

Secure and efficient data sharing in disaster rescue based on blockchain

Wu Minfei^{1,2}, Wang Huihui², Cheng Hongbing (✉)²

1. School of Internet, Jiaxing Vocational and Technical College, Jiaxing 314036, China

2. Zhejiang University of Technology, College of Computer Science and Technology, Hangzhou 310023, China

Abstract

In disaster areas, rescue vehicles (RVs) need to exchange large amounts of data, such as rescue commands and operational experience, to ensure driving safety and rescue efficiency. However, the communication infrastructure in these areas is often damaged, severely affecting normal communication and reducing rescue efficiency. In addition, vehicular networks in disaster scenarios are often untrustworthy and struggle to track malicious behavior, posing potential security risks and inefficiencies in data sharing among vehicles. To address these issues, a secure and efficient data sharing scheme for disaster rescue based on blockchain (SEDS-BDR) is proposed. First, a blockchain-assisted vehicular network framework tailored for disaster relief is designed. Second, a reputation-based consensus algorithm is developed, which securely and immutably tracks improper behavior and records shared data through the blockchain, thereby improving consensus efficiency and system security. Moreover, since blockchain transactions are typically packaged based on time or transaction fees, different weights are assigned to data based on geographic location and information type in the proposed SEDS-BDR. This ensures that urgent data in disaster areas is prioritized for processing, thereby enhancing rescue efficiency. Experimental results show that the reputation-based consensus algorithm effectively shortens consensus time and improves system security. Additionally, the prioritized transaction packaging mechanism optimizes rescue routes, saving time.

Keywords blockchain, Internet of vehicle (IoV), data sharing, disaster rescue

1 Introduction

In recent years, intensified global climate change has led to a rise in the frequency and severity of natural disasters, posing unprecedented threats to human life and property worldwide. According to a 2024 report^[1] from the Centre for Research on the Epidemiology of

Disasters (CRED), there were 399 natural disasters worldwide, resulting in 86 473 deaths, affecting 93.1 million people. When disasters occur, communication infrastructure such as roadside units (RSUs) and base stations often suffer significant damage, disrupting the structure and function of traffic networks and making it difficult to share critical data in disaster-stricken areas. The lack of data sharing in vehicular networks can hinder the coordination and execution of rescue operations, slowing down the response of rescue teams and delaying the transport of relief supplies, which can

pose serious risks to the safety of rescue personnel.

Ref. [2] integrates a unmanned aerial vehicle (UAV)-based Internet of vehicle (IoV) framework for real-time flood monitoring and rescue operations. Although existing literature has made some progress in improving the efficiency of vehicular networks for disaster relief, there has been little focus on the security of data sharing. First, centralized authorities responsible for storing disaster area data and tracking potential malicious nodes may be vulnerable to single-point failure attacks, leading to data security issues. Second, due to the openness of post-disaster rescue networks, RVs may be subjected to attacks during data sharing and dissemination. Attackers may delete or tamper with shared data for personal gain, misleading decision-makers, and increasing the risks associated with rescue operations. Finally, due to the large and dispersed scale of emergency supply logistics in disaster scenarios, problems such as information silos, lack of transparency, and rent-seeking behavior may arise, significantly reducing the efficiency of rescue efforts.

Therefore, it is crucial to develop a secure and efficient data-sharing solution for post-disaster rescue scenarios. Blockchain technology, as an advanced distributed ledger technology, with its transparency, immutability, and decentralization, shows great potential in ensuring the security of data sharing in disaster areas. Especially, in vehicular network applications, blockchain can achieve secure and decentralized data-sharing mechanisms, enabling RVs and emergency agencies to exchange information in real-time and accurately, something traditional centralized network systems struggle to achieve. In fact, blockchain technology has already been applied in several disaster relief cases, demonstrating its unique value in disaster emergency management. For example, the BitNation Refugee Emergency Response (BRER)^[3] project uses blockchain technology to provide emergency services and identity verification for refugees during the European refugee crisis; the HelperBit platform (<https://blog.helperbit.com/en/>) combines blockchain with geographic information system technology to create a transparent and secure post-

disaster relief platform. Additionally, in September 2022, China launched its first disaster emergency data blockchain service platform (<https://disaster.opendatachain.cn/>), establishing an open data alliance chain to lay the foundation for trusted data sharing and traceability among major disaster mitigation agencies. In addition to practical applications, theoretical research is also exploring more possibilities for blockchain technology in disaster scenarios. For example, Cui et al.^[4] combined the 5th generation (5G) network and blockchain consortium chains to achieve more efficient data sharing in vehicular networks. Lu et al.^[5] used a hybrid blockchain structure combined with RSUs and directed acyclic graphs to improve data-sharing efficiency. Kouicem et al.^[6] proposed a solution based on consortium blockchain and zero-knowledge proof to achieve decentralized and anonymous data sharing in vehicular networks.

However, these solutions generally rely on robust communication infrastructure, such as RSUs and 5G networks, which are significantly limited in disaster scenarios where communication infrastructure is severely damaged. To address this limitation, Su et al.^[7] and Wang et al.^[8] developed a lightweight blockchain framework under constrained communication conditions using UAV-assisted vehicular networks, enhancing the security of data sharing. Despite these advances, most existing studies, whether relying on conventional infrastructure or employing UAVs, focus primarily on blockchain transaction records, while neglecting the need to store and efficiently share critical data such as situational images, emergency instructions, and large files, a requirement that is especially vital in disaster-stricken areas.

To address the above shortcomings, a novel scheme that integrates blockchain technology with the InterPlanetary file system (IPFS) is proposed to achieve decentralized storage and efficient sharing of critical data in disaster scenarios. In SEDS-BDR, essential information is stored off-chain via IPFS, while its metadata is securely anchored on-chain, ensuring both data accessibility and integrity even in disaster

scenarios. Moreover, to address the challenges of the limited storage capacity of blockchain blocks and the inefficiency of traditional consensus mechanisms, where proof of work (PoW) prioritizes transactions by time and proof of stake (PoS) by gas fees, a new transaction packaging strategy is designed. A priority mechanism is introduced that gives precedence to urgent data uploads, guaranteeing that time-sensitive information is processed and disseminated without delay.

To address these challenges, the aforementioned secure and efficient data sharing scheme for disaster rescue based on blockchain, namely the SEDS-BDR framework, is further elaborated and implemented for vehicular network rescue scenarios. The main work and contributions of this study can be summarized as follows.

1) The SEDS-BDR framework is constructed as a secure and efficient vehicular network rescue scheme powered by blockchain technology. In this framework, the proof of authority (PoA) consensus algorithm is optimized by integrating a reputation points system. In this way, high-reputation nodes are guaranteed to conduct data packaging and block generation efficiently and securely, and the overall security of the system is significantly improved.

2) A weighted blockchain transaction prioritization mechanism is designed within the SEDS-BDR framework, which gives priority to the processing and on-chain uploading of time-sensitive urgent disaster information, thereby effectively improving the efficiency of disaster rescue. Meanwhile, the IPFS is adopted to store core blockchain data, which relieves the storage pressure of blockchain blocks and optimizes the utilization of limited on-chain storage space.

3) Comparative analysis is implemented, and targeted simulation experiments are carried out to test the performance of the SEDS-BDR. The obtained experimental results demonstrate the effectiveness and practical feasibility of the scheme in vehicular network-based disaster rescue scenarios.

The rest of the paper is organized as follows. Sect. 2 introduces the related works. Preliminaries are elaborated in Sect. 3. The SEDS-BDR is presented in

Sect. 4. Detailed performance analysis and corresponding simulation results are illustrated in Sect. 5. Finally, this study is concluded in Sect. 6.

2 Related work

The existing literature has conducted a large number of studies on the security and efficiency of data sharing in the IoV. The IoV uses blockchain technology to record transaction information to ensure the immutability and traceability of data, thereby guaranteeing the security and efficiency of shared data.

2.1 Blockchain-based secure data sharing in IoV

Due to the advantages of blockchain, many applications of blockchain in IoV have been studied recently. Karim et al.^[9] proposed the blockchain-based secure data collection and exchange scheme for IoV (BSDCE-IoV) scheme, which leveraged blockchain and elliptic curve cryptography to enhance security and efficiency in 5G-based IoV environments. Tong et al.^[10] proposed the traffic information interaction for a blockchain-based IoV (TI-BIoV) system that enhanced traffic information interaction in IoV by utilizing a nonsubjective trust mechanism and a Q-learning-based incentive strategy, ensuring secure, reliable, and accurate data exchange with partial inexplicit parameters. Regrettably, the aforementioned vehicular blockchain systems relied heavily on infrastructure components such as RSUs and 5G, making them unsuitable for deployment in disaster areas where infrastructure is severely damaged or nonexistent. Zhang et al.^[11] employed dynamic sharding to establish a temporary and mission-exclusive blockchain network for each rescue operation. Within this network, UAVs achieve trusted identity authentication and data sharing, while utilizing cross-shard communication to enable complex cross-domain collaborative rescue missions.

As a result, some data-sharing schemes are developed for IoV, targeting scenarios where the infrastructure is limited or significantly damaged. Su et al.^[7] developed a streamlined blockchain-based framework for collaborative data sharing and introduced

a reputation-driven delegated proof of stake (DPoS) algorithm to enhance consensus efficiency in disaster rescue operations. A trusted and efficient blockchain-based data sharing scheme (TEBChain) proposed by Wang et al.^[12] enhances secure and efficient data sharing in disaster scenarios using a blockchain-based framework, an improved key update mechanism, and a lightweight practical Byzantine fault tolerance (PBFT) consensus protocol. While the plan suggests a blockchain-based solution for disaster scenarios, it does not adequately account for the network instability common in such areas. This oversight could result in network partitioning, diminishing the solution's effectiveness.

In contrast, SEDS-BDR proactively selects highly trustworthy nodes in disaster scenarios and implements hierarchical management for these pre-vetted nodes. By dynamically adjusting consensus node membership based on the real-time reputation values of the pre-selected nodes, SEDS-BDR significantly improves the stability and operational efficiency of the blockchain-enabled IoV system even under highly unstable network conditions, filling the research gap left by existing schemes.

2.2 Efficient data sharing in IoV

With the development of UAV and IoV technologies, their application in disaster relief has become increasingly widespread. To address the challenges of path planning and communication in complex environments, various optimization algorithms are proposed to enhance the efficiency and reliability of UAVs and vehicle networks. Trojanowski et al.^[13] introduced a heuristic optimization algorithm for UAV path planning that leverages population density data to maximize victim localization in disaster areas. Diao et al.^[14] introduced the artificial potential field-improved rapidly-exploring random trees (APF-IRRT) algorithm to improve UAV path planning in disaster relief by enhancing path generation, convergence speed, and real-time performance in complex environments. Javed et al.^[15] proposed a solution that improves disaster communication by optimizing UAV-based connectivity and communication through the selection of the optimal

number of clusters, UAV trajectory planning, and cluster head selection. Husnain et al.^[16] presented a novel route optimization method using Harris Hawks' optimization for intelligent route clustering in IoV networks, enhancing cluster head selection and addressing challenges of cluster stability and dynamic topology changes. Zheng et al.^[17] presented a distributed real-time search path planning method for multi-UAVs, using a distributed stochastic algorithm based on an enhanced genetic algorithm (DSA-EGA) to improve search efficiency, connectivity, and collision avoidance.

3 Preliminaries

3.1 Network model

In the network model illustrated in Fig. 1, the disaster area comprises multiple key entities, including the trusted authority (TA), ground stations (GSs), and RVs. Due to the damage or inaccessibility of conventional communication infrastructure (e.g., base stations), they rely on wireless Ad hoc communication to exchange information and coordinate rescue activities.

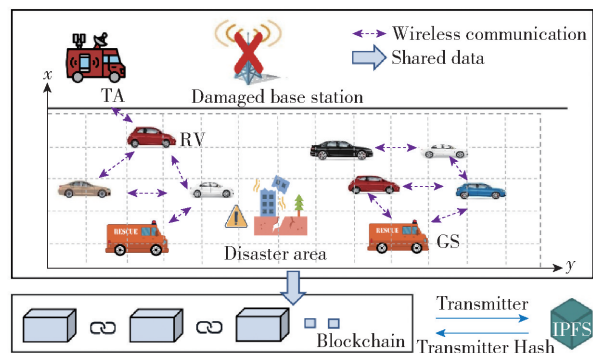


Fig. 1 Network model in disaster rescue

The TA is responsible for registering and authenticating RVs by issuing public and private key pairs to verify their identities, similar to issuing certified license plates. Using real-time disaster information provided by RVs, such as damage levels and road conditions, the TA assigns different priority levels to various areas, ensuring that resources are directed to the most critical regions while avoiding

heavily damaged ones. Additionally, the TA coordinates the distribution of rescue supplies and manpower, enhancing the safety and efficiency of rescue operations.

GSs function as full nodes in the blockchain network, equipped with advanced communication tools and storage for rescue supplies. These government-verified nodes are responsible for verifying and packaging transactions within the network and maintaining a complete copy of the blockchain. Their role is crucial for ensuring the validity of transactions and the integrity of the blockchain, contributing to the system's security and stability.

RVs operate as light nodes, focusing on collecting and sharing disaster information without storing a full copy of the blockchain. They send or relay transactions after being registered and authorized. RVs can publish transactions to share crucial information during emergencies, which are then broadcast to the entire network for processing by other authorized nodes, such as GSs and TA. The public and private key pairs of RVs are stored in tamper-proof devices to ensure the security of identity authentication and information exchange.

Each block in the system contains a block header and a block body. The block body includes all valid transactions organized in a Merkle tree, with the root Hash stored in the block header to ensure data integrity. Traditional blockchains use a chained data structure to record all transaction information. With the accumulation of time, the volume of ledger data expands exponentially, resulting in an increasingly heavy storage burden for all nodes and seriously restricting the scalability of the network. To break through this technical bottleneck, this solution deeply integrates blockchain with IPFS^[18] to construct a hierarchical storage architecture: the blockchain only stores the Hash values of IPFS files as data indexes, while large-capacity raw data, such as pictures, videos, and documents, are fragmented and stored in the IPFS distributed network. The disaster situation pictures, material lists, and other data collected on-site in the disaster-stricken areas are encrypted and fragmented by IPFS and then stored. The blockchain

only records the corresponding Hash fingerprints, which makes the full node not need to save the complete data copy, significantly reducing the storage cost. This design enables RVs to easily access the blockchain network as well, participating in data verification and sharing. In the disaster-stricken area application scenario, the system further collaborates with TA and GSs to manage data storage: TA is responsible for Hash verification and permission control of the files stored in IPFS, while GSs undertake the storage scheduling and distribution tasks of data fragmentation. Through this sharding storage strategy, not only the storage pressure of the blockchain system is reduced, but also the efficiency of data access is guaranteed, effectively enhancing the real-time performance and reliability of emergency data sharing in disaster-stricken areas. Importantly, when a participant needs to access shared data, it first queries the blockchain to obtain the relevant IPFS Hash, and then uses this Hash to retrieve the file from IPFS. The TA and GSs further manage node authentication and policy enforcement. This architecture ensures that large-scale, reliable data sharing can be achieved with minimal storage overhead and robust traceability, even under challenging post-disaster conditions.

Given the storage limitations of RVs and the large amount of shared data, the system uses IPFS for optimized data storage. This means full nodes do not need to store the entire blockchain. Instead, the block body contains only Hash pointers to data stored in IPFS, managed by GSs and the TA, effectively reducing storage needs while ensuring data accessibility.

3.2 Consensus protocol

Due to the openness of post-disaster rescue networks, GSs and RVs are at risk of attacks. Consensus algorithms play a crucial role in blockchain technology, allowing different nodes in the network to reach a distributed consensus on transactions. Currently, there are several mainstream consensus algorithms, including PoW, PoS, DPoS, PBFT, and PoA.

In the following, the basic concepts of these

consensus protocols will be introduced one by one, and the reasons why they are suitable (or unsuitable) for disaster scenario with fragile or no network connectivity will be explained.

1) PoW

The core idea of the PoW consensus algorithm^[19] lies in the fact that nodes need to explore specific random numbers by solving complex mathematical problems. During this process, the node that successfully finds the correct answer first will be granted the right to record accounts and be able to receive corresponding rewards. From the perspective of decentralization, PoW undoubtedly achieves a relatively high degree of decentralization because, in theory, any node can freely join the network. However, the PoW algorithm has significant drawbacks and consumes an extremely large amount of computing resources. For example, in the Bitcoin network, numerous nodes need to constantly perform Hash operations in order to compete for the right to record transactions, which requires a large amount of electricity and high-performance computing equipment. Moreover, the time it takes for PoW to reach a consensus is relatively long.

This might be acceptable in some conventional scenarios, but in disaster relief scenarios where resources are limited and a rapid response is required, this feature becomes extremely impractical. During the rescue process in the disaster-stricken area, every second is of vital importance. Prolonged consensus waiting may lead to serious consequences, such as the delayed transmission of rescue information and the delay in the allocation of rescue resources, thereby greatly affecting the efficiency and effectiveness of the rescue.

2) PoS

The PoS consensus algorithm^[20] has a different operating mechanism compared with PoW. When allocating rewards, the PoS consensus algorithm mainly considers factors such as the quantity of tokens held by nodes and the holding period. This allocation method reduces the demand for computing resources to a certain extent, because nodes do not need to engage in large-scale computing competitions as in PoW.

Meanwhile, due to the reduction of calculation links, its consensus time is shortened accordingly. However, the PoS algorithm is not perfect either. It may lead to the concentration of resources. This is because accounts holding more tokens tend to receive more rewards. Over time, these accounts will accumulate more resource advantages, thereby causing an increasingly unbalanced distribution of resources in the network.

In the disaster-stricken area where the network environment is unstable, this trend of resource concentration may further intensify the instability of the network. For instance, some RVs or GSs, due to the relatively small initial token allocation, have difficulty obtaining sufficient resource support during the subsequent network operation process, thereby affecting their data sharing and collaboration capabilities in the rescue network. In addition, PoS may also have the issue of unfair initial token distribution, especially in scenarios where RVs frequently change in disaster-stricken areas. Due to the high liquidity of RVs, newly joined RVs may have difficulty obtaining fair token distribution opportunities, which will to some extent affect their enthusiasm and effectiveness in participating in the network consensus.

3) DPoS

The DPoS consensus algorithm^[21] is further optimized and improved based on PoS. Its main innovation point lies in improving the consensus efficiency by electing a certain number of accounting representatives. In the DPoS algorithm, nodes in the network elect accounting nodes representing themselves through voting. These elected accounting representatives will be responsible for handling transactions in the network and reaching consensus. This approach centralizes the accounting power to a certain extent, thereby being able to increase the speed of consensus. However, the DPoS algorithm also has some potential problems. First of all, its election process may take too long. In disaster area rescue operations that require rapid deployment and response, this process may delay the best time for rescue. For instance, in the early stage of building the rescue network in the disaster-stricken area, RVs and GSs

need to quickly establish an effective blockchain network to ensure the sharing and collaboration of rescue data. If the election process of DPoS is overly complicated, it will seriously affect the progress of rescue work. Secondly, in the DPoS algorithm, some nodes may lack voting incentives, which may lead to a low voting participation rate and thereby reduce the consensus efficiency of the entire network.

In the rescue scenarios of disaster-stricken areas, as the task priorities of each RV and GS may vary, some nodes may believe that participating in the voting to elect accounting representatives does not bring them direct benefits or is of little help to the rescue work, and thus choose not to actively participate in the voting. This will have an adverse impact on the effective operation of the DPoS algorithm in the rescue network of disaster-stricken areas.

4) PBFT

The PBFT^[22] consensus algorithm is designed to achieve consensus in distributed networks, addressing the Byzantine Generals Problem. This mechanism allows the system to remain functional and consistent as long as no more than one-third of the nodes are malicious or faulty.

While PBFT can maintain system operation when some nodes fail, it relies on intensive message exchanges among all participants, causing communication complexity to increase quadratically as the network size grows. In post-disaster rescue networks, where the number of participating nodes is often large and network connectivity may be unstable or bandwidth-limited, this high communication overhead makes PBFT impractical. Therefore, PBFT is generally unsuitable for large-scale, resource-constrained, and dynamic disaster area environments.

5) PoA

The PoA^[23] consensus algorithm relies on a carefully selected group of validators to generate new blocks and verify transactions. The reason why these validators can obtain such privileges is usually that they have a reliable reputation or a confirmed identity. The main advantages of the PoA mechanism are reflected in efficient energy utilization and excellent scalability. Because it avoids the competition of computing power,

it can significantly reduce the waste of resources. In application scenarios such as rescue operations in disaster-stricken areas, the efficient utilization of resources is particularly important. For example, the energy supply of RVs is often limited. The adoption of the PoA consensus algorithm can reduce energy consumption to a certain extent, extend the operating time of RVs, and at the same time, its good scalability can also adapt to the scale changes of the rescue network in disaster-stricken areas at different stages. However, the traditional PoA algorithm also faces some challenges, most prominently its heavy reliance on selected validators, which leads to centralization and security vulnerabilities. If these selected validators malfunction, are attacked, or engage in malicious behavior, the entire blockchain system supporting the disaster area rescue network could be severely affected, potentially resulting in rescue data loss, tampering, or transaction errors, thereby endangering the smooth progress of rescue work and the effectiveness of rescue results.

Therefore, this article improves the PoA consensus algorithm by selecting GSs as validators of PoA for block generation and transaction verification. Uniquely, SEDS-BOR dynamically updates the credibility values of each GS based on their observed behavior. Only GSs with consistently high credibility are eligible to produce blocks, which mitigates the risks of centralization and malicious behaviors, and ensures efficient, secure, and resilient consensus in the context of emergency rescue operations.

4 SEDS-BDR

4.1 System initialization

In the network initialization stage, the traditional PoA consensus algorithm designates a group of authoritative nodes as validators responsible for generating blocks. However, over-reliance on this set of validators may lead to centralization and security risks. If some authoritative nodes are attacked, damaged by malicious attackers, or malfunction, it will endanger the security and stability of the entire

blockchain network. To mitigate these risks and enhance blockchain security, a set of blocks generated and selected based on the reputation value allocation architecture (see Fig. 1) is introduced as the PoA preselection. These reputation values serve as behavioral proof for each GS and are updated based on the behavior of the nodes after each consensus round. Honest and cooperative behaviors will gradually increase the reputation value of nodes over time, while malicious or uncooperative behaviors will lead to a significant decrease in reputation value. Only authoritative nodes with high credibility values are eligible to serve as block generators, thereby ensuring that only trusted nodes can contribute to the consensus process.

First, GSs are selected to act as validators and randomly divided into two roles: block generators and block generator candidates. Each GS is assigned an initial reputation value, which is updated according to its behavior in the consensus process and is used to select block generators in the next round. The reputation update rule is given by

$$R_i(t+1) = R_i(t) + \Delta R_i \quad (1)$$

where $R_i(t+1)$ represents the updated reputation value of the i th GS at round t , and ΔR_i represents the change in reputation value. To encourage GSs to act honestly and penalize misconduct during the consensus process, a reputation reward and punishment mechanism is implemented. If a GS successfully generates a new block that is validated by other nodes, both the block generator and the validators will obtain an increase in reputation value. The reputation rewards are denoted as C_{gen}^r for the block generator and C_{ver}^r for the validators, respectively. Let ΔR_i represent the reputation increment of the i th node, if node i is the generator $\Delta R_i = C_{\text{gen}}^r$, and if node i is a validator $\Delta R_i = C_{\text{ver}}^r$. Conversely, if the i th GS fails to generate a block in the consensus round or generates an incorrect block, its reputation value will be reduced by a penalty constant C_{gen}^p in this case, the reputation increment $\Delta R_i = C_{\text{gen}}^p$, i. e., a decrease of C_{gen}^p . This penalty is intended to discourage improper block-generation behavior.

Additionally, to encourage GSs to stay online and

ensure network activity and stability, GSs that remain online will receive a reputation reward C_{on}^r . In contrast, block generators that go offline will suffer a reputation penalty C_{off}^p . Here, $\Delta R_i = C_{\text{on}}^r$ if the i th node remains online, $\Delta R_i = C_{\text{off}}^p$ if the i th node goes offline.

At the end of each consensus round, all GSs are re-ranked based on their reputation values. The top-ranked GSs will be selected as block generators for the next cycle. If multiple GSs have the highest reputation values during the evaluation period, the block generators for the next cycle will be randomly chosen from among them to ensure fairness and transparency in the consensus process.

4.2 Consensus process

When the j th RV discovers information in a disaster area and intends to share data, it generates a corresponding transaction T_j and broadcasts it. The transaction format is shown as

$$T_j = (P_j, M_j, T, M, S_j) \quad (2)$$

where P_j is the public key of the j th RV that publishes the information, M_j represents the message type (rescue request or road condition) for location (x_j, y_j) . T is the current transaction timestamp, M represents the rescue message released by the j th RV, and S_j is the signature generated by the private key of the j th RV.

A group of block generators from the GSs is responsible for collecting and verifying all submitted transactions. They add valid transactions to the transaction pool based on the weight of the location information contained in the transactions. Blocks are generated by the group of GSs in a random order. If the selected GS fails to generate a block in its turn (e. g., due to being offline), the system automatically shifts to the next GS. After each round is completed, the order of the block generators is updated.

4.3 Priority packaging based on weight

In SEDS-BDR, the TA plays a crucial role, responsible for periodically setting and updating the weights of each grid, as well as publishing and broadcasting this weight information.

Initially, the TA sets an initial value for the weight

of each grid in the array. Subsequently, within each fixed time interval τ , the TA processes the newly verified transaction information and updates the grid weights. The weight information structure is given by

$$W_I = (W, T_s, P_{TA}, S_{TA}) \quad (3)$$

where W contains the weights of all grids in the disaster area, stored as a two-dimensional (2D) array $W = (l_{1,1}, l_{1,2}, \dots, l_{1,y}, \dots, l_{x,y})$, and $l_{x,y}$ denotes the weight of the grid at coordinates (x, y) . T_s is the timestamp of the current grid weight information release, P_{TA} is the public key of the TA, and S_{TA} is the signature generated by the TA.

The method of updating grid weights upon receiving rescue requests and road condition information is further illustrated as follows.

Case 1 When the transaction information type is a rescue request, GSs increase the weights of each grid on the shortest path from the TA to the rescue request location, with each weight increasing by β ($\beta > 0$). This adjustment is designed to speed up the arrival of rescue forces at the target location. The weight of the shortest path location is set using the following function $f(x, y)$

$$f(x, y) = \begin{cases} \alpha + \beta; & 0 \leq x < x_m, y = 0 \\ \alpha + \beta; & x = x_m, 0 < y \leq y_n \\ \alpha; & \text{otherwise} \end{cases} \quad (4)$$

where (x_m, y_n) denotes the rescue request position with an existing weight α .

Case 2 When the transaction information type is road conditions, the weight of the grid at the reported location will increase by θ ($\theta > 1$), and the weights of the surrounding grids will each increase by $\theta - 1$ and $\theta - 2$. The method is detailed as follows, where (x_p, y_q) represents the location of the road rescue information, and its weight is denoted by α . Let k and l be the horizontal and vertical offsets relative to the location (x_p, y_q) . When $|k| + |l| = 1$, it represents the points in the first surrounding layer; when $|k| + |l| = 2$, it represents the points in the second surrounding layer. The weight update function $f(x_p + k, y_q + l)$ is defined as

$$f(x_p + k, y_q + l) = \begin{cases} \alpha + \theta; & |k| + |l| = 0 \\ \alpha + \theta - 1; & |k| + |l| = 1 \\ \alpha + \theta - 2; & |k| + |l| = 2 \end{cases} \quad (5)$$

Case 3 When a rescue request path lacks some key location information, the weights of the grids at these key locations will be set to γ ($\alpha < \theta < \gamma$), highlighting their importance in the rescue operation.

After these weights are updated, the TA generates new weight information at the end of each time interval τ and broadcasts it. GSs receive this information and use the TA's public key to verify its authenticity. These updated weight information are stored locally by RVs and used when sharing information and planning rescue routes.

5 Performance evaluation

To evaluate the performance of the proposed weight-priority transaction packaging algorithm, simulation experiments are conducted on Windows 11 system equipped with an Intel®Core™ i5-12500H central processing unit (CPU) and 16 GB of random access memory (RAM). These experiments are implemented in Python using the PyCharm platform, specifically to simulate communication delays and block generation frequencies in disaster-stricken areas.

Table 1 presents the simulation parameters, which include the number of vehicles, their relative speeds, and positions. The simulation is carefully designed to adhere to the protocols and models that are likely to be used in real-world scenarios.

Table 1 Network simulation parameter

Parameter	Setting
Number of TA	1
Number of GSs	20
Number of RVs	400
Protocol	IEEE 802.11p
C_{ver}^r	2
C_{gen}^r	5
C_{on}^r	1
C_{gen}^p	5
C_{off}^p	1

The weight priority transaction packaging algorithm is evaluated by setting a maximum block size limit of 1 MB, with transaction sizes ranging from 500 B to

1 000 B^[24]. The disaster area is divided into 5 m × 5 m grid cells, and relief distribution points are established near reliable institutions. In this setup, GSs responsible for block generation prioritized transactions from the pending pool based on their weight, particularly focusing on urgent transactions, to ensure that critical rescue information is rapidly integrated into newly generated blocks.

In Fig. 2, a comparative analysis of the efficiency of two blockchain technologies over a 200 s simulation period is presented: one using the weight-priority strategy and the other employing a traditional time-ordered transaction packaging algorithm. The comparison is centered on the number of blocks generated when processing rescue requests at varying distances. As shown in Fig. 2, the weight-priority strategy, which prioritizes more urgent information by assigning higher weights, achieves the same rescue path confirmation with fewer blocks compared to the traditional algorithm. Moreover, greater efficiency in handling rescue requests from distant locations is demonstrated by SEDS-BDR. This is crucial in disaster scenarios where timely responses to distant rescue signals are essential. Through the optimization of transaction packaging priorities, swift processing of these signals is ensured, indicating that in blockchain applications for disaster rescue, the adoption of a weight-priority strategy is an effective method to enhance response speed and efficiency.

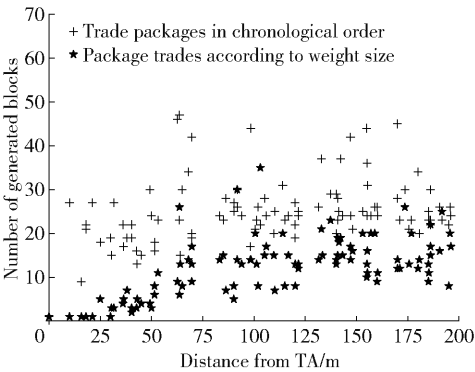


Fig. 2 Number of blocks generated by requests for rescue locations at different distances

Fig. 3 illustrates the trend of network communication time with an increasing number of RVs. In this

simulation, air is adopted as the signal propagation medium, and the signal propagation speed is configured to approximately 3×10^8 m/s. To guarantee data accuracy, the experiment is conducted 100 times, and the average and standard deviation of the communication time are calculated. The results demonstrate that network communication time ranges between 600 ms and 800 ms, which meets the communication requirements for disaster rescue operations. Additionally, the standard deviation of the communication time stays within 100 ms, confirming the high stability of network performance across varying numbers of RVs.

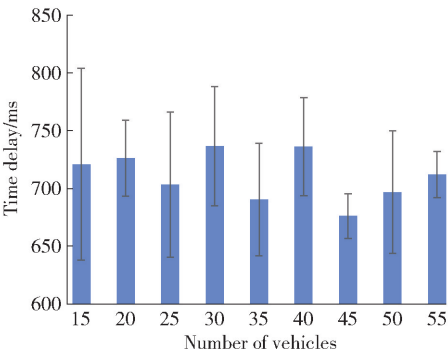


Fig. 3 Simulation of network communication time delay

Fig. 4 compares the time required to generate a single block across different consensus algorithms under varying numbers of nodes.

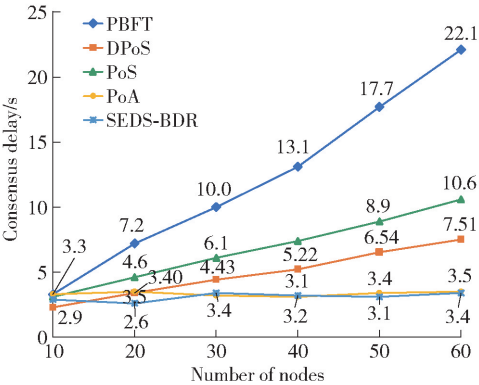


Fig. 4 Comparison of the time required to generate a single block across different consensus algorithms

From Fig. 4, the results demonstrate that the SEDS-BDR significantly outperforms existing popular consensus algorithms in terms of efficiency. The PBFT protocol requires complex message exchanges and

multiple rounds of confirmation, while DPoS and PoS involve selecting block producers through a voting process, which is time-consuming. Consequently, these protocols take longer to reach consensus compared to PoA. Although the difference in consensus time between the improved reputation-based PoA algorithm and the traditional PoA algorithm is minimal, SEDS-BDR enhances the process by ensuring the reputation and quality of the participants involved in the consensus.

Fig. 5 illustrates the changes in reputation values for both legitimate and malicious nodes across different consensus rounds.

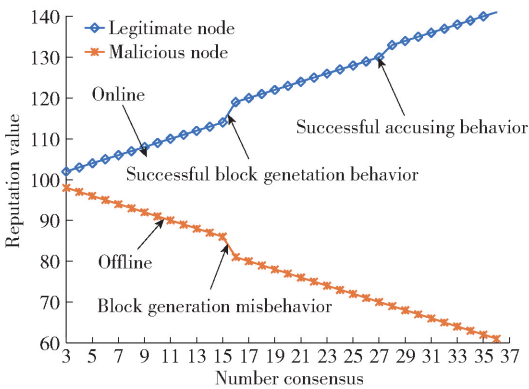


Fig. 5 Changes in the reputation values of both legitimate and malicious nodes

In Fig. 5, legitimate nodes remain consistently online and actively participate in each round of the consensus process, resulting in a steady increase in their reputation values. On the other hand, malicious

nodes, which frequently go offline during consensus rounds, experience a decline in their reputation. Over time, as shown in Fig. 5, the reputation gap between legitimate and malicious nodes widens. This growing disparity underscores the effectiveness of the reputation system in distinguishing between legitimate and malicious behavior. As a result, well-behaved nodes gain more opportunities to participate in the consensus process, while poorly-behaved nodes are gradually excluded, thereby preserving the overall integrity and health of the network.

Based on Table 2, SEDS-BDR offers several advantages over other blockchain-based vehicular data-sharing systems. Compared to consensus algorithms like DPoS and Tendermint, improved PoA mechanism provides significant benefits, including lower economic costs, fewer required bookkeeping nodes, and enhanced data security and efficiency. Furthermore, unlike systems such as lightweight vehicular blockchain for secure (LVBS) data sharing^[8] and energy-efficient and partition-tolerant blockchain based secure (RescueChain) information sharing^[9], which primarily focus on storing transaction information, SEDS-BDR adopts a different approach by directly storing shared data within the blocks, rather than just transaction details. This method significantly improves data accessibility and processing efficiency, which is particularly crucial in rescue operations and emergency response scenarios where quick access to and processing of shared data are essential.

Table 2 Comparison of existing work

Technical solutions or systems	Consensus algorithm	Economic cost	Data security	Block storage content
LVBS	DPoS	Relatively few	High	Transactions
RescueChain	Tendermint	Relatively many	Relatively high	Transactions
SEDS-BDR	Improved PoA	Few	High	Sharing data

Finally, experiments are conducted using IPFS to measure download time across varying data sizes. As presented in Table 3, the results show that download time stay below 0.5 s even for data sizes up to 1 MB. Given the challenges of unstable networks and limited resources in disaster rescue scenarios, these results are deemed acceptable and confirm the suitability of IPFS for such environments.

Table 3 Download time in different data sizes using IPFS

Type	Size/MB	Download time/s
One IPFS peer	1.0	[0.25 ± 0.05, 0.49 ± 0.05]
	0.5	[0.13 ± 0.02, 0.24 ± 0.02]
Two IPFS peers	1.0	[0.14 ± 0.05, 0.24 ± 0.05]
	0.5	[0.07 ± 0.02, 0.24 ± 0.02]

6 Conclusions

In this study, an efficient data sharing solution for vehicular networks in disaster rescue scenarios was introduced, utilizing a blockchain architecture with a reputation-based PoA consensus algorithm. This framework ensures secure, real-time recording, and storage of shared information. To further accelerate rescue operations, a weight-priority strategy for transaction packaging within the transaction pool is developed. Simulation experiments demonstrate the effectiveness of SEDS-BDR, highlighting significant improvements in both time savings and rescue efficiency.

In the future, deep learning techniques will be explored to optimize the weight-priority algorithm on the blockchain, so as to further improve rescue efficiency. Cooperation with the Internet of things will also be carried out to solve the security problems in vehicular networks.

References

- [1] CRED. 2023 Disasters in numbers. Brussels, Belgium: CRED, 2024.
- [2] LIU B, AYAZ F, ANH H D, et al. UAV integrated Internet-of-vehicle (IoV) system for flooding monitoring and rescue. Proceedings of the 2022 International Conference on Autonomous Unmanned Systems (ICAUS'22), 2022, Sep 21 – 24, Xi'an, China. Singapore: Springer Nature Singapore, 2022: 1004 – 1014.
- [3] BANSOD S, RAGHA L L. Blockchain impact of security and privacy in digital identity management. RAO U P, SHUKLA P K, TRIVEDI C, et al. (eds) Blockchain for Information Security and Privacy. Auerbach Publications, 2021: 275 – 291.
- [4] CUI J, OUYANG F Q, YING Z B, et al. Secure and efficient data sharing among vehicles based on consortium blockchain. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(7): 8857 – 8867.
- [5] LU Y L, HUANG X H, ZHANG K, et al. Blockchain empowered asynchronous federated learning for secure data sharing in Internet of vehicles. IEEE Transactions on Vehicular Technology, 2020, 69(4): 4298 – 4311.
- [6] KOUICEM D E, BOUABDALLAH A, LAKHLEF H. An efficient and anonymous blockchain-based data sharing scheme for vehicular networks. Proceedings of the 2020 IEEE Symposium on Computers and Communications (ISCC'20), 2020, Jul 7 – 10, Rennes, France. Piscataway, NJ, USA: IEEE, 2020: 6p.
- [7] SU Z, WANG Y T, XU Q C, et al. LVBS: lightweight vehicular blockchain for secure data sharing in disaster rescue. IEEE Transactions on Dependable and Secure Computing, 2022, 19(1): 19 – 32.
- [8] WANG Y T, SU Z, XU Q C, et al. Lifesaving with RescueChain: energy-efficient and partition-tolerant blockchain based secure information sharing for UAV-aided disaster rescue. Proceedings of the 2021 IEEE Conference on Computer Communications (INFOCOM'21), 2021, May 10 – 13, Vancouver, Canada. Piscataway, NJ, USA: IEEE, 2021: 10p.
- [9] KARIM S M, HABBAL A, CHAUDHRY S A, et al. BSDCE-IoV: blockchain-based secure data collection and exchange scheme for IoV in 5G environment. IEEE Access, 2023, 11: 36158 – 36175.
- [10] TONG W, DONG X W, ZHANG Y S, et al. TI-BIoV: traffic information interaction for blockchain-based IoV with trust and incentive. IEEE Internet of Things Journal, 2023, 10(24): 21528 – 21543.
- [11] ZHANG X H, ZHANG J S, GAO J B, et al. A sharding blockchain-based UAV system for search and rescue missions. Frontiers of Computer Science, 2025, 19(3): Article 193805.
- [12] WANG H, WANG C P, ZHOU K, et al. TEBChain: a trusted and efficient blockchain-based data sharing scheme in UAV-assisted IoV for disaster rescue. IEEE Transactions on Network and Service Management, 2024, 21(4): 4119 – 4130.
- [13] TROJANOWSKI K, MIKITUK A, GRZESZCZAK J, et al. Complete coverage and path planning for emergency response by UAVs in disaster areas. Proceedings of the 2023 International Conference on Computational Collective Intelligence (CCCI'23), 2023, Sep 27 – 29, Budapest, Hungary. Cham: Springer Nature Switzerland, 2023: 647 – 659.
- [14] DIAO Q F, ZHANG J F, LIU M, et al. A disaster relief UAV path planning based on APF-IRRT* fusion algorithm. Drones, 2023, 7(5): Article 323.
- [15] JAVED S, HASSAN A, AHMAD R, et al. UAV trajectory planning for disaster scenarios. Vehicular Communications, 2023, 39: Article 100568.
- [16] HUSNAIN G, ANWAR S, SHAHZAD F. An enhanced AI-enabled routing optimization algorithm for internet of vehicles (IoV). Wireless Personal Communications, 2023, 130(4): 2623 – 2643.
- [17] ZHENG J B, DING M H, SUN L, et al. Distributed stochastic algorithm based on enhanced genetic algorithm for path planning of multi-UAV cooperative area search. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(8): 8290 – 8303.
- [18] DWIVEDI S K, AMIN R, VOLLALA S. Smart contract and IPFS-based trustworthy secure data storage and device authentication scheme in fog computing environment. Peer-to-Peer Networking and Applications, 2023, 16: 1 – 21.
- [19] QI L L, TIAN J F, CHAI M J, et al. LightPoW: a trust based time-constrained PoW for blockchain in internet of things. Computer Networks, 2023, 220: Article 109480.
- [20] LI A Y, WEI X H, HE Z. Robust proof of stake: a new consensus protocol for sustainable blockchain systems. Sustainability, 2020, 12(7): Article 2824.
- [21] SAAD S M S, RADZI R Z R M. Comparative review of the blockchain consensus algorithm between proof of stake (POS) and delegated proof of stake (DPOS). International Journal of Innovative Computing, 2020, 10(2): DOI: 10.11113/ijic.v10n2.272.
- [22] MESHCHERYAKOV Y, MELMAN A, EVSUTIN O, et al. On performance of PBFT for IoT-applications with constrained devices. arXiv Preprint, arXiv:2104.05026, 2021.
- [23] SONG J, BAI F H, ZHU Y, et al. An improved-PoA consensus algorithm for blockchain-empowered data sharing system. Proceedings of the 4th Blockchain and Internet of Things Conference (BIOTC'22), 2022, Jul 8 – 10, Tokyo, Japan. New York, NY, USA: ACM, 2022: 128 – 134.
- [24] HUI Y L, SU Z, LUAN T H, et al. A game theoretic scheme for optimal access control in heterogeneous vehicular networks. IEEE Transactions on Intelligent Transportation Systems, 2019, 20(12): 4590 – 4603.

(Editor: Wang Xuying)