SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

July 2023, Vol. 66 172301:1–172301:13
https://doi.org/10.1007/s11432-022-3658-7

Blockchain-based vehicular edge computing networks: the communication perspective

Lin HE[1], Fuchang LI[1], Haikun XU[2], Wenbo XIA[2], Xuefei ZHANG[2*] & Xiaofeng TAO[2]

[1]*Research Institute, China United Network Communications Corporation Limited, Beijing* 100048*, China;*
[2]*National Engineering Research Center of Mobile Network Technologies, Beijing University of Posts and Telecommunications, Beijing* 100876*, China*

Received 19 June 2022/Revised 7 October 2022/Accepted 19 December 2022/Published online 12 June 2023

Abstract Vehicular edge computing (VEC) networks can satisfy the increasing demands of data processing by offloading the computation tasks to multiple distributed edge computing nodes assisted by servers. These edge servers generally combine with roadside units (RSUs). However, RSUs with edge servers cannot be fully trusted, possibly leading to serious security and privacy problems. Combining blockchain with VEC networks may establish a trusted and decentralized vehicular environment, but the coexistence of multiple communication modes comprising vehicle-to-vehicle (V2V), vehicle-to-RSU (V2R), and RSU-to-RSU (R2R) makes the block propagation patterns have different effects on the block consensus process. In this paper, we study the block propagation patterns between vehicles and RSUs with edge servers under three communication modes. We first give the closed-form expressions for the single-block and multiblock propagation times in two specific conditions to explore how the priority of a block generated from a specific node affects the block propagation process, in which multiblock propagation embodies competitive propagation due to blockchain forking. Then, an innovative consensus mechanism that fully invokes the communication capability of the nodes is proposed, and the block propagation time and frequency can be substantially reduced under this mechanism. In addition, an important finding is that under the conventional and proposed consensus mechanisms, an RSU or a vehicle that creates a new block plays a decisive role in the block propagation pattern.

Keywords block propagation, blockchain, consensus, VEC network

Citation He L, Li F C, Xu H K, et al. Blockchain-based vehicular edge computing networks: the communication perspective. Sci China Inf Sci, 2023, 66(7): 172301, https://doi.org/10.1007/s11432-022-3658-7

1 Introduction

Intelligent transportation systems supported by vehicular networks provide several services, such as autonomous driving and safety warnings, through collaborative work and information exchange between vehicles. Conventionally, a centralized node is responsible for vehicle and roadside unit (RSU) management in intelligent transportation systems. Because the number of vehicles and RSUs is growing exponentially, the centralized node must obtain and process massive data related to road status (e.g., road condition monitoring, traffic flow, and traffic accident information) and vehicle status (e.g., vehicle position and velocity). Likewise, the many demands of analyzed data from the centralized node are inevitable. The diversity and quantity of such data increase the pressure of the centralized node [1]. To reduce the stress of the centralized node while maintaining the characteristics of the Internet of Vehicles, vehicular edge computing (VEC) has shown immense potential. VEC permits computation task offloading to multiple distributed edge computing nodes associated with RSUs. However, ensuring information credibility is a challenge because RSUs, usually distributed along a road without strong security protection, are vulnerable to centralized attack and can incur severe information leakage [2].

VEC networks process and store information in a distributed way over the trustless vehicle environment, and network security and credibility cannot be guaranteed [3]. In contrast, blockchain, a promising and revolutionary distributed ledger technology that supports trusted and distributed communication, is a

* Corresponding author (email: zhangxuefei@bupt.edu.cn)

feasible solution. It allows a group of separated nodes, particularly nodes that do not trust each other, to credibly share data [4]. Networks with a distributed nature and high demands for information credibility, such as VEC networks, are potential scenarios for deploying blockchain. Most existing blockchain-based VEC networks [5] only employ blockchain in RSUs or edge servers, where vehicles can participate in the information exchange process but not in the consensus process. However, when RSUs are invalidated, the consensus process of the blockchain will be affected, even leading to a failure of the entire process. With the rapid development of vehicle intelligence [6], vehicles can be equipped with the capabilities for generating, forwarding, and verifying blocks to support blockchain protocols. In this way, vehicles can join the current consensus process to improve the robustness of the blockchain system in VEC networks.

In our previous work [7], we evaluated the impact of mobility on block propagation under vehicle-to-vehicle (V2V) communications in a wireless and dynamic network. The highly dynamic topologies and the limited communication range are proven inducements to longer consensus time. On this basis, we intend to implement blockchain in moving vehicles and RSUs with edge servers. Block propagation under V2V and vehicle-to-RSU (V2R) communications over wireless links and RSU-to-RSU (R2R) communications over wired links will then be evaluated. Particularly, wired communications between RSUs with edge servers provide high-speed and high-reliability information exchanges, while wireless communication between moving vehicles or moving vehicles and RSUs with edge servers provides opportunistic information exchanges due to the highly dynamic topologies caused by vehicle mobility.

Compared with our previous work, where blocks are only propagated between vehicles, the participation of RSUs with larger propagation capability can accelerate the block consensus process because an RSU can not only establish stable connections with all other RSUs in a negligible time but also communicate with more vehicles because of its broader wireless communication coverage compared to a vehicle. Thus, this paper focuses on the vehicular blockchain consensus between moving vehicles and RSUs with edge servers from the communication perspective. In particular, the main contributions of this paper are as follows.

• We analyze the dynamic process of block propagation between moving vehicles and RSUs. To explore the impact of the propagation capability of the nodes that create the new block on block propagation, we present and further discuss the dynamic equations of single-block propagation for two specific conditions. Then, we illustrate the dynamic state transitions of vehicles in multiblock propagation.

• Considering that an RSU is vulnerable to attacks and the dynamic nature of the scenario, we design a reputation-based consensus mechanism, which separates the consensus process between RSUs and vehicles and requires all nodes to participate in the forwarding process of the new block. This approach is advantageous because it shortens the block propagation time and reduces the verification overhead.

• By comparing the numerical and simulation results, the validity of our theoretical analysis and the feasibility of the proposed consensus mechanism are proved. The results show that the range of communication, the velocity of vehicles, the number of functioning RSUs, and the priority of block generation affect the block propagation time, and the proposed consensus mechanism can reduce the block propagation time and frequency.

The remainder of this paper is organized as follows. Related work regarding vehicular blockchain and the blockchain consensus process in a vehicular network is reviewed in Section 2, and the basic model of our study is given in Section 3. Then, in Section 4, after the block propagation between moving vehicles and RSUs with edge servers in vehicular blockchain consensus is analyzed, the dynamic equations for block propagation in different conditions and a reputation-based consensus mechanism are presented. Next, we simulate and validate our theoretical analysis, and the relative findings in our simulation are discussed in detail in Section 5. Finally, we conclude the paper in Section 6.

2 Related work

Several aspects of blockchain-based VEC networks have already been explored in the literature. For blockchain consensus protocols, Nakamoto [8] suggested using proof-of-work (PoW) to ensure security and decentralization in a public blockchain. To tackle the high-energy consumption problem caused by PoW consensus, similar proof-based algorithms are proposed as alternatives, such as proof-of-stake [9], proof-of-elapsed-time[1)], and proof-of-activity [10]. In addition, when a certain amount of trust is established between nodes, the specific blockchain systems applied to these scenarios are the permissioned

1) Sawtooth Documentation. https://goo.gl/izmMYn/.

blockchains, and lighter voting-based consensus protocols with reduced computational power demand can thus be adopted in these systems, such as Raft consensus [11] and practical Byzantine fault tolerance consensus [12].

Blockchain technology with tamper resistance and a distributed nature is potentially suitable for vehicular networks to reduce security risks in trustless vehicular environments and eliminate reliance on a centralized authoritative third party. Islam et al. [13] proposed a blockchain-based decentralized architecture to enhance transparency in intelligent VEC resource management and leverage edge consumers, such as vehicles, with a computation verification option. An SDN-enabled 5G-VANET model and the scheduling procedures of the blockchain-based framework are illustrated in [14]. However, in many existing studies where blockchain and vehicular networks are combined, most of the research is based on a similar assumption that the communications between the participants are always ideal. In realistic scenes, particularly where the relative position of participants changes dynamically, communication between them will inevitably be affected by delay, fading, interference, and other factors. Information exchanges between participants are essential for the blockchain consensus. Studies have analyzed the consensus process concerning the impact of communication in wireless and dynamic blockchain networks. Zhang et al. [15] found that frequent information exchanges between nodes during the consensus process affect the transaction throughput, consensus time, security, and scalability. Moreover, the vulnerable wireless links in a blockchain system also result in a lower blockchain transaction transmission success rate and transaction throughput [16]. Particularly, the impact of imperfect information exchanges on block propagation time during the consensus process will be larger if participants are moving [7]. Notably, research that systematically analyzes the block propagation between RSUs and moving vehicles with the coexistence of V2V, V2R, and R2R communication modes in dynamic and wireless networks is scarce and needed.

3 System model

As Figure 1 shows, we consider a vehicular blockchain system under the single-chain structure, which mainly includes multiple RSUs with edge servers and moving vehicles. Each blockchain-enabled vehicle is equipped with relative devices for generating, forwarding, verifying, or storing each specific block. Each blockchain-enabled RSU processes the computation tasks with the assistance of a connected server, and the RSU itself is mainly responsible for communicating with vehicles. Vehicles and server-assisted RSUs can compete for the priority to create the upcoming new block. The required capabilities of vehicles and RSUs in the system are listed as follows.

• Vehicles. The communications between any two vehicles or between vehicles and RSUs adopt IEEE 802.11p or the DSRC protocol [17]. We assume that the moving pattern of a vehicle follows a random direction mobility model, and the information transmission time between two vehicles is ignorable compared to their convergence time [18,19].

• RSUs. The communications between any two RSUs adopt a wired connection channel. In this condition, the information transmission time between two RSUs is negligible.

An RSU does not need to forward the same block repeatedly to other RSUs because of the stable communication topology among them. In contrast, vehicles or RSUs are encouraged to forward the block repeatedly to vehicles within their communication coverage to compensate for the unstable communication caused by vehicle mobility. We assume that the consensus is far faster in wired communication networks than in wireless communication networks of the same scale, so the final phase of the vehicular blockchain consensus between moving vehicles and server-assisted RSUs generally occurs in the wireless transmission environment. A new block is added to the vehicular blockchain once the number of vehicles that receive and verify the block reaches a threshold βN_{v}, where β is in the range of $(0, 1)$, and N_{v} is the number of vehicles in the system.

4 Analysis of block propagation between moving vehicles and server-assisted RSUs in a vehicular blockchain consensus

In this section, by using the relevant theories of the dynamic equation of information propagation, the closed-form expressions of the single-block and multiblock propagation times in two specific cases are derived exhaustively. Specifically, for multiblock propagation, we consider it to embody competitive

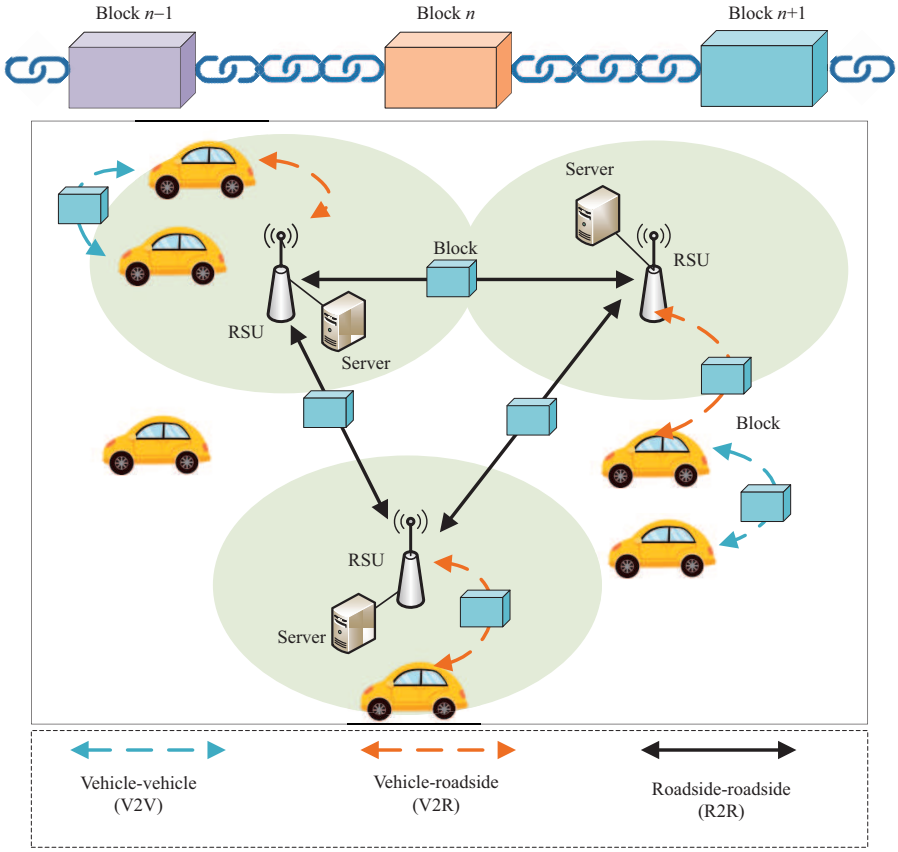

Figure 1 Vehicular blockchain consensus between moving vehicles and server-assisted RSUs.

propagation due to blockchain forking. Finally, we propose an innovative consensus mechanism that can fully invoke the communication capabilities and thus reduce the block propagation time and frequency.

4.1 Analysis of the block propagation time during the vehicular consensus

4.1.1 *Contact rate between any two participating nodes*

We assume that the occurrences of the contacts between any two participating nodes follow the Poisson distribution with contact rate λ [20]. For example, when the moving pattern of vehicles follows a random direction mobility model, the contact rate $\lambda_{\rm vv}$ between any two vehicles is given by

$$\lambda_{\rm vv} \approx \frac{2r_{\rm v}E[V^*]}{L^2}, \tag{1}$$

where $r_{\rm v}$ is the radius of the communication coverage of a vehicle, commonly $r_{\rm v} \ll L$. L is the side length of the square area that a vehicular blockchain is deployed. $E[V^*]$ is the average relative velocity between vehicles, derived in detail in [7].

In particular, when one participating node is stationary but another node moves at a velocity following the uniform distribution in $[V_{\min}, V_{\max}]$, the average relative velocity $E[V^*]$ between the stationary node (i.e., the RSU) and the moving node (i.e., the vehicle) is $(V_{\min} + V_{\max})/2$. Thus, the contact rate $\lambda_{\rm vR}$ between a vehicle and an RSU is given by

$$\lambda_{\rm vR} \approx \frac{V_{\min} + V_{\max}}{L^2} r_{\rm R}, \tag{2}$$

where $r_{\rm R}$ is the radius of the communication coverage of the RSU.

If $N_{\rm v}$ vehicles and $N_{\rm R}$ RSUs are in the vehicular blockchain system, then a specific vehicle contacts $\lambda_{\rm vv}(N_{\rm v} - 1)$ other vehicles per unit time, where ($N_{\rm v} - 1$ means excluding the specific vehicle itself); a vehicle contacts $\lambda_{\rm vR}N_{\rm R}$ RSUs per unit time; an RSU contacts $\lambda_{\rm vR}N_{\rm v}$ vehicles per unit time. The block propagation between moving vehicles and server-assisted RSUs in vehicular blockchain consensus is

considered the state transitions of participating nodes, and information propagation dynamic equations are used to formalize this situation. Network latency in a blockchain system easily accounts for the forking problem, which may worsen under the highly dynamic topology. In this condition, the blockchain forking problem during the consensus process is characterized as multiblock competitive propagation. For ease of explanation, we first describe the dynamic process of a single block being propagated in the vehicular blockchain system and then describe the dynamic process of multiple blocks simultaneously propagating in the system.

4.1.2 *Single-block propagation*

In the case of single-block propagation, all vehicles and RSUs propagate the same block (e.g., block a) in a vehicular blockchain system. With the propagation of block a, a vehicle is either in an informed state (I_{va}) or an uninformed state (U_{va}). The informed state represents that the vehicle has received and verified block a, and the uninformed state represents that the vehicle has not received block a. $I_{\mathrm{va}}(t)$ is the number of vehicles that have already received block a in time t, and $U_{\mathrm{va}}(t)$ is the number of vehicles that have not received block a in time t. Analogously, an RSU is either in an informed state (I_{Ra}) or an uninformed state (U_{Ra}). The definitions of $I_{\mathrm{Ra}}(t)$ and $U_{\mathrm{Ra}}(t)$ are similar to those of $I_{\mathrm{va}}(t)$ and $U_{\mathrm{va}}(t)$, respectively. Either a vehicle or an RSU might generate a new block. The impact of the priority of the generation of a new block on block propagation is discussed as follows.

Case 1. If an RSU creates a new block (e.g., block a) before a vehicle, it will forward the block to other RSUs over the wired communication in a negligible period. In this condition, all RSUs, denoted as N_{R}, receive block a. After verifying block a, all RSUs repeatedly forward the block to any vehicle within their communication coverage. If a vehicle receives block a, it will further forward the block to its neighboring vehicles over wireless communication to accelerate the blockchain consensus process. In this way, block propagation includes the following two parts:

• Initial propagation. The propagation from RSUs to vehicles. This event occurs when the block has just been generated from an RSU, and none of the vehicles have received the block.

• Follow-up propagation. The propagation from RSUs to vehicles as well as from vehicles to vehicles. This event occurs when the block has been generated for a certain period, and at least one of the vehicles has received the block.

First, we derive the time t_1 for the first vehicle to receive block a from nearby RSUs:

$$t_1 = \frac{\ln \frac{N_{\mathrm{v}}}{N_{\mathrm{v}}-1}}{\lambda_{\mathrm{vR}} N_{\mathrm{R}}}. \tag{3}$$

As discussed above, t_1 can be used as the dividing line between the initial propagation phase and the follow-up propagation phase. When $t < t_1$, the block is only being propagated between RSUs and from RSUs to vehicles. Otherwise, in addition to the above two propagation patterns, the block will also be propagated between vehicles. Given the initial condition $I_{\mathrm{va}}(0) = 0$, we can derive the equation for $I_{\mathrm{va}}(t)$ as follows:

$$\begin{cases} I_{\mathrm{va}}(t) = N_{\mathrm{v}}(1 - \mathrm{e}^{-\lambda_{\mathrm{vR}} N_{\mathrm{R}} t}), \quad t \leqslant t_1, \\ I_{\mathrm{va}}(t) = \dfrac{N_{\mathrm{v}}(\lambda_{\mathrm{vv}} + N_{\mathrm{R}}\lambda_{\mathrm{vR}})\mathrm{e}^{(N_{\mathrm{R}}\lambda_{\mathrm{vR}} + N_{\mathrm{v}}\lambda_{\mathrm{vv}})(t-t_1)} - N_{\mathrm{R}}\lambda_{\mathrm{vR}}(N_{\mathrm{v}}-1)}{(\lambda_{\mathrm{vv}} + N_{\mathrm{R}}\lambda_{\mathrm{vR}})\mathrm{e}^{(N_{\mathrm{R}}\lambda_{\mathrm{vR}} + N_{\mathrm{v}}\lambda_{\mathrm{vv}})(t-t_1)} + \lambda_{\mathrm{vv}}(N_{\mathrm{v}}-1)}, \quad t > t_1 \ \&\ I_{\mathrm{va}}(t_1) = 1. \end{cases} \tag{4}$$

A detailed derivation of the equations in Case 1 can be found in Appendix A.

Case 2. If a vehicle creates a new block (e.g., block a) before an RSU, it will forward the block to neighboring RSUs and vehicles over wireless communication. Note that only one vehicle forwards block a to neighboring participating nodes, compared to N_{R} RSUs forwarding the block simultaneously in Case 1. If an RSU receives block a, it will forward the block to other RSUs over the wired communication in a negligible period. Then, all RSUs can participate in the block propagation from RSUs to vehicles. In this way, block propagation includes the following two parts.

• Initial propagation. The propagation from vehicles to vehicles as well as from vehicles to RSUs. This event occurs when the block has just been generated from a vehicle, and none of the RSUs have received the block.

• Follow-up propagation. The propagation from vehicles to vehicles as well as from RSUs to vehicles. This event occurs when the block has been generated for a certain period, and at least one of the RSUs has received the block.

Similarly, we derive the time t_2 for the first RSU to receive block a from nearby vehicles:

$$t_2 = \frac{\ln \frac{N_{\mathrm{v}}}{\frac{\lambda_{\mathrm{vR}}}{\lambda_{\mathrm{vv}}}\sqrt{\frac{N_{\mathrm{R}}-1}{N_{\mathrm{R}}}}}}{\lambda_{\mathrm{vv}} N_{\mathrm{v}}}. \tag{5}$$

t_2 can be used as the dividing line between the initial propagation phase and the follow-up propagation phase. When $t < t_2$, the block is only being propagated between vehicles and from vehicles to RSUs. Otherwise, in addition to the above two propagation patterns, the block will also be propagated between RSUs. Given the initial condition $I_{\mathrm{va}}(0) = 1$, we can derive the equation for $I_{\mathrm{va}}(t)$ as follows:

$$\begin{cases} I_{\mathrm{va}}(t) = \dfrac{N_{\mathrm{v}}}{1 + (N_{\mathrm{v}} - 1)\,\mathrm{e}^{-\lambda_{\mathrm{vv}} N_{\mathrm{v}} t}}, & t \leqslant t_2, \\ I_{\mathrm{va}}(t) = \dfrac{N_{\mathrm{v}}(I_{\mathrm{va}}(t_2)\lambda_{\mathrm{vv}} + N_{\mathrm{R}}\lambda_{\mathrm{vR}})\mathrm{e}^{(N_{\mathrm{R}}\lambda_{\mathrm{vR}} + N_{\mathrm{v}}\lambda_{\mathrm{vv}})(t-t_1)} - N_{\mathrm{R}}\lambda_{\mathrm{vR}}(N_{\mathrm{v}} - I_{\mathrm{va}}(t_2))}{(I_{\mathrm{va}}(t_2)\lambda_{\mathrm{vv}} + N_{\mathrm{R}}\lambda_{\mathrm{vR}})\mathrm{e}^{(N_{\mathrm{R}}\lambda_{\mathrm{vR}} + N_{\mathrm{v}}\lambda_{\mathrm{vv}})(t-t_1)} + \lambda_{\mathrm{vv}}(N_{\mathrm{v}} - I_{\mathrm{va}}(t_2))}, & t > t_2. \end{cases} \tag{6}$$

Here, $I_{\mathrm{va}}(t_2) = N_{\mathrm{v}}/[1 + (N_{\mathrm{v}} - 1)\,\mathrm{e}^{-\lambda_{\mathrm{vv}} N_{\mathrm{v}} t_2}]$.

A detailed derivation of the equations in Case 2 can be found in Appendix B.

4.1.3 *Multiblock propagation*

The generation, consensus, and confirmation of a new block commonly lasts a period, during which other blocks with the same height as the block undergoing the consensus and confirmation process may create/coexist in the blockchain system, which can be described as a blockchain forking problem. We characterize the blockchain forking problem as multiblock competitive propagation, i.e., a participating node with a collection of blocks that have not yet reached consensus probabilistically selecting a block among the collection and forwarding it to its neighboring nodes. Probabilistic forwarding is essentially a block competition to reduce forking.

Suppose that n blocks are competitively spreading over a vehicular blockchain system where $n > 1$. We take the two-block case (e.g., blocks a and b) as an example. For simplicity, we focus on the case where RSUs have received blocks a and b. A vehicle is in one of the four possible states, i.e., uninformed of blocks a and b (represented by $U_{\mathrm{a}}U_{\mathrm{b}}$), uninformed of block a but informed of block b (represented by $U_{\mathrm{a}}I_{\mathrm{b}}$), informed of block a but uninformed of block b (represented by $I_{\mathrm{a}}U_{\mathrm{b}}$), and informed of blocks a and b (represented by $I_{\mathrm{a}}I_{\mathrm{b}}$). A vehicle in state $U_{\mathrm{a}}U_{\mathrm{b}}$ transfers to state $I_{\mathrm{a}}U_{\mathrm{b}}$ or $U_{\mathrm{a}}I_{\mathrm{b}}$ once it contacts a vehicle or an RSU that forwards block a or b; a vehicle in state $I_{\mathrm{a}}U_{\mathrm{b}}$ or $U_{\mathrm{a}}I_{\mathrm{b}}$ transfers to state $I_{\mathrm{a}}I_{\mathrm{b}}$ once it contacts a vehicle or an RSU that forwards block b or a. The state transitions of vehicles are shown in Figure 2.

In contrast to other blockchain systems, vehicles and RSUs are encouraged to probabilistically select a block among all those that have not yet reached consensus and forward it to neighboring vehicles. This probabilistic forwarding uses the difference in block propagation capabilities to increase the propagation time gap between blocks and further reduce forking. Specifically, a vehicle or an RSU with blocks a and b forwards block a or b with the possibility of μ_{a} or $\mu_{\mathrm{b}} = 1 - \mu_{\mathrm{a}}$. In this way, the average number of vehicles in state $I_{\mathrm{a}}I_{\mathrm{b}}$ that forward block a or b in time t is $\mu_{\mathrm{a}} I_{\mathrm{a}}I_{\mathrm{b}}(t)$ or $(1 - \mu_{\mathrm{a}})I_{\mathrm{a}}I_{\mathrm{b}}(t)$. Meanwhile, the average number of RSUs that forward block a or b in time t is $\mu_{\mathrm{a}} N_{\mathrm{R}}$ or $(1 - \mu_{\mathrm{a}})N_{\mathrm{R}}$. Particularly, vehicles in state $I_{\mathrm{a}}U_{\mathrm{b}}$ or $U_{\mathrm{a}}I_{\mathrm{b}}$ forward block a or b in time t with the possibility of 1.

4.2 A block consensus mechanism to improve the use of node communication capacity

To reach a consensus for a newly generated block in our blockchain-based VEC network model, the consensus process of the new block demands the collaborative participation of the vehicle nodes and the RSU nodes. However, as discussed above, RSUs are apt to be attacked, resulting in the other nodes in the network having difficulty verifying the legitimacy of the new block through existing consensus mechanisms. Furthermore, in a practical application scenario, a certain number of vehicle nodes are bound to not approve the block generated by a specific RSU. In this way, on the basis of the existing consensus mechanism, these vehicle nodes will refuse to partake in the consensus process, including the forwarding and verification processes of the new block. Consequently, the communication capacities offered by these vehicle nodes will not be put into use, and the consensus process for the new block can

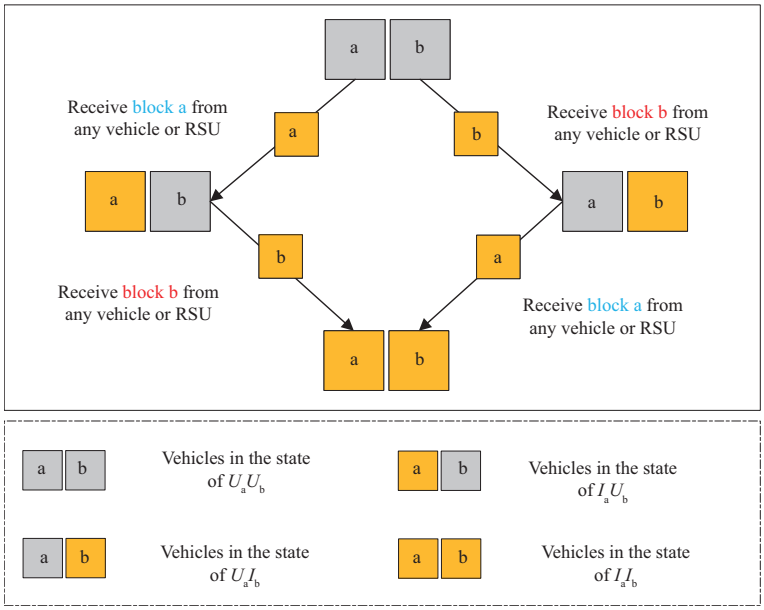

Figure 2 State transitions of vehicles in the case of two-block propagation.

only rely on those that do approve the block, increasing the time consumption of the block propagation and consensus.

To tackle these two problems, for the scenario where the new block is generated by an RSU, we further propose a reputation-based consensus mechanism, which has the major innovation of separating the forwarding and verification processes of the consensus, enabling any vehicle node to immediately forward the block to other nodes upon receiving without any modification. By adopting the proposed consensus mechanism, the communication capacity of each node can be fully invoked so that the time required for block propagation and consensus reaching can be shortened compared to the conventional mechanism. Specifically, we divide the consensus process into an RSU consensus phase and a vehicle consensus phase, and the results of these two progressive phases are treated as two indicators, which are "RSU valid" and "Vehicle valid", respectively. The specific process of the proposed consensus mechanism is shown in Figure 3.

4.2.1 *RSU consensus phase*

According to the related theories of reputation management in a VEC network, we set up a trust authority (TA), which is responsible for issuing the identity information and maintaining the specific reputation value of the network nodes. On the basis of the reputation value, the TA proactively selects an RSU for the generator of the new block, denoted as $\mathrm{RSU_{Ge}}$. Because the communication quality between RSUs is favorable, upon generating, the new block will be forwarded to any other RSUs by $\mathrm{RSU_{Ge}}$. We take a specific RSU, denoted as RSU_i, as an example. After receiving the new block, RSU_i verifies its validity; that is, the block number conforms to the current block height, the transactions in the block are legal and valid, the block generation time is valid. The results can be described as the following two cases.

Case 1. RSU_i approves the new block generated by $\mathrm{RSU_{Ge}}$. In this case, RSU_i generates approved information, denoted as $\mathrm{AP_{RSU_i}}$. The specific format is as follows:

$$\mathrm{AP_{RSU_i}} = [\mathrm{ID_{RSU_i}}||E_{\mathrm{SK_{RSU_i}}}(\mathrm{timestamp}||\mathrm{Block\_Hash}||\mathrm{Approve\_Message})]. \tag{7}$$

Among them, $\mathrm{SK_{RSU_i}}$ represents the private key of RSU_i. timestamp and Block_Hash ensure that $\mathrm{AP_{RSU_i}}$ is real-time and credible. Approve_Message is used to indicate that RSU_i approves the new block generated by $\mathrm{RSU_{Ge}}$. $\mathrm{AP_{RSU_i}}$ will be subsequently forwarded to any other RSU, except for $\mathrm{RSU_{Ge}}$. Simultaneously, on the basis of the verification result and the behavior of $\mathrm{RSU_{Ge}}$, RSU_i generates reputation reference information, denoted as $\mathrm{RR_{RSU_i}}$. The specific format is as follows:

$$\mathrm{RR_{RSU_i}} = [\mathrm{ID_{RSU_i}}||E_{\mathrm{PK_{RSU_i}}}(\mathrm{timestamp}||\mathrm{Block\_Hash}||\mathrm{Reputation\_Validation})]. \tag{8}$$

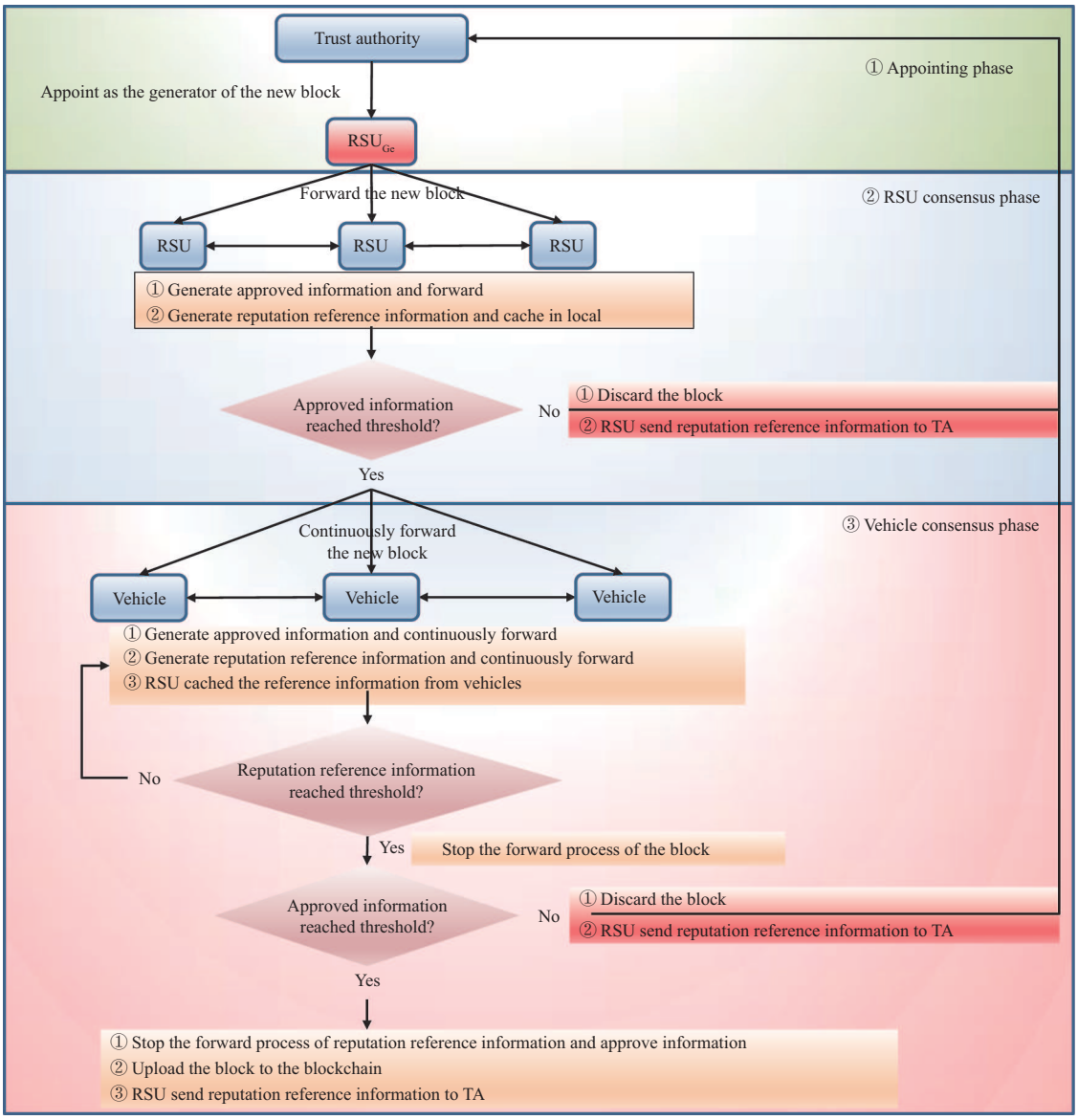

Figure 3 Specific process of the improved consensus mechanism.

Among them, $\mathrm{PK}_{\mathrm{RSU}_i}$ represents the public key of RSU_i. timestamp and Block_Hash ensure that $\mathrm{RR}_{\mathrm{RSU}_i}$ is real-time and credible. Reputation_Validation is used to indicate the reputation evaluation of $\mathrm{RSU}_{\mathrm{Ge}}$ by RSU_i. $\mathrm{RR}_{\mathrm{RSU}_i}$ will subsequently be cached in the local pool of RSU_i.

Case 2. RSU_i disapproves of the new block generated by $\mathrm{RSU}_{\mathrm{Ge}}$. In this case, RSU_i will not generate approved information, but the reputation reference information, denoted as $\mathrm{RR}_{\mathrm{RSU}_i}$, will still be generated and cached in the local pool of RSU_i. The specific format of the reputation reference information is similar to (8).

During the above steps, RSU_i monitors the approved information originating from other RSUs except for $\mathrm{RSU}_{\mathrm{Ge}}$, denoted as $\mathrm{AP}_{\mathrm{RSU}_j}$. In a preset interval, if the quantity of the approved information is greater than a preset threshold, the new block generated by $\mathrm{RSU}_{\mathrm{Ge}}$ will be considered "RSU Valid" by RSU_i. An "RSU Valid" block will be continuously forwarding to any vehicle nodes within the communication range of RSU_i until the termination condition for block forwarding is reached. Conversely, if the quantity of the approved information fails to reach the threshold in a given interval, the new block generated by $\mathrm{RSU}_{\mathrm{Ge}}$ will be considered "RSU Invalid" by RSU_i. An "RSU Invalid" block will be discarded by RSU_i, and the cached reputation reference information $\mathrm{RR}_{\mathrm{RSU}_i}$ will be sent to the TA progressively.

4.2.2 *Vehicle consensus phase*

The new block that has been considered "RSU Valid" will be continuously forwarded to any vehicle nodes within the communication range of RSU_i. Taking vehicle V_i as an example, once V_i receives a new block forwarded by an RSU, it will store the copy of the new block locally and then immediately forward the block to any other node, including RSU nodes and vehicle nodes, within its communication range without any modification to the block. This forwarding process will proceed until the termination condition for block forwarding is reached. At the same time, V_i verifies the validity of the new block received; that is, the block number conforms to the current block height, the transaction in the block is legal and valid, the block generation time is valid. The results can be described as the following two cases.

Case 1. V_i approves the new block generated by $\mathrm{RSU_{Ge}}$. In this case, V_i generates an approve information, denoted as AP_{V_i}. The specific format is as follows:

$$\mathrm{AP}_{V_i} = [\mathrm{ID}_{V_i} || E_{\mathrm{SK}_{V_i}}(\mathrm{timestamp}||\mathrm{Block\_Hash}||\mathrm{Approve\_Message})]. \tag{9}$$

Among them, SK_{V_i} represents the private key of V_i. timestamp and Block_Hash ensure that AP_{V_i} is real-time and credible. Approve_Message is used to indicate that V_i approves the new block generated by V_{Ge}. AP_{V_i} will subsequently be continuously forwarded to all other nodes within the communication range of V_i, including RSU nodes and vehicle nodes. Simultaneously, based on the verification result and the behavior of $\mathrm{RSU_{Ge}}$, V_i generates reputation reference information, denoted as RR_{V_i}. The specific format is as follows:

$$\mathrm{RR}_{V_i} = [\mathrm{ID}_{V_i} || E_{\mathrm{PK}_{V_i}}(\mathrm{timestamp}||\mathrm{Block\_Hash}||\mathrm{Reputation\_Validation})]. \tag{10}$$

Among them, PK_{V_i} represents the public key of V_i. timestamp and Block_Hash ensure that RR_{V_i} is real-time and credible. Reputation_Validation is used to indicate the reputation evaluation of $\mathrm{RSU_{Ge}}$ by V_i. RR_{V_i} will subsequently be continuously forwarded to all other nodes within the communication range of V_i, including RSU nodes and vehicle nodes.

Case 2. V_i disapproves of the new block generated by $\mathrm{RSU_{Ge}}$. In this case, V_i will not generate approved information, but reputation reference information, denoted as RR_{V_i}, will still be generated and continuously forwarded to all other nodes within its communication range until the termination condition is reached. The specific format of reputation reference information is similar to (10).

During the above steps, RSU_i as well as V_i monitors the approved information and reputation reference information originating from other vehicles, denoted as AP_{V_j} and RR_{V_i}, respectively. Upon receiving AP_{V_j} or RR_{V_i}, if the termination condition has not yet been reached, RSU_i or V_i will proceed with the forwarding process by forwarding the received information within its communication range. In a given interval, if the quantity of RR_{V_i} counted by a specific node is greater than a preset threshold, then the new block is considered propagated thoroughly in the VEC network, and the block forwarding process of this node then terminates. Particularly, for an RSU node, once it receives the reputation reference information originating from a vehicle, except for forwarding it to any other nodes within its communication range, it will also need to cache it in the local pool.

In a preset interval, if the quantity of AP_{V_j} is greater than a preset threshold, the new block generated by $\mathrm{RSU_{Ge}}$ will be considered "Vehicle Valid" by RSU_i or V_i. A "Vehicle Valid" block will be uploaded to the blockchain maintained by RSU_i or V_i, and the forwarding process of the approved information and reputation reference information will then be terminated. Conversely, if the quantity of AP_{V_j} fails to reach the threshold in a given interval, the new block generated by $\mathrm{RSU_{Ge}}$ will be considered "Vehicle Invalid" by RSU_i or V_i. A "Vehicle Invalid" block will be discarded by RSU_i or V_i, and the cached reputation reference information $\mathrm{RR}_{\mathrm{RSU}_i}$ and RR_{V_i} on an RSU node will be sent to the TA progressively.

Note that after appointing the generator of the new block, the TA will monitor the reputation reference information fed back from any RSU node. According to the content of the reputation reference information, the reputation of the generator $\mathrm{RSU_{Ge}}$ will be updated.

5 Simulation and discussion

In this section, we evaluate the block propagation time during the vehicular blockchain consensus. First, we compare the numerical and simulation results to validate the theoretical analysis. The results show that the range of communication, the velocity of the vehicles, and the number of deployed RSUs will affect

the block propagation time. Then, we prove that RSU participation can accelerate blockchain consensus. Notably, an RSU or a vehicle that creates a new block plays a decisive role in block propagation due to the different communication modes in the two cases. Finally, we compare the simulation results of our proposed consensus mechanism to those of the conventional consensus mechanism and prove that the blockchain propagation time and frequency can be substantially reduced using the proposed consensus mechanism.

5.1 Scenario description

We consider a 12 km × 12 km square region with 0–50 RSUs and 200 vehicles. The moving pattern of vehicles follows a random direction mobility model, with the moving direction following the uniform distribution in $[0, 2\pi)$, and the locations of the RSUs are evenly distributed in the area. The communication range is 200 m for a vehicle and 500 m for an RSU [5]. The contact rates λ_{vv} and λ_{vR} depend on the area of the entire region, the communication range of the nodes, and the average relative velocity between nodes [21]. The velocity of vehicles follows a uniform distribution in [20, 60] km/h.

Recalling the assumption that a new block is added to the vehicular blockchain once the number of vehicles that receive and verify the block reaches a threshold βN_{v}, we take $\beta = 2/3$ as an example. Of course, we may adopt other threshold values (such as $\beta = 3/4, 4/5$), as long as they satisfy the idea of a blockchain, i.e., following the most participants. In the case of single-block propagation, we randomly select an RSU or a vehicle from all participants as the node that creates a new block. In the case of n-block propagation, we assume that RSUs have received n blocks, and the forwarding probability for any block is $1/n$.

5.2 Results and discussion

Figure 4 illustrates the impact of the number of deployed RSUs on the average block propagation time in single-block and multiblock conditions. Obviously, the more numerous the RSUs are, the faster the block propagates. This result is obtained because with an increasing number of deployed RSUs, the aggregated contact rate (i.e., $\lambda_{\mathrm{vR}} N_{\mathrm{R}}$) between vehicles and RSUs also increases, leading to a shorter time for an RSU to receive a new block from nearby vehicles. However, as discussed, a multiblock propagation scenario means that a competitive propagation relationship is established between the blocks. More numerous competitive propagation blocks result in a longer block propagation time, as the competitive relationship leads to a decrease in the average propagation rate of a block. For example, in the case of single-block propagation where a vehicle creates a new block and $N_{\mathrm{R}} = 1$, according to (6), an RSU cannot receive the new block from vehicles until more than 99% of the vehicles have received the block. In this condition, block propagation can be approximately considered a propagation process between vehicles only, and thus, the block propagation time will be much longer. Once at least two RSUs are participating in the propagation process, the average block propagation time will decrease substantially.

Figure 5 illustrates the effect of the proportion of vehicle nodes that approve the new block on the block propagation time. Obviously, as the proportion of vehicle nodes that disapproves of the new block increases, the block propagation time increases substantially under the conventional consensus mechanism and rather negligibly under the proposed consensus mechanism. The trend of the required time for the new block to reach consensus should be highly similar to Figure 5, given the condition of a different proportion of vehicle nodes that approves the new block. The reason is that for a conventional consensus mechanism, reaching a consensus also means that the new block has been propagated thoroughly in the VEC network, whereas for the proposed consensus mechanism, it means that the approved information and reputation reference information are thoroughly propagated in the network.

Now, we look at the trade-off between our proposed mechanism and the conventional mechanism. Here, we define the communication overhead as the number of times the transmission information (including blocks, approved information, and reputation reference information) is forwarded in the network and the verification overhead as the sum of the number of times the verification process is performed on each node. We preserve the same scenario setup and limit the number of unapproving vehicles to 25%. Figure 6(a) shows that the communication overhead of the proposed mechanism is larger than that of the conventional mechanism, which is obtained because the proposed mechanism encourages all nodes in the network to participate jointly in the propagation of the new blocks and the forwarding of other consensus information. The proposed mechanism is beneficial because it allows all network nodes to reach consensus faster. In addition, Figure 6(b) shows that the verification overhead required for adopting the

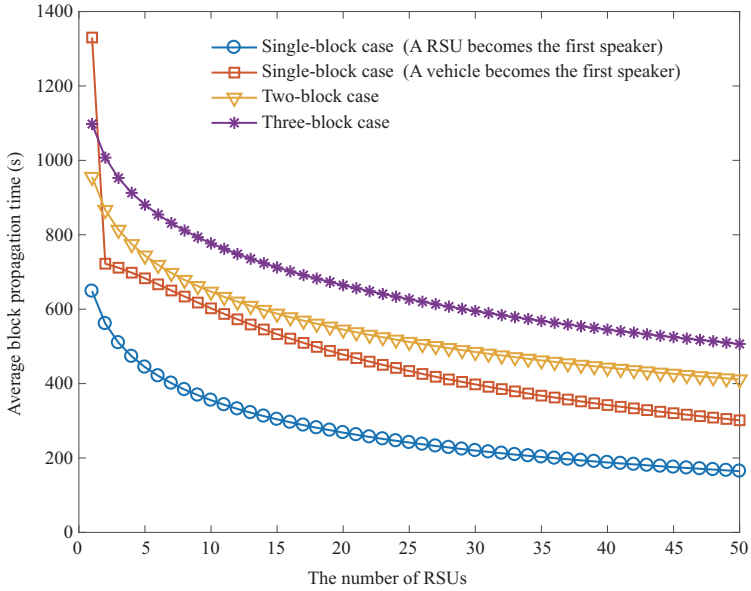

Figure 4 Influence of the scale of deployed RSUs on the average block propagation time in single-block and multiblock conditions over a 12 km × 12 km square region ($N_{\mathrm{v}} = 200$, $N_{\mathrm{R}} = 1 - 50$, $r_{\mathrm{vv}} = 200$ m, $r_{\mathrm{vR}} = 500$ m).

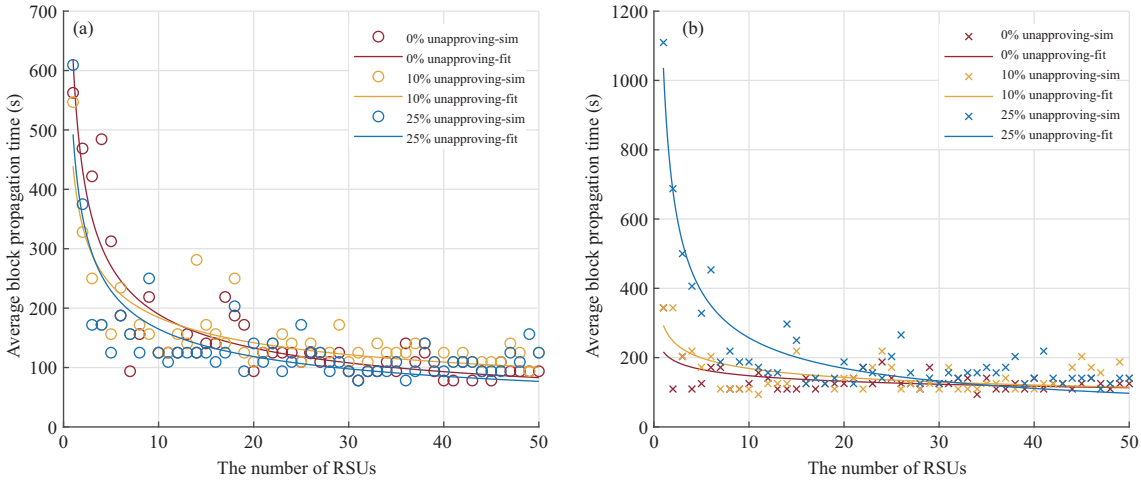

Figure 5 Average block propagation time with different proportions of unapproving vehicle nodes over a 12 km × 12 km square region ($N_{\mathrm{v}} = 200$, $N_{\mathrm{R}} = 1 - 50$, $r_{\mathrm{vv}} = 200$ m, and $r_{\mathrm{vR}} = 500$ m). (a) Proposed mechanism; (b) conventional mechanism.

proposed mechanism is actually smaller. As the block is thoroughly propagated and cached in each node, these nodes only need to forward the generated verification information (approved and reputation reference information) instead of repeating the verification process for the received block, thus reducing the verification overhead.

6 Conclusion

In this paper, we investigated the block propagation between moving vehicles and server-assisted RSUs with the coexistence of V2V, V2R, and R2R communication modes during vehicular blockchain consensus. First, based on the relevant theories of the dynamic equation, the closed-form expressions for single-block and multiblock propagation times were given for two specific cases in which multiblock propagation embodies blockchain forking competitive propagation. We further proposed a consensus mechanism that can fully invoke the communication capabilities of network nodes. The numerical and simulation results verify our theoretical analysis. Additionally, we prove that under the conventional and proposed consensus mechanisms, an RSU or a vehicle that creates a new block plays a decisive role in the block propagation

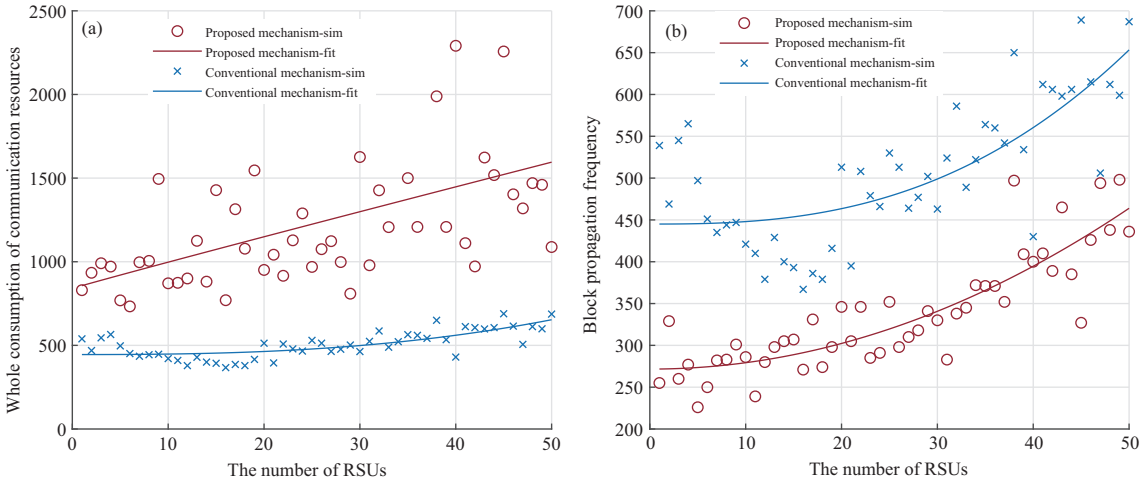

Figure 6 (a) Communication and (b) computation overhead with 25% unapproving vehicle nodes over a 12 km × 12 km square region ($N_{\rm v} = 200$, $N_{\rm R} = 1 - 50$, $r_{\rm vv} = 200$ m, and $r_{\rm vR} = 500$ m).

pattern due to the different communication modes in the two cases.

Acknowledgements This work was supported in part by National Natural Science Foundation of China (Grant No. 62271073), Beijing Natural Science Foundation (Grant No. L212003), and 111 Project of China (Grant No. B16006).

References

1 Xu W, Zhou H, Cheng N, et al. Internet of vehicles in big data era. IEEE CAA J Autom Sin, 2018, 5: 19–35
2 Yang Z, Yang K, Lei L, et al. Blockchain-based decentralized trust management in vehicular networks. IEEE Int Things J, 2019, 6: 1495–1505
3 Zhang X, Zhang J, Liu Z, et al. MDP-based task offloading for vehicular edge computing under certain and uncertain transition probabilities. IEEE Trans Veh Technol, 2020, 69: 3296–3309
4 Lu Y, Huang X, Dai Y, et al. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. IEEE Trans Ind Inf, 2020, 16: 4177–4186
5 Kang J, Yu R, Huang X, et al. Blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Int Things J, 2019, 6: 4660–4670
6 You X, Wang C X, Huang J, et al. Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts. Sci China Inf Sci, 2021, 64: 110301
7 Zhang X, Xia W, Wang X, et al. The block propagation in blockchain-based vehicular networks. IEEE Int Things J, 2022, 9: 8001–8011
8 Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. 2008. http://bitcoin.org/bitcoin.pdf
9 King S, Nadal S. PPcoin: peer-to-peer crypto-currency with proof-of-stake. 2012. https://bitcoin.org/bitcoin.pdf
10 Bentov I, Lee C, Mizrahi A, et al. Proof of activity. SIGMETRICS Perform Eval Rev, 2014, 42: 34–37
11 Ongaro D, Ousterhout J. In search of an understandable consensus algorithm. In: Proceedings of the Annual Technical Conference, 2014. 305–320
12 Castro M, Liskov B. Practical Byzantine fault tolerance. In: Proceedings of the 3rd Symposium on Operating Systems Design and Implementation, New Orleans, 1999
13 Islam S, Badsha S, Sengupta S, et al. Blockchain-enabled intelligent vehicular edge computing. IEEE Netw, 2021, 35: 125–131
14 Xie L, Ding Y, Yang H, et al. Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs. IEEE Access, 2019, 7: 56656–56666
15 Zhang L, Xu H, Onireti O, et al. How much communication resource is needed to run a wireless blockchain network? IEEE Netw, 2022, 36: 128–135
16 Sun Y, Zhang L, Feng G, et al. Blockchain-enabled wireless Internet of Things: performance analysis and optimal communication node deployment. IEEE Int Things J, 2019, 6: 5791–5802
17 Amoretti M, Brambilla G, Medioli F, et al. Blockchain-based proof of location. In: Proceedings of IEEE International Conference on Software Quality, Reliability and Security Companion, Lisbon, 2018
18 Khabbaz M. Modelling and analysis of a novel vehicular mobility management scheme to enhance connectivity in vehicular environments. IEEE Access, 2019, 7: 120282
19 Patra M, Thakur R, Murthy C S R. Improving delay and energy efficiency of vehicular networks using mobile femto access points. IEEE Trans Veh Technol, 2017, 66: 1496–1505
20 Zhang X, Neglia G, Kurose J, et al. Performance modeling of epidemic routing. Comput Netw, 2007, 51: 2867–2891
21 Ghandriz T, Jacobson B, Nilsson P, et al. Computationally efficient nonlinear one- and two-track models for multitrailer road vehicles. IEEE Access, 2020, 8: 203854

Appendix A Single-block propagation Case 1: equation derivation

First, we give the dynamic equation for single-block propagation from RSUs to vehicles:

$$\frac{{\rm d}I_{\rm va}(t)}{{\rm d}t} = N_{\rm R} \times \lambda_{\rm vR} N_{\rm v} \times \frac{U_{\rm va}(t)}{N_{\rm v}}, \tag{A1}$$

where $U_{\rm va}(t)/N_{\rm v}$ is the proportion of vehicles that have not received block a out of all vehicles in time t. A vehicle in state $U_{\rm va}$ transfers to state $I_{\rm va}$ once it contacts an RSU that forwards block a. Given the initial condition $I_{\rm va}\,(0)=0$, the general solution to (A1) is given by

$$I_{\rm va}(t)=N_{\rm v}(1-{\rm e}^{-\lambda_{\rm vR}N_{\rm R}t}). \tag{A2}$$

On the basis of (A2), the time t_1 for the first vehicle to receive block a from nearby RSUs is given by

$$t_1=\frac{\ln\frac{N_{\rm v}}{N_{\rm v}-1}}{\lambda_{\rm vR}N_{\rm R}}. \tag{A3}$$

When $t\geqslant t_1$, the block propagates not only from RSUs to vehicles but also between vehicles. In this way, the dynamic equation of a single-block propagation is given by

$$\frac{{\rm d}I_{\rm va}(t)}{{\rm d}t}=N_{\rm R}\times\lambda_{\rm vR}N_{\rm v}\times\frac{U_{\rm va}(t)}{N_{\rm v}}+I_{\rm va}(t)\times\lambda_{\rm vv}(N_{\rm v}-1)\times\frac{U_{\rm va}(t)}{N_{\rm v}-1}, \tag{A4}$$

where $I_{\rm va}\,(t_1)=1$. The second term in (A4) indicates the growth of the number of vehicles in state $I_{\rm va}$ due to block propagation between vehicles. If a vehicle or an RSU that has received block a forwards the block to the vehicles that never received the block previously, the aggregated number of vehicles with block a increases. Under the initial condition of $I_{\rm va}\,(t_1)=1$, the general solution to (A4) is given by

$$I_{\rm va}(t)=\frac{N_{\rm v}(\lambda_{\rm vv}+N_{\rm R}\lambda_{\rm vR}){\rm e}^{(N_{\rm R}\lambda_{\rm vR}+N_{\rm v}\lambda_{\rm vv})(t-t_1)}-N_{\rm R}\lambda_{\rm vR}(N_{\rm v}-1)}{(\lambda_{\rm vv}+N_{\rm R}\lambda_{\rm vR}){\rm e}^{(N_{\rm R}\lambda_{\rm vR}+N_{\rm v}\lambda_{\rm vv})(t-t_1)}+\lambda_{\rm vv}(N_{\rm v}-1)}. \tag{A5}$$

Appendix B Single-block propagation Case 2: equation derivation

First, we give the dynamic equation for single-block propagation from vehicles to RSUs:

$$\begin{cases}\dfrac{{\rm d}I_{\rm va}(t)}{{\rm d}t}=I_{\rm va}(t)\times\lambda_{\rm vv}(N_{\rm v}-1)\times\dfrac{U_{\rm va}(t)}{N_{\rm v}-1},\\[2ex] \dfrac{{\rm d}I_{\rm Ra}(t)}{{\rm d}t}=I_{\rm va}(t)\times\lambda_{\rm vR}N_{\rm R}\times\dfrac{U_{\rm Ra}(t)}{N_{\rm R}},\end{cases} \tag{B1}$$

where $U_{\rm Ra}(t)/N_{\rm R}$ is the proportion of RSUs that have not received block a out of all RSUs in time t. An RSU in state $U_{\rm Ra}$ transfers to state $I_{\rm Ra}$ once it contacts a vehicle that forwards block a. Under the initial condition of $I_{\rm va}(0)=1$, the general solution to (B1) is given by

$$\begin{cases}I_{\rm va}\,(t)=\dfrac{N_{\rm v}}{1+(N_{\rm v}-1)\,{\rm e}^{-\lambda_{\rm vv}N_{\rm v}t}},\\[2ex] I_{\rm Ra}(t)=N_{\rm R}-N_{\rm R}\times\left(\dfrac{N_{\rm v}}{{\rm e}^{N_{\rm v}\lambda_{\rm vv}t}+N_{\rm v}-1}\right)^{\frac{\lambda_{\rm vR}}{\lambda_{\rm vv}}}.\end{cases} \tag{B2}$$

On the basis of (B2), the time t_2 for the first RSU to receive block a from nearby vehicles is given by

$$t_2=\frac{\ln\dfrac{N_{\rm v}}{\frac{\lambda_{\rm vR}}{\lambda_{\rm vv}}\sqrt{\frac{N_{\rm R}-1}{N_{\rm R}}}}}{\lambda_{\rm vv}N_{\rm v}}, \tag{B3}$$

where $I_{\rm Ra}\,(t_2)=1$. When $t\geqslant t_2$, under the initial condition of $I_{\rm va}\,(t_2)=N_{\rm v}\Big/[1+(N_{\rm v}-1)\,{\rm e}^{-\lambda_{\rm vv}N_{\rm v}t_2}]$, similar to (A4), the general solution is given by

$$I_{\rm va}\,(t)=\frac{N_{\rm v}(I_{\rm va}(t_2)\lambda_{\rm vv}+N_{\rm R}\lambda_{\rm vR}){\rm e}^{(N_{\rm R}\lambda_{\rm vR}+N_{\rm v}\lambda_{\rm vv})(t-t_1)}-N_{\rm R}\lambda_{\rm vR}(N_{\rm v}-I_{\rm va}(t_2))}{(I_{\rm va}(t_2)\lambda_{\rm vv}+N_{\rm R}\lambda_{\rm vR}){\rm e}^{(N_{\rm R}\lambda_{\rm vR}+N_{\rm v}\lambda_{\rm vv})(t-t_1)}+\lambda_{\rm vv}(N_{\rm v}-I_{\rm va}(t_2))}. \tag{B4}$$