



Consortium blockchain-based secure cross-operator V2V video content distribution

Hang Shen¹ · Beining Zhang¹ · Tianjing Wang¹ · Xin Liu¹ · Guangwei Bai¹

Received: 9 November 2023 / Accepted: 20 February 2024
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2024

Abstract

Vehicle-to-vehicle (V2V) video content sharing is promising for connected and autonomous vehicles. However, various security, trust, and privacy risks, coupled with conflicts of interest among different operators, hinder the large-scale promotion of such an application. To address these issues, a consortium blockchain-based framework for cross-operator V2V video content distribution is presented, breaking operators' barriers and achieving a fair value transfer. First, a two-tier consortium blockchain architecture is designed for cross-operator transaction data management. Ledger maintenance and consensus verification are performed within subchains, while user information storage and smart contract execution are conducted between the mainchain and subchains. A multi-constrained vehicle-group selection algorithm is then designed, which minimizes service fees under vehicle reputation, connection duration, and transmission rate constraints. Lastly, an incentive mechanism is developed to promote the rapid upload of transaction data for cross-operator contract invocation. Extensive security analysis and simulation results demonstrate the proposed scheme's feasibility, superiority, and effectiveness.

Keywords V2V content sharing · Cross-operator · Consortium blockchain · Vehicle-group selection · Service fee

1 Introduction

The fifth-generation (5G) wireless network brings unprecedented connection speeds and performance to connected vehicles (IoV) [1, 2], promoting the rapid development of video applications such as autonomous driving, environmental awareness, and on-road entertainment. As a resource-intensive application, video content distribution has characteristics such as long transmission duration and strict quality of service (QoS) requirements. Due to the scarcity of

radio spectrum, it is difficult for 5G base stations (BSs) alone to support large-scale video services [3, 4]. Another difficulty is that the frequent switching of vehicle-to-infrastructure (V2I) connections caused by the high-speed movement of vehicles reduces the stability of video provision. Due to the limited cache capacity at the edge of 5G networks, there will inevitably be low cache hit rates in the face of numerous content requests from connected and autonomous cars.

Vehicle-to-vehicle (V2V) video content delivery helps alleviate the storage and communication burden on fixed network infrastructure, expand the transmission range of video content, and reduce delivery delay [5, 6], especially in traffic congestion, where video content between vehicles can be quickly shared. Moreover, most electric cars are powered by lithium-ion batteries and V2V communication can help them save energy [7, 8]. Although very promising, large-scale promotion has some technical and non-technical challenges. First, a car cannot determine the authenticity of transaction object identities. Thus, the car is vulnerable to a Sybil attack with a fake identity [9]. Malicious nodes may tamper with video content, such as implanting illegal links and packet forgery [10, 11]. Many users are unwilling to share content or distrust V2V communications out of concerns about security and privacy. This requires enhancing security to dispel

✉ Tianjing Wang
wangtianjing@njtech.edu.cn

Hang Shen
hshen@njtech.edu.cn

Beining Zhang
202161120012@njtech.edu.cn

Xin Liu
liuxin990224@njtech.edu.cn

Guangwei Bai
bai@njtech.edu.cn

¹ College of Computer and Information Engineering (College of Artificial Intelligence), Nanjing Tech University, Nanjing 211816, China

users' doubts and introducing incentives to increase user acceptance. Second, due to mobility and network dynamics, connection duration and achievable transmission rates must be considered to guarantee V2V transmission delay and reliability. Finally, one reality is that vehicles belonging to different operators under traditional management mode make achieving secure and trusted content sharing difficult.

The vision of cross-operator V2V video content caching, computing, and communications is to build an open, secure, and agile vehicle interaction architecture, break down barriers among operators, and integrate the in-vehicle content services of different operators through V2V technologies, improving flexibility and coverage of vehicular content services and reducing communication pressure on network infrastructure including BSs. Blockchain offers a distributed public database that stores traceable logs [12], on which smart contracts can automate business transactions. The tamper-proof nature of blockchain enables reliable data storage and management, which ensures dependable content transfer among vehicles [13].

Compared to public blockchains, consortium blockchains [14] provide customizable data management through adaptable processing capabilities and scalable verification nodes. This flexibility enables tailored data support for cross-operator V2V video content delivery. The consortium architecture effectively manages multi-party trust issues common in collaborative V2V video transactions [15]. This contrasts with the public blockchain, where users can participate without authentication. Stringent authentication protocols in a consortium blockchain establish mutual trust among participants. This is crucial for cross-operator V2V communications, where verified identities and trustworthiness matter. Furthermore, inherent consortium blockchain security features ensure traceability and accountability of incidents, strengthening regulation of transaction behaviors [16, 17]. Such security provides a robust environment for cross-operator data exchange, fortifying the trustworthiness and dependability of V2V interactions.

1.1 Challenges and related works

Although consortium blockchain empowers multi-operator V2V video content transactions with many potential advantages, there are still some challenges to be addressed:

1) *Multi-operator blockchain architecture*: In a blockchain network, multi-operator V2V video content distribution may generate massive transaction records. Under a conventional single-chain architecture, the distributed nodes of the network may bear a heavier storage and query burden [18]. Under the consortium blockchain architecture, service providers can design and customize according to application requirements, which can provide flexible

architectural support for vehicular applications. Liu et al. [19] propose a consortium blockchain-based collaborative credential management scheme for anonymous authentication in vehicular networks. This scheme builds a service provider consortium to collaboratively manage user subscriptions for network access and service billing after identity verification. A consortium blockchain-based distributed architecture is presented in [20] for virtualized network function management for reliable and transparent coordination among heterogeneous network resource providers, but blockchain's costly storage and computation remain challenging. Based on consortium blockchain, the authors study trusted sharing of network topology among distributed software-defined networking (SDN) controllers for preventing privacy leakage in vehicular edge networks [21]. A blockchain-based V2V transaction model is investigated in [22], in which electric vehicles form a consortium. The authors develop the consortium entry strategies and matching mechanisms for V2V power transactions. Unlike the above applications, the scenario considered in this study involves multi-vehicle collaboration and video content transfer among cross-operators, requiring the blockchain architecture and secured V2V interaction mechanism to be reimaged.

2) *Cross-operator V2V collaboration*: Cross-operator V2V video services provide more choices for content requesters than single-operator vehicle collaboration. However, the limited transmission rate of in-vehicle WiFi makes high-definition video sharing suffer from high latency. Reducing latency and optimizing video quality through multi-vehicle collaboration needs further exploration. Zaidi et al. [23] propose an enhanced user datagram protocol, which improves video transmission quality in vehicular networks by protecting video frames according to their importance. Bradai et al. [24] propose an efficient video transmission mechanism that reduces interference by selecting the minimum subset of relay vehicles to achieve high-quality video propagation in vehicular *ad hoc* networks. In [25], the authors study an adaptive video streaming scheme based on scalable video coding (SVC) to support video services in highway scenarios. The requester can obtain video data from neighboring vehicles or multi-hop paths to BSs through vehicle relays.

3) *Cross-operator value transfer*: Minimizing service fees while ensuring video QoS is the primary concern for users, while fair value exchange is crucial for operators. BSs and vehicles can only trade videos published by said operators. Transactions between vehicles under different operators cannot be verified, making it challenging to achieve cross-operator value exchange. Transaction requests between vehicles under other operators rely on BSs for uploading and contract invocation. If a BS fails to assist vehicles in uploading and verifying cross-operator transactions within

the valid time, subsequent content transactions must be interrupted. Little literature focuses on value transfer among different vehicle operators. Ren et al. [26] propose a scalable consortium blockchain system for value transfer between medical institutions. An off-chain structure is designed with a mainchain for metadata consensus of all chains, and each node maintains a transaction chain. The system realizes the complete consistency and correctness conditions and meets the effectiveness under the value transfer ledger model. In [27], the authors identify multiple network-sharing scenarios, including centralized network-sharing to decentralized spectrum sharing. However, several challenges are associated with their deployment, such as ensuring accountability and trust among operators.

1.2 Contributions and organization

To resolve the barriers to transactions among IoV operators, we propose a consortium blockchain-based secure cross-operator V2V video content distribution framework. The main contributions are three folded:

- A hierarchical consortium blockchain architecture is designed that combines a cross-operator mainchain and multiple parallel operator subchains. This solution supports cross-operator transaction data management and value exchanging among operators;
- A vehicle-group selection algorithm based on integrative matching is developed to help requesters find an optimal decision of content-providing vehicles, aiming to minimize service fees while meeting video quality requirements;
- To enhance V2V service stability and real-time performance, we study a cross-operator contract invocation mechanism that prevents transaction interruptions due to excessive transaction data upload time by incentivizing transaction data uploading. Security analysis and simulation results verify the feasibility and superiority of the proposed method.

The subsequent content is arranged as follows. Section 2 presents a consortium blockchain-based framework for multi-operator collaboration. Section 3 develops a secured V2V video content distribution approach based on this framework. In Section 4, we analyze defenses in the face of security threats. Section 5 evaluates the proposed scheme's transmission delay and economics through simulation methodology. Finally, we summarize the study and discuss future research work.

2 Consortium blockchain architecture

Figure 1 shows the designed cross-operator V2V architecture, divided into three layers: content delivery, information management, and transaction consensus.

1) *Content delivery layer* covers vehicles and BSs with caching and communication capabilities. It is responsible for enabling cross-operator video content delivery. Under the cross-operator V2V trading environment, this layer's functionality ensures stable video transmission and complete uploading of content transaction information.

2) *User management layer* authenticates vehicle user identities and conducts security checks to ensure vehicles meet safety and communication protocol requirements. In addition, this layer needs to record and store video content publication information and transaction execution results to prevent video content tampering.

3) *Transaction consensus layer* is responsible for consensus verification of cross-operator V2V video content transactions to achieve value exchange among vehicles from different operators. The transaction consensus layer stores smart contracts that execute content transactions and vehicle reputation values that need frequent reading and writing for transaction verification. Nodes participating in consensus must ensure the credibility of all transactions.

2.1 Hierarchical multi-chain architecture

In the cross-operator V2V scenario, video content delivery generates many transaction records. To coordinate management, a hierarchical multi-chain architecture is built, containing two types of chains, as shown in Fig. 1:

1) *Cross-operator mainchain*. The mainchain is co-built by a consortium of multiple operators to deploy smart contracts and record reputation values. After setting and deploying smart contracts for video content through an authorized operator, the content and contracts are broadcasted to the vehicular network environment through BSs. V2V video content transactions need to reach transaction consensus on the mainchain to ensure global consistency of transaction processing results. After transactions initiated by vehicles are verified, the reputation values of the trading parties are updated in the mainchain. Content transaction results verified through the mainchain are stored in subchains via cross-chain interaction.

2) *Operator subchains*. Each operator maintains a subchain to record published video content and related transactions. These subchains are parallel. Under the unified association of the mainchain, operators realize transac-

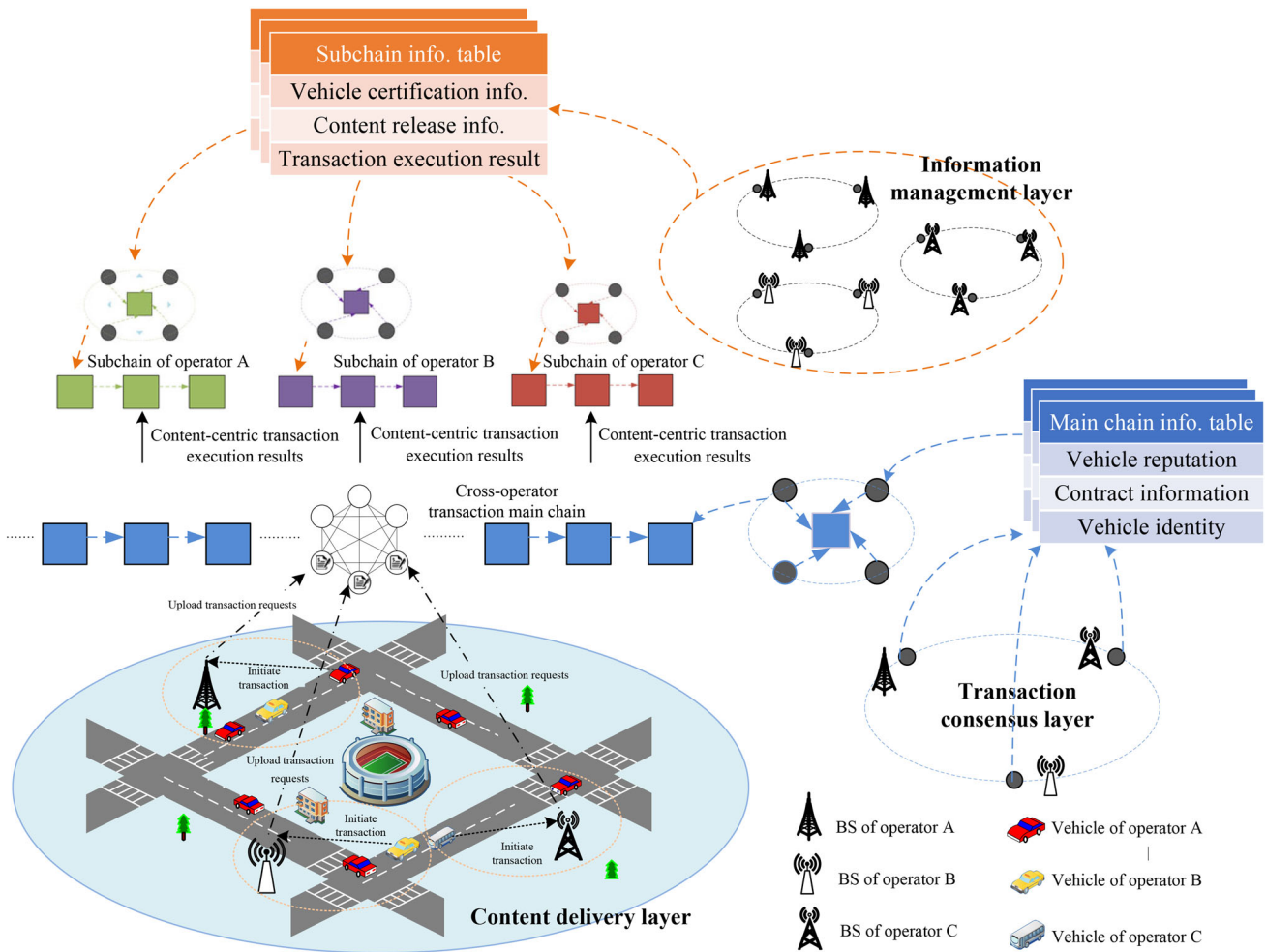


Fig. 1 Consortium blockchain-based cross-operator V2V network architecture

tion data partitioning and storage centered around content, reducing the mainchain’s storage burden for cross-operator transactions. Operators can also quickly query content circulation information through subchain transaction records.

2.2 Trusted cross-chain interaction

A verification mechanism based on signature and Merkle hash tree is designed to ensure the authenticity of value exchange. The mainchain and subchains are equipped with a proof module to verify the authenticity of cross-chain interaction for node identities and data sources, achieving trusted data queries and updates.

Taking the transaction query from the mainchain to a subchain as an example, the information interaction process mainly contains the following steps as shown in Fig. 2:

① When querying transaction information in operator A’s subchain, nodes can send a transaction record query with query identifier q by calling smart contracts on the mainchain.

② The mainchain’s proof module assigns an authorization identifier, ε , then packages and signs the related information into $Sign(q, \varepsilon)$, sending it to operator A’s subchain.

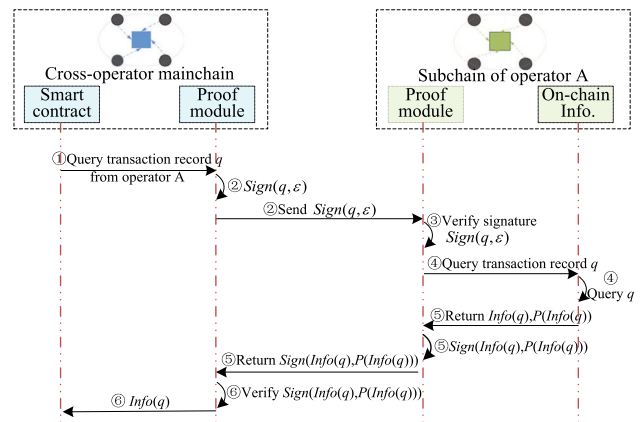


Fig. 2 Interaction between the mainchain and subchains

③ Upon receiving $Sign(q, \varepsilon)$, the proof module on operator A's subchain is responsible for verifying the authenticity of the signature information $Sign(q, \varepsilon)$.

④ If the authentication passes, request q will be queried in subchain A's data records.

⑤ To prove the authenticity of the query result from $Info(q)$, operator A's subchain must provide additional proof information, denoted as $P(Info(q))$, representing the Merkle verification path of $Info(q)$ in the subchain. The signed query result, $Sign(Info(q), P(Info(q)))$, is transferred to the mainchain.

⑥ Smart contracts can obtain the transaction query result after $Sign(Info(q), P(Info(q)))$ passes the verification of the mainchain's proof module.

3 Cross-operator V2V video content sharing

In this section, we study cross-operator V2V video content distribution. First, a fair reward allocation strategy is formulated for vehicle and BS content delivery. Second, the service fee minimization problem is modeled as a multi-constraint programming problem, and an integrative matching degree-based algorithm is developed for problem-solving. Finally, a cross-operator contract invocation policy is developed to verify vehicle transactions and achieve value transfer among operators.

3.1 Fair reward allocation

SVC, which offers a layered approach to scalability [28], is adopted for V2V video content delivery. Video content n is encoded into M layers and the set of video layer indices is denoted as \mathcal{N} . Video quality is related to the number of video layers. $\mathcal{C} = \bigcup_{n \in \mathcal{N}} c_n$ represents the set of video content in the system, where \mathcal{N} is the set of video content indexes. $c_{n,m}$ represents the m th layer of content n . The utility a content requester can obtain is proportional to the popularity and size of the obtained video. When a requester receives video layer $c_{n,m}$ from vehicle j , the obtained utility is calculated as

$$\omega_{j,n,m} = \frac{\chi}{1 + e^{-\delta f_{n,m}}} \log \left(1 + \frac{\varphi}{1 + e^{-\tau \left(\frac{s_{j,n,m}}{\bar{s}} \right)}} \right) \quad (1)$$

where $f_{n,m}$ represents the popularity of content $c_{n,m}$, $s_{n,m}$ is the size of $c_{n,m}$ obtained by the requester from vehicle j , \bar{s} is the average size of video layers in the vehicular network, χ , δ , φ , and τ are adjustable parameters.

Let \mathcal{I}_i represent the set of adjacent vehicles of vehicle i , in which the cars that cache video content n are denoted as $\mathcal{I}_{i,n}$. After requester i obtains video content n from vehicle

$j \in \mathcal{I}_{i,n}$, the generated utility is calculated as

$$\omega_n = \sum_{m \in \mathcal{M}_n} \sum_{j \in \mathcal{I}_{i,n}} \omega_{j,n,m}. \quad (2)$$

The service fee a vehicle can earn positively correlates with its reputation value. The fee generated when vehicle i obtains $c_{n,m}$ from vehicle $j \in \mathcal{I}_{i,n}$ is calculated as

$$\kappa_{j,n,m} = \frac{\partial r_j \omega_{j,n,m}}{(t_{i,j,n,m} - t'_{i,j,n,m} + 1)} + \lambda p_{n,m} \quad (3)$$

where $t_{i,j,n,m}$ denotes the time when a BS uploads the $c_{n,m}$ transaction for vehicle j , $t'_{i,j,n,m}$ is the time when vehicle $j \in \mathcal{A}_{i,n}$ initiates the transaction request, r_j represents the reputation value of vehicle j , $p_{n,m}$ is the price of video layer $c_{n,m}$, ∂ , λ are adjustable parameters.

Another possible situation is that vehicle i has to obtain $c_{n,m}$ from BSs at a high cost when neighboring vehicles do not cache $c_{n,m}$. The generated service fee when car i obtains $c_{n,m}$ from BS b is calculated as

$$\kappa_{b,n,m} = \varsigma \omega_{x,n,m} + \lambda p_{n,m}, \quad (4)$$

where ς is an adjustable weight factor.

3.2 Problem formulation and algorithm design

In the proposed framework, a vehicle refers to an entity with an on-board unit (OBU) [29], which can actively cache popular content with the help of operator BSs. Each vehicle has a pair of public and private keys generated based on the elliptic curve algorithm and is equipped with a trusted platform module to store personal information and perform calculations on demand [30]. Each vehicle obtains surrounding vehicles' speed, driving direction, and content cache through the beaconing protocol [31]. Vehicle users can either initiate content requests to neighboring vehicles or share their cached content with neighboring cars.

For ease of understanding, we construct a case where operators are isolated from each other. As shown in Fig. 3, vehicles 1, 2, and 3 belong to operator A, and vehicles 4 and 5 belong to operator B. Suppose the reputation of these vehicles can satisfy the minimum requirement. Each vehicle's communication resources can deliver one video layer at a time. Vehicles 1-5 are adjacent to vehicle i and carry video layers related to video c_1 . Suppose vehicle i of operator A makes a request for video c_1 with quality level $v_{i,1} = 4$. In the case of V2V video content distribution only within an operator, vehicles 1, 2, and 3 become the content providers of $c_{1,1}$, $c_{1,2}$, and $c_{1,3}$. Due to the limitations in caching and communication resources, $c_{1,4}$ lacks content providers, so vehicle i

| | | | | |
|-----------|-----------------------|-----------------------|-----------------------|-----------------------|
| Vehicle 1 | $\kappa_{1,1,1} = 85$ | $\kappa_{1,1,2} = 83$ | | |
| Vehicle 2 | $\kappa_{2,1,1} = 89$ | $\kappa_{2,1,2} = 86$ | | |
| Vehicle 3 | | $\kappa_{3,1,2} = 81$ | $\kappa_{3,1,3} = 77$ | $\kappa_{3,1,4} = 72$ |
| Vehicle 4 | $\kappa_{4,1,1} = 86$ | | $\kappa_{4,1,3} = 80$ | $\kappa_{4,1,4} = 74$ |
| Vehicle 5 | $\kappa_{5,1,1} = 84$ | $\kappa_{5,1,2} = 82$ | $\kappa_{5,1,3} = 78$ | $\kappa_{5,1,4} = 73$ |
| BS | $\kappa_{b,1,1} = 95$ | $\kappa_{b,1,2} = 91$ | $\kappa_{b,1,3} = 88$ | $\kappa_{b,1,4} = 82$ |

Fig. 3 Vehicle-group selection when operators are isolated from each other

has to obtain it from BSs, indicating that the closed management mode of each operator limits V2V content acquisitions. Exploring a multi-operator collaborative approach becomes necessary to expand potential content providers.

We now formulate the vehicle-group (as content providers) selection problem under the multi-operator collaborative mode. Binary decision variable $a_{i,j,n,m} = 1$ represents vehicle i choosing vehicle $j \in \mathcal{I}_{i,n}$ to provide video layer $c_{n,m}$, otherwise set to 0. For a request for content n from vehicle i , the optimization problem is modeled as $\mathcal{P}1$, which is essentially to minimize service fees by finding $\mathcal{A}_{i,n} = \cup_{m \in \mathcal{M}_n} a_{i,j,n,m}$ under video quality, vehicle reputation, connection duration, and transmission rate constraints.

$$\mathcal{P}1: \min_{\{\mathcal{A}_{i,n}\}_{j \in \mathcal{I}_{i,n}, n \in \mathcal{N}}} : \sum_{m \in \mathcal{M}_n} \left(\sum_{j \in \mathcal{I}_{i,n}} a_{i,j,n,m} \kappa_{j,n,m} - \kappa_{b,n,m} \right)$$

$$\text{s.t.} \begin{cases} r_j \geq \alpha r^{(\max)} + \beta \log(1 + f_{n,m}), & (5a) \\ \forall j \in \mathcal{I}_{i,n}, m \in \mathcal{M}_n \\ d_{i,j} \geq \sum_{m \in \mathcal{M}_n} \frac{a_{i,j,n,m} s_{n,m}}{w_j}, j \in \mathcal{I}_{i,n} & (5b) \\ t_{i,j,n,m} \leq t'_{i,j,n,m} + t_0 & (5c) \\ a_{i,j,n,m} \in \{0, 1\} & (5d) \end{cases}$$

If vehicle i cannot obtain the required content through V2V, it has to switch to V2I connection with $\sum_{m \in \mathcal{M}_n} \sum_{j \in \mathcal{I}_{i,n}} a_{i,j,n,m} = 0$. In this case, the service fee rises to a high level, calculated as $\sum_{m \in \mathcal{M}_n} \kappa_{b,n,m}$. If all video layers can be obtained via V2V, we have $\sum_{m \in \mathcal{M}_n} \sum_{j \in \mathcal{I}_{i,n}} a_{i,j,n,m} = v_{i,n}$. The optimization goal of $\mathcal{P}1$ changes to

$$\min_{\{\mathcal{A}_{i,n}\}_{j \in \mathcal{I}_{i,n}, n \in \mathcal{N}}} : \sum_{m \in \mathcal{M}_n} \sum_{j \in \mathcal{I}_{i,n}} a_{i,j,n,m} \kappa_{j,n,m},$$

equivalent to finding a subset from $\mathcal{I}_{i,n}$ that can minimize service fees.

Constraint (5a) states that the provider of content $c_{n,m}$ must meet the minimum reputation requirement. Under constraint (5b), content-providing car j must complete the delivery of $c_{n,m}$ within a sustainable connection period, $d_{i,j}$, where w_j represents the transmission rate vehicle j can achieve. Before video content trading, the content-providing vehicle must upload the transaction request to the mainchain through a BS to invoke transaction contracts. If the BS upload transaction duration, $t_{i,j,n,m} - t'_{i,j,n,m}$, exceeds the specified time limit t_0 , it leads to termination of subsequent vehicle content transactions. If vehicle $j \in \mathcal{I}_{i,n}$ is selected as the provider of $c_{n,m}$, $t_{i,j,n,m}$ must satisfy (5c).

Algorithm 1 Multi-constrained vehicle-group selection

algorithm: search ($m, \rho, \mu, \mathcal{A}_{i,n}, \mathcal{A}'_{i,n}, v_{i,n}, \mathcal{J}_n$).

```

input :  $m \leftarrow 1, \rho \leftarrow +\infty, \mu \leftarrow +\infty, \mathcal{A}_{i,n} \leftarrow \emptyset, \mathcal{A}'_{i,n} \leftarrow \emptyset;$ 
1 Update provider set  $\mathcal{J}_{n,m}$  for  $c_{n,m}$  under (5a), (5b), and (5c);
2  $\mathcal{J}_n \leftarrow \cup_{m \in \{1,2,\dots,v_{i,n}\}} \mathcal{J}_{n,m};$ 
3 if  $m == v_{i,n} + 1$  then
4   if  $\rho > \mu$  then
5      $\rho \leftarrow \mu;$ 
6      $\mathcal{A}_{i,n} \leftarrow \mathcal{A}'_{i,n};$ 
7   end
8 end
9 else if  $\mathcal{J}_{n,m} == \emptyset$  then
10    $\mu \leftarrow \mu + \kappa_{b,n,m};$ 
11   search ( $m + 1, \rho, \mu, \mathcal{A}_{i,n}, \mathcal{A}'_{i,n}, v_{i,n}, \mathcal{J}_n$ );
12    $\mu \leftarrow \mu - \kappa_{b,n,m};$ 
13 end
14 else
15   foreach  $j \in \mathcal{J}_{n,m}$  do
16      $a_{i,j,n,m} \leftarrow 1;$ 
17      $\mathcal{A}'_{i,n} \leftarrow \mathcal{A}'_{i,n} \cup \{j\};$ 
18      $\mu \leftarrow \mu - \kappa_{j,n,m};$ 
19      $m \leftarrow m + 1;$ 
20     search ( $m, \rho, \mu, \mathcal{A}_{i,n}, \mathcal{A}'_{i,n}, v_{i,n}, \mathcal{J}_n$ );
21      $a_{i,j,n,m} \leftarrow 0;$ 
22      $\mathcal{A}'_{i,n} \leftarrow \mathcal{A}'_{i,n} \setminus \{j\};$ 
23      $\mu \leftarrow \mu - \kappa_{j,n,m};$ 
24   end
25 end

```

To solve Problem $\mathcal{P}1$, we develop a multi-constrained vehicle-group selection algorithm, summarized as Algorithm 1, with the implementation details as follows:

1. The global variable, ρ , is used to record the total service fees required to obtain content n . The optimal content providers are recorded in $\mathcal{A}_{i,n}$.
2. The provider set for content $c_{n,m}$ is updated according to reputation value, connection duration, and transaction upload delay (lines 1-2). If the content quality requirement of requester i has been met (line 3), the scheme

compares the current total service fees with ρ (line 4). If the service fee is minor, update ρ , and store the current decision scheme.

3. When the video quality requirement of content requester i is not yet met, we need to observe the number of vehicles as optional providers for the current video layer. If no vehicle can provide $c_{n,m}$ (line 9), this content has to be obtained from BSs.
4. If there are vehicles that can provide $c_{n,m}$, we traverse all possible decision schemes and update the temporary decision scheme (lines 17-18). After selecting a content-providing vehicle for $c_{n,m}$, the scheme continues to choose providers for the next layer (line 20). When backtracking other decision schemes, some variables must be restored to previous states (lines 22-23).
5. After the search is complete, the scheme that minimizes service fees is updated to $\mathcal{A}_{i,n}$.

In the proposed framework, vehicles belonging to operator B can share the required content to car i of operator A. To facilitate understanding, we provide an example of Algorithm 1 being applied to the scenario of Fig. 3, and the calculation results are shown in Fig. 4. In the example, each vehicle only has enough communication resources to deliver one video layer at a time, though multi-vehicle collaborative content delivery is supported. Since vehicle 5 has the lowest service fee but cannot provide $c_{1,1}$ and $c_{1,2}$ concurrently, the algorithm selects vehicle 1 with the next lowest fee as the provider for content $c_{1,1}$, while vehicle 5 handles $c_{1,2}$. Although retrieving $c_{1,3}$ from vehicle 3 is the cheapest individually, the overall price is not optimal. Hence, vehicles 4 and 3 are selected as the providers for $c_{1,3}$ and $c_{1,4}$, respectively. Despite vehicle 3's lower $c_{1,3}$ quotation, partitioning content delivery across vehicles based on constrained individual capacities minimizes collective expenses. By consolidating layered dissemination duties, the approach allows cooperating vehicles to jointly share video data, reducing the probability of downloading content from BSs.







| | | | | |
|---|-----------------------|-----------------------|-----------------------|-----------------------|
|  Vehicle 1 | $\kappa_{1,1,1} = 85$ | $\kappa_{1,1,2} = 83$ | | |
|  Vehicle 2 | $\kappa_{2,1,1} = 89$ | $\kappa_{2,1,2} = 86$ | | |
|  Vehicle 3 | | $\kappa_{3,1,2} = 81$ | $\kappa_{3,1,3} = 77$ | $\kappa_{3,1,4} = 72$ |
|  Vehicle 4 | $\kappa_{4,1,1} = 86$ | | $\kappa_{4,1,3} = 80$ | $\kappa_{4,1,4} = 74$ |
|  Vehicle 5 | $\kappa_{5,1,1} = 84$ | $\kappa_{5,1,2} = 82$ | $\kappa_{5,1,3} = 78$ | $\kappa_{5,1,4} = 73$ |
|  BS | $\kappa_{b,1,1} = 95$ | $\kappa_{b,1,2} = 91$ | $\kappa_{b,1,3} = 88$ | $\kappa_{b,1,4} = 82$ |

Fig. 4 Vehicle-group selection by Algorithm 1

The algorithm adopts a recursive structure, in which each recursive search occurs $\mathcal{O}(|\mathcal{J}_n|)$ times. The overall time complexity is exponential due to the exhaustive backtracking search through possible vehicle groups, where $|\mathcal{J}_{n,m}|$ is all content providers and $v_{i,n}$ is the number of video layers. By unrolling the recursion, we can get an overall complexity of $\mathcal{O}(\prod_{m \in \{1,2,\dots,v_{i,n}\}} |\mathcal{J}_{n,m}|)$, which can be approximately expressed as $\mathcal{O}(|\mathcal{J}_n|^{v_{i,n}})$.

3.3 Cross-operator contract invocation

Before triggering a transaction contract, content-providing vehicles must upload transaction information through a BS. This subsection presents an incentive strategy to encourage operator BSs to accelerate uploading transaction requests and avoid interruptions.

Suppose BS b has uploaded transaction information of video layer $c_{n,m}$ for vehicle $j \in \mathcal{I}_{i,n}$. The contribution of this BS to the video request is calculated as

$$E_b = \frac{\omega_{j,n,m}}{\omega_n}, \tag{6}$$

which can continue accumulating when BS b uploads transaction requests for other layers of video content n .

After a transaction is completed, the reward amount that the assisting BS b can obtain from other operators is calculated as

$$\phi_b = g \frac{E_b}{(t_{i,j,n,m} - t'_{i,j,n,m} + 1)} \tag{7}$$

where $t_{i,j,n,m} < t'_{i,j,n,m} + t_0$ and g is an adjustable parameter. The shorter the interval for a BS to upload the transaction, the higher the reward it can obtain. If a BS fails to upload the transaction to the mainchain within the valid time limit t_0 , it cannot get benefits.

Below is the explanation of transaction processing in a cross-operator scenario. Suppose vehicle j belonging to operator A caches video layer $c_{n,m}$ from operator B. When vehicle $j \in \mathcal{A}_{i,n}$ distributes content $c_{n,m}$ to vehicle i , the submitted transaction needs to go through the following steps shown in Fig. 5.

① Car j as a content provider signs the contract address of $c_{n,m}$ sent by vehicle i using $Sign(Sign(SmartConAddress_{c_{n,m}})_{K_i^s})_{K_j^s}$, and then uploads the transaction signature to a BS of operator A.

② The BS of operator A uploads the transaction requests initiated by both parties to the mainchain.

③ According to the signature, the proof module in the mainchain invokes and executes smart contract $SmartCon_{c_{n,m}}$.

④ The mainchain that maintains global reputation values updates the reputation of the trading parties.

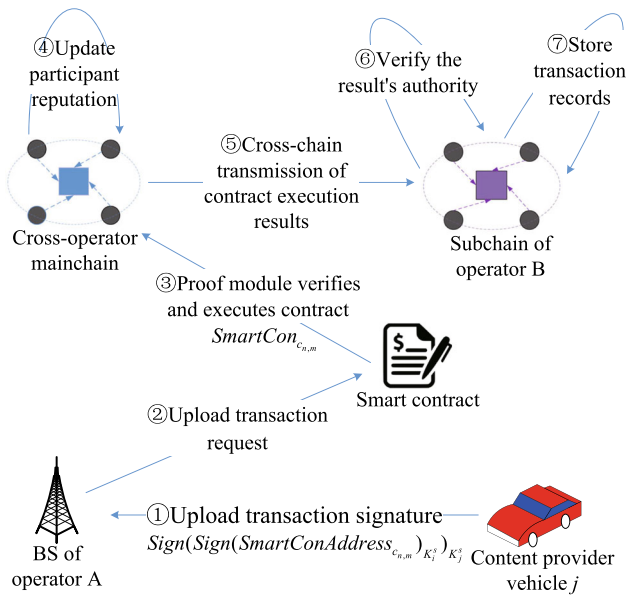


Fig. 5 Cross-operator transaction processing example

⑤ After transaction verification, the mainchain transfers the transaction results to the subchain of operator B to achieve content-centric transaction record storage.

⑥ Operator B's subchain verifies the credibility of the results sent by the mainchain through the proof module.

⑦ Operator B updates and stores transaction records related to $c_{n,m}$.

Algorithm 2 Cross-operator contract invocation algorithm.

```

input :  $account_i, account_j, account_b, \tilde{c}_{n,m},$ 
 $SmartConAddress_{c_{n,m}}$ ;
1 Requester  $i$  and content provider  $j$  sign the contract address to
be initiated;
2  $Sign(Sign(SmartConAddress_{c_{n,m}})_{K_i^s})_{K_j^s}$  is uploaded to the
mainchain by BS  $b$ ;
3 if Contract call successful then
4 Mainchain executes  $SmartCon_{c_{n,m}}$  and pre-deducts funds
from the accounts of both parties to the transaction;
5 BS collects the requester's transaction score and
transaction certification;
6 Calculate the service fee of content provider  $j$  and the
reward of BS uploading transaction;
7 send  $(account_j, \kappa_{j,n,m})$ ;
8 send  $(account_b, \phi_b)$ ;
9 Update the reputation of vehicle  $j$ ;
10 Send cross-chain contract execution results to the subchain
publishing  $SmartCon_{c_{n,m}}$ ;
11 return true;
12 end
13 else
14 Contract call failed;
15 return false;
16 end

```

The process of contract invocation for transactions is shown in Algorithm 2. After requester i initiates a transaction with content provider j , content provider j sends the transaction information with signature to a BS, and the BS uploads the transaction to the mainchain for it. After the successful invocation of contracts in the mainchain, automatic account lock-in is executed for both parties. After verification of transaction consensus, smart contracts distribute rewards to the participants according to the collected transaction ratings and certificates. The execution result of $SmartCon_{c_{n,m}}$ is submitted to the subchain for content-centric transaction storage.

4 Security analysis

This section theoretically analyzes whether the proposed solution can achieve the security design goals.

- *Prevent double-spending fraud*: There is a risk of double-spending in cross-operator V2V video transactions. Attackers may initiate content transactions across subchains belonging to different operators to obtain improper benefits. For example, multiple vehicles could use the same fee when creating requests for various operators' content. This would destroy transaction fairness. An account-locking mechanism via smart contracts can temporarily lock a vehicle's account before transaction completion, only unlocking after confirmation. Thus, vehicles cannot complete a second transaction during the lock period of the first, effectively preventing cross-chain double-spending fraud and ensuring fairness. The temporary account lock enables the system to validate transaction finality across subchains before permitting additional blockchain activity.
- *Prevent content tampering*: In cross-operator transactions, vehicles could implant malicious links into content belonging to other operators, illegally benefiting themselves. However, vehicle-initiated transactions are only published and disseminated after mainchain consensus verification under a content-centric cross-operator ledger. Moreover, each transaction is stored centrally within the corresponding subchain. This content-centric storage and verification prevents unauthorized video content tampering. Even if tampering did occur by another operator's vehicle, the immutable subchain ledger traces details of altered content.
- *Prevent transaction forgery*: When vehicle j provides content $c_{n,m}$ to vehicle i , both parties must sign the contract address of $c_{n,m}$, namely $SmartConAddress_{c_{n,m}}$. This serves as credentials for the transaction request, preventing the transaction request from being forged or denied. In addition, the verification mechanism based on

the Merkle hash tree makes it impossible for an attacker to construct a Merkle verification path corresponding to a nonexistent transaction information to ensure that the transaction information on the subchain is difficult to forge and prevent vehicles from malicious swiping in cross-operator V2V transactions.

- **Prevent Sybil attacks:** Malicious vehicles may create numerous fake identities to initiate video content requests and occupy network resources. Under the proposed consortium blockchain framework, anonymous nodes are not permitted to join V2V content sharing. Participating nodes must be authenticated through protocols to join each operator's subchain. Vehicle users must sign their queries, increasing attackers' difficulty spoofing identities.
- **Prevent distributed denial-of-service (DDoS) attacks:** Malicious vehicles may initiate excessive video requests to rapidly drain attacked vehicles' computational and storage resources, paralyzing normal chain operations. In our scheme, transaction fees are generated alongside video requests, increasing economic costs for attackers to launch DDoS attacks. Properties like closed membership, smaller node scales, multi-signatures, and access controls equip consortiums over public blockchains with enhanced DDoS resilience.
- **Prevent man-in-the-middle (MITM) attacks:** Attackers may intercept and alter data exchanged between the mainchain and operator subchains. Signature-based and Merkle hash tree verifications are employed to safeguard against this. The mainchain proof module signs queries before publishing to subchains. Subchains then validate the signatures to trust the source. When responding, subchains attach Merkle validation paths, enabling the mainchain to swiftly verify transaction completion and data integrity against tampering. Data accountability and integrity are maintained despite potential attacks by cryptographically signing interactions and leveraging Merkle verification.

5 Performance evaluation

Our experiments simulate a vehicular network environment with multiple coexisting operators. To obtain a more realistic simulation effect, the simulation randomly generated 100 video contents using the method described by Zhu et al. [32]. SVC encodes each video content to achieve $M = 4$ video quality levels. Each vehicle caches the more popular content among these 100 videos. Content requests are randomly initiated following the Zipf distribution [33]. The values of

simulation parameters ϑ , δ , ζ , and g are set to 0.0135, 0.0001, 0.015, and 0.15, respectively.

To analyze the impact of the proposed scheme on video content delivery delay and service cost, the following two video delivery methods are selected for comparison:

- **Baseline-1 [34]** is a collaborative video delivery approach whose optional range of content providers is limited to vehicles belonging to the same operator.
- **Baseline-2 [35]** employs non-cooperative video transmissions. A single vehicle is chosen to provide all the required video content for each request.

5.1 BS reward analysis

In this subsection, we examine the BS rewards obtained with different upload contributions (defined in (6)) of 1/4, 1/2, and 1 for a single video request. As shown in Fig. 6, the higher the contribution ratio of a BS for a single video request, the higher the reward it can earn. In addition, the timely uploading of vehicles' transaction requests can bring higher returns to the BS. The upload interval time is inversely proportional to the upload reward obtained by the BS. If the upload interval time approaches the time limit, t_0 , that video transactions can tolerate, the reward is close to 0.

5.2 Impact of cache space on delay

Distribution latency depends on achievable transmission rates and content volume. Some redundancy schemes, like [36], can enable reliable packet delivery for V2V content

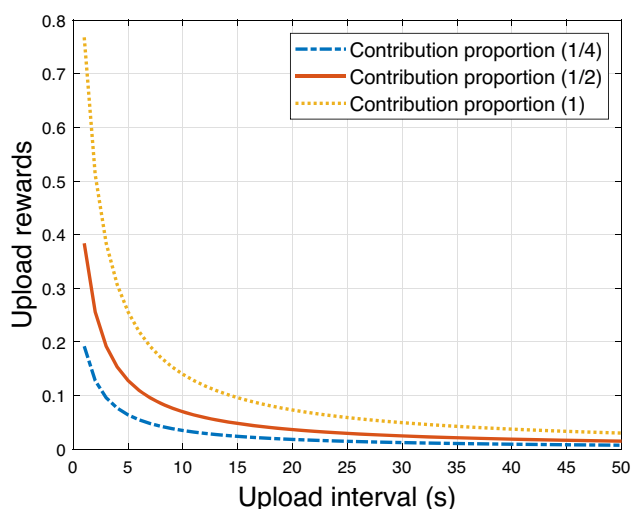


Fig. 6 BS upload bonus

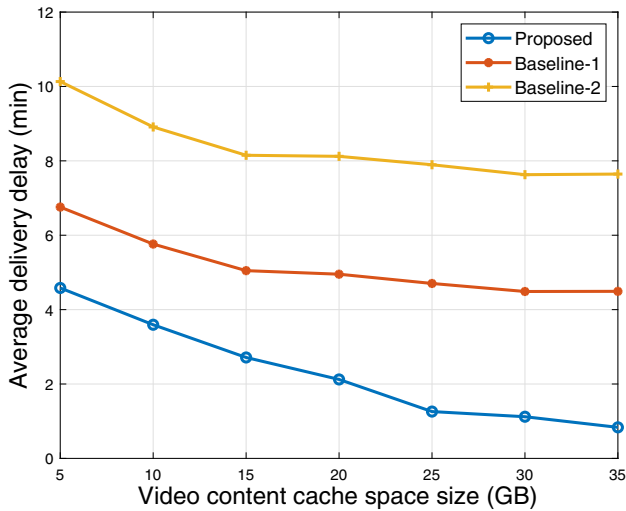


Fig. 7 Average delivery delay

distribution without affecting the proposed scheme's execution.

Figure 7 compares average delivery delays under different methods, given a consistent video quality requirement of 4. Assumptions include: 1) Vehicle cache spaces range from 5GB-35GB; 2) Video content volumes range from 0.2GB-0.8GB; 3) Requested videos are evenly cached across vehicles, eliminating infrastructure downloads. Larger cache space is beneficial to improving the cache hit rate and reducing the average delivery delay. Baseline-1 has lower average delivery delays than Baseline-2 since the latter relies on single-vehicle delivery, which is more time-consuming. In contrast, Baseline-1 allows requesters to retrieve different video layers from multiple neighboring vehicles, shortening durations. The proposed method further reduces delays by expanding alternative providers beyond a single operator's neighbors.

Under a single operator, available content sources are limited if specific pieces are required - neighboring vehicles may hold needed content but temporarily lack communication resources. This forces the requester to wait in line. By enabling cross-operator coordination, the proposed technique mitigates this through an enlarged discoverable cache base, reducing wait times accordingly. Thus, even given small individual cache spaces, collaboration decreases infrastructure burden by uncovering potential providers.

5.3 Comparison of service fees

Figure 8 shows the service fees of different methods when the popularity of requested content is increasing with quality

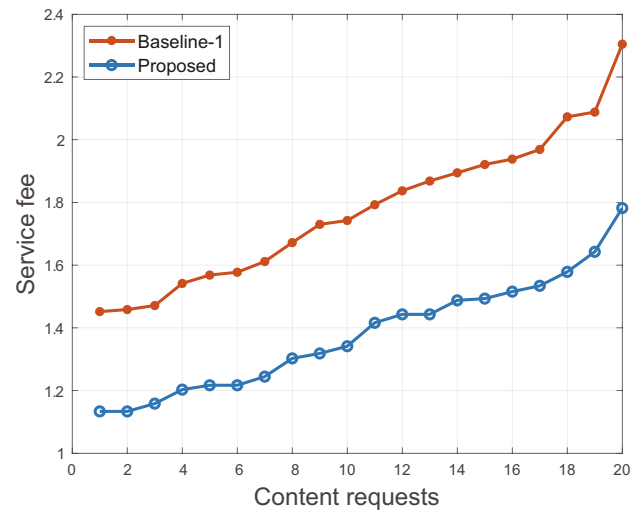


Fig. 8 Comparison of service fees under different schemes

levels of 4. The purpose is to observe the impact of multi-operator coordination on vehicle content service fees. With fewer optional vehicles under a single operator, it may be impossible to match all the content the requester needs. In this case, the car has to obtain the missing video layers from BSs at high costs. Therefore, the service fee generated by the proposed method is lower than that of baseline-1. The cross-operator V2V video content delivery mode has a broader selection range and lower total service costs. In Fig. 9, the proposed method can save more service fees for the requester under the same conditions. To characterize vehicle content requests, we initiate 100 requests following the Zipf distribution for different quality levels of video content. The average

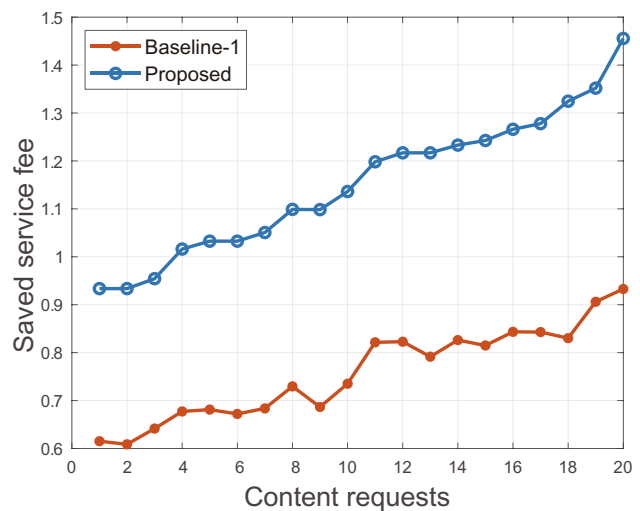


Fig. 9 Comparison of saved service fees

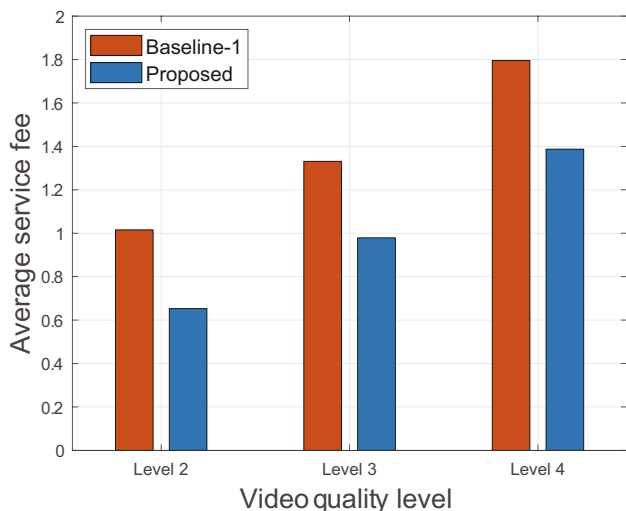


Fig. 10 Comparison of the average service cost

service fees under the two strategies are shown in Fig. 10. High video quality levels require more vehicles to participate in V2V collaboration. As can be seen, the proposed method expands the set of alternative vehicles, improves communication, computing, and caching resource utilization, and saves more service fees for the requester.

It is assumed that video content is randomly cached in vehicles. Fig. 11 compares the service cost ratio to delay under different methods when the popularity of requested content is increasing. More vehicles participating in V2V distribution helps save service fees. With the increase in content requests, the available vehicles become limited, the

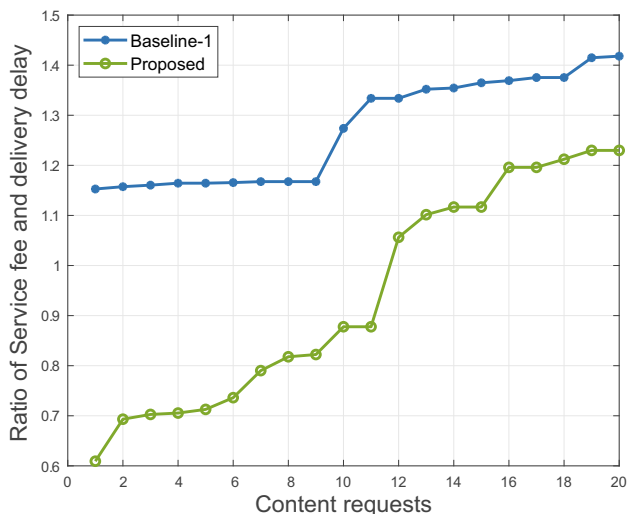


Fig. 11 Ratio of service cost and delay

achievable transmission rate gradually shrinks to the constrained value, and the curve in the figure tends to be flat. Under a single operator, the requester often has to obtain content through V2I, resulting in higher service costs. In the proposed V2V content-sharing framework, the delivery speed of vehicles may be slower than that of BSs. Still, it can provide most of the content to requesters at a lower service cost.

6 Conclusion

We have presented a two-tier consortium blockchain architecture combining a cross-operator transaction mainchain and multiple parallel operator subchains. This framework aims to break down barriers among operators to enable content-centric, cross-operator V2V transaction management. Security analysis indicates the proposed method helps establish a safe and feasible V2V collaboration ecosystem. Simulation results confirm the approach reduces distribution delay and service fees over baseline methods.

Transaction verification involves trust and cooperation among operators. Although employing cross-chain protocols can help improve blockchain scalability, the mainchain may face an enormous consensus burden with multi-party transactions across chains. As vehicles become more autonomous and connected, scalable cross-operator coordination is essential for robust V2V content sharing. In future work, we will explore efficient hierarchical consensus protocols to enable secure cross-operator interactions across blockchains. Cross-chain protocols like atomic commits, hash-locking, and sidechains warrant investigation to coordinate transactions across ledgers. Game mechanisms can also incentivize consensus participation among operators. Combining fee delegation and light client validation may also mitigate the mainchain burden. Advancing such cross-chain techniques can bolster the real-world viability of blockchain-assisted V2V content distribution.

Acknowledgements The authors gratefully acknowledge the financial assistance provided by the National Natural Science Foundation of China and the Natural Science Foundation of Jiangsu Province.

Author Contributions Hang Shen, Beining Zhang, and Xin Liu wrote the main manuscript text. Tianjing Wang and Guangwei Bai provided guiding ideas and suggestions. All authors reviewed the manuscript.

Funding This work was supported in part by the National Natural Science Foundation of China under Grants 61502230 and 61501224, in part by the Natural Science Foundation of Jiangsu Province under Grant BK20201357, and in part by the Six Talent Peaks Project in Jiangsu Province under Grant RJFW-020.

Availability of supporting data Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Declarations

Ethical Approval and Consent to participate This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication All authors agree to publish the paper and related research results of the paper.

Competing interests We declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. We declare that there is no financial interest/personal relationship which may be considered as potential competing interests.

Informed consent Hang Shen, Beining Zhang, Tianjing Wang, and Guangwei Bai are with the College of Computer and Information Engineering (College of Artificial Intelligence), Nanjing Tech University, Nanjing 211816, China.

References

- Zhuang W, Ye Q, Lyu F, Cheng N, Ren J (2020) SDN/NFV-empowered future IoV with enhanced communication, computing, and caching. *Proceedings of the IEEE* 108(2):274–291
- Ye Q, Shi W, Qu K, He H, Zhuang W, Shen X (2021) Joint ran slicing and computation offloading for autonomous vehicular networks: A learning-assisted hierarchical approach. *IEEE Open J Veh Technol* 2:272–288
- Shen H, Heng Y, Shi N, Wang T, Bai G (2022) Drone-small-cell-assisted spectrum management for 5G and beyond vehicular networks. In: *IEEE Symposium on computers and communications (ISCC)*, pp 1–8
- Shen H, Tian Y, Wang T, Bai G (2023) Slicing-based task offloading in space-air-ground integrated vehicular networks. *IEEE Trans Mobile Comput*, to be published. <https://doi.org/10.1109/TMC.2023.3283852>
- Wang S, Chen G, Jiang Y, You X (2023) A cluster-based V2V approach for mixed data dissemination in urban scenario of IoVs. *IEEE Trans Veh Technol* 72(3):2907–2920
- Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo K-KR (2020) A systematic literature review of blockchain cyber security. *Digit Commun Netw* 6(2):147–156
- Zhang F, Hu X, Liu T, Xu K, Duan Z, Pang H (2021) Computationally efficient energy management for hybrid electric vehicles using model predictive control and vehicle-to-vehicle communication. *IEEE Trans Veh Technol* 70(1):237–250
- Kim Y, Guanetti J, Borrelli F (2021) Compact cooperative adaptive cruise control for energy saving: Air drag modelling and simulation. *IEEE Trans Veh Technol* 70(10):9838–9848
- Benadla S, Merad-Boudia OR, Senouci SM, Lehsaini M (2022) Detecting sybil attacks in vehicular fog networks using RSSI and blockchain. *IEEE Trans Netw Serv Manag* 19(4):3919–3935
- Cheng H, Zhang X, Yang J, Liu Y (2023) PPRT: Privacy preserving and reliable trust-aware platoon recommendation scheme in IoV. *IEEE Syst J* 17(3):4922–4933
- Chen C, Wang Cong, Qiu Tie, Lv Ning, Pei Q (2019) A secure content sharing scheme based on blockchain in vehicular named data networks. *IEEE Trans Ind Inform* 16(5):3278–3289
- Shen XS, Liu D, Huang C, Xue L, Yin H, Zhuang W, Sun R, Ying B (2022) Blockchain for transparent data management toward 6G. *Engineering* 8:74–85
- Huang C, Wang W, Liu D, Lu R, Shen X (2023) Blockchain-assisted personalized car insurance with privacy preservation and fraud resistance. *IEEE Trans Veh Technol* 72(3):3777–3792
- Liu D, Huang C, Ni J, Lin X, Shen XS (2022) Blockchain-cloud transparent data marketing: Consortium management and fairness. *IEEE Trans Comput* 71(12):3322–3335
- Kavya KR, Kavitha M (2020) Military message passing using consortium blockchain technology. In: *International conference on communication and electronics systems (ICCES)* pp 1273–1278
- Cheng G, Huang J, Wang Y, Zhao J, Kong L, Deng S, Yan X (2023) Conditional privacy-preserving multi-domain authentication and pseudonym management for 6G-enabled IoV. *IEEE Trans Inform Forensic Secur*, to be published. <https://doi.org/10.1109/TIFS.2023.3314211>
- Xu Y, Yu E, Song Y, Tong F, Xiang Q, He L (2023) \mathcal{R} -tracing: Consortium blockchain-based vehicle reputation management for resistance to malicious attacks and selfish behaviors. *IEEE Trans Veh Technol* 72(6):7095–7110
- He Y, Zhang C, Wu B, Yang Y, Xiao K, Li H (2021) A cross-chain trusted reputation scheme for a shared charging platform based on blockchain. *IEEE Internet Things J* 9(11):7989–8000
- Liu D, Wu H, Huang C, Ni J, Shen X (2022) Blockchain-based credential management for anonymous authentication in SAGVN. *IEEE J Sel Areas Commun* 40(10):3104–3116
- Liu D, Huang C, Xue L, Hou J, Shen X, Zhuang W, Sun R, Ying B (2022) Authenticated and prunable dictionary for blockchain-based VNF management. *IEEE Trans Wirel Commun* 21(11):9312–9324
- Ren Y, Chen X, Guo S, Guo S, Xiong A (2021) Blockchain-based VEC network trust management: A DRL algorithm for vehicular service offloading and migration. *IEEE Trans Veh Technol* 70(8):8148–8160
- Zhang Q, Su Y, Wu X, Zhu Y, Hu Y (2022) Electricity trade strategy of regional electric vehicle coalitions based on blockchain. *Electr Power Syst Res* 204:107667
- Zaidi S, Bitam S, Mellouk A (2017) Enhanced user datagram protocol for video streaming in VANET. In: *IEEE International conference on communications (ICC)*, pp 1–6
- Bradai A, Ahmed T (2014) ReViV: Selective rebroadcast mechanism for video streaming over VANET. In: *IEEE Vehicular technology conference (VTC Spring)*, pp 1–6
- Xing M, Cai L (2012) Adaptive video streaming with inter-vehicle relay for highway VANET scenario. In: *IEEE International conference on communications (ICC)*, pp 5168–5172
- Qiao R, Luo X-Y, Zhu S-F, Liu A-D, Yan X-Q, Wang Q-X (2020) Dynamic autonomous cross consortium chain mechanism in e-healthcare. *IEEE J Biomed Health Inform* 24(8):2157–2168
- Zeydan E, Arslan SS, Turk Y (2023) Exploring blockchain architectures for network sharing: Advantages, limitations, and suitability. *IEEE Trans Netw Serv Manag*, to be published. <https://doi.org/10.1109/TNSM.2023.3331307>
- Shen H, Tong Z, Wang T, Bai G (2023) UAV-relay-assisted live layered video multicast for cell-edge users in NOMA networks. *IEEE Trans Broadcast*, to be published. <https://doi.org/10.1109/TBC.2023.3327642>
- Shah G, Valiente R, Gupta N, Gani SMO, Toghi B, Fallah YP, Gupta SD (2019) Real-time hardware-in-the-loop emulation framework for DSRC-based connected vehicle applications. In: *IEEE Connected and automated vehicles symposium (CAVS)*, pp 1–6

30. Gao F, Zhu L, Shen M, Sharif K, Wan Z, Ren K (2018) A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks. *IEEE Network* 32(6):184–192
31. Ni Y, Cai L, He J, Vinel A, Li Y, Mosavat-Jahromi H, Pan J (2019) Toward reliable and scalable internet of vehicles: Performance analysis and resource management. *Proceedings of the IEEE* 108(2):324–340
32. Zhu H, Cao Y, Jiang T, Zhang Q (2018) Scalable NOMA multicast for SVC streams in cellular networks. *IEEE Trans Commun* 66(12):6339–6352
33. Zhang X, Zhu Q, Poor HV (2020) Sequential hypothesis criterion based optimal caching schemes over mobile wireless networks. In: *IEEE International symposium on information theory (ISIT)* pp 1254–1258
34. Shen H, Liu X, Shi N, Wang T, Bai G (2023) Blockchain-enabled solution for secure and scalable V2V video content dissemination. *Peer-to-Peer Netw Appl* 16(2):554–570
35. Zhang K, Cao J, Liu H, Maharjan S, Zhang Y (2019) Deep reinforcement learning for social-aware edge computing and caching in urban informatics. *IEEE Trans Ind Inform* 16(8):5467–5477
36. Shen H, Bai G (2018) QoS-guaranteed wireless broadcast scheduling with network coding and rate adaptation. *IEEE Trans Veh Technol* 67(7):6492–6503

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.



Hang Shen received the Ph.D. degree (with honors) in Computer Science from the Nanjing University of Science and Technology. He worked as a Full-Time Postdoctoral Fellow with the Broadband Communications Research (BBCR) Lab, ECE Department, University of Waterloo, Waterloo, ON, Canada, from 2018 to 2019. He is an Associate Professor with the Department of Computer Science and Technology, Nanjing Tech University, Nanjing, China. His research

interests involve V2X communication networks, space-air-ground integrated networks, and blockchain technology for cybersecurity and privacy preservation. He serves as an Associate Editor for the *Journal of Information Processing Systems* and *IEEE ACCESS* and an Academic Editor for *Mathematical Problems in Engineering*. He was a TPC member of the 2021 Annual International Conference on Privacy, Security and Trust (PST). He is a Senior Member of CCF, a member of IEEE, and an Executive Committee Member of the ACM Nanjing Chapter.



Beining Zhang received the BS degree in Information Security from Xi'an University of Posts and Telecommunications, Xi'an, China. She is pursuing an MS degree in Computer Science from Nanjing Tech University, Nanjing, China. Her research interests include blockchain-based covert communications and trusted distributed systems.



Tianjing Wang holds a B.Sc. in Mathematics from Nanjing Normal University in 2000, an M.Sc. in Mathematics from Nanjing University in 2002, and a Ph.D. in Signal and Information System from the Nanjing University of Posts and Telecommunications (NUPT) in 2009. From 2011 to 2013, she was a Full-Time Postdoctoral Fellow with the School of Electronic Science and Engineering at NUPT. She was a Visiting Scholar with the ECE Department at the State University of New York at Stony Brook from 2013 to 2014. She is an Associate Professor with the Department of Communication Engineering at Nanjing Tech University. Her research interests include distributed machine learning for V2X communication networks and blockchain technology for network security. She has published research papers in prestigious international journals and conferences, including the *IEEE TRANSACTIONS ON MOBILE COMPUTING*, *IEEE TRANSACTIONS ON BROADCASTING*, *Peer-to-Peer Networking and Applications*, *Journal of Systems Architecture*, *IEEE ICC*, and *IEEE ISCC*. She is a member of IEEE and CCF.



Xin Liu received the BS degree in Network Engineering from Hunan University of Humanities, Science and Technology, Changsha, China, and the MS degree in Computer Science from Nanjing Tech University, Nanjing, China. Her research interests are in blockchain and vehicular networks.



Guangwei Bai received the B.Eng. and M.Eng. degrees in computer engineering from Xi'an Jiaotong University, Xi'an, China, in 1983 and 1986, respectively, and the Ph.D. degree in Computer Science from the University of Hamburg, Hamburg, Germany, in 1999. From 1999 to 2001, he worked as a Research Scientist at the German National Research Center for Information Technology, Germany. In 2001, he joined the University of Calgary, Calgary, AB, Canada, as a Research

Associate. Since 2005, he has been working at Nanjing Tech University, Nanjing, China, as a Professor in Computer Science. From October to December 2010, he was a Visiting Professor with the ECE Department at the University of Waterloo, Waterloo, ON, Canada. His research interests include architecture and protocol design for future networks, wireless multimedia and QoS provisioning, blockchain, and cybersecurity. He has authored and co-authored more than 70 peer review papers in prestigious international journals and conferences, including the IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE TRANSACTIONS ON BROADCASTING, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, *Performance Evaluation*, *Ad Hoc Networks*, *Journal of Systems Architecture*, *Computer Communications*, IEEE ICC, and IEEE LCN. He is a member of ACM and a Distinguished Member of CCF.