Digital Communications and Networks 6 (2020) 177–186

Contents lists available at ScienceDirect

Digital Communications and Networks

journal homepage: www.keaipublishing.com/dcan

A new type of blockchain for secure message exchange in VANET

Rakesh Shrestha [a], Rojeena Bajracharya [b], Anish P. Shrestha [c], Seung Yeob Nam [b,*]

[a] Yonsei Institute of Convergence Technology, Yeonsei University, Songdogwahak-ro, Yeonsu-gu, Incheon, 21983, South Korea
[b] Department of Information and Communication Engineering, Yeungnam University, 280 Daehak-Ro, Gyeongsan-si, Gyeongsangbuk-do, South Korea
[c] Computer Science and Engineering Department, Sejong University, 209 Neungdong-ro, Gunja-dong, Gwangjin-gu, Seoul, South Korea

ARTICLE INFO

Keywords:
VANET
Blockchain
Message trustworthiness
Node trustworthiness
Edge computing

ABSTRACT

In the Vehicular Ad-hoc NETworks (VANET), the collection and dissemination of life-threatening traffic event information by vehicles are of utmost importance. However, traditional VANETs face several security issues. We propose a new type of blockchain to resolve critical message dissemination issues in the VANET. We create a local blockchain for real-world event message exchange among vehicles within the boundary of a country, which is a new type of blockchain suitable for the VANET. We present a public blockchain that stores the node trustworthiness and message trustworthiness in a distributed ledger that is appropriate for secure message dissemination.

1. Introduction

In recent decades, there has been a persistent increase in the number of smart and autonomous vehicles. In the Vehicular Ad-hoc NETworks (VANET), the lives and properties of drivers depend on the efficiency of communication among vehicles. The main goal of a vehicular network is to accurately disseminate information about life-threatening events, such as traffic jam and accident reports, in a short time. However, it is still a challenge to disseminate critical event information in a targeted area under a dynamic VANET environment and in the presence of malicious vehicles. The existing VANETs have numerous security issues. Due to false and untrustworthy information sent by malicious vehicles, some important messages cannot be disseminated accurately in real time. And this leads to collateral damage to neighboring vehicles and drivers. One of the challenges faced by the VANET is due to its ephemeral characteristics. In a distributed VANET, vehicular nodes can join and leave the network dynamically as in the Mobile Ad-hoc NETwork (MANET) [1]. The blockchain has recently gained the attention of researchers and has great potentials in diverse fields. We use the blockchain to resolve critical issues of information dissemination in VANETs. The blockchain is an emerging decentralized and distributed computing paradigm that underpins the Bitcoin cryptocurrency [2], which provides privacy and security in Peer-to-Peer (P2P) networks. In the case of VANET, the blockchain can be used to manage the ground truth of information for vehicles because any vehicle can access the history of event information in the public blockchain.

We propose a scheme to determine the node trustworthiness and message trustworthiness in the VANET and then store them in a public blockchain that acts as the ground truth for other vehicles. A simple adoption of an existing blockchain is not directly applicable for VANET scenarios. Therefore, we will introduce a new type of blockchain appropriate for the VANET and use event messages as transactions in the VANET, which is unlike that using cryptocurrency as transactions in the Bitcoin. We believe that the blockchain can resolve the major issues faced by current VANETs and provide security for critical information dissemination. In our scheme, new blocks are built based on event messages similar to transactions in Bitcoin, and hashes of consecutive blocks are linked together in a sequential manner to make a blockchain. Recently, there has been much interest in blockchain technology, and many researchers have investigated ways in which the blockchain can be used in geospatial systems. In the case of Bitcoin, a newly minted block is shared among all nodes globally. However, in the case of the VANET, there is no need to share blocks beyond the scope of a country. For instance, Japan and Korea are geographically separated from each other, and they are not connected by roads. So, the traffic and accident information in Japan is not useful for vehicles in Korea. Hence, it is more suitable to maintain a separate blockchain which only considers the vehicle node trust level and message trustworthiness in each country based on geographical location. The main objective of this paper is to study how to securely deliver trustworthy event messages by applying blockchain technology in VANETs. We will deal with a local blockchain that is independent of chains from other countries to improve the scalability and timeliness of message dissemination in the VANET. We consider a public blockchain that independently manages and stores all

[*] Corresponding author.
E-mail address: synam@ynu.ac.kr (S.Y. Nam).

https://doi.org/10.1016/j.dcan.2019.04.003
Received 18 December 2018; Received in revised form 5 April 2019; Accepted 19 April 2019
Available online 26 April 2019

node trustworthiness and message trustworthiness in a given country. We also present different types of blockchain consensus mechanisms based on a private or public blockchain. The consensus mechanism plays an important role in determining the security and scalability of a blockchain. We will focus on the Proof of Work (PoW) consensus mechanism that has strong and provable security and is appropriate for a public blockchain. We introduce edge computing for the blockchain, as it can reduce delay for block generation by offloading the high computational PoW to the edge servers for the miner vehicles to mine the blocks. Furthermore, the block propagation delay can be reduced by using edge cloud computing.

In this paper, we introduce a blockchain that can be used to effectively handle the trustworthiness of nodes and event messages in the VANET. The key contributions of our paper can be summarized below:

a. We propose a blockchain scheme to store the node and message trustworthiness in the VANET. In this scheme, the node and message trustworthiness acts as transactions similar to Bitcoin blockchain that provides ground truth for other vehicles.
b. We attempt to improve the scalability of the blockchain by using a local blockchain, which is a concept based on geographical locations and independent of chains from other different countries.
c. We aim to reduce the latency for block generation by introducing edge computing in the VANET blockchain as a future perspective. The edge computing would reduce latency by offloading the complex computation to the edge devices, thus provides real-time applications in the VANET.

The remaining part of the paper is structured as follows: Section 2 describes the related work based on blockchain technology in the VANET. Section 3 gives a brief technical overview of the VANET and the types of trust models used in VANET. In addition, it gives the background of blockchain technology and introduces different types of consensus mechanisms used in existing blockchains. Section 4 explains the proposed a new type of blockchain. Section 5 discusses the implementation of the proposed blockchain for secure message dissemination in the VANET. In Section 6, we present the future perspective of blockchain in the VANET by incorporating edge cloud computing for reducing latency in the VANET. Finally, Section 7 provides a conclusion of the paper.

2. Related works

A blockchain can be defined as a distributed and decentralized public database of all transactions or digital events that have been executed or shared among participating nodes. Each event in the public database is validated based on the agreement of a large number of nodes in the blockchain network. The popularity of the blockchain is due to its advantages, which include decentralization, anonymity, chronological order of data, distributed security, transparency, and immutability and suitability for trustless environments [3]. The blockchain consists of two types of nodes. A full node is a node that stores and maintains the complete history of blockchain transactions. It begins a transaction directly and independently, and it authoritatively verifies all transactions in the network. Every node in the blockchain network knows the genesis block's hash. Every node in the network builds a trusted blockchain based on the genesis block that acts as a secure root. The genesis block does not have the hash of a previous block. If a node is new, then it only knows the genesis block, and it will have to download all blocks starting from the genesis block to synchronize with the blockchain network and is constantly updated when new blocks are found [4]. The chaining of blocks is performed by appending hashes of the previous blocks to the current block so that the hash of the current block is in a sequential manner to the following block [2,4]. Then, it is shared with other nodes in a distributed P2P network in a secure way without the need for a central authority. The sequential hashes of blocks ensure a sequential order of transactions. Then, previous transactions cannot be modified without modifying their blocks and all subsequent blocks. The blockchain is verified by the consensus of anonymous nodes in the generation of blocks. It is considered secure if the aggregated computational power of malicious nodes is not larger than the computational power of honest nodes [2,5]. In the case of Bitcoin, the concept of PoW makes sure that a miner is not manipulating the network to make fake blocks. A PoW is a mathematical puzzle that is very hard to solve and easy to verify so that it protects the blockchain from double-spending attacks.

In the research on the VANET, some of the previous works related to secure event message dissemination are based on voting [6,7]. Most voting approaches attempt to solve the issues of node security by asking the opinions of other nodes to determine the trustworthiness of a node. However, this type of approach have the problem of whether the nodes providing the feedback can be trusted. In our approach, we assume all information is kept in a distributed database based on blockchain technology. Generally speaking, limited work has been done to study vehicular networks using the blockchain. The authors in Ref. [8] used a basic blockchain concept to simplify the distributed key management in heterogeneous vehicular networks. The authors in Ref. [9] combined the VANET and Ethereum's blockchain-based application concepts and enabled a transparent, self-managed and decentralized system. They used Ethereum's smart contract system to run all types of applications on an Ethereum blockchain. In contrast, our proposed work applies a different type of blockchain for secure message dissemination in vehicular networks. In Ref. [10], the authors proposed a blockchain technology for automotive security by using an overlay network in the blockchain and additional nodes called overlay block managers. The overlay network nodes are clustered by cluster heads, and these cluster heads are accountable for handling the blockchain and operating its main functions. However, the introduction of additional overlay nodes might cause high latency and might be the center point of failure if the cluster head is compromised. In Ref. [11], the authors proposed a blockchain for securing the communication of intelligent vehicles by using visible light communication and acoustic side channels. They used the blockchain public keys to verify their proposed mechanism through cryptographic session keys, utilizing both side channels and blockchain public key infrastructure. And they used different types of communication for securing the vehicular network.

3. Technical overview

This section delivers a technical overview of the underlying concepts and background information related to the VANET and the blockchain. First, we present some fundamentals and trust models of the VANET. Subsequently, we will focus on the blockchain concept, list out its features, and then categorize different types of consensus mechanisms used in blockchain technology.

3.1. Fundamentals of VANET

Recently, with the advancement of vehicular technology, the VANET plays an important role in saving the lives and properties of drivers by disseminating critical event information. In the VANET, there are two types of communication: Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. In these days, Vehicle-to-Everything (V2X) is more popular, where everything represents pedestrian, cyclist, and anything that can communicate with the vehicle. In the case of V2I communication, the vehicles communicate with Road Side Units (RSU) that are installed along a road's two sides. The Wireless Access in Vehicular Environments (WAVE) protocol provides the basic radio standard for Dedicated Short Range Communication (DSRC) operating in the 5.9 GHz frequency band. The WAVE is based on the IEEE 802.11p standard [12]. Vehicles communicate with neighboring vehicles using On-Board Units (OBUs) form an ad-hoc network that allows communications in a distributed manner [13]. There are several studies on Cellular V2X (CV2X), but currently, the network is not completely 5G compatible, and it does not provide full coverage for vehicular networks. One of the main objectives of the VANET is to communicate with other vehicles using safety messages to report events, such as accident information, safety warnings, information on traffic jams, weather reports, reports of ice on the road, etc. Certain event information is required to be disseminated rapidly and accurately, with minimum delay. Failure in timely and accurate dissemination of such time-critical information might lead to collateral damage to drivers and neighboring vehicles. Node trust and event message trust are among the major issues used to secure communication in the VANET, so it is essential to periodically evaluate the node and message trustworthiness based on trust models.

Trust models

The existing trust models can be classified into three main categories, as shown in Fig. 1. They include: entity-based trust models, data-centric based trust models, and hybrid trust models [14,15]. Entity-based trust models focus on evaluating the trustworthiness of each vehicle by considering the opinions of the peer vehicles. In Ref. [16], the authors presented a fuzzy approach for verifying the trustworthiness of nodes by using feedback from its adjacent vehicular nodes. However, the trustworthiness of a message may not agree with the trustworthiness of the node itself every time. Usually, it is very hard to gather all information to estimate the real-time node trust of the vehicle nodes due to their high mobility. Similarly, data-centric trust models focus on evaluating the trustworthiness of events received from adjacent vehicles instead of the trustworthiness of the vehicular node itself [13,17]. The authors in Refs. [13,18] used a Bayesian inference decision module to evaluate reported events. The inference module is based on the prior probability, which is difficult to obtain because of the dynamic topology of the VANET. In addition, the trustworthiness of the vehicular nodes does not guarantee the trustworthiness of the message itself, as the trustworthy vehicles may transmit false messages when they are compromised by the malicious vehicles. Hence, a hybrid trust model was introduced, and it combines the entity based and data-centric based trust models to evaluate the trustworthiness of a message [15,19,20]. The authors in Ref. [21] proposed a hybrid trust management where the data trustworthiness is evaluated using messages received from several vehicular nodes. And the node's trustworthiness is evaluated using recommendation and functional trust. However, their mechanisms do not consider data sparsity in the VANET.

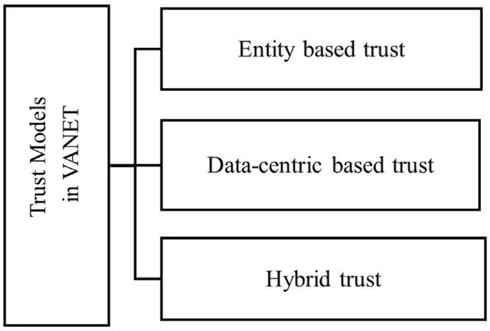


Fig. 1. Trust models in the VANET.

Thus, we try to overcome the disadvantages of the existing mechanisms by improving the hybrid trust model for message and node trustworthiness. We propose a node trust level and a message trust level using blockchain technology that meets all requirements of the hybrid trust model for the VANET. By using blockchain technology in our scheme, we can store node and message trust levels efficiently in a distributed database, and provide privacy and security that are suitable for the dynamic VANET topology.

3.2. Overview of blockchain

A blockchain is a distributed public database of all digital events that have been accomplished and shared among participating nodes. It contains a definite and verifiable record of every single event ever occurred. Each event in the blockchain database is validated by the consensus of the majority of the nodes in the network. There are mainly two types of blockchains, i.e., public blockchain and private blockchain. The public blockchain is an open blockchain where anyone can join and interact with the blockchain with no need to get permission from a central authority. On the other hand, the private blockchain is based on an access control mechanism. It allows administrators to control the participants in a network and things like who can join, view and write to the blockchain. In the private blockchain, the administrator can create a consensus group. As a result, the private blockchain can converge to be centralized, which makes it vulnerable to a single point of failure. However, the public blockchain is a purely decentralized blockchain that does not have a single point of failure problem and is able to withstand malicious attacks. In a public blockchain, once a full node is connected to its peers, it first tries to construct a complete blockchain.

The root of the blockchain is a genesis block that is the first block in the blockchain. It is the common origin of all blocks and contains the information that is generally known to all nodes. The block consists of cryptographic hashes of records, with each block holding the information about the previous block's hash, forming a chain of data, and creating a blockchain, as shown in Fig. 2. The blockchain begins with a genesis block on top of which stacked the successor blocks. The structure of each block contains a block header and a block body. The block header consists of a previous block's hash, nonce, timestamp, as well as the Merkle root, as shown in Fig. 3. The block body contains lists of transactions and some additional data, depending on the requirement of the blockchain.

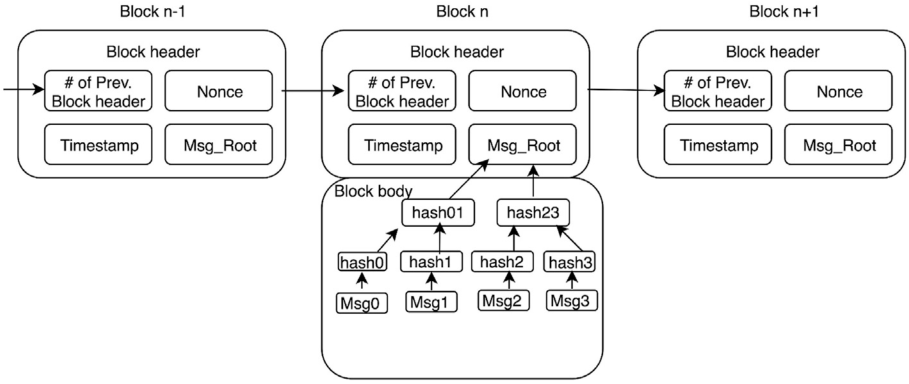
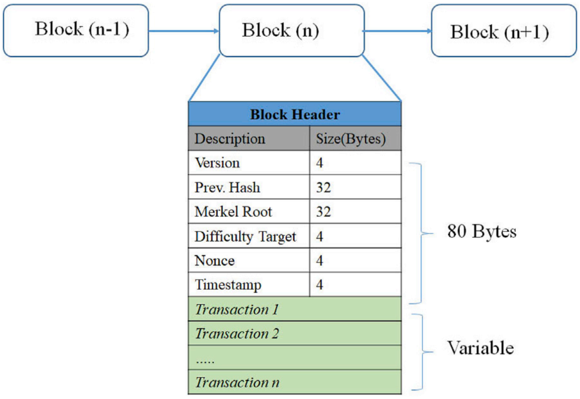


Fig. 2. The structure of blocks in a blockchain [2].



Block Header	
Description	Size(Bytes)
Version	4
Prev. Hash	32
Merkel Root	32
Difficulty Target	4
Nonce	4
Timestamp	4
Transaction 1	
Transaction 2	
.....	
Transaction n	

Fig. 3. Block header format [2].

Each current block is interconnected with the previous block, using the hash of the previous block like a chain.

For immutability, the transactions should be hashed using a Merkle hash, which needs to be included in the block header. The Merkle hash is derived from the Merkle algorithm [22], which is a cryptographic algorithm that hashes all transactions of the block to get the Merkel root. The Merkle root is the hash of all hashes of all transactions, and it is eventually appended in the block header. The benefit of Merkel tree is that it is able to verify transactions as required and does not include the body of all transactions in the block header, while still giving a way to validate the whole blockchain. It generates a unique hash value that verifies the integrity of all transactions underneath it, and the size of the Merkel hash is very small as compared with the whole size of all transactions. The blockchain has gained huge popularity due to its security features of using cryptography. Nowadays, several researchers from different fields, such as academia, financial institutions, medical and banking industries, etc., are attracted to the blockchain due to its immense advantages.

3.2.1. Features of blockchain

Some of the basic features of the blockchain are as follows:

a. Immutability: One of the important features of the blockchain is immutability. Once a piece of information is recorded and confirmed in the blockchain, then it cannot be modified or deleted from the network. Also, information cannot be added arbitrarily.
b. Distributed and trustless environment: In the blockchain, any node that can be added can synchronize and validate all contents of the blockchain in a distributed manner without central control. It provides security and prevents from a single point of failure. It provides trust in a trustless environment.
c. Privacy and anonymity: The blockchain provides privacy to the users. A user can join the network anonymously. i.e., the information about the user cannot be known by other users. It means that personal information is private, secure, and anonymous.
d. Faster transactions: It is very easy to set up a blockchain, and the transactions are confirmed very fast. It takes only a few seconds to a few minutes to process the transactions or events.
e. Reliable and accurate data: Because of the decentralized network, the data in the blockchain are reliable, accurate, consistent, timely and widely accessible. It can withstand malicious attacks and do not have a single point of failure.
f. Transparency: It is completely transparent as it stores details of every single transaction or event that occurs in the blockchain network. Anybody in the network can view the transactions transparently.

3.2.2. Blockchain consensus mechanisms

In the blockchain, a consensus is a fault-tolerant mechanism, which is used to accomplish necessary agreement on a single state of the network in a distributed multi-node system. It is a set of rules that decide on the contributions of different participating nodes of the blockchain. In a decentralized blockchain network, the publicly shared database needs a secure, real-time, efficient, and reliable scheme to ensure that all transactions occurring in the network are trustworthy and all participating nodes agree on a particular consensus [23]. Based on the type of blockchain, i.e., public or private blockchain, the consensus mechanism can be categorized as shown in Fig. 4.

In the public blockchain, the PoW and Proof of Stake (PoS) consensus are the most common and popular consensus algorithms.

a. In the PoW consensus, a miner computes the value of the previous block header's hash, while the Merkel root of transactions uses different nonce values repeatedly till the resulting hash value is less than the difficulty target [4]. A PoW consensus algorithm is a cryptographic puzzle that is very hard to solve, but once all inputs are known, it is easy for others to verify.
b. In the PoS, a miner or validator who creates a new block is chosen in a deterministic manner depending on its wealth or stake [24]. The miners are required to stake their assets in terms of coins and validate ownership without being required to prove the legitimacy of each transaction. The validators take the transaction fees, and there are no block rewards in some PoS algorithms. The PoS is a cheaper and greener distributed form of the consensus algorithm. It is further categorized into Byzantine Fault Tolerant-based Proof-of-Stake (BFT-PoS) and chain-based PoS. The BFT-PoS protocol works as a round-based voting mechanism that pseudo-randomly delegate a

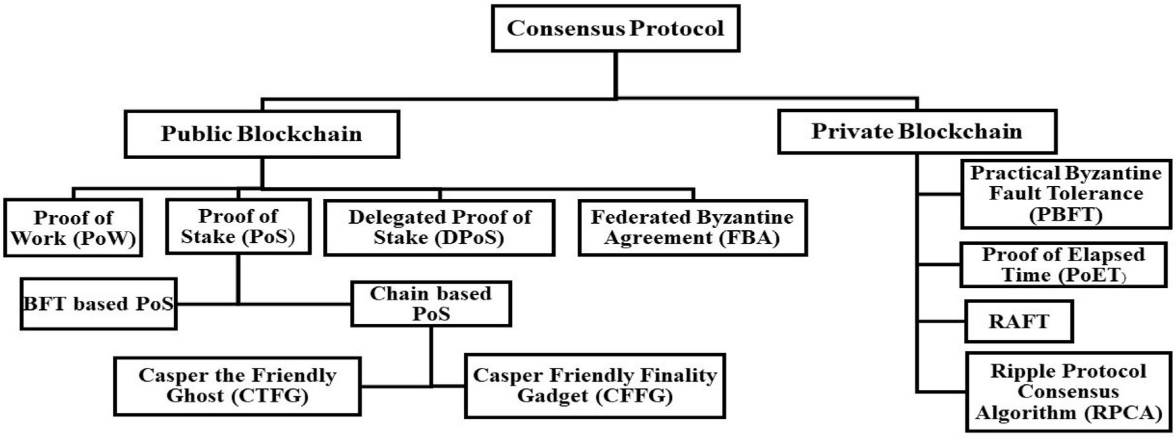

Consensus Protocol
Public Blockchain
Private Blockchain
Proof of Work (PoW)
Proof of Stake (PoS)
Delegated Proof of Stake (DPoS)
Federated Byzantine Agreement (FBA)
BFT based PoS
Chain based PoS
Casper the Friendly Ghost (CTFG)
Casper Friendly Finality Gadget (CFFG)
Practical Byzantine Fault Tolerance (PBFT)
Proof of Elapsed Time (PoET)
RAFT
Ripple Protocol Consensus Algorithm (RPCA)

Fig. 4. Blockchain consensus mechanisms.

validator to propose a new block during a multi-round voting process [25]. In this mechanism, the validators keep a full copy of the blockchain and are identified by their public keys. However, committing and finalizing blocks depend upon the majority, i.e., 2/3 of all validators, to sign off on the proposed block, which may take several rounds before the block gets finalized. A chain-based PoS imitates the PoW consensus where the protocol assigns the right to commit a new block to a pseudo-randomly selected validator. The new block is linked with the hash of the previous block of the longest chain [26]. A block is consensus safe, i.e., finalized, when there is no chance of being revised. Taking inspiration from Practical Byzantine Fault Tolerance (PBFT), a team from Ethereum blockchain came up with Casper that requires the validators to vote and sign their votes before propagating it in the network. Casper uses a single type of message, i.e., vote, which combines the roles of preparing and committing. The key components of the Caspers PoS consensus are checkpoints. The team came up with two protocols called Casper the Friendly Ghost, a research led by Vlad Zamfir, and Casper the Friendly Finality Gadget, a research led by Vitalik Buterin [27].

c. Delegated Proof of Stake (DPoS) was introduced to incentivize small stakeholders and encourage them to participate in the network by delegating or transferring their coins to bigger stakeholders [28]. In the DPoS, the small users or stakeholders are allowed to delegate their rights to other participants who can then stake coins on behalf of smaller stakeholders. The smaller stakeholders get a share of staking incentive as a reward from the consensus protocol. However, blockchain centralization may occur as only a few nodes control the majority of the network due to higher returns margins for larger stakeholders.

d. In the Federated Byzantine Agreement (FBA) consensus, nodes can choose whom they trust, and the control is decentralized [29]. It is a public blockchain where the membership is open, and each node does not have to be known and verified ahead of time. An FBA uses quorum slices, which is a subset of a quorum. A quorum is the number of nodes required to reach an agreement within a network. If a node finds a certain quorum slice completely trustworthy, it can agree to go along with whatever that quorum slice agrees with. A consensus decision among validators can be made on the new block and can be stored in the local blockchain permanently.

In the private blockchain, PBFT is a common consensus algorithm. It is fast and efficient, and the trust is decoupled from the resource bearer.

a. PBFT is an improved version of BFT that ensures a consensus regardless of malicious behaviors on the part of some participating nodes [30]. For the PBFT model to work, all nodes interconnect with each other, and the legitimate nodes achieve a system agreement based on the majority rule. The supposition is that the sum of malicious nodes cannot be equal to or greater than 1/3 of the overall nodes in the network. The more the nodes join the PBFT network, the securer the network is.

b. Proof of Elapsed Time (PoET) is a private blockchain consensus mechanism that needs all participating nodes to identify themselves before they participate in the network [31]. The PoET is based on a fair lottery system where every single participant has an equal opportunity to be a winner among all network participants. In the PoET, for the nodes to win the lottery, they need to select a short random time and have to complete certain waiting time. It is energy efficient and utilizes low resources by the fair lottery system.

c. Raft is a crash-fault tolerant consensus algorithm proposed by a team of researchers from Stanford University [32]. In Raft, the Raft cluster consists of several servers, usually five server nodes. The system allows two nodes to fail at the same time. The server node has three states: leader, follower, and candidate. Usually, there is only one leader who is responsible for handling all of the client requests while other servers are followers. The third state, i.e., the candidate state, elects a new leader. A candidate receiving votes from the majority of the cluster now becomes the new leader of the consensus mechanism.

d. Ripple Protocol Consensus Algorithm (RPCA) is a consensus algorithm used by Ripple. It consists of a Ripple server, an open and a last-closed ledger, a proposer and a Unique Node List (UNL) [33]. The Ripple server participates in the consensus protocol. The RPCA protocol is used every few seconds by all nodes to retain the correctness and agreement of the network. When a consensus is achieved, the recent ledger is regarded as closed and turns into the last-closed ledger. Assume that the consensus algorithm is successful without a fork in the network, the last-closed ledger maintained by all nodes in the network will be the same. There are five validators (which only trust each other) selected through a static configuration that is operated by Ripple. As a consequence, it might lead to centralization.

However, all other protocols, without exceptions of PoW and PoS mentioned above, and their implementation are still subject to a thorough, peer-reviewed correctness and reliability analysis. There might be several vulnerabilities, security issues and protocol weakness in these mechanisms. So, till now, the PoW is considered as a secure consensus mechanism although it has some flaws, such as scalability, transaction finalization, etc. In this paper, we adopt a PoW consensus mechanism because of its success, reliability and security in cryptocurrencies such as the Bitcoin.

4. Blockchain scheme in VANET

A new type of blockchain is proposed to solve the issues related to trustworthy message dissemination in the VANET. The approach is new as we use the concept of an immutable distributed public database for secure message dissemination in the VANET, where any node can access the information. In addition, it can be maintained independently by each country. In recent years, this has become feasible due to the introduction of the Bitcoin blockchain. However, the nature of our problem is different from the Bitcoin, as we are dealing with event messages rather than cryptocurrency transactions. Some pieces of event information, such as traffic jams, road accidents, and environmental hazards, are relevant to a particular geographical location. The local information is not of much interest to other regions or countries. All vehicles can know their positions by using a location certificate based on Proof of Location (PoL) [34]. There are millions of vehicles in the world, so if each country manages a blockchain independently, then there will be less amount of scalability issues as compared with the global blockchain.

4.1. Assumptions

We assume that vehicles can communicate with other entities using Vehicle-to-Vehicle (V2V) and Vehicle-to-Everything (V2X) communications [35], and that vehicles can connect to the Internet efficiently. We assume that all vehicles have required equipments like OBUs, sensors, and GPS. We assume that the number of legitimate RSUs is greater than that of the malicious RSUs. The RSUs are usually fixed entities alongside roads. The legitimate RSU creates a genesis block to start a blockchain based on local events. We assume that the vehicles that have great computing power and high trust levels are considered as full node vehicles that can participate in the mining process. Also, normal vehicles outnumber malicious vehicles in the network. We assume that critical event messages are disseminated within a Region of Interest (RoI) in a specific geographical location. The critical messages are not encrypted so that they are available to any nearby vehicle. We assume the number of messages required to confirm the event is fifteen so that the message is considered correct.

4.2. Components of proposed blockchain scheme

RSU: The RSUs are used for V2I communication and are responsible

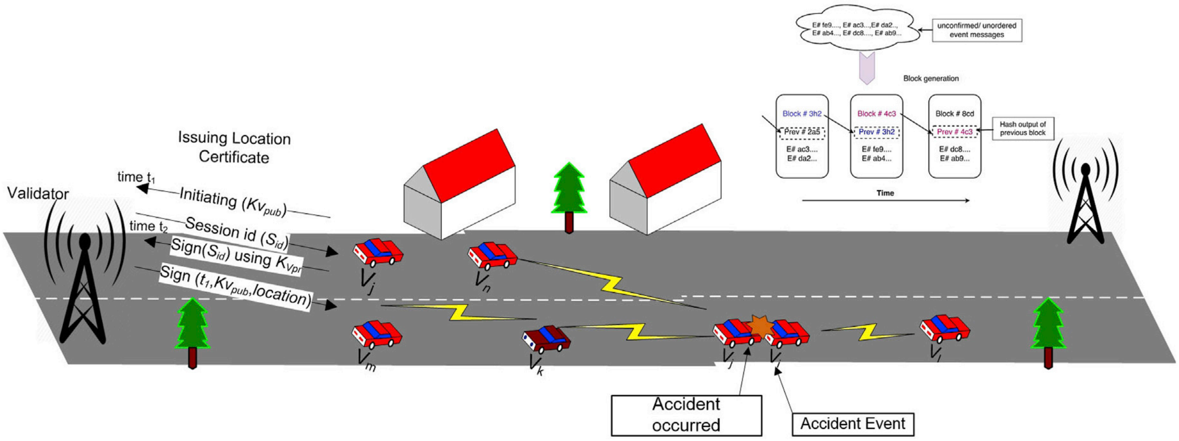


Fig. 5. Blockchain scheme for secure message dissemination.

for authentication and providing a location certificate to vehicles within its communication range. The legitimate RSU creates a genesis block based on the local events.

Vehicles: Vehicles are the main elements of the VANET blockchain system. They generate event messages, mine new blocks, and store the event messages in the blockchain after verification. There are two types of vehicular nodes, i.e., full node and normal node. The full node has a high trust level and strong computing power that is responsible for mining the blocks. And other nodes are normal nodes that help in message generation during accidents, and the forwarding and verification of received messages.

VANET messages: There are two types of messages in the VANET. They are beacon messages and safety event messages. Beacon messages are broadcast periodically to inform neighboring vehicles of the driving status and positions of vehicles to achieve cooperative awareness among other vehicular nodes on the road for traffic management. The safety event messages are broadcast when critical events that occur on the road, such as traffic accidents and road hazards, etc. Depending on the severity of the emergency, event messages are categorized into different levels based on priority, such as level 1, level 2 and level 3, where level 1 indicates highly critical event messages with the highest priority, and so on. We only consider safety messages as transactions in the blockchain because they play an important role in securing the life and property of the driver. As beacon messages are broadcast frequently, they incur overhead when each beacon message is signed and authenticated.

Blocks: A block consists of a block header and a block body. The block header consists of the previous block's hash, nonce, difficulty target, timestamp and Merkle root. The block body consists of a list of safety event messages that behave as transactions in the block body.

Location certificate: A location certificate based on the PoL is used to provide proof of the location of a vehicle at a given time [34]. Each vehicle requires the PoL to verify that the vehicle is located near the event spot. In addition, the PoL is used as a location proof in an event message that assists in the blockchain. The RSU acts as a validator to provide a location certificate to the vehicles within its communication range. We consider that all vehicles and RSUs have their own public and private key pairs. The requesting vehicle sends an initiation message with its public key (K_{vpub}) to the RSU, and then the RSU sends a random Session ID (S_{id}) to the vehicle. The vehicle sends back the signed session ID ($sign(S_{id})$) to the RSU. The RSU verifies the authenticity of the signature of ($sign(S_{id})$) with the vehicle's public key (K_{vpub}) and checks the elapsed time for exchanging the session ID. If the time difference between sending and receiving the session ID is less than a few milliseconds, the RSU publishes a Location Certificate (LC), which includes the location, time and vehicle's public key (K_{vpub}) that is signed by the RSUs' private key (K_{Rpr}) as shown in Fig. 5. GPS cannot be used because it can be easily spoofed [36]. The PoL is secure as the vehicles cannot create a fake location certificate without the valid signature of the RSU. However, only using the PoL does not guarantee the trustworthiness of messages, so we need a blockchain mechanism to make the message more trustworthy.

4.3. Proposed blockchain in VANET

We propose a new type of blockchain because simply adopting existing blockchains is not suitable for our scenario. Conventional blockchains deal with cryptocurrency, whereas our blockchain deals with safety event messages without using any crypto-coins. From here onwards, we will use a safety event message as an event message. Our blockchain is appropriate for the trustworthiness of safety messages in the VANET that relates to the real world. The blockchain stores and manages the history of event messages along with the trust levels of the vehicles in a distributed, immutable, and reliable manner. In each country, there will be a single unique blockchain that is managed and maintained independently for recording vehicle information.

In the VANET, all vehicles broadcast their positions through beacon messages. We use the LC as a digital proof to indicate that a vehicle is located at a specific place at a particular time [34]. Every vehicle needs an LC to prove its position at a given time. An LC is provided by a legitimate RSU. The RSU issues an LC to the requesting vehicle using its own public and private key pair. This location certificate acts as a Proof of Location (PoL) for the vehicles that help to identify the event messages in a given geographical area. There are issues of scalability and timeliness in existing blockchains, which may not be appropriate for real-time VANET applications. In our scheme, all of the events are local, i.e., event messages are confined to the vehicles within a particular geographical area. In conventional blockchains, the newly minted block is broadcast globally. However, in our scheme, VANET messages need not go beyond the border of a country, as the traffic and accident information of one country is irrelevant to vehicles that are located in another country. Hence, a new concept of blockchain that is different from conventional blockchains is needed. In each independent blockchain, all miners mine new blocks based on event messages and send the newly minted block to the local blockchain network. The blockchain acts as a global ground-truth for the node trustworthiness within the country. In other words, any vehicle can query the vehicle's trust level at any time in the blockchain. The new blocks are generated by aggregating the list of unconfirmed event messages from the message pool. The hashes of all blocks are chained together in sequential order to build a blockchain, as shown in Fig. 6. After generation, the new block is broadcast, and all vehicles in the network will verify and update their blockchain.

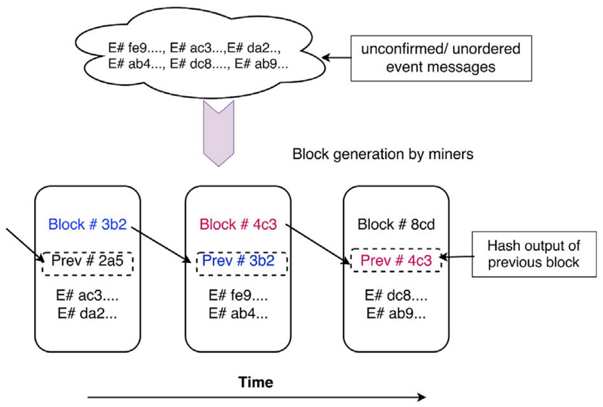

E# fe9...., E# ac3...,E# da2..,
E# ab4..., E# dc8....., E# ab9...
unconfirmed/ unordered event messages
Block generation by miners
Block # 3b2
Prev # 2a5
E# ac3....
E# da2...
Block # 4c3
Prev # 3b2
E# fe9....
E# ab4...
Block # 8cd
Prev # 4c3
E# dc8....
E# ab9...
Hash output of previous block
Time

Fig. 6. The generation of a blockchain from unconfirmed event messages.

5. Blockchain implementation for secure message dissemination in VANET

The proposed blockchain scheme for secure message dissemination is shown in Fig. 7. All vehicles in the network download and update the blockchain. In our scheme, the blockchain acts as a distributed public ledger, which stores the complete history of vehicles' trust levels in the blockchain along with event messages. The vehicle that encounters an event, such as an accident, will broadcast the event message with several parameters to neighboring vehicles in the blockchain network [37]. When other vehicles receive a new event message, they first verify whether it is in the same area based on the LC embedded in the event message. The vehicles consider the event message and check if it belongs to the same area. Then, the neighboring vehicles check other parameters of the event message. Every vehicle independently checks each event message before propagating it further in order to prevent spamming, denial-of-service, and other nuisance attacks against the system.

Whenever there are events, nearby vehicular nodes will broadcast an event message M_i. The neighboring vehicles will collect the information from the broadcasting vehicles. The event message contains all associated information, such as type of event, pseudo ID, event ID, trust level, time-stamp, PoL, etc., as given in Table 1. The vehicles receiving the event message first check the trust level of the sender vehicle from the blockchain and then verify the event message. They check each event message based on pieces of evidence regarding the sender vehicle's trust level, event location, event ID, driving direction, PoL, speed, time-stamp, etc., and store the message in the local memory pool if the message is considered to be trustworthy. Otherwise, the message is discarded. The event message is broadcast on the local blockchain network, and each vehicle in the network validates the event message. The mining vehicles collect different event messages from an unconfirmed event message pool and verify if the parameters of the accepted messages are valid.

The mining vehicle uses message verification policies to know the message trustworthiness as follows:

- Check the sender vehicle's previous trust level from the main blockchain
- Check the PoL based on the location certificate
- Check if it is first-hand information
- Check the time-stamp

If the received event message is valid and trustworthy based on the verification policy, then its trust level will be updated. The trust level is defined as the fraction of true event messages m sent by vehicle V_i to the total event messages $m+n$, i.e., $TL = m/(m+n)$, where n is the number of false event messages. The trust level varies over time, depending upon true or false messages. The trust level of a vehicle increases as the number of true messages increases. The mining vehicles will calculate the updated trust level of the sender vehicle and send this trust level to the blockchain after a new block is added to the local chain as follows:

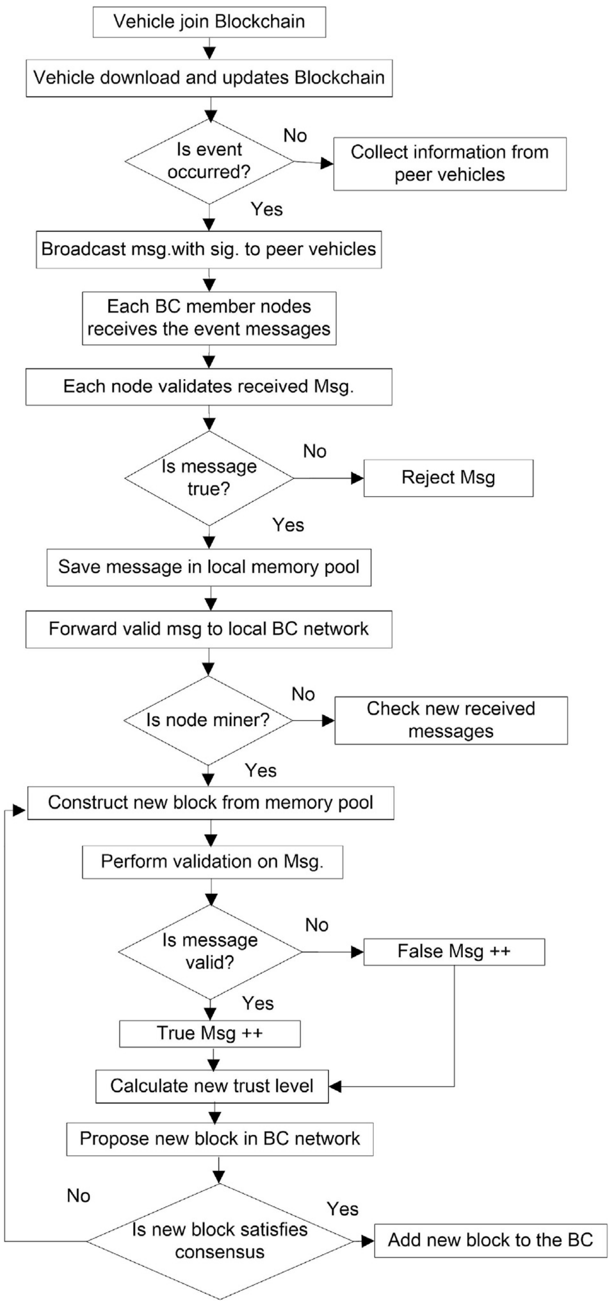

Vehicle join Blockchain
Vehicle download and updates Blockchain
Is event occurred?
No
Collect information from peer vehicles
Yes
Broadcast msg.with sig. to peer vehicles
Each BC member nodes receives the event messages
Each node validates received Msg.
Is message true?
No
Reject Msg
Yes
Save message in local memory pool
Forward valid msg to local BC network
Is node miner?
No
Check new received messages
Yes
Construct new block from memory pool
Perform validation on Msg.
Is message valid?
No
False Msg ++
Yes
True Msg ++
Calculate new trust level
Propose new block in BC network
No
Is new block satisfies consensus
Yes
Add new block to the BC

Fig. 7. Proposed blockchain scheme in the VANET.

Table 1
Event message format.

Message body	
PID	Pseudo ID
Pub address	Public address
Event ID	Specific type of event
Event Type	Types of event
TimeStamp	Event timestamp
Location	Event location
Trust Level (TL)	$m/(m+n)$
Direction	Driving direction
PoL	Location Certificate (LC)

$$TL = \frac{m}{m+n}\begin{cases} \textit{If message is true then, } m = m+1 \\ \textit{If message is false then, } n = n+1 \end{cases} \tag{1}$$

where *m* is true and *n* is a false message counter.

Each mining vehicle will create a new block B_i as shown in Fig. 2. The block header consists of the previous block's hash (B_{i-1}), the nonce value *N,* and the hash of all unordered event messages M_i. The mining vehicles try to find a nonce such that the hash of $(H(M_i)\|\mathrm{H}(B_{i-1})\|N)$ is less than the difficulty target (D).

$$H(H(M_i)||H(B_{i-1})||N) \leq D \tag{2}$$

The difficulty target is adjusted periodically to the current computation power of the vehicle nodes such that new blocks are created continuously at a regular interval. The difficulty can be determined in two different ways. The first way to know the difficulty is to check the number of preceding zeros at the beginning of the hash result, and the second way is to estimate the difficulty target. The required target value can be expressed as the number of calculated hash to mine a new block [4]. The difficulty target can be calculated as

$$target = coefficient*2^{(8*(exp-3))} \tag{3}$$

Similar to the Bitcoin difficulty format, the exponent is the first two hexadecimal bits, and the coefficient is the remaining part of the difficulty bit value in hexadecimal. The lower the target is, the greater the difficulty, and vice versa. If the network finds the block faster than the block generation time, the network difficulty target increases, whereas if the network finds the block slower than expected, then the difficulty target decreases. The network has to recalculate the difficulty so that blocks are generated consistently. This is known as difficulty retargeting, and it is calculated as

$$D_N = D_O * \frac{actual\ time\ span}{target\ time\ span} \tag{4}$$

where D_N is the new difficulty target and D_O is the old difficulty target.

The miner vehicle is said to have the PoW done when it solves a difficulty puzzle by finding a nonce value as a solution to meet the network difficulty target, i.e., the resulting hash value must be below this difficulty target value. After finding the nonce, it broadcasts B_i to the blockchain network. Other vehicles receive the new block and, based on the verification policies, independently verify if the event message is correct. This guarantees that only legitimate blocks are broadcast on the network. The independent validation also guarantees that mining vehicles who behave in an honest way get their blocks integrated in the blockchain and thus earn the reward. The mining vehicles who behave in a dishonest way get their blocks rejected. As a result, they not only lose the reward, but also waste the energy used to compute a PoW solution. If the new block information is correct, then the mining vehicles accept it and begin to mine new blocks on top of it. The existence of an event message in the blockchain is a kind of confirmation that the event message is trustworthy.

The new block is stored in the blockchain permanently based on the consensus decision among the miner vehicles. The PoW consensus mechanism is used to prevent malicious vehicles from invalidating the database. As the size of the network increases, the blockchain becomes increasingly difficult to compromise for attackers who use double-spending attacks [38]. The information in the new block can still be publicly verified; thus, the public nature of the blockchain allows all participants to verify the correctness of event messages. If any subsequent vehicle at the event spot needs to know about the event information, it needs to check the blockchain to verify the correctness of event messages and act accordingly. Therefore, we can keep track of all vehicles' recent trustworthiness.

Sometimes, two or more mining vehicles mine a new block at the same time and instantly broadcast the message to their immediate neighbors who begin to propagate the new block across the network. The block might arrive at different vehicles at different times, causing the vehicles to have different blockchain perspectives. As a result, blockchain forks occur. In order to solve forks, the mining vehicles should select the blockchain with the longest chain of blocks that represent the most PoW done.

Hence, the public nature of the blockchain and the independent validation of each new block by all vehicles on the network ensure a distributed and secure database. The blockchain stores the history of all trust levels of the vehicles with corresponding event messages. Thus, we can keep track of all vehicles' recent trustworthiness. The information stored in the blockchain acts as a ground truth for other vehicles. Each block is based on the hash of its previous block and hence manipulating and forging a block is so hard that it needs significant computation power to change the succeeding blocks. The malicious vehicles cannot insert fake blocks into the distributed blockchain without being noticed by other peer vehicles. As the network size grows, the blockchain becomes more difficult to be compromised by the malicious vehicles. So, the event information can be disseminated securely using the new type of blockchain. In addition, the insurance companies for insurance settlements can use the history of vehicle information from the blockchain and the traffic police can use the history as a forensic to solve the hit and run as well as traffic accident disputes.

6. Evaluation

In this section, we discuss the scalability of the proposed blockchain scheme for the VANET. We evaluate the storage and message overhead of the blockchain in the VANET. Most of the today's technology based on the blockchain have scalability issues. As we have discussed earlier, we consider the safety message as transaction in our scheme.

Storage and message overhead: The size of the block header is about 80 bytes as shown in Fig. 3. The Bitcoin blockchain size grows a lot up to petabyte when considering global scale transactions. In our scheme, each safety message would be about 512 bytes and the block header will be about 80 bytes. So the block size with a single message would be about 600 bytes approximately. In our scheme, we assume that the block generation rate is 100 s to prevent attacks, such as double-spending attack. There will be about 36 blocks generated in one hour. Hence, the storage overhead for one blockchain with a message would be 600 bytes*36*24*365 = 180.45 MB per year. We carefully designed the block structure on a VANET network to support a large amount of data without scalability issues. Let us assume that the VANET system consists of 2000 vehicles traveling on a particular location, where vehicles send reporting messages in that location for a given period of time. We can calculate the message transaction per time period in the blockchain as Tx*(B*t), where Tx is the number of message transactions per time period, B is the size of the block and t is the time in units. The total size of the blocks generated in the VANET system is shown in Table 2. The table shows the estimated blockchain growth of the network with different amounts of message transactions per period of time. It shows cases where there are 2000 vehicles running on a particular location with 200 vehicles to a maximum of 1500 vehicles sending report messages in that location. Since we use the local blockchain for the VANET, the blockchain network growth can be controlled, while the scalability issue still remains.

7. Future perspective: edge computing for blockchain in VANET

As for the future perspective, we have introduced edge computing for the blockchain, which can reduce the delay of block generation by offloading the high computational PoW to the edge servers to mine the blocks by the miner vehicles. Furthermore, the block propagation delay can be reduced by using the edge cloud computing. The Mobile Edge Computing (MEC) can provide edge cloud service at the edge for the VANET nodes and offload resource-intensive work from vehicular nodes to the edge servers [39,40]. The application of the MEC in the VANET

Table 2
Evaluation of the growth of the VANET blockchain network.

Message transaction	per second	per minute	per hour	per day	per year
Tx	Tx*(B*1)	Tx*(B*60)	Tx*(B*60*60)	Tx*(B*60*60*24)	Tx*(B*60*60*24*365)
200	117.18 KB	6.87 MB	0.402 GB	9.66 GB	206.51 TB
500	292.96 KB	17.17 MB	1.006 GB	24.14 GB	516.27 TB
1000	585.93 KB	34.33 MB	2.012 GB	48.28 GB	1032.55 TB
1500	878.91 KB	51.49 MB	3.017 GB	72.42 GB	1548.82 TB

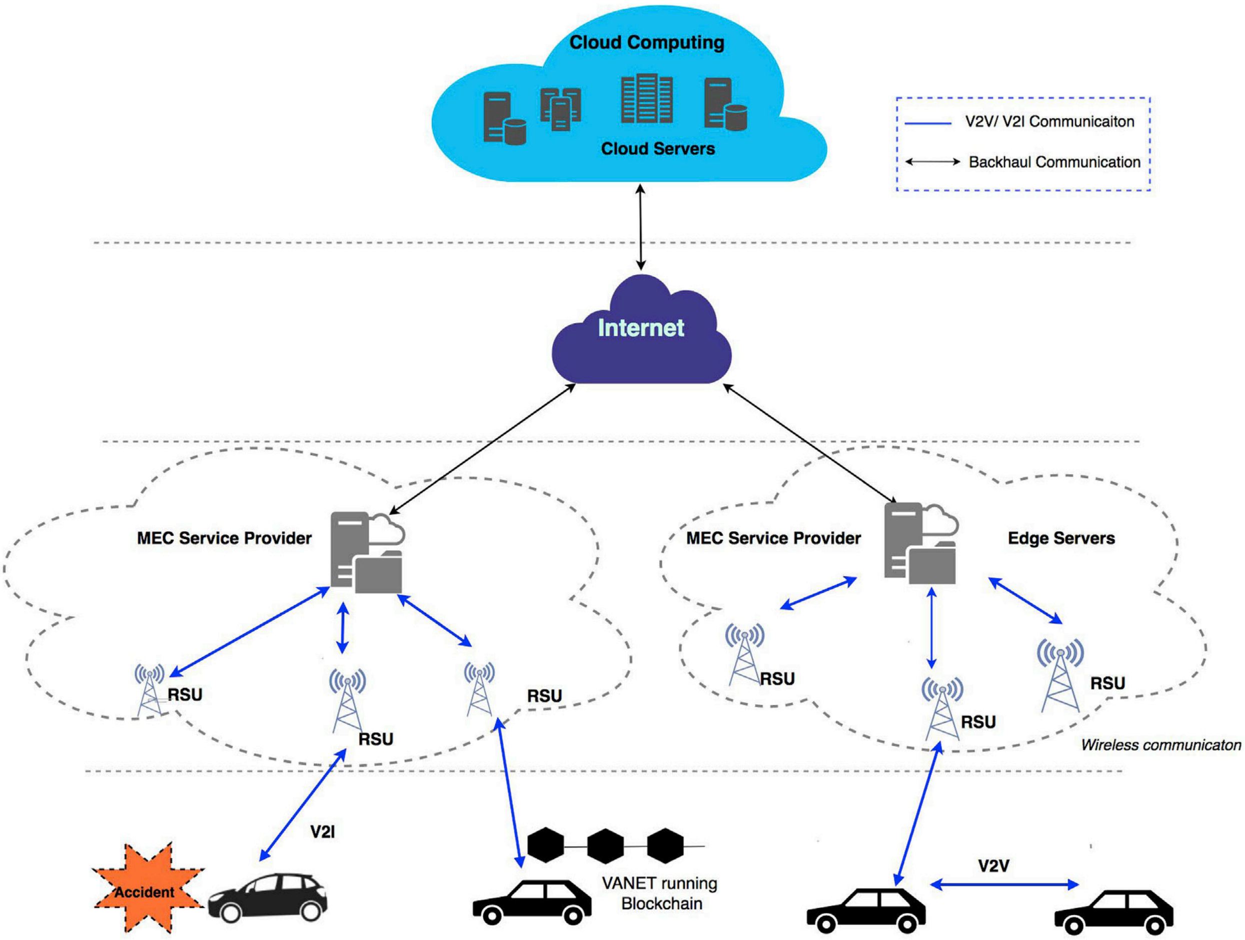


Fig. 8. MEC for the blockchain in the VANET.

blockchain is shown in Fig. 8. The MEC can be used to propagate block messages between the miner nodes that can reduce the propagation delay. In addition to this, the vehicular nodes offload the mining process to the MEC servers to speed up the mining process that helps in frequent block generation, which is suitable for the VANET. As we are dealing with emergency event messages, timeliness of message dissemination is of high priority. The edge computing can be used to mine the blocks faster in our proposed scheme. We assume that the MEC service providers deploys their edge servers for vehicular miner nodes. The miner can offload the computational intensive PoW to the MEC servers and the service provider charge the miner nodes for providing their services. The miner node has to pay a small amount of fee to the edge service provider which will be less than the reward gained when a new block is mined. The miner nodes request for edge service and offload the PoW computation. The MEC servers accept and compute the PoW, and provide solutions to the miner nodes. The miner nodes then broadcast the PoW solution to the network. If a miner is successful in mining a block, then it will receive an incentive in the form of rewards. The MEC also handles other resource intensive tasks, such as computing, storing multimedia tasks like car black box videos, and photo processing, etc.

8. Conclusion

Our proposed scheme can effectively handle the problem of the trustworthiness of event messages in a reliable way by using blockchain technology. We have introduced a new type of blockchain that can be independently managed within a country, which stores the node trustworthiness and message trustworthiness in the distributed ledger for secure message dissemination in the VANET that acts as ground truth for other vehicles. In our scheme, we deal with event messages as transactions instead of cryptocurrency. We present and discuss different categories of blockchain consensus mechanisms based on the type of blockchain. In this paper, we adopt the PoW consensus mechanism. A consensus of all mining vehicles in the blockchain network can be established to generate a new block that can be used as a ground truth for the next block. The evaluation and analysis show that our proposed local blockchain scheme can be used efficiently in the VANET without storage overhead. In our future work, we will provide a detailed analysis of the new type of blockchain and show how our scheme can deal with critical event message dissemination in real time with low delay in the VANET environment. We will use hybrid consensus mechanism, which is a combination of the PoW algorithm and the PoS algorithm that helps in reducing the block generation time and improves the scalability of the vehicular network.

Competing interests

The authors declare no conflicts of interest.

Acknowledgements

This research was supported in part by Basic Science Research Program through National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2013R1A1A2012006, 2015R1D1A1A01058595). This research was supported in part by the MSIP (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2019-2016-0-00313) supervised by the IITP (Institute for Information and Communications Technology Planning & Evaluation). This work was supported in part by the Brain Korea 21 Plus Program (No. 22A20130012814) funded by the National Research Foundation of Korea (NRF).

References

[1] G. Martuscelli, A. Boukerche, P. Bellavista, Discovering traffic congestion along routes of interest using vanets, in: IEEE Global Telecommunications Conference, IEEE GLOBECOM, 2013.

[2] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash SyNakamoto, S. (2008), Bitcoin: a peer-to-peer Electronic Cash System, 39, 2008, p. 5367. Consulted, 19. doi:10.1007/s10838-008-9062-0stem, J. Gen. Philos. Sci., 1.

[3] Z. Zheng, S. Xie, H.N. Dai, H. Wang, Blockchain Challenges and Opportunities: A Survey, Work Pap, December, 2016, pp. 1–9, 2016.

[4] A.M. Antonopoulos, Mastering Bitcoin, First Edit. United States of America: OReilly Media, Inc., 2015.

[5] N.Z. Aitzhan, D. Svetinovic, Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams, IEEE Trans. Dependable Secur. Comput. 15 (5) (2018), 840852.

[6] B. Ostermaier, F. Dotzer, M. Strassberger, Enhancing the security of local dangerwarnings in vanets-A simulative analysis of voting schemes, in: The 2nd International Conference on Availability, Reliability and Security, 2007, pp. 422–431.

[7] R. Shrestha, S.Y. Nam, Access point selection mechanism to circumvent rogue access points using voting-based query procedure, IET Commun. 8 (16) (6 11 2014) 2943–2951.

[8] A. Lei, C. Ogah, E. Al, A Secure Key Management Scheme for Heterogeneous Secure Vehicular Communication Systems, vol. 111, ZTE Communication Magazine, 2016.

[9] B. Leiding, P. Memarmoshrefi, D. Hogrefe, Self-managed and blockchain-based vehicular ad-hoc networks, in: Proc. 2016 ACM Int. Jt. Conf. Pervasive Ubiquitous Comput. Adjun. - UbiComp, vol. 16, 2016, p. 137140. January.

[10] A. Dorri, M. Steger, S. Kanhere, R. Jurdak, BlockChain: a distributed solution to automotive security and privacy, IEEE Commun. Mag. Mag. 55 (12) (2017), 119125.

[11] S. Rowan, M. Clear, M. Gerla, M. Huggard, and C. Mc Goldrick, Securing Vehicle to Vehicle Communications Using Blockchain through Visible Light and Acoustic Side-Channels, eprint arXiv:1704.02553 (Accessed on Nov. 12)..

[12] Y.L. Morgan, Notes on DSRC and WAVE standards suite: its architecture, design, and characteristics, IEEE Commun. Surv. Tutorials 12 (4) (2010), 504518.

[13] M. Raya, P. Papadimitratos, V.D. Gligor, J. Hubaux, On data-centric trust establishment in ephemeral ad hoc networks, in: IEEE INFOCOM 2008 - the 27th Conference on Computer Communications, Phoenix, AZ, 2008, pp. 1238–1246.

[14] J. Zhang, A survey on trust management for VANETs, in: Proc. IEEE International Conference on Advanced Information Networking and Applications, 2011, pp. 105–112.

[15] R. Shrestha, S.Y. Nam, Trustworthy Event-Information Dissemination in Vehicular Ad Hoc Networks vol. 2017, Mobile Information Systems, Hindawi, 2017, pp. 1–16.

[16] F. Gmez Mrmol, G. Martnez Prez, TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks, J. Netw. Comput. Appl. 35 (3) (2012), 934941.

[17] S. Gurung, D. Lin, A. Squicciarini, E. Bertino, Information-oriented trustworthiness evaluation in vehicular ad-hoc networks, network and system security, in: NSS 2013. Lecture Notes in Computer Science, vol. 7873, Springer, Berlin, Heidelberg, 2013, pp. 94–108.

[18] R. El Sibai, T. Atechian, J.B. Abdo, J. Demerjian, R. Tawil, A new software-based service provision approach for vehicular cloud, in: Proc. Global Summit on Computer and Information Technology (GSCIT), 2015, pp. 1–6. Sousse.

[19] D. Florian, L. Fischer, P. Magiera, VARS: a vehicle ad hoc network reputation system, in: Proc. Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, Taormina-Giardini Naxos, 2005, pp. 454–456.

[20] C. Chen, J. Zhang, R. Cohen, P. Ho, A trust-based message propagation and evaluation framework in VANETs, in: Proc. Int. Conf. on Information Technology Convergence and Services, 2010.

[21] W. Li, H. Song, ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks, IEEE Trans. Intell. Transp. Syst. 17 (4) (2015), 960969.

[22] R.C. Merkle, A digital signature based on a conventional encryption function, in: Proceedings of CRYPTO87, 1987, p. 1620.

[23] Consensus mechanism in cryptocurrency, Online, https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency, 2018. (Accessed 4 October 2018).

[24] S. King, S. Nadal, PPCoin: peer-to-peer crypto-currency with proof-of-stake, Online, https://peercoin.net/assets/paper/peercoin-paper.pdf, 2012. (Accessed 14 November 2018).

[25] E. Zhang, A Byzantine Fault Tolerance Algorithm for Blockchain (White Paper), 2018. Online, http://docs.neo.org/en-us/basic/consensus/whitepaper.html. (Accessed 15 November 2018).

[26] O. Moindrot, C. Bournhonesque, Proof of stake made simple with casper, Online, http://www.scs.stanford.edu/17au-cs244b/labs/projects/moindrot bournhonesque.pdf, 2017. (Accessed 10 September 2018).

[27] V. Buterin, V. Griffith, Casper the friendly finality Gadget, CoRR J. 110 (2017).

[28] D. Larimer, Delegated proof of stake, Bitshares. org, 2014. Online. (Accessed 19 September 2018).

[29] D. Mazieres, The stellar consensus protocol: a federated model for internet-level consensus, in: Proc. Marzires2015TheSC, 2015, pp. 1–45.

[30] M. Castro, B. Liskov, Practical Byzantine Fault tolerance miguel, in: Proc. Third Symposium on Operating Systems Design and Implementation, 2002, p. 114.

[31] Intel Corporation, Proof of Elapsed Time, Sawtooth Lake, 2017. Online, https://sawtooth.hyperledger.org/docs/core. (Accessed 10 September 2018).

[32] D. Ongaro, J. Ousterhout, D. Ongaro, J. Ousterhout, In search of an understandable consensus algorithm in search of an understandable consensus algorithm, in: Annual Technical Conference, 2014, pp. 305–319 (USENIX, ATC 14).

[33] D. Schwartz, N. Youngs, A. Britto, The Ripple Protocol Consensus Algorithm, 2014. Online, https://ripple.com/consensus-whitepaper/. (Accessed 21 September 2018).

[34] T. Dasu, Unchain your blockchain, in: Proc. Symposium on Foundations and Applications of Blockchain 1, 2018, p. 1623, 2018.

[35] S. Chen, J. Hu, Y. Shi, Y. Peng, J. Fang, R. Zhao, L. Zhao, Vehicle-to-Everything (V2x) Services Supported by LTE-Based Systems and 5g, 2017, p. 7076, no. June.

[36] N. Tippenhauer, C. Popper, K. Rasmussen, S. Capkun, On the requirements for successful gps spoofing attacks, in: 18th ACM Conference on Computer and Communications Security, 2011, pp. 75–86.

[37] R. Shrestha, R. Bajracharya, S.Y. Nam, Blockchain-based message dissemination in VANET, in: 2018 IEEE 3rd International Conference on Computing, Communication and Security, ICCCS), Kathmandu, 2018, pp. 161–166.

[38] G.O. Karame, E. Androulaki, M. Roeschlin, A. Gervais, S. apkun, Misbehavior in bitcoin: a study of double-spending and accountability, ACM Trans. Inf. Syst. Secur. 18 (1) (2015) 132.

[39] R. Shrestha, R. Bajracharya, S.Y. Nam, Challenges of future VANET and cloud-based approaches, Wireless Commun. Mobile Comput. 15 (2018) 2018.

[40] ETSI GS MEC, Report V1.1.1, MEC - Framework and Reference Architecture, vol. 1, 2016, p. 118. Online, https://www.etsi.org/. (Accessed 25 August 2018).