packet loss reduction.

This work involved a survey of current techniques and experiments to demonstrate not only the need for lightweight blockchains, but to analyze the network overhead reduction through simulation. These simulations provide insight to pruning's effectiveness as a means to reduce network usage. However, for a chain network to properly work in these environments, a full implementation of a lightweight blockchain is needed. This includes choosing an efficient consensus mechanism, which makes up the bulk of current literature. To help support the claims made in this work, a real-world test bed and implementation must be used to get conclusive measurements and a more in-depth understanding of the ephemeral network environment.

## 5.2 Future Research

A future resource avenue from this work exists in when to prune a chain. A chain's security is based on its length; the longer the chain, the more transactions are considered to be immutable. However, this pruning method allows for the chain to be shortened and less secure. Special consideration must be taken into account when deciding how long the chain should be. The number of participating nodes, what and how much data should be kept and for how long, and how secure a chain needs to be must all be taken into consideration when deciding on the chain length.

However, VANET activity can vary wildly, from heavily used during rush hour to a sparse network late at night. The exact level of security required will vary as vehicles join and leave the chain network. A static algorithm may not perform well within this dynamic network environment as vehicular situations can involve many cars traveling at high speeds in many different directions. This could be determined through research involving machine learning or artificial intelligence.

### 5.2.1 Suggested Research Area

Through collection of traffic data, an algorithm could consume this data and learn patterns in traffic to determine specific chain lengths for different scenarios. The machine learning algorithm or artificial intelligence would need to read through unlabeled data to determine the how to optimize the chain for the current network environment. Moreover, this algorithm would need to determine when to prune the chain or what size blocks would be most efficient. The chain length, block size, and prune timing are vital to optimize a chain's network impact. Depending on the application needs, this should be dynamic to respond to the traffic fluctuations. Some unsupervised learning techniques, or possibly some artificial intelligence, may fulfill this need.

Pruning may not be possible for all chains if the application requires all historical data. For chains that can be pruned, another consideration for research is how to determine what information can be pruned. This would depend on application specifics, but the logic to decide what data can be safely pruned must be determined before pruning can begin.

### 5.2.2 Impact of Future Research

These future avenues will provide a more efficient blockchain network for VANETs and other highly mobile ad-hoc networks. As these networks may provide similar challenges to VANETs, pruning and block size optimization can enable more efficient network bandwidth utilization. If pruning is introduced, or more specifically refined, for other resource-constrained networks, greater acceptance of blockchain technology can be achieved in these fields. Although the specifics of pruning vary highly depending upon the application, the general idea could be applied to virtually any chain network with an extensive understanding of the implementation and network behavior.

# Bibliography

[1] *Available at: https://atonomi.io/ (Accessed: 10th February, 2023)*.

[2] *Available at: https://www.iota.org/ (Accessed: 10th February, 2023)*.

[3] A. Z. Al-Marridi, A. Mohamed, and A. Erbad. Reinforcement learning approaches for efficient and secure blockchain-powered smart health systems. *Computer Networks*, 197:108279, Oct. 2021.

[4] T. Alam. Blockchain-Enabled Deep Reinforcement Learning Approach for Performance Optimization on the Internet of Things. *Wireless Personal Communications*, 126(2):995–1011, Sept. 2022.

[5] V. Amelin, N. Romanov, R. Vasilyev, R. Shvets, Y. Yanovich, and V. Zhygulin. Machine Learning View on Blockchain Parameter Adjustment. In *2021 3rd Blockchain and Internet of Things Conference*, pages 38–43, Ho Chi Minh City Vietnam, July 2021. ACM.

[6] B. Appasani, S. K. Mishra, A. V. Jha, S. K. Mishra, F. M. Enescu, I. S. Sorlei, F. G. Bîrleanu, N. Takorabet, P. Thounthong, and N. Bizon. Blockchain-Enabled Smart Grid Applications: Architecture, Challenges, and Solutions. *Sustainability*, 14(14):8801, July 2022.

[7] F. Ayaz, Z. Sheng, D. Tian, and Y. L. Guan. A proof-of-quality-factor (poqf)-based blockchain and edge computing for vehicular message dissemination. *IEEE Internet of Things Journal*, 8(4):2468–2482, 2021.

[8] F. Azam, S. K. Yadav, N. Priyadarshi, S. Padmanaban, and R. C. Bansal. A Comprehensive Review of Authentication Schemes in Vehicular Ad-Hoc Network. *IEEE Access*, 9:31309–31321, 2021.

[9] E. Bellini, Y. Iraqi, and E. Damiani. Blockchain-Based Distributed Trust and Reputation Management Systems: A Survey. *IEEE Access*, 8:21127–21151, 2020.

[10] S. BelMannoubi, H. Touati, M. Hadded, K. Toumi, O. Shagdar, and F. Kamoun. A comprehensive survey on blockchain-based C-ITS applications: Classification, challenges, and open issues. *Vehicular Communications*, page 100607, May 2023.

[11] E. W. Bowlin and M. S. Khan. On utilizing prune-able blockchains for secure message dissemination in vanets. In *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*, pages 295–300, 2021.

[12] E. W. Bowlin, M. S. Khan, and B. Bajracharya. A blockchain application on bootstrapping mobile nodes within vanet. In *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 1011–1016, 2023.

[13] D. Bryson, D. Penny, D. C. Goldenberg, and G. Serrao. Blockchain technology for government. Technical report, MITRE CORP MCLEAN VA, 2017.

[14] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac. Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles. *IEEE Communications Magazine*, 56(10):50–57, Oct. 2018. arXiv:1802.00561 [cs].

[15] H. Chai, S. Leng, F. Wu, and J. He. Secure and efficient blockchain-based knowledge sharing for intelligent connected vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 23(9):14620–14631, 2022.

[16] X. Chen, Y. Chen, X. Wang, X. Zhu, and K. Fang. DSVN: A Flexible and Secure Data-Sharing Model for VANET Based on Blockchain. *Applied Sciences*, 13(1):217, Dec. 2022.

[17] S. K. Dwivedi, R. Amin, A. K. Das, M. T. Leung, K.-K. R. Choo, and S. Vollala. Blockchain-based vehicular ad-hoc networks: A comprehensive survey. *Ad Hoc Networks*, 137:102980, Dec. 2022.

[18] E. W. Bowlin and M. S. Khan. On Utilizing Prune-able Blockchains for Secure Message Dissemination in VANETs. In *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*, pages 295–300, July 2021. Journal Abbreviation: 2021 IEEE 7th World Forum on Internet of Things (WF-IoT).

[19] E. W. Bowlin, M. S. Khan, and B. Bajracharya. A Blockchain Application on Bootstrapping Mobile Nodes within VANET. In *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 1011–1016, Mar. 2023. Journal Abbreviation: 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC).

[20] V. Elagin, A. Spirkina, M. Buinevich, and A. Vladyko. Technological Aspects of Blockchain Application for Vehicle-to-Network. *Information*, 11(10):465, Sept. 2020.

[21] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar. A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications*, 126:45–58, Jan. 2019.

[22] C. P. Fernandes, C. Montez, D. D. Adriano, A. Boukerche, and M. S. Wangham. A blockchain-based reputation system for trusted VANET nodes. *Ad Hoc Networks*, 140:103071, Mar. 2023.

[23] P. Gaba, R. S. Raw, M. A. Mohammed, J. Nedoma, and R. Martinek. Impact of Block Data Components on the Performance of Blockchain-Based VANET Implemented on Hyperledger Fabric. *IEEE Access*, 10:71003–71018, 2022.

[24] J. Grover. Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review. *Vehicular Communications*, 34:100458, Apr. 2022.

[25] M. Gupta, R. Kumar, S. Shekhar, B. Sharma, R. B. Patel, S. Jain, I. B. Dhaou, and C. Iwendi. Game Theory-Based Authentication Framework to Secure Internet of Vehicles with Blockchain. *Sensors*, 22(14):5119, July 2022.

[26] V. Hassija, V. Chamola, V. Gupta, and G. S. S. Chalapathi. A Framework for Secure Vehicular Network using Advanced Blockchain. In *2020 International Wireless Communications and Mobile Computing (IWCMC)*, pages 1260–1265, Limassol, Cyprus, June 2020. IEEE.

[27] J. He, Y. J. Chun, and H. C. So. Modeling and performance analysis of blockchain-aided secure TDOA localization under random internet-of-vehicle networks. *Signal Processing*, 206:108904, May 2023.

[28] T. Hewa, M. Ylianttila, and M. Liyanage. Survey on blockchain based smart contracts: Applications, opportunities and challenges. *Journal of Network and Computer Applications*, 177:102857, Mar. 2021.

[29] H. Hexmoor, S. Alsamaraee, and M. Almaghshi. Blockchain for improved platoon security. *International Journal of Information*, 7(2):1–6, 2018.

[30] M. A. Hossain, R. Md Noor, S. R. Azzuhri, M. R. Z'aba, I. Ahmedy, K.-L. A. Yau, and C. Chembe. Spectrum sensing challenges & their solutions in cognitive radio based vehicular networks. *International Journal of Communication Systems*, 34(7):e4748, May 2021. Publisher: John Wiley & Sons, Ltd.

[31] M. A. Hossain, R. Md Noor, K.-L. A. Yau, S. R. Azzuhri, M. R. Z'aba, I. Ahmedy, and M. R. Jabbarpour. Machine Learning-Based Cooperative Spectrum Sensing in Dynamic Segmentation Enabled Cognitive Radio Vehicular Network. *Energies*, 14(4):1169, Feb. 2021.

[32] B. Hou, H. Zhu, Y. Xin, J. Wang, and Y. Yang. MPoR: A Modified Consensus for Blockchain-Based Internet of Vehicles. *Wireless Communications and Mobile Computing*, 2022:1–17, Aug. 2022.

[33] J. Huang, L. Kong, J. Wang, G. Chen, J. Gao, G. Huang, and M. K. Khan. Secure Data Sharing over Vehicular Networks Based on Multi-Sharding Blockchain. *ACM Transactions on Sensor Networks*, page 3579035, Jan. 2023.

[34] J. D. Hunter. Matplotlib: A 2d graphics environment. *Computing in Science & Engineering*, 9(3):90–95, 2007.

[35] R. Hussain, F. Hussain, and S. Zeadally. Integration of VANET and 5G Security: A review of design and implementation issues. *Future Generation Computer Systems*, 101:843–864, Dec. 2019.

[36] N. H. Hussein, C. T. Yaw, S. P. Koh, S. K. Tiong, and K. H. Chong. A Comprehensive Survey on Vehicular Networking: Communications, Applications, Challenges, and Upcoming Research Directions. *IEEE Access*, 10:86127–86180, 2022.

[37] U. Javaid, M. N. Aman, and B. Sikdar. DrivMan: Driving Trust Management and Data Sharing in VANETs with Blockchain and Smart Contracts. In *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, pages 1–5, Kuala Lumpur, Malaysia, Apr. 2019. IEEE.

[38] A. R. Javed, M. A. Hassan, F. Shahzad, W. Ahmed, S. Singh, T. Baker, and T. R. Gadekallu. Integration of Blockchain Technology and Federated Learning in Vehicular (IoT) Networks: A Comprehensive Survey. *Sensors*, 22(12):4394, June 2022.

[39] S. Kably, M. Arioua, and N. Alaoui. Lightweight Direct Acyclic Graph Blockchain for Enhancing Resource-Constrained IoT Environment. *Computers, Materials & Continua*, 71(3):5271–5291, 2022.

[40] D. Kevin and B. David. HACIT2: A Privacy Preserving, Region Based and Blockchain Application for Dynamic Navigation and Forensics in VANET. In J. Zheng, W. Xiang, P. Lorenz, S. Mao, and F. Yan, editors, *Ad Hoc Networks*, pages 225–236, Cham, 2019. Springer International Publishing.

[41] S. Kudva, S. Badsha, S. Sengupta, I. Khalil, and A. Zomaya. Towards secure and practical consensus for blockchain based VANET. *Information Sciences*, 545:170–187, Feb. 2021.

[42] S. Kudva, S. Badsha, S. Sengupta, H. La, I. Khalil, and M. Atiquzzaman. A scalable blockchain based trust management in VANET routing protocol. *Journal of Parallel and Distributed Computing*, 152:144–156, June 2021.

[43] Q. Lan, D. Wen, Z. Zhang, Q. Zeng, X. Chen, P. Popovski, and K. Huang. What is semantic communication? a view on conveying meaning in the era of machine intelligence. *Journal of Communications and Information Networks*, 6(4):336–371, 2021.

[44] B. Lashkari and P. Musilek. A Comprehensive Review of Blockchain Consensus Mechanisms. *IEEE Access*, 9:43620–43652, 2021.

[45] H. Liu, D. Han, and D. Li. Behavior analysis and blockchain based trust management in VANETs. *Journal of Parallel and Distributed Computing*, 151:61–69, May 2021.

[46] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. M. Leung. Blockchain and Machine Learning for Communications and Networking Systems. *IEEE Communications Surveys & Tutorials*, 22(2):1392–1431, 2020.

[47] M. T. Lwin, J. Yim, and Y.-B. Ko. Blockchain-Based Lightweight Trust Management in Mobile Ad-Hoc Networks. *Sensors*, 20(3):698, Jan. 2020.

[48] P. M., S. Bourouis, A. N. Ahmed, V. M., V. K.G.S., W. Alhakami, and M. Hamdi. A Novel Secured Multi-Access Edge Computing based VANET with Neuro fuzzy systems based Blockchain Framework. *Computer Communications*, 192:48–56, Aug. 2022.

[49] M. Maad Hamdi, L. Audah, S. Abduljabbar Rashid, A. Hamid Mohammed, S. Alani, and A. Shamil Mustafa. A Review of Applications, Characteristics and Challenges in Vehicular Ad Hoc Networks (VANETs). In *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pages 1–7, Ankara, Turkey, June 2020. IEEE.

[50] R. Matzutt, B. Kalde, J. Pennekamp, A. Drichel, M. Henze, and K. Wehrle. Coinprune: Shrinking bitcoin's blockchain retrospectively. *IEEE Transactions on Network and Service Management*, 18(3):3064–3078, 2021.

[51] B. Mikavica and A. Kostić-Ljubisavljević. Blockchain-based solutions for security, privacy, and trust management in vehicular networks: a survey. *The Journal of Supercomputing*, 77(9):9520–9575, Sept. 2021.

[52] T. M. Mohamed, I. Z. Ahmed, and R. A. Sadek. Efficient vanet safety message delivery and authenticity with privacy preservation. *PeerJ Computer Science*, 7:e519, 2021.

[53] M. B. Mollah, J. Zhao, D. Niyato, Y. L. Guan, C. Yuen, S. Sun, K.-Y. Lam, and L. H. Koh. Blockchain for the Internet of Vehicles towards Intelligent Transportation Systems: A Survey. *IEEE Internet of Things Journal*, 8(6):4157–4185, Mar. 2021. arXiv:2007.06022 [cs].

[54] S. More, R. Sonkamble, U. Naik, S. Phansalkar, P. More, and B. S. Saini. Secured Communication in Vehicular Adhoc Networks (VANETs) using Blockchain. *IOP Conference Series: Materials Science and Engineering*, 1022(1):012067, Jan. 2021. Publisher: IOP Publishing.

[55] A. S. Mustafa, M. M. Hamdi, H. F. Mahdi, and M. S. Abood. VANET: Towards Security Issues Review. In *2020 IEEE 5th International Symposium on Telecommunication Technologies (ISTT)*, pages 151–156, Shah Alam, Malaysia, Nov. 2020. IEEE.

[56] N. Aung, T. Kechadi, T. Zhu, S. Zerdoumi, T. Guerbouz, and S. Dhelim. Blockchain Application on the Internet of Vehicles (IoV). In *2022 IEEE 7th International Conference on Intelligent Transportation Engineering (ICITE)*, pages 586–591, Nov. 2022. Journal Abbreviation: 2022 IEEE 7th International Conference on Intelligent Transportation Engineering (ICITE).

[57] V. S. Naresh, V. V. L. D. Allavarpu, and S. Reddi. Blockchain iota sharding-based scalable secure group communication in large vanets. *IEEE Internet of Things Journal*, 10(6):5205–5213, 2023.

[58] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, and E. Dutkiewicz. Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities. *IEEE Access*, 7:85727–85745, 2019.

[59] S. O. Ogundoyin and I. A. Kamil. An efficient authentication scheme with strong privacy preservation for fog-assisted vehicular ad hoc networks based on blockchain and neuro-fuzzy. *Vehicular Communications*, 31:100384, Oct. 2021.

[60] D. P. Oyinloye, J. S. Teh, N. Jamil, and M. Alawida. Blockchain Consensus: An Overview of Alternative Protocols. *Symmetry*, 13(8):1363, July 2021.

[61] C. Peng, C. Wu, L. Gao, J. Zhang, K.-L. Alvin Yau, and Y. Ji. Blockchain for Vehicular Internet of Things: Recent Advances and Open Issues. *Sensors*, 20(18):5079, Sept. 2020.

[62] G. D. Putra, V. Dedeoglu, S. S. Kanhere, and R. Jurdak. Blockchain for Trust and Reputation Management in Cyber-Physical Systems. In D. A. Tran, M. T. Thai, and B. Krishnamachari, editors, *Handbook on Blockchain*, pages 339–362. Springer International Publishing, Cham, 2022.

[63] A. Quyoom, A. A. Mir, and D. A. Sarwar. Security Attacks and Challenges of VANETs : A Literature Survey. *Journal of Multimedia Information System*, 7(1):45–54, Mar. 2020.

[64] K. Raheja, M. Mahajan, and A. Goel. Implementation of GPSR protocol with various mobility models in VANET Scenario. *Journal of Physics: Conference Series*, 1950(1):012080, Aug. 2021.

[65] S. Islam, S. Badsha, and S. Sengupta. A Light-weight Blockchain Architecture for V2V Knowledge Sharing at Vehicular Edges. In *2020 IEEE International Smart Cities Conference (ISC2)*, pages 1–8, Oct. 2020. Journal Abbreviation: 2020 IEEE International Smart Cities Conference (ISC2).

[66] M. Saad, M. K. Khan, and M. B. Ahmad. Blockchain-Enabled Vehicular Ad Hoc Networks: A Systematic Literature Review. *Sustainability*, 14(7):3919, Mar. 2022.

[67] C. Schinckus. The good, the bad and the ugly: An overview of the sustainability of blockchain technology. *Energy Research & Social Science*, 69:101614, Nov. 2020.

[68] C. Schinckus. Proof-of-work based blockchain technology and Anthropocene: An undermined situation? *Renewable and Sustainable Energy Reviews*, 152:111682, Dec. 2021.

[69] C. Sey, H. Lei, W. Qian, X. Li, L. D. Fiasam, S. L. Kodjiku, I. Adjei-Mensah, and I. O. Agyemang. VBlock: A Blockchain-Based Tamper-Proofing Data Protection Model for Internet of Vehicle Networks. *Sensors*, 22(20):8083, Oct. 2022.

[70] R. Sharma, A. Thanvi, S. Singh, M. Kumar, and S. K. Jangir. *Blockchain for Vehicular Ad Hoc Network and Intelligent Transportation System: A Comprehensive Study*, chapter 7, pages 145–173. John Wiley  Sons, Ltd, 2021.

[71] R. Shrestha, R. Bajracharya, and S. Y. Nam. Blockchain-based message dissemination in vanet. In *2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS)*, pages 161–166, 2018.

[72] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam. A new type of blockchain for secure message exchange in VANET. *Digital Communications and Networks*, 6(2):177–186, May 2020.

[73] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam. A new type of blockchain for secure message exchange in vanet. *Digital communications and networks*, 6(2):177–186, 2020.

[74] P. K. Singh, R. Singh, S. K. Nandi, and S. Nandi. *INTEGRATING BLOCKCHAIN WITH CACC FOR TRUST AND PLATOON MANAGEMENT*, chapter 5, pages 77–97. John Wiley & Sons, Ltd, 2020.

[75] A. Srivastava, A. Prakash, and R. Tripathi. Location based routing protocols in VANET: Issues and existing solutions. *Vehicular Communications*, 23:100231, June 2020.

[76] T. Alladi, V. Chamola, N. Sahu, V. Venkatesh, A. Goyal, and M. Guizani. A Comprehensive Survey on the Applications of Blockchain for Securing Vehicular Networks. *IEEE Communications Surveys & Tutorials*, 24(2):1212–1239, 2022.

[77] I. Tal and G.-M. Muntean. Clustering and 5g-enabled smart cities: A survey of clustering schemes in vanets. In *Research Anthology on Developing and Optimizing 5G Networks and the Impact on Society*, pages 1012–1050. IGI Global, 2021.

[78] V. S. R. Tappeta, B. Appasani, S. Patnaik, and T. S. Ustun. A Review on Emerging Communication and Computational Technologies for Increased Use of Plug-In Electric Vehicles. *Energies*, 15(18):6580, Sept. 2022.

[79] L. Vishwakarma and D. Das. SmartCoin: A novel incentive mechanism for vehicles in intelligent transportation system based on consortium blockchain. *Vehicular Communications*, 33:100429, Jan. 2022.

[80] L. Vishwakarma, A. Nahar, and D. Das. Lbsv: Lightweight blockchain security protocol for secure storage and communication in sdn-enabled iov. *IEEE Transactions on Vehicular Technology*, 71(6):5983–5994, 2022.

[81] W. Yang, X. Dai, J. Xiao, and H. Jin. LDV: A Lightweight DAG-Based Blockchain for Vehicular Social Networks. *IEEE Transactions on Vehicular Technology*, 69(6):5749–5759, June 2020.

[82] H. Wan, K. Li, and Y. Huang. Blockchain: A Review from The Perspective of Operations Researchers. In *2020 Winter Simulation Conference (WSC)*, pages 75–89, Orlando, FL, USA, Dec. 2020. IEEE.

[83] C. Wang, X. Cheng, J. Li, Y. He, and K. Xiao. A survey: applications of blockchain in the Internet of Vehicles. *EURASIP Journal on Wireless Communications and Networking*, 2021(1):77, Dec. 2021.

[84] E. K. Wang, Z. Liang, C.-M. Chen, S. Kumari, and M. K. Khan. PoRX: A reputation incentive scheme for blockchain consensus of IIoT. *Future Generation Computer Systems*, 102:140–151, Jan. 2020.

[85] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim. A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. *IEEE Access*, 7:22328–22370, 2019.

[86] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng. Survey on blockchain for Internet of Things. *Computer Communications*, 136:10–29, Feb. 2019.

[87] X. Hao, W. Ren, Y. Fei, T. Zhu, and K. -K. R. Choo. A Blockchain-Based Cross-Domain and Autonomous Access Control Scheme for Internet of Things. *IEEE Transactions on Services Computing*, 16(2):773–786, Apr. 2023.

[88] X. Zhang, R. Li, and H. Zhao. A Parallel Consensus Mechanism Using PBFT Based on DAG-Lattice Structure in the Internet of Vehicles. *IEEE Internet of Things Journal*, 10(6):5418–5433, Mar. 2023.

[89] Y. Wei, Z. An, S. Leng, and K. Yang. Evolved PoW: Integrating the Matrix Computation in Machine Learning Into Blockchain Mining. *IEEE Internet of Things Journal*, 10(8):6689–6702, Apr. 2023.

[90] Y. Zhou, Z. Cao, X. Dong, and J. Zhou. BLDSS: A Blockchain-Based Lightweight Searchable Data Sharing Scheme in Vehicular Social Networks. *IEEE Internet of Things Journal*, 10(9):7974–7992, May 2023.

[91] D. Yaga, P. Mell, N. Roby, and K. Scarfone. Blockchain technology overview. Technical Report NIST IR 8202, National Institute of Standards and Technology, Gaithersburg, MD, Oct. 2018.

[92] S. Zalte, V. Ghorpade, and R. K. Kamat. Synergizing Blockchain, IoT, and AI with VANET for Intelligent Transport Solutions. In *Emerging Computing Paradigms*, pages 193–210. July 2022.

[93] C. Zhang, C. Wu, and X. Wang. Overview of Blockchain Consensus Mechanism. In *Proceedings of the 2020 2nd International Conference on Big Data Engineering*, pages 7–12, Shanghai China, May 2020. ACM.

[94] X. Zhang, R. Li, and B. Cui. A security architecture of VANET based on blockchain and mobile edge computing. In *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, pages 258–259, Shenzhen, Aug. 2018. IEEE.

[95] X. Zhang, R. Li, W. Hou, and H. Zhao. V-Lattice: A Lightweight Blockchain Architecture Based on DAG-Lattice Structure for Vehicular Ad Hoc Networks. *Security and Communication Networks*, 2021:1–17, May 2021.

# VITA

## EDGAR WALLACE BOWLIN, III

| | |
|---|---|
| Education: | M.S. Computer and Information Sciences, Applied Computer Science, East Tennessee State University, Johnson City, Tennessee, 2023<br>B.S. Computer Science, East Tennessee State University, 2021 |
| Professional Experience: | Graduate Teaching Assistant , Department of Computing, Johnson City, Tennessee, 2021 - 2023 |
| Publications: | E. W. Bowlin III, M. S. Khan, and B. Bajracharya, *A blockchain application on bootstrapping mobile nodes within vanet*, DOI: 10.1109/CCWC57344.2023.10099315<br>E. W. Bowlin III and M. S. Khan, *On Utilizing Prune-able Blockchains for Secure Message Dissemination in VANETs*, DOI: 10.1109/WF-IoT51360.2021.9595965 |
| Honors and Awards: | Epsilon Pi Upsilon Honor Society Inductee, 2023<br>Andrew CBAT Leadership Academy Graduate, 2023<br>Outstanding Graduate Student in Computing Award, 2023<br>Dean’s List, 2019-2021 |