5-2021

# On Utilizing Prunable Blockchains for Secure Message Dissemination in VANETs

Edgar Bowlin III`

# On Utilizing Prunable Blockchains for Secure Message Dissemination in VANETs

**Edgar Wallace Bowlin III**

An Undergraduate Thesis Submitted in Partial Fulfillment
of the Requirements for the
University Honors Scholars Program
Honors College
and the
Honors-in Computing Program
College of Business and Technology
East Tennessee State University

# On Utilizing Prunable Blockchains for Secure Message Dissemination in VANETs

Edgar Wallace Bowlin III, *Undergraduate*, *East Tennessee State University*

***Abstract*—Blockchain's use in Vehicular Ad-Hoc Networks (VANETs) research demonstrates that the technology provides useful attributes to allow for the safe and secure operation of VANET applications. The growth of blockchain applications pose a threat to the efficient operation of the MANET-like environment found within VANETs. Floating Genesis Blocks (FGB) can be used to preserve the state of the blockchain up to a certain point, and allows for the safe pruning of the chain without information loss. The early work presented here demonstrates two pruning techniques and compares the effects of each blockchain through simulation measurement of the chain's space requirements. A discussion on the results and recommendations for future work conclude the author's work.**

***Index Terms*—VANETs, blockchain, pruning, floating genesis block**

## I. Introduction

DUE to the maturity of VANET research, many different technologies have applications within the field. One such technology is blockchain. Blockchains allow for a decentralized ledger to contain information across nodes participating in the network. Due to the nature of VANETs, the idea becomes an attractive option for the secure storage of data; however, one possible disadvantage is rapid blockchain growth which, if left unchecked, requires unreasonable network traffic and data storage requirements.

The work demonstrated here discusses VANETs, blockchains, and applications of blockchains in VANETs. In section 2, the salient points of VANETs describe attributes needed to maintain a safe and secure network environment. In section 3, the attributes and structure of blockchains demonstrate aspects useful in VANET environments. Section 4 describes blockchain applications in VANETs and some weaknesses of those applications.

The primary issues of network performance degradation and unrealistic requirements caused by full sized blockchains may be resolved by the implementation of blockchain pruning techniques. The author's contribution in comparing various blockchain pruning techniques is illustrated in sections 5-6.

In section 7, an experiment is conducted to compare the sizes of blockchains after the application of two different pruning techniques. The results are discussed and elaborated on in section 8. Concluding the author's work are sections 9 and 10, which contain recommendations based on the research accomplished during the author's work and the conclusion of paper.

## II. Background Information

### A. VANETs

VANETs are created when two or more vehicular devices form a network [1]. The nature of vehicular movement demands the networks form spontaneously [1]. Consequently, VANETs share similarities with Mobile Ad-hoc Networks. However, the differences between the concepts [1], [2] are crucial in the application of theory to the areas of application. Unique characteristics of VANETs include variable node densities, large scale networks, and rapidly changing network topologies [2]. VANETs must also achieve certain characteristics to operate optimally, safely, and securely for all involved. In [3] the following security requirements are discussed:

- Authentication
  - Users must be authenticated to send messages
- Availability
  - Information is available on demand
- Message Integrity
  - Assures unalterable message in transmission
- Message Non-Repudiation
  - Assures users cannot deny a message that is sent from the user's vehicle
- Entity authentication
  - Assures senders of messages are authorized to use the network
- Access Control
  - Assures each node can only act within the node's permission level
- Message Confidentiality
  - Messages must remain private except to the recipient and to relevant law enforcement
- Privacy
  - Users must remain private during use of the network, except to relevant law enforcement.

The requirements create challenges for the deployment of VANETs on the massive scales indicated by [2]. From a networking perspective, availability and message integrity introduce problems involving the flow of data on the network. Severe attacks on VANETs may endanger lives directly, and thus, requires mitigation at all costs. Attacks that do not directly harm life create an opportunity to harm indirectly through violations of privacy. A system that does not implement the proper requirements cannot create a suitable virtual environment for accurate VANET operation.

A shared factor in each of the requirements is secure data storage. The data storage scheme must have the ability to be immutable to maintain records of what occurs in the network and when. The records help entities such as insurance companies and law enforcement agencies to complete legal forms.

*1) VANET INFRASTRUCTURE:* VANET nodes largely consist of vehicles and roadside infrastructure [4]. On-Board Units (OBUs) reside within vehicles in the network that handle communication between the vehicle and other nodes. The ability to outfit the vehicle with multiple sensors and processors allows for the power of the OBU to be increased. In theory, the upgrades allows for the possibility of increased computational power of any of the nodes within the network. [2]. To accommodate for the ad-hoc, mobile nature of OBUs, Road Side Units (RSUs) must reside on or near the roadside and facilitate the role of stationary nodes for the network. The RSUs make-up for the shortcomings of a network consisting entirely of mobile nodes. RSUs are tasked with running safety applications and providing Internet connectivity to the OBUs [2].

*2) VANET COMMUNICATION:* The names of the communications between the nodes represent which nodes are participating within the data exchange. Vehicles' communication with other vehicles represent vehicle to vehicle communication (V2V). V2V allows for the direct communication of vehicles. [1]. Outside services bolster the communication using vehicle to everything (V2X) communication [1]. Another form of communication highlighted often in literature is vehicle to infrastructure communication (V2I) [2], [5].

The communication types have varying overheads due to the nature of the connection. Assume a stretch of empty highway with two vehicles traveling down it. V2V connections can maintain the same average distance over time if two vehicles are traveling with the same velocity. Vehicles having equal and opposite velocities create incredibly small windows for the transmission of data during V2V communications. The situations can also occur when the vehicle is at rest, or the vehicle is moving away from a relatively stationary node respectively while communicating in V2E situations.

To facilitate communication, research into DSRC [6], 5G [7], and adapting existing cellular networks [2] within VANETs has been conducted. Regardless of the methods used, the amount of data sent over the network from a VANET within a dense vehicular situation creates a bottleneck in the successful operation of the networks. Challenges in the implementation of VANETs create unique avenues of research that enable the future function of the networks [8].

Therefore, the strain on the network necessitates research into the management of the amount of data sent over the network in a secure fashion.

### *B. BlockChains*

BlockChain's debut paper based on ideas from the 1980s and 1990s[9] provided a novel storage solution. Blockchain's peer-to-peer distributed networks [10] allow for a ledger of transactions to be created and maintained by all nodes within a network [11]. The data structure provides security and privacy while remaining public through mechanisms involving the smaller data structure, the block.

*1) The Block Data Structure:* A block consists of two parts. The first part is the header populated with metadata of the block and the block data, which houses the transactions made on the network with the possibility of other data[9].

*2) The Block Header:* The block header contains information that varies depending on how a blockchain is implemented. The following are commonly found within blockchain headers[9]:

- Block number (height)
- The previous block's hash
- A cryptographic representation of the block's data (often a merkle tree[9])
- Timestamp
- Size of Block
- Nonce value,

The header blocks allow for the security of the blockchain, due to previous block's hash stored in a block's header. Thanks to the nature of a hashing algorithm[9], each block should have a unique hash based on the data stored within. The previous block's hash inclusion into the hash function's input of a block is what links blocks together. If a malicious attacker were to attempt to alter a block within the chain, the hash of the block in question and every block afterward must be recalculated to have a fully linked chain. The longer the blockchain, the more difficulty an attacker encounters in attempting to manipulate data on the chain.

*3) The Block Data:* The block data contains the transactions and events in the network[9] available for public perusal which allows the blockchain to act as a public ledger.

*4) Blockchain Operation:* A blockchain consists of an initial block, the genesis block[10], followed by blocks added on to the chain by nodes participating within the network. An example of a blockchain can be seen in Figure 1. Depending on how nodes join the network, the chain is classified as either a permissioned or permission-less blockchain. Permissioned blockchains require nodes to be authorized before network participation whereas permission-less chains allows any node to participate in the network[9]. Permission-less chains' nature allows for decentralization to a higher degree than a permissioned blockchain. Regardless of permission type, addition of blocks to the chain, requires a secure mechanism for accepting blocks onto the chain, although with differing requirements[9]. Without a secure mechanism, malicious users could add blocks to the chain, causing havoc in the network.

*5) Consensus Models:* Security requirements demand a secure mechanism for adding blocks to the chain. The mechanisms allow a node to add a block to the chain in a secure fashion. For example, Proof of Work (PoW) requires complex computational puzzles that involve finding a hash for a block that is less than some difficulty target[9], [12]. The hash of the block must have at least a certain amount of leading zeros and is affected by the nonce found in the block header[9]. Other consensus models exist, such as Proof of Stake which allows nodes to stake some form of currency (usually cryptocurrency) to bid for the chance to add a block[9]. The described models

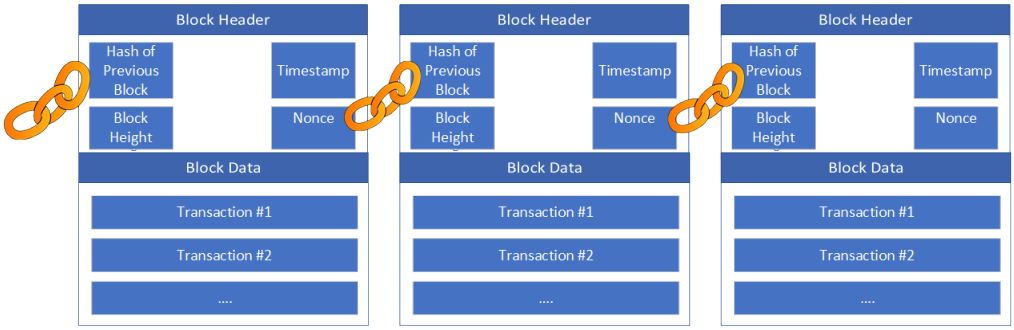


Fig. 1. Anatomy of a Blockchain.

work best in permission-less block chains. Consensus methods better suited for permissioned blockchains include Proof of Elapsed Time, Proof of Authority, Round Robin [9].

The near-immutability [9] and tampering difficultly of the blockchain creates a secure data storage mechanism that creates a decentralized method of storing data [10], [12], [11]. The attributes inspired new research toward blockchains that operate efficiently in a VANET environments. A prime example is the security tied to the size of the chain. A larger blockchain consumes a larger portion of storage in each node in the network, yet would require more work to tamper with one of the early blocks. The size of a blockchain yields security at the expense of storage and increased network traffic when a new node joins the network.

### *C. Blockchain applications within VANETs*

The blockchain's attributes entice researchers to delve into applications for VANETs. An example of blockchains in VANETs can be seen in Figure 2. Five areas of application are message dissemination, trust management, access control, malicious user detection, and authentication of vehicles operating within the network. The applications allow for different services to exist within a VANET environment.

In [13], the authors adapt a blockchain to act as an Access Control mechanism and a global data storage mechanism in a decentralized manner. Two chain exist in the solution. An identity blockchain holds the information of the users within the network. Only through a smart contract could a user attempt to retrieve the encrypted information from the blockchain, thereby protecting the users identity [13]. A data chain controls the metadata for the Inter Planetary File System. The file system allows for a peer-to-peer solution for file storage in a decentralized manner[13]. After one million transactions, the combined size of each chain is almost 2GB in size[13].

Not all blockchain solutions on VANETs require complete decentralization. In [14], a trust management system with a certificate authority (CA) allows for the distribution of trust levels. A vehicle must first register with a CA to participate within the network. The registration allows for the unlinkability of the encryption keys issued to the vehicle and the real identity of said vehicle[14]. During the authors evaluation, the size of single blockchain over the course of a year, assuming blocks are created at 10 second intervals, is found to be 1602 MB in size[14]. Another example of blockchain scheme that uses a CA is found in [15]. In the work, the authors introduce the use of cloud servers to offload storage of data from the VANET nodes and to allow for public access of that data.

For privacy concerns, the authors in [16] cite key factors in preserving privacy in general blockchains. Two factors specifically play a role within VANETs. Anonymity and Transactions unlinkability [16] provide mechanisms to establish the goal. Anonymity in the circumstance described here refers to the use of non-identifiable information during use of the network. An example of the anonymity is using pseudo-identities when participating within the network [17].

Permissioned and Permission-less blockchains can coexist in a singular solution. The authors in [18] explore such a solution. Using a trusted authority [18] and the concept of restricting blockchains to a geographical location, the authors detail a system to create a private blockchain containing the identities of new vehicles in the network, and a public blockchain allows for message dissemination across the network. The authors introduce a blockchain to replace RSUs, known as RSU-Blockchain[18].

The authors in [19] use regional blockchains in an attempt to manage the blockchain's requirements. Moreover, hierarchical partitioning, as the authors discuss, allows for trees of blockchains to represent countries and the various blockchains that would exist in such a system.

In an attempt to further augment blockchain for VANET use, The authors of [20] use mini blockchains. The chains include an account tree, transaction tree, and proof of chain. However, when new blocks are added to the chain, the last block on the account tree and transaction tree are removed, but the proof of chain information remained untouched. The authors argued mini blockchains allow for the blockchain to maintain a reasonable size[20]. Every vehicle in the scheme has a copy of the blockchain.

The ephemeral aspects of VANETs prevent the proper function of a PoW based blockchain [21]. The previous factor pushes researchers to find other consensus mechanisms that maintain the security of the blockchain. [22], [17].

With the growth of blockchain use in VANET research, special care must be taken into the mundane aspects of network maintenance. As the blockchains continue to increase in size, so too does the storage requirements for full nodes. Any nodes that may download the entire chain adds an extra

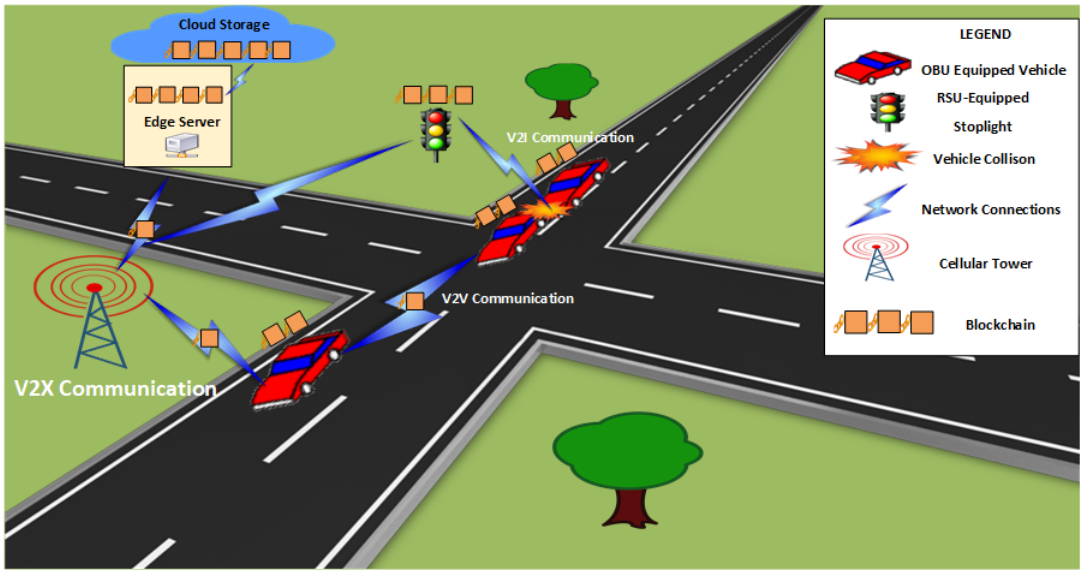


Fig. 2. An example of blockchains within VANET environment.

burden to the network traffic and routing.

## III. Contributions

The constantly growing blockchain provides an obstacle to overcome if the use of blockchain is to be included within VANETs' various applications. If the blockchain grows without bound, relying on the entire ledger to store information without some form of data compression creates bottlenecks at various times. For example, a vehicle needs to download the entire blockchain to enable participation within the network as a full node. In another example, vehicles who reside in the network for some time accumulates blocks that may ultimately overwhelm the storage capabilities of that vehicle. For a blockchain based on Bitcoin's implementation, the growth rate can reach 1.548 terabytes per year [23]. If the blockchain networks are split geographically, as seen in [23], the obstacle is lessened, but still remains. VANETs require a method to decrease the size of the blockchain without compromising the information and integrity of the blockchain.

Two methods of pruning blockchains are investigated. The first method is CoinPrune [24]. Originally researched for Bitcoin's blockchain, the method can be adapted to preserve information within a VANET blockchain. The second method is the FGB method[25], which accomplishes the task in a different, albeit similar manner. A simulation is run to demonstrate how much space a blockchain would occupy on a node's storage medium according to three styles of trimming; a control blockchain (no pruning), a CoinPrune blockchain, and an FGB blockchain. Recommendations and conclusions are discussed after the experimental results.

## IV. Literature Review

In [24], the authors present a method of pruning the bitcoin blockchain while maintaining information from the data pruned. The method involves the concept of pulse blocks [24]. The pulse blocks are the nth block on the chain. The pulse block initiates the pulse duration. During the pulse duration time, a snapshot is created of all the blocks up to and including the pulse block's height by all nodes. All blocks up to and including the pulse block are used in chunks to create a hash value, alongside a set serialized unspent transaction outputs[24] that are stored in the snapshot. The snapshot allows for the preservation of the information stored within the pruned blocks without storing the blocks.

After the snapshot is created, each node places the hash of the snapshot inside of the transactions created by that node. After the mth block, where m is less than n, nodes search through the m blocks to count reaffirmations [24] of the snapshot hashes in the transactions. Assuming a majority of non-malicious nodes, a majority of affirmations to a single hash allows the nodes in the network to prune the block data of all blocks up to and including the pulse block. The majority must be made up of some minimum number of members to prevent attacks during low participation in the network[24].

During pruning, the headers of the pruned blocks are maintained to provide an ability to bootstrap new nodes within the bitcoin application. To bootstrap a joining node, the node downloads a snapshot from nearby nodes or some third-party service[24], the headers of the blocks pruned from the snapshot, and a chain tail that contains an amount of blocks after the pulse block to maintain the security provided by blockchains of an arbitrarily long length. After the procedure and validation of the data given to the node, the node accepts the chain and begins participation in the network.

Another method of pruning the blockchain is discussed in [25]. The method allows for the state of the blockchain to be affixed to a block, instead of an off-chain data structure. Every nth block is known as a fixing block[25]. The block stores the state of the network up to that block. After some time, the blocks included in that fixing block can be safely pruned and the fixing block becomes the new genesis block. The technique is known as Floating Genesis Block[25]. The method does not

require the header blocks of the pruned nodes and have been adapted for use in VANET environments[25]. To the author's knowledge, no direct comparison has been conducted between the blockchain pruning techniques.

## V. Research Methods

Three blockchains are created using identical transactions. Transactions in the scenario are safety event messages. The messages provide information about the local driving environment, including accident information and incoming emergency vehicles. Vehicles were generated and assigned simple integer IDs to track which vehicle sent a transaction and a trust level based on a normal distribution to provide a range of various trust levels to track if information was being retained after pruning. The focus of the experiment is to measure the space occupied by blockchains maintained by two separate pruning techniques and to compare those with a control blockchain.

The size of the blockchain is determined by the amount of UTF-8 characters stored in the block. As mentioned in [23], the size of the headers in the authors' simulation are 80 bytes total. Information stored in the header include a timestamp, hash of the previous block and the rest of the 80 bytes in random UTF-8 characters. Transactions fill the block data and are 512 bytes in size. The information stored within the transactions include the pseudo ID of the vehicle involved, the timestamp, and the trust level of the message. The remaining bytes are filled with random UTF-8 characters.

Trust relates to the validity of the message. If the message is valid, the message is rated with a one. If the message is not, the message is rated with a zero. The number of valid messages divided by the total number of messages sent by the vehicle in question determines the vehicles trustworthiness [23]. The metrics are included to assure the pruned blockchain maintained informational integrity through pruning cycles. The simulation write blockchains to text files to assure the blockchain assembly succeeded. The state of the network in the experiment represents the trust levels of all vehicles within the simulation. Only one vehicle is simulated as a proof-of-concept.

The three blockchains created span three groups. The first blockchain contains a control that does nothing to attempt to save space.

The second blockchain prunes itself using a technique derived from [24]. The technique creates a pulse block every one hundred blocks and waits fifty blocks to prune the chain. The snapshot in the scenario contains the vehicles total messages sent and valid messages sent for each vehicle in the network. The snapshot contents aid in determining the trust of the vehicles involved in the network at the end of the simulation to ensure no information loss occurs.

The final blockchain prunes itself according to an FGB method as seen in [25]. In the simulation, for every 100 blocks, an extra block is added containing the state of the network at that point (in the experiment, the same snapshot as used in the previous blockchain). The snapshot again aids in the accuracy of the information retention scheme. However, the snapshot is placed in one of the blocks on the chain, instead of an off-chain message. Every fiftieth block, the blockchain is allowed to prune itself to just before the newly added fixing block. Three runs of the experiment use three blockchain sizes: one, five, and ten thousand blocks in length. The runs use fifty, one hundred, and two hundred transactions per block for each size of blockchain. The final sizes of the blockchains are recorded and compared to one another.

The experiment assumes the following: the use of a VANET friendly consensus mechanism to implement the security of the blockchains in a real-world scenario, information must persist over the time, the amount of malicious users is negligible, all blockchain pruning mechanisms achieve consensus every time and therefore successfully prune each blockchain's respective blocks, vehicles can be full nodes and must download the entire chain to participate.

TABLE I
One-Thousand Block Blockchain Results

| Number of Transactions | Control(in Megabytes) | CoinPrune(in Megabytes) | FGB(in Megabytes) |
|---|---|---|---|
| 50 | 25.68008 | 2.64008 | 2.568304 |
| 100 | 51.28008 | 5.20008 | 5.128304 |
| 200 | 102.48008 | 10.32008 | 10.248304 |

TABLE II
Five-Thousand Block Blockchain Results

| Number of Transactions | Control(in Megabytes) | CoinPrune(in Megabytes) | FGB(in Megabytes) |
|---|---|---|---|
| 50 | 128.40008 | 2.96008 | 2.568304 |
| 100 | 256.40008 | 5.52008 | 5.128304 |
| 200 | 512.40008 | 10.64008 | 10.248304 |

TABLE III
Ten-Thousand Block Blockchain Results

| Number of Transactions | Control(in Megabytes) | CoinPrune(in Megabytes) | FGB(in Megabytes) |
|---|---|---|---|
| 50 | 256.80008 | 3.36008 | 2.568304 |
| 100 | 512.80008 | 5.92008 | 5.128304 |
| 200 | 1024.80008 | 11.04008 | 10.248304 |

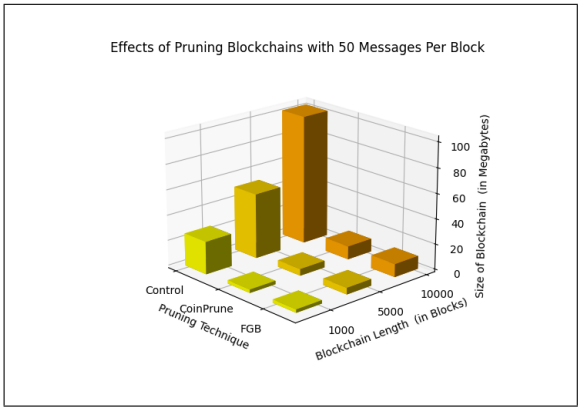


Fig. 3. Blockchain sizes with 50 messages

## VI. Experimental Results

The results are shown in Figures 3,4,5 and in Tables I,II,III. The blockchains that are pruned are an order of magnitude

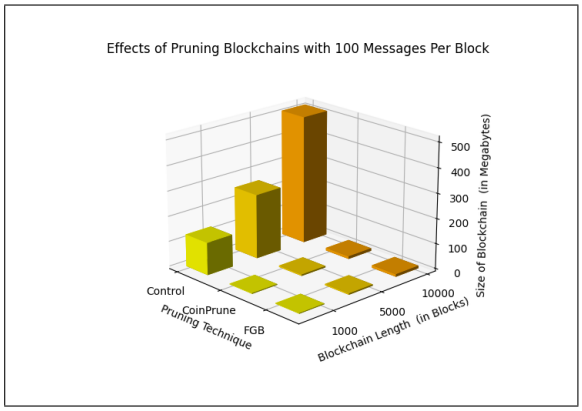


Fig. 4. Blockchain sizes with 100 messages

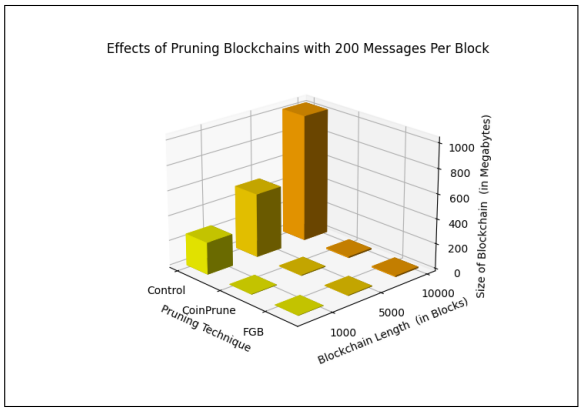


Fig. 5. Blockchain sizes with 200 messages

smaller in size than the unpruned counterpart. The header chain found in CoinPrune provides a negligible overhead, Although in arbitrarily long chains, the overhead becomes a problem. Each pruned blockchain is able to return the same trust values as the control block, showing that the state of the network is accurately preserved during the loss of data. The information preservation demonstrates that both blockchain pruning methods can dramatically decrease the size required to represent the state of a network, with an FGB scheme being superior with the constant size blockchain.

## VII. Recommendations

Blockchains within VANETs demand special care regarding growth. If a blockchain is allowed to grow without bound, having the full blockchain stored locally creates unacceptable storage requirements for vehicles and RSUs in the network. Both forms of pruning discussed here allow for an order of magnitude reduction in size. The FGB method provides the reduction in size without having a header chain and can remain a target size indefinitely. Blockchains used in VANET applications that condense information into a single snapshot should adapt FGB to form a pruning mechanism. The pruning is an effort to curb increasing network usage when new nodes join and to decrease storage requirements for nodes in the network.

An idea that may need further investigation is the use of Cloud computing[15] and mobile edge computing[17] to assist in the chain. Cloud computing, specifically storage, would allow the storage of pruned blocks for longer periods of time. The pruned blocks may still prove useful to law enforcement and insurance companies conducting work business while being irrelevant to a vehicle. Edge computing can be used to help offload the burden of the consensus mechanism to nearby edge servers during low network participation times. Combining the ideas could allow for the expansion of VANETs into less populous regions.

Implementing either mechanism benefits from a non-static pruning technique. The amount of blocks that are pruned each time can be varied to support the current activity on the network. The longer the chain past the prune, the more difficult the information is to change. However, the number of blocks also affects performance [21] and cause the network to behave slowly. There must be a balance on the size of the blockchain in regards to storage and security issues.

## VIII. Conclusion

Successful blockchain applications in VANETs are certainly possible and show promise if blockchain size is managed and limited as an integral part of the blockchain implementation. Unbounded blockchains, such as traditional blockchains, become prohibitive to operate in VANETs due to the ephemeral connections between nodes. In applications where the data can be condensed into a single snapshot of the state of the network, an FGB mechanism should be implemented to provide a way to relieve storage issues while maintaining the security found inherently within blockchains. The use of cloud computing and storage allows for the relevant authorities to review the information when needed.

## References

[1] M. Lee and T. Atkison, "VANET applications: Past, present, and future," *Vehicular Communications*, p. 100310, Oct. 2020.

[2] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular Ad Hoc network," *Journal of Network and Computer Applications*, vol. 37, pp. 380–392, Jan. 2014.

[3] A. K. Goyal, A. Kumar Tripathi, and G. Agarwal, "Security Attacks, Requirements and Authentication Schemes in VANET," in *2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, (GHAZIABAD, India), pp. 1–5, IEEE, Sept. 2019.

[4] A. Kchaou, R. Abassi, and S. G. El Fatmi, "Towards a Secured Clustering Mechanism for Messages Exchange in VANET," in *2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, (Krakow), pp. 88–93, IEEE, May 2018.

[5] M. A. Alazzawi, K. Chen, A. A. Yassin, H. Lu, and F. Abedi, "Authentication and Revocation Scheme for VANETs Based on Chinese Remainder Theorem," in *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, (Zhangjiajie, China), pp. 1541–1547, IEEE, Aug. 2019.

[6] A. Fitah, A. Badri, M. Moughit, and A. Sahel, "Performance of DSRC and WIFI for Intelligent Transport Systems in VANET," *Procedia Computer Science*, vol. 127, pp. 360–368, 2018.

[7] 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.

[8] R. Al-ani, B. Zhou, Q. Shi, and A. Sagheer, "A Survey on Secure Safety Applications in VANET," in *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, (Exeter, United Kingdom), pp. 1485–1490, IEEE, June 2018.

[9] 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.

[10] H. Khelifi, S. Luo, B. Nour, H. Moungla, S. H. Ahmed, and M. Guizani, "A blockchain-based architecture for secure vehicular Named Data Networks," *Computers & Electrical Engineering*, vol. 86, p. 106715, Sept. 2020.

[11] I. Ali, M. Gervais, E. Ahene, and F. Li, "A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs," *Journal of Systems Architecture*, vol. 99, p. 101636, Oct. 2019.

[12] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A Privacy-Preserving Trust Model Based on Blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655–45664, 2018.

[13] H. Li, L. Pei, D. Liao, S. Chen, M. Zhang, and D. Xu, "FADB: A Fine-Grained Access Control Scheme for VANET Data Based on Blockchain," *IEEE Access*, vol. 8, pp. 85190–85203, 2020.

[14] 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.

[15] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A Traceable Blockchain-Based Access Authentication System With Privacy Preservation in VANETs," vol. 7, p. 11, 2019.

[16] L. Peng, W. Feng, Z. Yan, Y. Li, X. Zhou, and S. Shimizu, "Privacy preservation in permissionless blockchain: A survey," *Digital Communications and Networks*, p. S2352864819303827, June 2020.

[17] 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.

[18] B. Guehguih and H. Lu, "Blockchain-Based Privacy-Preserving Authentication and Message Dissemination Scheme for VANET," in *Proceedings of the 2019 5th International Conference on Systems, Control and Communications*, (Wuhan China), pp. 16–21, ACM, Dec. 2019.

[19] R. Shrestha and S. Y. Nam, "Regional Blockchain for Vehicular Networks to Prevent 51% Attacks," *IEEE Access*, vol. 7, pp. 95033–95045, 2019.

[20] Computer Networks Department Faculty of Informatics and Computer Science The British University in Egypt and A. Mostafa, "VANET Blockchain: A General Framework for Detecting Malicious Vehicles," *Journal of Communications*, pp. 356–362, 2019.

[21] S. Kim, "Impacts of Mobility on Performance of Blockchain in VANET," *IEEE Access*, vol. 7, pp. 68646–68655, 2019.

[22] 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, pp. 2468–2482, Feb. 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] R. Matzutt, B. Kalde, J. Pennekamp, A. Drichel, M. Henze, and K. Wehrle, "How to Securely Prune Bitcoin's Blockchain," *arXiv:2004.06911 [cs]*, Apr. 2020. arXiv: 2004.06911.

[25] A. Busygin, M. Kalinin, and A. Konoplev, "Supporting connectivity of VANET/MANET network nodes and elastic software-configurable security services using blockchain with floating genesis block," *SHS Web of Conferences*, vol. 44, p. 00020, 2018.