Blockchain-Enabled Security and Privacy for Internet-of-Vehicles

Ferheen Ayaz, Zhengguo Sheng, Daxin Tian, and Victor C. M. Leung

1 Introduction

The proliferation of Internet-of-Things (IoT) have revolutionised the concept of conventional Vehicular Ad-Hoc Networks (VANETs) into Internet-of-Vehicles (IoV), ensuring an overall connectivity of a vehicle with not only other vehicles on road but also with every other object including passengers' smart phones, external management platform, navigation systems and other road users, thereby forming an Intelligent transportation system (ITS). The potential benefits of IoV include increased passengers' safety, smooth traffic flow and availability of infotainment. Also, with an increase in vehicle density on road over the past few decades, high risk of accidents and traffic jams appear very common in daily transport and thus seriously threat road safety [1]. Safe driving conditions can be achieved by implementing IoV in which a vehicle or other connected device can initiate timely and efficient message dissemination in emergency situations, such as accidents [2]. The oncoming vehicles may re-route themselves to avoid traffic congestion by receiving an alert prior to entering into an affected area. However, IoV encounters many challenges in implementation of an efficient message dissemination solution because the vehicles behave differently than other wireless nodes. Due to the

F. Ayaz (✉) · Z. Sheng
Department of Engineering and Design, University of Sussex, Brighton, UK
e-mail: f.ayaz@sussex.ac.uk

D. Tian
School of Transportation Science and Engineering, Beihang University, Beijing, China

V. C. M. Leung
Department of Electrical and Computer Engineering, University of British Columbia (UBC), Vancouver, BC, Canada

N. Gupta et al. (eds.), *Internet of Vehicles and its Applications in Autonomous Driving*, Unmanned System Technologies, https://doi.org/10.1007/978-3-030-46335-9_9

dynamic characteristics and complexity of vehicular networks, IoV possesses some specific characteristics and demands to look after some particular challenges discussed below.

1.1 Characteristics and Challenges of IoV

The communication environment in IoV is variable. For example, a motorway is open and allows one direction movement of vehicles with high mobility. A lane change or a brake event must be communicated timely to the concerned vehicles in order to avoid collision. Therefore, a lightweight networking protocol is required. Multiple vehicles sending the same message may result in packet collision and broadcast storm. The connected vehicles must be able to select appropriate relay nodes among themselves, which can effectively forward a message to a large number of vehicles [3]. A central node like a Road Side Unit (RSU) can be used for message dissemination. However, it requires a large investment for installation [4] and its volume and placement positions are crucial for system performance [5]. Moreover, RSU assisted routing protocol may result in higher latency because of increased route discovery time and hops per route [6]. Since low latency is an important criteria when propagating messages to fast moving vehicles, a decentralised network in which vehicles can select relay nodes among themselves independently without any central authority (CA) is desired as a more scalable and cost-effective approach than the networks dependent upon RSU [7].

On the other hand, a residential area contains random movements and obstacles like tall buildings with the presence of relatively larger number of connected devices. An incident occurring in a street cannot be directly witnessed by passengers travelling on an adjacent road. In such situations, it is also essential for vehicles in IoV to authenticate a message before dissemination to maintain trust and security in the network. A malicious vehicle may generate a false message about an incident which did not actually occur on road or deliberately mark an authentic message as fake [8]. Moreover, due to increasing privacy concerns, the identity of a vehicle must not be revealed if it sends a message. However, anonymous announcements can affect the credibility of a message [9]. Public key management by CA is one of the solutions to privacy but large scale networks in dense areas would result in running of several cryptographic operation requests at the same time which is not a feasible solution [10].

Although message dissemination, trust management, privacy and security in connected vehicles are widely discussed in literature [11–13], there is a need to develop an integrated approach in which efficient and trusted communications of IoV can be managed in a decentralised fashion. Furthermore, to maintain the sustainability of message dissemination in IoV, economic modelling is needed which results in an efficient incentive distribution strategy to encourage positive cooperation and punish negative behaviour of vehicles. There are two common types of incentive strategies: price based and reputation based. In price based strategy, messages are treated as commodities which are exchanged for virtual

credits [14, 15]. On the contrary, reputation based strategies use measurement of trustworthiness to enforce cooperation. A threshold of reputation is set to distinguish a node behaviour as malicious or non-malicious. A punishment scheme is usually applied for malicious behaviour [16, 17]. Game theoretical analysis [18] suggests that an integrated strategy including the advantages of both price based and reputation based schemes is more effective in promoting cooperation and detecting malicious behaviour in Mobile Ad-hoc Networks (MANETs) [19].

1.2 Blockchain as a Potential Solution

In this chapter, we briefly explain the concept of a blockchain-enabled IoV to overcome the discussed challenges. A blockchain is basically a peer-to-peer electronic cash system in which transaction data is maintained in a ledger as immutable timestamped blocks and each block is linked to the previous block with the help of a cryptographic hash [20]. To complete a transaction in a blockchain, a client needs to first submit a proposal which is then verified by a network of peers using an algorithm known as consensus. If a proposal is verified, it is stored in the blockchain as a unique record. A blockchain is encrypted, decentralised, secure and immutable. Therefore, it is able to solve issues related to security and privacy, and has the potential to contribute towards IoT applications [21, 22]. Our chapter shows how blockchain can be used to implement distributed, secure and privacy-preserving communications in IoV. The goal is to introduce a secure, lightweight and decentralised peer-to-peer vehicular network in which untrusted vehicles can interact with each other in a verifiable manner. The key challenge in IoV is ensuring the authenticity of message in a decentralised manner. It is interesting to point out that the feature of consensus in blockchain can be applied to resolve this challenge. Blockchain provides robustness against dissemination of false messages as long as the honest vehicles collectively possess more controlling power than malicious vehicles. The basic idea of blockchain implementation for security and privacy in IoV is shown in Fig. 1. A blockchain-enabled IoV would be able to record messages

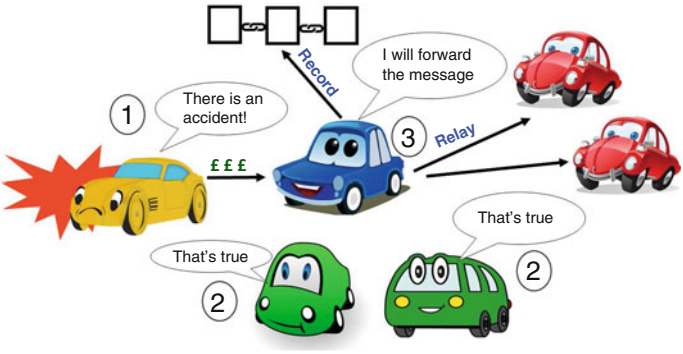


Fig. 1 Basic idea of blockchain for security in IoV

into an ongoing chain along the broadcast route, forming a ledger that cannot be changed. All vehicles can collectively act as peers to authenticate messages and select a relay node to forward message and manage the history of publicly available previous record of messages. To discourage accidents, ensure smooth traffic and promote positive cooperation, the vehicles causing accident can compensate by paying reward to the vehicles participating in message dissemination.

2 Fundamentals of Blockchain

This section briefly describes the fundamentals of blockchain, including its structure, types, basic consensus algorithms and their suitability with respect to IoV.

2.1 Structure of Blockchain

As shown in Fig. 2, a blockchain is used to store transactions in a sequence of blocks chained together by including a cryptographic link to the previous block known as hash [23]. In a conventional blockchain, whenever a new transaction is made, it is announced across the network. Nodes are able to verify a transaction and record the verified transaction into a block containing an encrypted hash of previous block, thereby making it cryptographically secure. Nodes which append a block to the blockchain after verification and broadcast it in the network are known as miners. Miners have to go through a mutual agreement called consensus algorithm to create a block which makes it fraud-proof [24]. All nodes in a network update their copy of blockchain regularly in order to ensure consistency in the entire distributed ledger [25].

A typical blockchain is permissionless and open to public where anyone in a network can make entry into the ledger. Bitcoin and Ethereum are the examples of permissionless blockchain [23]. On the other hand, Hyperledger family offers various versions of permissioned blockchain, where specific roles and access

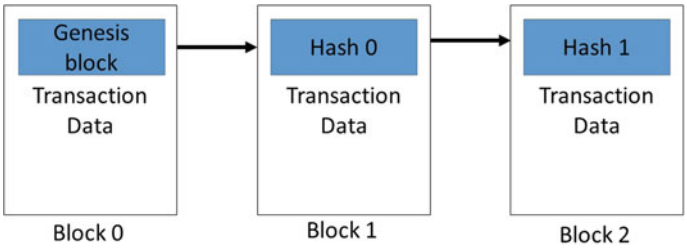


Fig. 2 The blockchain structure

limitation can be associated to certain nodes. Considering different roles in ITS, such as automotive manufacturers, government and transportation authorities, a permissioned blockchain is considered to be appropriate for vehicular applications [26].

2.2 Consensus Algorithm

The core of a blockchain mechanism is consensus algorithm. It is an agreement to validate a transaction and unanimously take a decision. The Bitcoin uses an incentive based Proof-of-Work (PoW) consensus for block-mining. In PoW, the nodes have to solve an extremely difficult puzzle to become a miner, which requires high computational power and results in large propagation delay. However, a difficult cryptographic puzzle which cannot be solved and tampered easily makes the blockchain highly secure. An alternative of PoW is Proof-of-Stake (PoS) [27]. New versions of Ethereum are PoS-based [28]. PoS replaces the mining operation of PoW with a miner selection on the basis of highest amount of stakes or virtual currency owned, which makes it unfair for members possessing smaller stakes [29]. A permissioned blockchain usually adopts voting based Practical Byzantine Fault Tolerant (PBFT) algorithm for achieving consensus among a group of nodes in a permissioned environment [30]. PBFT consists of three stages as shown in Fig. 3. In first stage, a client sends a transaction proposal to validating peers. In second stage, a transaction proposal is validated by receiving votes from at least a certain minimum number of peers. In third stage, the block is committed to the blockchain. The minimum number of votes required to validate a transaction proposal is usually specified in a smart contract of a blockchain. A novel PBFT based voting algorithm known as Yet Another Consensus (YAC) is implemented in Hyperledger Iroha blockchain platform. It tolerates f faulty nodes out of $2f+1$ participants taking part in consensus [31]. A comparison of basic blockchain technologies is summarised in Table 1, which indicates that consensus algorithm of Hyperledger; PBFT is the most promising algorithm for vehicular applications, as it overcomes the limitations of PoW and PoS. However, PBFT does not scale well with large number of nodes, as the number of messages broadcasted to validate a transaction proposal increases with raising number of nodes. Nevertheless, with moving vehicles, the number of nodes within a limited transmission range of a vehicle initiating a transaction

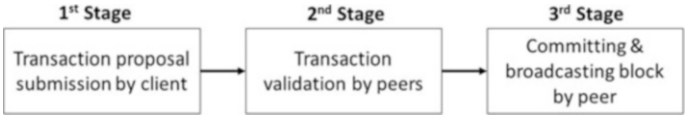


Fig. 3 PBFT consensus algorithm

Table 1 Comparison of blockchain technologies

	Bitcoin	Ethereum	Hyperledger
Consensus	PoW	PoS	PBFT
Mode	Permissionless	Permissionless	Permissioned
Currency	Bitcoin	Ether	Not required
Smart contract	No	Yes	Yes
Pros	Highly secure	Time and energy saving	Time and energy saving
Cons	Time and energy consuming	Biased towards peers with high amount of stakes	Message count increases with number of nodes

proposal is always limited and cannot be increased to a large extent. Therefore, despite the drawback of PBFT, it is well-suited to be used with IoV.

3 Related Work

In this section, the related work which utilises blockchain technology as a potential solution to existing challenges in IoT and IoV applications is discussed with referenced literature. The discussion is focussed on how blockchain can the existing challenges of privacy and trust in IoT and IoV.

3.1 Privacy

The transactions in a blockchain are recorded with the use of cryptographic public and private keypairs. The public key can also be changed for different transactions. The anonymity in network is maintained by keeping the identity of participants private. This features makes blockchain useful in many applications which include confidentiality, for example, storing patients' record and history [32]. A permissioned blockchain solution to keep the privacy of identity and location of electric vehicles during payment at charging stations was proposed in [33]. Due to lack of scalability in permissioned blockchain's consensus, public blockchain for urban areas with large number of vehicles was also suggested in [33]. It can be deduced that greater privacy can be achieved through permissioned blockchain by trading off scalability. Apart from payment transactions, the privacy-preserving feature of blockchain can also be used to ensure anonymous message exchange. In [34], a blockchain-based incentive anonymous announcement network was proposed, which used virtual credits, known as, CreditCoin as a reward for forwarding the message. The transactions of CreditCoins were managed by blockchain, whereas vehicle-to-vehicle (V2V) communications were implemented separately.

The privacy of vehicles was maintained because their identities were encrypted during communications. The message dissemination system was not completely decentralised because it relied on RSUs or official public vehicles as servers which undertake the work of consensus. In [35], the concept of blockchain managed by a Certificate Authority was proposed, which assigned or revoked encrypted keys. It provided a privacy-preserving solution because vehicles communicated with each other using public key instead of revealing their original identities. For reputation management, the vehicles needed to report to a centralised law enforcement agency whenever they observed a malicious behaviour.

3.2 Trust and Reputation

In a blockchain network, nodes have to go through a consensus algorithm to verify a transaction in a block. A consensus algorithm ensures trust in a network because fake transactions cannot be verified by all nodes [36]. By use of blockchain in IoV, a malicious vehicle cannot easily initiate a false message, because it has to be propagated after validation. One way to judge the validity of a message is on the basis of reputation of sender. This is why reputation management is one of the subjects where blockchain research is rapidly progressing. Many researches have employed reputation to reach consensus because PoW is not feasible to be used with moving vehicles. A blockchain-based reputation management with the consensus algorithm of PoS, where reputation was the stake of vehicles was proposed in [37]. The vehicles reported their reputation opinions of other vehicles to a nearby RSU. To carry out consensus algorithms, the reputation values were downloaded from RSU and a mining vehicle was elected on the basis of highest reputation. The vehicle was considered malicious if its reputation value was below a certain threshold. A similar approach was presented by Yang et al. [38] where RSUs stored reputation of vehicles and maintained blockchain. To carry out consensus algorithm, mining RSUs underwent a joint PoW and PoS algorithm where reputation was regarded as a stake. It also considered Bayesian Inference for authentication of incidents occurring on road. Both mechanisms relied upon RSUs for blockchain management. Consensus processing by RSUs to store trust ratings of vehicles in a blockchain was also proposed in [39]. Blockchain managed by RSUs was recommended in [40] because of their higher storage capacity and processing power than vehicles. However, the issues of short connection time between a RSU and a vehicle as well as security attacks on RSUs which control blockchain are still not addressed in existing literature. In [41], permissioned blockchain of reputation, not dependent upon RSUs, was proposed and messages were authenticated on the basis of sender's reputation. It followed conventional PoW algorithm for miner election.

3.3 Decentralisation

The blockchain methodology is independent of third party to finalise transactions. This feature makes it suitable for distributed networks, for example, supply chain [42] and IoV [43]. In [44], authors discussed the strategies to design decentralised applications using blockchain and pointed out that the challenges in developing blockchain-based processes including selection of blockchain network type (permissioned or permissionless) and consensus model. Decentralisation in IoV by the use of Ethereum blockchain was proposed by Leiding et al. [45]. It was suggested to automatically punish negative behaviour of vehicles, for example, over-speeding and ignoring traffic lights, by imposing fine or recalculate tax or insurance by the use of smart contract without requiring a central authority. In [46], an incentive mechanism which was used to motivate vehicles to forward messages was proposed. Only the transactions of incentives were managed by blockchain in a decentralised manner, whereas the relay node selection mechanism was employed separately.

To summarise, it can be stated that the existing literature contains proposed incentive mechanisms for vehicles to participate in message dissemination using blockchain or blockchain-enabled reputation management systems, usually depending upon a central authority or RSUs. However, a consolidated solution can potentially be formulated by involving blockchain not only for transaction of virtual currency but also for transaction of messages to implement completely decentralised, private and trusted IoV communications.

4 Blockchain-Enabled IoV

In this section, the blockchain-enabled solution for message dissemination among connected vehicles, along with reputation management and incentive distribution mechanism [47] is explained. The key notations used in this chapter are defined in Table 2. The proposed solution consists of the following components:

1. **Central Authority** (CA) Before joining the blockchain network, a vehicle needs to be registered with the CA. It assigns a wallet address and a pair of public and private keys to the vehicle for communications and records its original identity. The key pair is used for anonymous transmissions. The role of CA is to grant vehicles an access to a permissioned blockchain system. CA monitors the network and is also in-charge of setting the rules in the system, for example, the minimum amount of balance in a credit wallet and a vehicle's initial reputation value.
2. **Originator** (ORG) An ORG is the vehicle which is involved in an incident and originates a $transaction\ proposal$.
3. **Transaction Proposal** A $transaction\ proposal$ contains an unendorsed message sent by ORG including details about the incident, for example, its location

Table 2 Key notations

Notation	Definition	Notation	Definition
CA	Central authority	ORG	Originator
i	Hop index	$\overline{END}(i)$	Endorsers at ith hop
$RLY(i)$	Relay node at ith hop	TC	Transmission charge
CC	Call compensation paid by ORG	R_j	Reputation of vehicle j
R_T	Reputation threshold	N_{END}	Number of endorsers at hop i
N_{HOP}	Number of hops	Q_j	Quality factor of vehicle j
t_{END}^{max}	Maximum waiting time for *endorsements*	t_{max}	Maximum time limit for message dissemination
df_j	Distance factor of vehicle j	$d_{j,k}$	Distance between vehicle j and k
d_{HOP}^{min}	Minimum distance a message should reach per hop	CQ_j	Channel quality parameter of vehicle j
CP_j	Collision probability of vehicle j	t_W	Time window
N_j^s	Number of successful transmissions by vehicle j	N_j^o	Number of overall transmissions by vehicle j
t_j^{occ}	Channel occupancy time when vehicle j is trying to transmit	$RSSM_j$	Received signal strength matrix of vehicle j
RSS_j	Received signal strength of vehicle j	RSS_T	Received signal strength threshold
G_j^r	Receiving antenna gain of vehicle j	G_j^t	Transmitting antenna gain of vehicle j
TP_j	Transmitting power of vehicle j	λ	Wavelength used in VANET
w_1, w_2	Weight of $\overline{END}$, $RLY(i)$ share in CC	α_1, α_2	Weight of df_j and CQ_j to compute Q_j
TR_j	Transmission range of vehicle j	$P_j(i)$	Profit of vehicle j at hop i
β	Reputation reward	γ	Reputation penalty
ACT_j	Action of player j	U_j	Utility of player j

and time. The voting based blockchain system confirms the authenticity of a *transaction proposal* through *endorsements*.

4. **Endorsement** An *endorsement* is a vote confirming that a *transaction proposal* is authentic. A minimum number of *endorsements*, N_{END}^{min}, is required to consider a *transaction proposal* as an endorsed message.
5. **Endorsers at hop i, ($\overline{END}(i)$)** At each hop i, $\overline{END}(i)$ is a set of vehicle j which vote for a suitable relay node. When $i = 0$, $\overline{END}(i)$ are vehicles adjacent to ORG and they also endorse a *transaction proposal*, if they have witnessed the incident itself or made confirmation through camera equipped device or any other service as described in [26].

6. **Relay node at hop i, ($RLY(i)$)** It is the vehicle which further disseminates an endorsed message. It is mutually selected by the voting of $\overline{END}(i)$. It is also one of the $\overline{END}(i)$ and may vote for itself. It also acts as a miner by committing the block to record transfer of virtual credits and reputation updates in the blockchain and finalising the consensus algorithm at each hop i.
7. **Credit Wallet** Each vehicle possesses a credit wallet in which virtual credit is stored.
8. **Transmission Charge (TC)** It is a fee deducted from a vehicle's credit wallet when it originates or endorses a $transaction\ proposal$ or further disseminates an endorsed message. This fee is deposited to CA. CA regulates TC according to the incident recovery cost estimated at the location of incident and time of the day. The purpose of introducing TC is to demotivate vehicles to make a fake $transaction\ proposal$ or $endorsement$, as it is generated at the expense of their virtual credit.
9. **Call compensation (CC)** As a compensation of causing an incident, CC is the amount deducted from the credit wallet of ORG. It is inversely proportional to its reputation. ORG with higher reputation can pay less CC. This is the reason why vehicles are motivated to increase their reputation.
10. **Reputation (R_j)** It is a reputation value of vehicle j. A vehicle is only eligible to endorse a $transaction\ proposal$ if its reputation value exceeds a certain reputation threshold, R_T, that is, $j \epsilon \overline{END}(0)$ if $R_j > R_T$.

4.1 Voting Based Consensus Algorithm

The consensus algorithm of proposed blockchain-enabled IoV follows the voting mechanism of YAC [28] where ORG acts as a client and $\overline{END}(i)$ perform the role of a peer and is illustrated in Fig. 4. When an incident occurs, ORG originates a $transaction\ proposal$. Upon receiving a $transaction\ proposal$, a vehicle j that can confirm the incident becomes an endorser, i.e. $j \epsilon \overline{END}(0)$, broadcasts its cryptographically encrypted signature as a part of $endorsement$ phase and votes for a suitable $RLY(0)$. The selection criteria of $RLY(i)$ are described later in this section. If N_{END}^{min} endorsements are obtained within the time limit, t_{END}^{max}, the $transaction\ proposal$ is considered to be an endorsed message. In order to simplify our assumption, we only consider a static case in which N_{END}^{min} is fixed. An adaptive N_{END}^{min} corresponding to real traffic conditions is out of the scope of this paper, but can be partially solved by using the traffic density estimation method [48]. When a $transaction\ proposal$ is classified as an endorsed message, $RLY(0)$ will further disseminate it in its transmission range and generate a block. The block generation details are described later in this section. Voting based selection of $RLY(i)$ for $i > 0$ is continued until reaching a maximum number of hops, that is, $i > N_{HOP}^{max}$ or the endorsed message has been disseminated until a time limit, d_{max}. It is noted that $\overline{END}(i)$ need to send $endorsements$ for a $transaction$

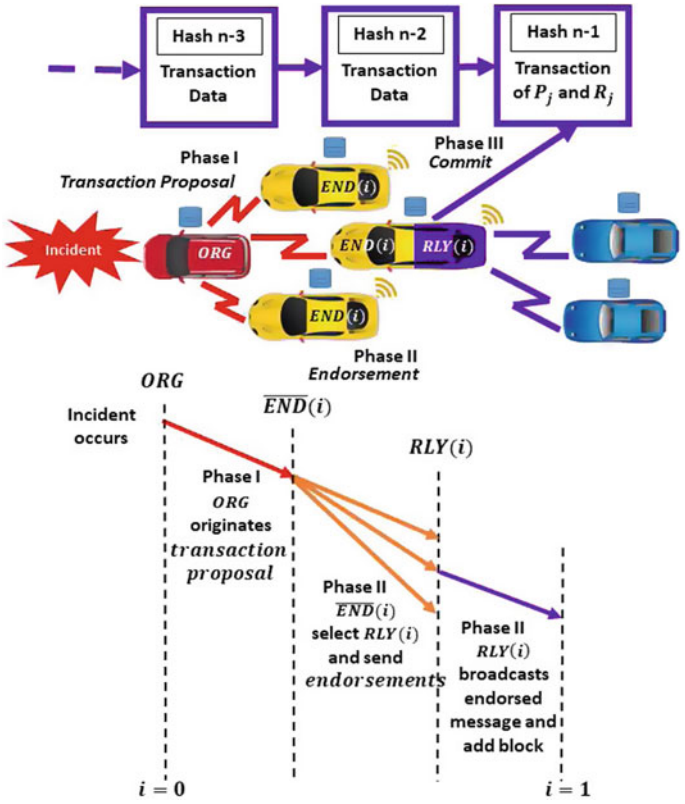


Fig. 4 Proposed voting based consensus algorithm

proposal only when $i = 0$. At $i > 0$, $\overline{END}(i)$ only take part in consensus of $RLY(i)$ selection, because they already receive an endorsed message instead of a *transaction proposal*.

4.2 Relay Selection Mechanism

In our proposed solution, $\overline{END}(i)$ vote for the most appropriate $RLY(i)$ which can further disseminate an endorsed message to a wider area. In this work, we assume that each vehicle j is sharing its location coordinates, channel quality parameter CQ_j, collision probability CP_j, receiving antenna gain G_j^r, transmitting antenna gain G_j^t, maximum transmitting power TP_j and transmission range TR_j during their regular beacon message exchange. The parameters of $RLY(i)$ are stored in the blockchain and are regularly audited by CA to detect and investigate potential fraud if a vehicle cheats by sending fake parameters to achieve highest Q_j. $j \epsilon \overline{END}(i)$

computes the quality factor Q_j and determines its own choice of $RLY(i)$ with the highest Q_j, that is,

$$RLY(i) = index(max(Q_{\overline{END}(i)})), \tag{1}$$

and,[1]

$$Q_j = \alpha_1 df_j + \alpha_2 CQ_j(1 - CP_j) + RSSM_j, \tag{2}$$

where $j \epsilon \overline{END}(i)$, df_j is the distance factor of vehicle j, $RSSM_j$ is the received signal strength matrix, α_1 and α_2 are corresponding weights. df_j is defined as

$$df_j = \begin{cases} \frac{d_{j,ORG}}{d_{HOP}^{min}}, & \text{if } d_{j,ORG} \geq d_{HOP}^{min}, i = 0, \\ \frac{d_{j,RLY(i-1)}}{d_{HOP}^{min}}, & \text{if } d_{j,RLY(i-1)} \geq d_{HOP}^{min}, i > 0, \\ 0, & \text{otherwise}, \end{cases} \tag{3}$$

where d_{HOP}^{min} is the minimum distance a message should be disseminated per hop to restrict $RLY(i)$ selection outside a distance limit [49]. CQ_j and CP_j depend upon internal statistical parameters of medium access control (MAC) as described in [50]. CQ_j is defined as

$$CQ_j = \begin{cases} \frac{N_j^s}{N_j^o}, & \text{if } N_j^o > 0, \\ 0, & \text{otherwise}, \end{cases} \tag{4}$$

where N_j^s is the number of successful transmissions and N_j^o is the number of overall transmissions in a time window. CP_j is estimated as likelihood of collision occurrence if a message is forwarded by vehicle j. It is defined as

$$CP_j = \frac{t_j^{occ}}{t_W}, \tag{5}$$

where t_j^{occ} is the accumulated time at which the channel was occupied or busy when vehicle j was trying to transmit and t_W is a fixed time window. The Received Signal Strength RSS_j, as defined in [51], can be calculated from a distance between locations of vehicle j and j', where $j' \epsilon \overline{END}(i)$, as

$$RSS_j = \frac{G_j^r \times G_j^t \times TP_j}{(4\pi d_{j,j'}/\lambda)^2}, \tag{6}$$

[1] Any other algorithm instead of the proposed method for computation of Q_j can also be used in blockchain-enabled IoV.

where λ is the wavelength used in VANET. The threshold of the received signal strength is defined as

$$RSS_T = \frac{G_j^r \times G_j^t \times TP_j}{(4\pi \times 0.9054TR_j/\lambda)^2}. \tag{7}$$

The range of the antennas is assumed as the circular area of radius TR_j. From [52], it shows that the average distance between two random mobile nodes in a circular region of radius TR_j is $0.9054TR_j$. The purpose of using RSS_T as a threshold parameter is to estimate the reliability of connection with vehicle j. If $RSS_j \geq RSS_T$, the connection can successfully be maintained for a certain time period. Otherwise, the connectivity may be lost before completing a voting consensus [53]. $RSSM_j$ is calculated as

$$RSSM_j = \begin{cases} 1 - \frac{RSS_T}{RSS_j}, & \text{if } RSS_j \geq RSS_T, \\ 0, & RSS_j < RSS_T. \end{cases} \tag{8}$$

4.3 Incentive Distribution Mechanism

The incentive distribution of proposed solution is managed by the blockchain. The proposed voting based blockchain is used to store parameters related to $Q_(RLY(i))$, transactions related to distribution of CC and updated reputation of vehicles. As shown in Fig. 5, the blocks are committed by $RLY(i)$ at each hop. Every vehicle in permissioned network possesses the blockchain. Addition of block is announced by $RLY(i)$ to vehicles in its transmission range. Each vehicle is responsible for updating its blockchain and coordinating it with CA regularly.

CC is used as a monetary incentive in the proposed approach. It is divided into two parts with ratio $w1 : w2$, where w_1 and w_2 are corresponding weights to divide the share of CC among $\overline{END}(0)$ and $RLY(i)$, $RLY(i+1),\ldots,RLY(N_{HOP}^{max})$ respectively and $w_1 + w_2 = 1$. The profit, P_j of a vehicle j is given as

$$P_j = \begin{cases} \frac{w_1 CC}{N_{END}^{min}}, & \text{if } j \epsilon \overline{END}(0), \\ \frac{w_2 CC}{N_{HOP}}, & \text{if } j = RLY(i), \\ 0, & \text{otherwise.} \end{cases} \tag{9}$$

The transactions into credit wallets of $\overline{END}(i)$ are committed as a block by $RLY(i)$ only when $i = 0$ and transactions into credit wallets of $RLY(i)$, $RLY(i+1),\ldots,$ $RLY(N_{HOP}^{max})$ are committed as a block at last hop by $RLY(N_{HOP}^{max}+1)$. If N_{END}^{min} *endorsements* are not obtained for a *transaction proposal* until t_{END}^{max}, it is considered as fake and CC is transferred to CA as a penalty to ORG. The penalty

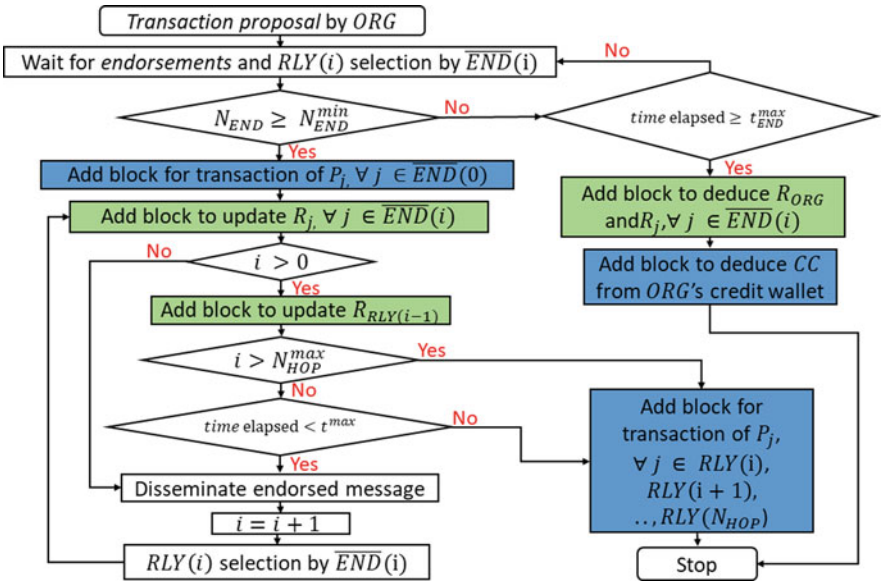


Fig. 5 Flowchart of blockchain-enabled message dissemination in IoV

is recorded as a transaction in the blockchain by $RLY(i)$ which is selected by ORG itself while originating a *transaction proposal*. No share of CC is paid to $\overline{END}(0)$ which endorsed a fake *transaction proposal*.

Reputation is affected by the behaviour of vehicle. Honest behaviour of $\overline{END}(i)$ and $RLY(i)$ is recognised as the successful action performed during message dissemination. Malicious behaviour refers to a fake *transaction proposal* initiated by ORG or endorsed by $\overline{END}(i)$ and selfish $RLY(i)$ without disseminating an endorsed message. Reputation updates are committed as transactions in the blockchain by $RLY(i)$ at each hop i. $R_{\overline{END}(i)}$ are updated at ith hop and $R_{RLY(i)}$ is updated at $(i+1)$th hop. If $RLY(i)$ itself behaves maliciously, its reputation deduction is processed in the blockchain by CA after being reported by $\overline{END}(i)$. If a vehicle j behaves honestly, its reputation is updated with

$$R_j = R_j + \beta, \tag{10}$$

where β is the reputation reward. If it behaves maliciously, its reputation is updated with

$$R_j = R_j - \gamma, \tag{11}$$

where γ is the reputation penalty. The credit and reputation management follows an economic model defined in Table 3.

Table 3 Economic model for credit and reputation management

	Credit		Reputation	
Vehicle	Honest	Malicious	Honest	Malicious
ORG	$-TC - CC$	$-TC - CC$	–	$R_{ORG} - \gamma$
$j \epsilon \overline{END}(i = 0)$	$P_j - TC$	$-TC$	$R_{\overline{END}(i)} + \beta$	$R_{\overline{END}(i)} - \gamma$
$j \epsilon \overline{END}(i > 0)$	–	–	$R_{\overline{END}(i)} + \beta$	–
$j = RLY(i)$	$P_j - TC$	0	$R_{RLY(i)} + \beta$	$R_{RLY(i)} - \gamma$

Game Theory Analysis

We apply game theory to analyse the performance of our incentive distribution mechanism against collusion of $RLY(i)$, $RLY(i+1)$,...,$RLY(n)$, where n is equivalent to the number of colluding relay nodes. We find the best action for players and associated conditions so as to provide positive utility to honest players. By setting up a suitable condition, we can guarantee the security of our solution against colluding behaviour of relay nodes. The model of our blockchain-enabled message dissemination game is described as follows

- **Players** This game has N_{END}^{min} number of $\overline{END}(0)$ and one $RLY(i)$ at each hop i. The number of hops is N_{HOP}.
- **Actions** At hop $i = 0$, $j \epsilon \overline{END}(0)$ has three possible actions, honest (H), malicious (M) and selfish (S). If it votes for a true message, it is honest. If it votes for a false message, it is malicious. If it does not cooperate, it is selfish. At each hop i, $RLY(i)$ has two possible actions: honest (H) and selfish (S). If it forwards the message and commits block, it is honest. If it does not cooperate, it is selfish. We denote the action of player j by ACT_j, which is either H, M or S.
- **Utilities** Without colluding with its neighbours, the utility U_j is

$$U_j = \begin{cases} -TC, & \text{if } j \epsilon \overline{END}(0), ACT_j = M, \\ P_j - TC, & ACT_j = H, \\ 0, & \text{otherwise.} \end{cases} \tag{12}$$

We present the following definitions for the security analysis of our incentive distribution mechanism.

Definition 1 The best response action for a player is such that it brings the maximum expected utility to itself, regardless of the actions of all other players.

Definition 2 The incentive distribution mechanism is $RLY(i)$ collusion resistant if $RLY(i)$ and any group of its colluding neighbours cannot increase the expected sum of their utilities by using any action other than the one in which everybody plays honestly.

The following proposition and theorem are also presented here.

Proposition 1 *In blockchain-enabled message dissemination game, playing honest is the best response action of all players if* $0 \leq TC \leq P_j$.

Proof According to (12), if $TC < 0$, the utility of player j, for $j \epsilon \overline{END}(i)$ would be positive if it plays maliciously. On the other hand, if $TC \geq P_j$, the utility of player j would be negative if it plays honestly. In either of these cases, the best response action of players would be to play maliciously or selfishly. Therefore TC must be set such that the action results in positive U_j or profit gain in credit wallets of all players only if they play honestly. □

Theorem 1 *The incentive distribution mechanism is resistant against collusion of* $RLY(i)$, $RLY(i+1),\ldots,RLY(n)$ *if* $TC \geq 0$.

Proof Lets consider the case with one conspired $RLY(i)$. Suppose $CG = \{RLY(i), RLY(i+1)\}$ is a collusion group. CG conspires to form a bogus path with an additional hop, i.e., $ORG \rightarrow RLY(i) \rightarrow RLY(i+1)$ instead of the most appropriate path, i.e. $ORG \rightarrow RLY'(i+1)$. Let p be the probability with which $RLY(i)$ encounters, where $p \epsilon [0, 1]$. Therefore, p^2 is the probability with which it encounters both ORG and $RLY(i+1)$. The expected utility sum of CG, $E(U_{CG})$ is

$$E(U_{CG}) = p^2(U_{RLY(i)} + U_{RLY(i+1)}) + (1 - p^2)(U_{RLY'(i+1)}), \tag{13}$$

or,

$$\begin{aligned} E(U_{CG}) = p^2(P_{RLY(i)} - TC + P_{RLY(i+1)} - TC) \\ + (1 - p^2)(P_{RLY'(i+1)} - TC). \end{aligned} \tag{14}$$

Since $N_{HOP} = 2$ for collusion case and $N_{HOP'} = 1$ for non-collusion, $E(U_{CG}$ becomes

$$E(U_{CG}) = p^2\Big(\frac{w_2 CC}{2} + \frac{w_2 CC}{2} - 2TC\Big) + (1 - p^2)(w_2 CC - TC), \tag{15}$$

or,

$$E(U_{CG}) = w_2 CC - TC - p^2 TC. \tag{16}$$

To avoid collusion of relay nodes, we want $E(U_{CG}) \leq U_{RLY'(i+1)}$, that is,

$$w_2 CC - TC - p^2 TC \leq w_2 CC - TC. \tag{17}$$

It follows that

$$- p^2 TC \leq 0, \tag{18}$$

or,

$$p^2 TC \geq 0. \tag{19}$$

Similarly, by generalising cases when $n > 2$, we can derive the collusion resistant condition, that is, $p^n TC \geq 0$. Hence, for any $p \epsilon [0, 1]$, we can prove that the incentive distribution mechanism is relay node collusion resistant if $TC \geq 0$. □

4.4 Annual Road Tax

The blockchain-enabled IoV can also be used to calculate road tax. It can be annually calculated on the basis of remaining balance of each vehicle's credit wallet at the end of the year. The motivation behind this approach is due to the amount in a credit wallet reflecting a vehicle's behaviour. A vehicle which is involved in less number of incidents would have spent less credit in originating $transactionproposals$, leaving higher balance remaining in its credit wallet which can be redeemed into road tax. Furthermore, the vehicles which are near to the incident's location would be motivated to take part in message dissemination and earn the credit as a compensation of being affected by the incident.

5 Simulation Results and Discussion

In this section, the performance of our blockchain-enabled solution is discussed on the basis of results obtained through extensive simulations using OMNeT++ integrated with SUMO (Simulation of Urban Mobility) which can be seen in Fig. 6.

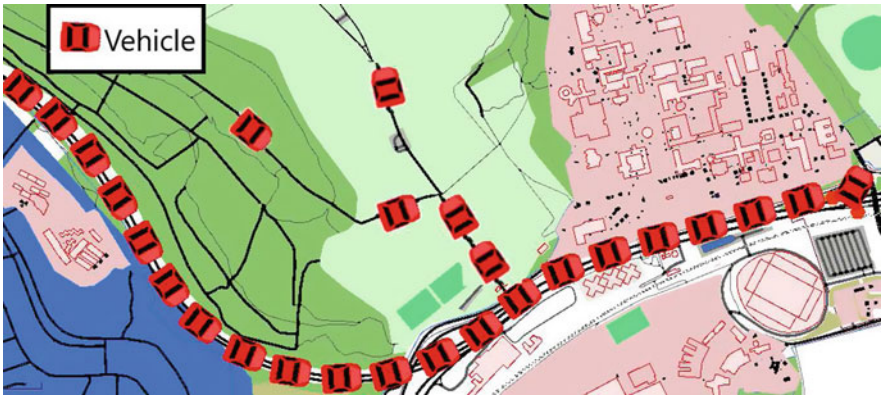


Fig. 6 Simulation map of University of Sussex campus

Table 4 Simulation parameters

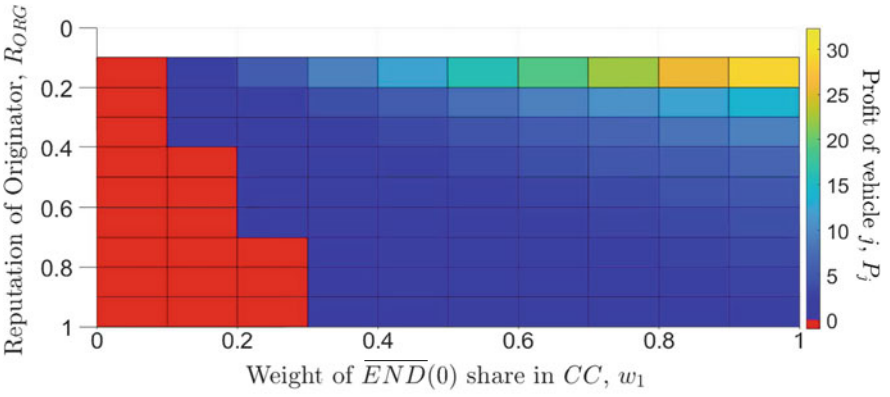
Parameter	Value	Parameter	Value
Run time	1000 s	Size of area	$12.5\times 12.5\,\text{km}^2$
No. of vehicles	[50, 200]	Cryptography	SHA-256
Protocol	IEEE 802.11p	Average speed	40 km/h
Data rate	6 Mbps	Sensitivity	−89 dBm
t_{END}^{max}	600 ms	N_{END}^{min}	3
N_{HOP}^{max}	6	CC	$\frac{10}{R_{ORG}}$
w_1	0.35	w_2	0.65
TC	1	R_j	[0,1]
R_T	0.5	β	0.1
γ	0.2	α_1	[1, 10]
α_2	[1, 4]	d_{HOP}^{min}	100 m
t_W	10 s	t_{max}	4 s

5.1 Simulation Setup

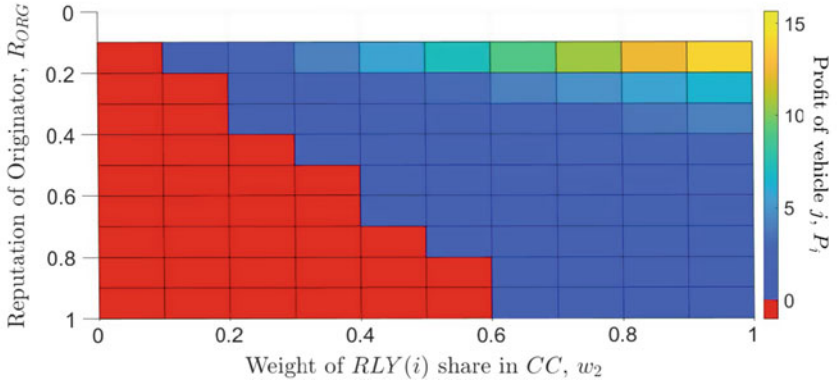
The simulation parameters in Table 4 are set so that Proposition 1 holds true regardless of the value of CC which is inversely proportional to R_{ORG}. In our simulations, we have arbitrarily set $CC = 10/R_{ORG}$. Higher R_{ORG} leads to lower amount of CC, thereby resulting in less profit for $\overline{END}(0)$ and $RLY(i)$, $RLY(i+1)$,...,$RLY(N_{HOP}^{max})$. However, it must be ensured that the message dissemination solution results in profit gain in credit wallets of all, despite of deduction of TC. As shown in Fig. 7, $w_1 > 0.3$ and $w_2 > 0.6$ would always result in positive profit, P_j, irrespective of the value R_{ORG}. Therefore, in order to ensure profit gain, we have set $w_1 = 0.35$ and $w_2 = 0.65$ in simulation. For efficient $RLY(i)$ selection, α_1 and α_2 have to be optimised. Figure 8 shows the percentage of vehicles which received the message within a specified period of time, t_{max}, with respect to α_1 and α_2 under different traffic densities. It shows that the selection of α_1 and α_2 depends upon the number of vehicles and affects $RLY(i)$ selection defined in (2). Thus in our simulation, we choose α_1 and α_2 such that they achieve the maximum reception rate.

5.2 Latency

Figure 9 shows average time consumption per hop over 100 simulation runs. As a comparison, reputation based blockchain [37, 41], only allowed vehicles with reputation above a certain threshold to disseminate messages. CreditCoin was witnesses based blockchain, in which ORG required a threshold number of witnesses to vote for authentication of a transaction proposal [34] and then allowed only authentic transaction proposals to be forwarded as messages. The latency was increased in



(a)



(b)

Fig. 7 P_j with respect to R_{ORG}, w_1 and w_2. (**a**) P_j for $j \epsilon \overline{END}(i)$. (**b**) P_j for $j = RLY(i)$

this approach because it relied on ORG to wait for the witnesses before generating the actual announcement packet. On the contrary, in our approach, the integrated authentication and relaying is implemented in a distributed manner and therefore, waiting time of ORG to rebroadcast after authentication is eliminated, which saves an average of 56 ms (or 11%) of time consumed in each consensus. Moreover, in CreditCoin, transactions in blockchain were processed by RSU, whereas in our solution, this task is performed by $RLY(i)$. Figure 9 also shows that reputation based method takes the least time to complete one hop as it does not involve waiting time for endorsements. The only time it consumes is to access blockchain to find reputation of ORG. However, average time increases with raising number of vehicles. This is because when there is a large number of vehicles registered in a blockchain network, it takes more time to access and find reputation of a vehicle. In proposed approach and CreditCoin, average time decreases with raising number of vehicles. This is because N_{END}^{min} endorsements are gathered in less time in heavy

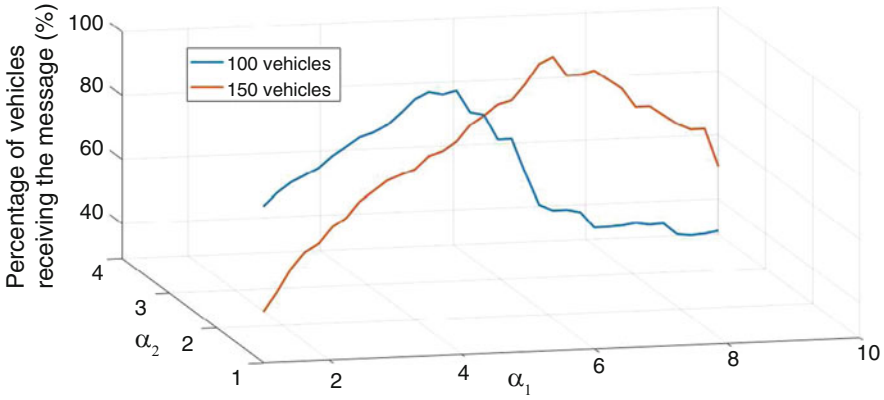


Fig. 8 Percentage of vehicles which received message with respect to α_1 and α_2

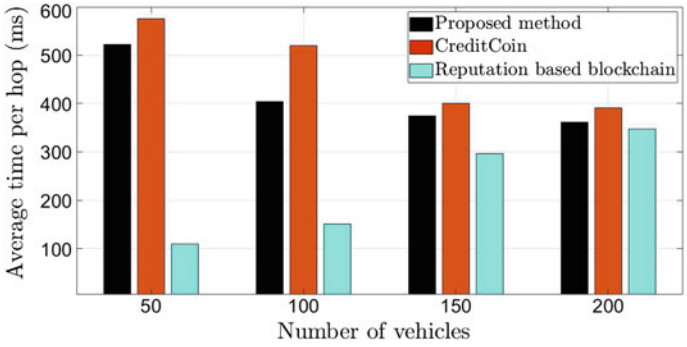


Fig. 9 Average time consumption per hop

traffic conditions. Therefore, time difference between reputation and voting based approaches becomes negligible with large number of vehicles in a network. With 50 vehicles, our solution consumes 522 ms for completing one consensus process. Given the average speed of vehicle is 40 km/h, it only incurs a moving distance of approximately 5 m, which can be easily mitigated within 300 m coverage of typical IEEE 802.11p radio [54]. Therefore, the proposed solution can be practically applied and vehicles are not likely to lose connectivity during a consensus process. The worst case scenario is presented in Fig. 10, where low density of vehicles, i.e. 50 and 100, at speeds beyond 100 and 110 km/h, respectively, cannot successfully complete a consensus algorithm within the time limit of 600 ms, which is practically suitable for threshold based authentication methods in VANETs [55]. However, such high speeds are not likely to be attained in an area affected by an incident or traffic jam. Overall, it shows that the proposed approach is suitable for vehicular networks, particularly for high density traffic with lower speed.

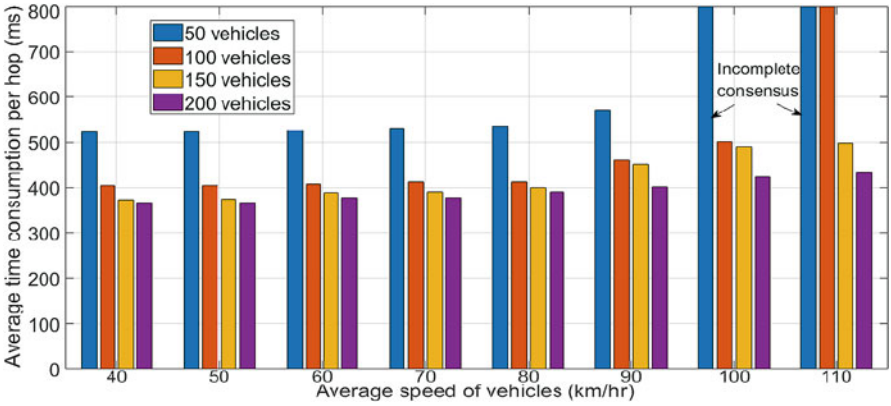


Fig. 10 Average time consumption per hop with respect to speed and number of vehicles

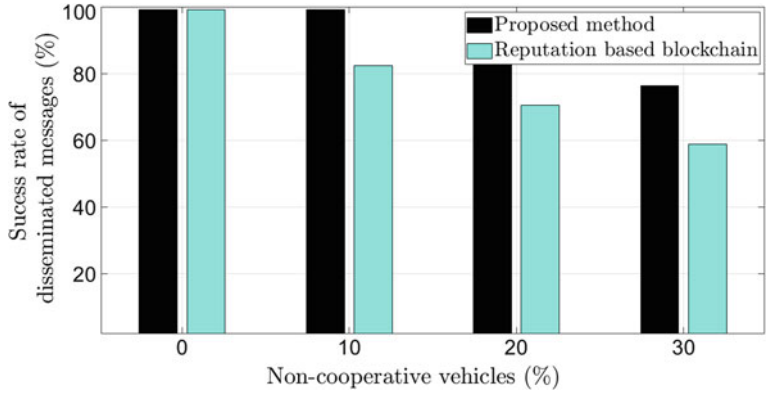


Fig. 11 Success rate of message dissemination in presence of low-reputed vehicles

5.3 Success Rate

Figure 11 shows number of messages disseminated successfully in presence of low-reputed vehicles. In our simulation, we have considered low-reputed vehicles as those vehicles whose reputation fall below R_T due to their malicious behaviour. The reputation based blockchain approaches [37, 41] authenticated a message on the basis of reputation of ORG. They did not allow a low-reputed vehicle to originate a transaction proposal in order to prevent dissemination of potentially false messages. This is how they discouraged vehicles with low reputation to contribute actively in blockchain extension and ultimately preventing some valid transaction proposals to be disseminated. Our approach authenticates transaction proposals through voting based consensus algorithm. Therefore, a low-reputed vehicle can also originate a transaction proposal. The trust among vehicles is

still maintained because a message cannot be further disseminated without getting N_{END}^{min} endorsements for a transaction proposal. The proposed consensus algorithm results in dissemination of greater number of messages despite the presence of higher percentage of low-reputed vehicles in a network, by equally promoting all vehicles to contribute in blockchain extension even if they have low reputation values. Our proposed approach disseminates on an average 17% more authenticated messages as compared to reputation based blockchain approach in presence of low-reputed vehicles.

5.4 Complexity

To support a completely decentralised message dissemination solution, each vehicle in the reputation based blockchain has the whole copy of blockchain in order to find reputation of any vehicle whenever needed. Therefore, the storage complexity of reputation based blockchain is $O(B)$, where B is the total number of blocks in a blockchain [56]. On the other hand, our proposed solution does not require each vehicle to store the whole copy of blockchain for $RLY(i)$ selection and message dissemination. To add a block in blockchain, the vehicle needs only the address of previous block and therefore its storage complexity is $O(1)$. However, all vehicles are required to update and synchronise their last block responsibly in order to avoid forks and discrepancies.

In terms of communication, the conventional PBFT requires at least N_{END}^{min} signatures both during endorsement and committing a block, as shown in Fig. 12a. Therefore, PBFT results in an overall communication complexity of $O((N_{END}^{min})^2)$ [57], whereas our proposed solution, shown in Fig. 12b, requires N_{END}^{min} signatures only during endorsement and hence results in communication complexity of $O(N_{END}^{min})$.

6 Conclusion

This chapter presents the concept of implementing blockchain technology for secure and private communications in IoV. Various blockchain types and their consensus algorithms are compared on the basis of their suitability in vehicular applications. The advantages of using blockchain for enhancing security and privacy of IoT and IoV are also discussed.

This chapter further proposes a voting based consensus algorithm incentivising vehicles through credit and reputation rewards for message dissemination in emergency situations. For efficient message dissemination, relay selection is made a part of consensus. The proposed solution is analysed by game theory and is proved to be secure against collusion of relay nodes. Further evaluation is conducted through simulations and results show that it saves on an average of 11% time consumption

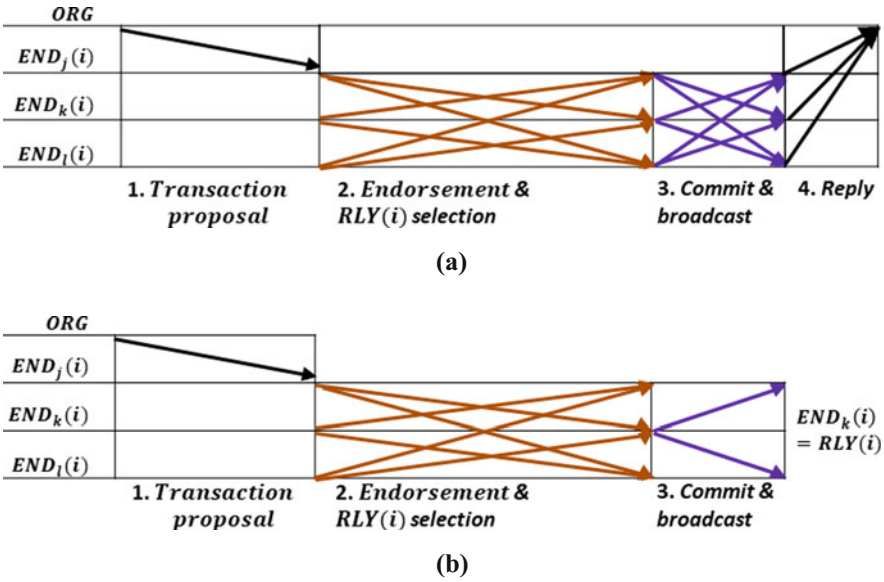


Fig. 12 Flow of voting based consensus algorithms. (**a**) Conventional PBFT. (**b**) Proposed

in authenticating and disseminating message as compared to another voting based validation method. Moreover, it improves successful dissemination of authenticated messages by 17% as compared to reputation based blockchain. As a trade-off, it requires more time to generate block. However, the latency difference is negligible with increasing number of vehicles. The complexity of proposed solution is also less than reputation based consensus and conventional PBFT based consensus algorithm in terms of storage and communication respectively. However, PBFT is less secure as compared to PoW. The design of future blockchain models for IoV should include improved security, reduced latency and complete independence from central authorities.

References

1. Aldegheishem, A., Yasmeen, H., Maryam, H., Shah, M. A., Mehmood, A., Alrajeh, N., et al. (2018). Smart road traffic accidents reduction strategy based on intelligent transportation systems (TARS). *Sensors, 18*(7), 1983–2006.
2. Chen, R., Jin, W. L., & Regan, A. (2010). Broadcasting safety information in vehicular networks: Issues and approaches. *IEEE Network, 24*(1), 20–25.
3. Yáñez, A., Céspedes, S., & Rubio-Loyola, J. (2018). CaSSaM: Context-aware system for safety messages dissemination in VANETs. In *Abstracts of the IEEE Colombian Conference on Communications and Computing, Medellin, Colombia, 16–18 May 2018*.

4. Martuscelli, G., Boukerche, A., Foschini, L., & Bellavista, P. (2016). V2V protocols for traffic congestion discovery along routes of interest in VANETs: A quantitative study. *Wireless Communications and Mobile Computing, 16*(17), 2907–2923.
5. Cataldi, P., & Harri, J. (2011). User/operator utility-based infrastructure deployment strategies for vehicular networks. In *Abstracts of the IEEE Vehicular Technology Conference, San Francisco, CA, USA, 5–8 September 2011*.
6. Yasser, A., Elzorkany, M., & Kader, N. A. (2017). Vehicle to vehicle implementation in developing countries. In A. Hassanien, K. Shaalan, T. Gaber, & M. Tolba (Eds.), *Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2017. AISI 2017. Advances in Intelligent Systems and Computing* (Vol. 639, pp. 809–819). Cham: Springer.
7. Kazmi, A., Khan, M. A., & Akram, M. U. (2016). DeVANET: Decentralized software-defined VANET architecture. In *Abstracts of the IEEE International Conference on Cloud Engineering Workshop, Berlin, Germany, 4–8 April 2016*.
8. Gazdar, T., Belghith, A., & Abutair, H. (2017). An enhanced distributed trust computing protocol for VANETs. *IEEE Access, 6*, 380–392.
9. Zhang, L., Wu, Q., Domingo-Ferrer, J., Qin, B., & Hu, C. (2016). Distributed aggregate privacy-preserving authentication in VANETs. *IEEE Transactions on Intelligent Transportation Systems, 18*(3), 516–525.
10. Manvi, S. S., & Tangade, S. (2017). A survey on authentication schemes in VANETs for secured communication. *Vehicular Communications, 9*, 19–30.
11. Rehman, O., & Ould-Khaoua, M. (2019). A hybrid relay node selection scheme for message dissemination in VANETs. *Future Generation Computer Systems, 93*, 1–17.
12. He, Y., Yu, F. R., Wei, Z., & Leung, V. (2019). Trust management for secure cognitive radio vehicular ad hoc networks. *Ad-hoc Networks, 86*, 154–165.
13. Hasrouny, H., Samhat, A. E., Bassil, C., & Laouiti, A. (2019). Misbehavior detection and efficient revocation within VANET. *Journal of Information Security and Applications, 46*, 193–209.
14. Janzadeh, H., Fayazbakhsh, K., & Dehghan, M. (2008). A secure credit-based cooperation stimulating mechanism for MANETs using hash chains. *Future Generation Computer Systems, 25*(8), 926–934.
15. Crowcroft, J., Gibbens, R., Kelly, F., & Östring, S. (2004). Modelling incentives for collaboration in mobile ad hoc networks. *Performance Evaluation, 57*(4), 427–439.
16. Refaei, M. T., DaSilva, L. A., Eltoweissy, M., & Nadeem, T. (2010) Adaptation of reputation management systems to dynamic network conditions in ad hoc networks. *IEEE Transactions on Computers, 59*(5), 707–719.
17. Dewan, P., Dasgupta, P., & Bhattacharya, A. (2004). On using reputations in ad hoc networks to counter malicious nodes. In *Abstracts of the IEEE 10th International Conference on Parallel and Distributed Systems, Newport Beach, CA, USA, 9 July 2004*.
18. Srivastava, V., Neel, J., MacKenzie, A. B., Menon, R., DaSilva, L. A., Hicks, J. E., et al. (2005). Using game theory to analyze wireless ad hoc networks. *IEEE Communications Surveys and Tutorials, 7*(4), 46–56.
19. Li, Z., & Shen, H. (2011). Game-theoretic analysis of cooperation incentive strategies in mobile ad hoc networks. *IEEE Transactions on Mobile Computing, 11*(8), 1287–1303.
20. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved February 09, 2020, from https://bitcoin.org/bitcoin.pdf
21. Jindal, A., Aujla, G. S., & Kumar, N. (2019). SURVIVOR: A blockchain based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment. *Computer Networks, 153*, 36–48.
22. Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., et al. (2019). Survey on blockchain for Internet of Things. *Computer Communications, 136*, 10–29.
23. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *Abstracts of the IEEE International Congress on Big Data, Honolulu, HI, USA, 25–30 June 2017*.

24. Gao, W., Hatcher, W. G., & Yu, W. (2018). A survey of blockchain: Techniques, applications, and challenges. In *Abstracts of the IEEE International Conference on Computer Communication and Networks, Hangzhou, China, 30 July–2 August 2018*.
25. Decker, C., & Wattenhofer, R. (2013). Information propagation in the bitcoin network. In *Abstracts of the IEEE International Conference on Peer-to-Peer Computing, Trento, Italy, 9–11 September 2013*.
26. Ortega, V., Bouchmal, F., & Monserrat, J. F. (2018). Trusted 5G vehicular networks: Blockchains and content-centric networking. *IEEE Vehicular Technology Magazine, 13*(12), 121–127.
27. Sankar, L. S., Sindhu, M., & Sethumadhavan, M. (2017). Survey of consensus protocols on blockchain applications. In *Abstracts of the IEEE 4th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 6–7 January 2017*.
28. Fairley, P. (2018). Ethereum will cut back its absurd energy use. *IEEE Spectrum, 56*(1), 29–32.
29. Baliga, A. (2017). Understanding blockchain consensus models. *Persistent, 4*, 1.
30. Wang, W., Hoang, D. T., & Hu, P. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access, 7*, 22328–22370.
31. Muratov, F., Lebedev, A., Iushkevich, N., Nasrulin, B., & Takemiya, M. (2018). YAC: BFT consensus algorithm for blockchain. Preprint. arXiv:1809.00554.
32. Dagher, G. G., Mohler, J., Milojkovic, M. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society, 39*, 283–297.
33. Samuel, O., Javaid, N., Shehzad, F., Iftikhar, M. S., Iftikhar, M. Z., Farooq, H., et al. (2020). Electric vehicles privacy preserving using blockchain in smart community. In L. Barolli, P. Hellinckx, & T. Enokido (Eds.), *Advances on Broad-band Wireless Computing, Communication and Applications. BWCCA 2019. Lecture Notes in Networks and Systems* (Vol. 97). Cham: Springer.
34. Li, L., Liu, J., Cheng, L., Qiu, S., Wang, W., Zhang, X., et al. (2018). Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. *IEEE Transactions on Intelligent Transportation Systems, 19*(7), 2204–220.
35. Lu, Z., Wang, Q., Qu, G., et al. (2018). Bars: a blockchain-based anonymous reputation system for trust management in VANETs. In *Abstracts of the IEEE 17th International Conference on Trust, Security and Privacy in Computing and Communications/12th International Conference on Big Data Science and Engineering, New York, NY, USA, 1–3 August 2018*.
36. Liu, L., & Loper, M. (2018). Trust as a service: building and managing trust in the internet of things. In *Abstracts of the IEEE International Symposium on Technologies for Homeland Security (HST), Woburn, MA, USA, 23–24 October 2018*.
37. Kang, J., Xiong, Z., Niyato, D., Ye, D., Kim, D. I., & Zhao, J. (2018). Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory. *IEEE Transactions on Vehicular Technology, 68*(3), 2906–2920.
38. Yang, Z., Yang, K., Lei, L., Zheng, K., & Leung, V. C. (2018). Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet of Things Journal, 6*(2), 1495–1505.
39. Khan, A. S., Balan, K., Javed, Y., Tarmizi, S., & Abdullah, J. (2019) Secure trust-based blockchain architecture to prevent attacks in VANET. *Sensors, 19*(22), 4954.
40. Ali, N. A., Taha, A. E. M., & Barka, E. (2020). Integrating blockchain and IoT/ITS for safer roads. *IEEE Network, 34*(1), 32–37.
41. Yang, Z., Zheng, K., Yang, K., & Leung, V. C. (2017). A blockchain-based reputation system for data credibility assessment in vehicular networks. In *Abstracts of the IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications, Montreal, QC, Canada, 8–13 October 2017*.
42. Tian, F. (2017). A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things. In *Abstracts of the International Conference on Service Systems and Service Management, Dalian, China, 16–18 June 2017*.
43. Sharma, P. K., Moon, Y. S., & Park, H. J. (2017). Block-VN: A distributed blockchain based vehicular network architecture in smart city. *Journal of Information Processing Systems, 13*(1), 184–195.

44. Dao, T. C., Nguyen, B. M., & Do, B. L. (2019). Challenges and strategies for developing decentralized applications based on blockchain technology. In L. Barolli, M. Takizawa, F. Xhafa, & T. Enokido (Eds.), *Advanced Information Networking and Applications. AINA 2019. Advances in Intelligent Systems and Computing* (Vol. 926). Cham: Springer.
45. Leiding, B., Memarmoshrefi, P., & Hogrefe, D. (2016). Self-managed and blockchain-based vehicular ad-hoc networks. In *Abstracts of the ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct, Heidelberg, Germany, 12–16 September 2016*.
46. Alouache, L., Nguyen, N., Aliouat, M., & Chelouah, R. (2018). Credit based incentive approach for V2V cooperation in vehicular cloud computing. In A. Skulimowski, Z. Sheng, S. Khemiri-Kallel, C. Cérin, & C. H. Hsu (Eds.), *Internet of Vehicles, Technologies and Services Towards Smart City. IOV 2018. Lecture Notes in Computer Science* (Vol. 11253, pp. 92–105). Cham: Springer.
47. Ayaz, F., Sheng, Z., Tian, D., Guan, YL., & Leung, V. (2020, accepted). A voting blockchain based message dissemination in vehicular ad-hoc networks (VANETs). In *IEEE International Conference on Communications, Virtual Conference, 7–11 June 2020*.
48. Pescaru, D. (2013). Urban traffic congestion prediction based on routes information. In *Abstracts of the IEEE 8th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, Romania, 23–25 May 2013*.
49. Abedi, O., Berangi, R., Azgomi, M. A. (2009). Improving route stability and overhead on AODV routing protocol and make it usable for VANET. In *Abstracts of the 29th International Conference on Distributed Computing Systems Workshops, Montreal, QC, Canada, 22–26 June 2009*.
50. Iza-Paredes, C., Mezher, A. M., Aguilar Igartua, M., & Forné, J. (2018). Game-theoretical design of an adaptive distributed dissemination protocol for VANETs. *Sensors, 18*(1), 294–325.
51. Fatemidokht, H., & Rafsanjani, M. K. (2018). F-Ant: An effective routing protocol for ant colony optimization based on fuzzy logic in vehicular ad hoc networks. *Neural Computing and Applications, 29*(11), 1127–1137.
52. Bettstetter, C., Hartenstein, H., & Pérez-Costa, X. (2004). Stochastic properties of the random waypoint mobility model. *Wireless Networks, 10*(5), 555–567.
53. Chatterjee, S., & Das, S. (2015). Ant colony optimization based enhanced dynamic source routing algorithm for mobile ad-hoc network. *Information Science, 295*, 67–90.
54. Boban, M., & d'Orey, P. M. (2016). Exploring the practical limits of cooperative awareness in vehicular communications. *IEEE Transactions on Vehicular Technology, 65*(6), 3904–3916.
55. Shao, J., Lin, X., Lu, R., & Zuo, C. (2015). A threshold anonymous authentication protocol for VANETs. *IEEE Transactions on Vehicular Technology, 65*(3), 1711–1720.
56. Ahmad, A., Saad, M., Njilla, L., Kamhoua, C., Bassiouni, M., & Mohaisen, A. (2018). Blocktrail: A scalable multichain solution for blockchain-based audit trails. In *Abstracts of the IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019*.
57. Choi, B., Sohn, J. Y., Han, D. J., & Moon, J. (2019). Scalable network-coded PBFT consensus algorithm. In *Abstracts of the IEEE International Symposium on Information Theory (ISIT), Paris, France, 7–12 July 2019*.