Trustworthy VANET: Hierarchical DAG-Based Blockchain Solution with Proof of Reputation Consensus Algorithm

Zhongxu Dong, Huanyu Wu, Zongyao Li, De Mi, Olaoluwa Popoola and Lei Zhang

Abstract—**The new paradigm edge computing demonstrates significant advantages in quality of service including low latency and bandwidth efficiency when deployed in autonomous vehicle applications. However, deploying edge computing in the context of a widely used vehicular ad hoc network (VANET) leads to potential security issues. Blockchain is a promising technology to solve security and trust issues with the identically distributed structure as edge computing and VANET, but its efficiency and scalability limitations constrain the usage in VANET. This paper proposes a hierarchical Directed Acyclic Graph (DAG)-based blockchain architecture to overcome these integration challenges. The hierarchical architecture divides the whole system into multiple local chains according to geographical regions to improve scalability while also maintaining a global chain to facilitate security. The DAG-based blockchain structure can better support simultaneous operations to further improve scalability and efficiency. In addition, in recognition of VANET's unique requirements, we design a reputation-based consensus for tip selection algorithm (TSA) to replace the widely used Proof-of-Work TSA in DAG, which ensures security in VANET without heavy computational burden. Our experimental simulations reveal that our proposed scheme not only fortifies security but also elevates scalability and efficiency.**

Index Terms—**VANET, Blockchain, Directed Acyclic Graph (DAG), Hierarchical Architecture, Reputation Consensus Model**

I. Introduction

As an emerging technology in the autonomous vehicle (AV) domain, cloud computing has been considered to offer real-time analysis and processing capabilities to enhance vehicle environmental perception and decision-making. However, due to the overreliance on the centralized communication structures facilitated through the Radio Access Network (RAN), contemporary cloud computing is under the threat of single-point attacks and the constraints of bandwidth. To address these challenges, there is an emerging interest in harnessing the potential of distributed edge computing (EC) for the AV ecosystem. In EC, edge computing nodes (ECN) offload a significant portion of the computational tasks within the core network to the network edge, thereby circumventing communication delays between the RAN, User Plane Function (UPF), and Core Network (CN). Meanwhile, through parallel computation across multiple nodes, the computational resource gap between edge computing systems and cloud computing is narrowed [1].

At present, a growing applications emphasizes the benefits of incorporating distributed Vehicle Ad-hoc Networks (VANETs) in conjunction with edge computing, as opposed to conventional centralized cloud systems, especially in scenarios where low-latency performance is imperative [2]. However, data sharing in an open and highly dynamic ad-hoc network faces security and privacy threats. Typically, solutions to the security issues in VANET rely on a fully trustworthy Certification Authority (CA) to certify entities participating in distributed systems [3]. Yet, schemes employing authentication authorities have inherent flaws, including vulnerabilities to single-point attacks and challenges posed by the increasing number of AVs to the processing capabilities of CA. [4]. Therefore, security and trustworthy platform tailored for VANET scenarios integrated with edge computing are needed.

Blockchain technology, with its intrinsic properties of decentralization, immutability, and traceability, is perceived as a solution that can address the security challenges of distributed systems while circumventing the drawbacks associated with CA. A primary obstacle of applying blockchain in VANET scenarios stems from the global single-chain structure. This design results in a single-threaded pipeline operation across all nodes, where every participant must await the completion of the preceding operation before initiating the next. Consequently, when the network has a vast number of nodes, they experience long waiting times to issue transactions, and the confirmation of these transactions necessitates extensive communication or intense computational power competition. Therefore, in addressing the challenges posed by the global single-chain structure, we contemplate the adoption of two optimization strategies: a hierarchical blockchain architecture and a Directed Acyclic Graph (DAG)-based blockchain.

In the hierarchical blockchain architecture, nodes within the VANET are organized into several local clusters based on geographical information. Nodes within each cluster maintain a local chain (LCs). The ECNs within these local clusters collectively form a global cluster, wherein a global chain (GC) is maintained. The information collected by the basic units in VANET, AVs, determines the consensus scope based on its impact radius. For instance, data such as vehicle position and speed, which influence short-term autonomous driving strategies, only need to be aware within the LC of the data

Zhongxu Dong, Huanyu Wu, Zongyao Li, Olaoluwa Popoola and Lei Zhang (corresponding author) are with the James Watt School of Engineering, University of Glasgow, G12 8QQ, U.K.; email:{z.dong.2, h.wu.3, l.zongyao.1}@research.gla.ac.uk; {Olaoluwa. Popoola, Lei. Zhang}@glasgow.ac.uk.

De Mi is with the College of Computing, Birmingham City University, Birmingham, B4 7XG, U.K.; email:{de. mi@bcu.ac.uk}

collector. On the other hand, data with a global scope, such as vehicle registration information, is uploaded to GC, allowing all nodes within the VANET to query it. This approach distributes participants across different chains based on their requirements, thereby reducing the complexity of each chain and enabling the network to accommodate a larger number of participating nodes.

The adoption of a DAG-based blockchain is motivated by the inherent ability of graphs to naturally support parallel operations more than chains, allowing DAG-based blockchains to achieve higher throughput [5]. Additionally, most popular DAG projects, such as IOTA, employ a Proof-of-Work (PoW) consensus algorithm to combat spam transaction and attacks. However, in VANET, given the requirements for vehicle registration and the fact that both vehicles and edge computing devices are registered or certified, malicious nodes could exist but are manageable, characterizing it as a permission network [6]. Consequently, the Poof of Reputation (PoR) mechanism is proposed in lieu of PoW to minimise the energy consumption during the consensus process.

By integrating the scalability strengths of hierarchical blockchains with the efficient concurrent transaction advantages of DAG-based blockchains, the challenge of applying blockchain technology to VANET scenarios can be effectively addressed. This makes blockchain technology a viable solution for ensuring communication security in VANET that leverages edge computing capabilities. The contributions of this paper can be summarized as follows:

- A hierarchical DAG-based blockchain architecture is proposed. This architecture consists of one GC and multiple LCs. Improved scalability of the blockchain by decoupling global consensus into a hierarchical consensus.
- Building upon the DAG-based blockchain, and considering the specific application scenarios and requirements of VANET, a vehicle reputation model is introduced to enhance the TSA capability against Byzantine attacks, while the communication security is ensured and the energy consumption of the system is reduced.
- Modelling the consensus time delay of hierarchical DAG-based blockchain. Simulation results show that the consensus time delay of the proposed architecture is significantly lower than single-chain blockchain. The reputation model is developed and the ability of the model to shield false information is verified through simulation.

II. System Architecture Design

A. Hierarchical Blockchain Architecture

This section proposes a hierarchical blockchain architecture, introduces the data sharing mechanism within the architecture and presents the security analysis against attacks in blockchains. The hierarchical system structure is illustrated in Fig. 1, which comprises two layers, the Local Chain (LC) and the Global Chain (GC). The whole system consists of one GC and multiple LC which interact with the GC. Our structure reduces the communication overhead and improves scalability by disseminating data and achieving consistency within different LCs instead of the whole system. We provide a detailed description in the following sections.

1) Local Chain: The LC layer is defined by the communication range of edge computing-capable RAN nodes within a road unit, such as an intersection or a section of a street. Within each LC, a DAG-based blockchain ledger is generated and maintained by the RAN nodes and all AVs within the communication range. The local ledger records data with a smaller range of influence, such as vehicle status information. The shared data is encapsulated by the AVs in a transaction format and transmitted to neighboring ECNs. This provides the ECNs with the ability to sense road conditions and generate dispatch instructions. The format of the sharing information f

$$TX^{LC} =< H(\sigma_f), I, Url, S_f, Sig_{AV}, Sig_{ECN} >$$

where I is the identification information array of f, $\sigma_f = \{I, Url, H(f)\}$ is the identification vector of f. Url is the storage address of data, $H(\sigma_f)$ is the hash value obtained by hashing the identification vector, S_f is the range of influence of data, Sig_{AV} and Sig_{ECN} are the signatures of AVs and ECNs for the transaction, respectively. Only the hash of the data storage index rather than the metadata itself is recorded on the chain to reduce the communication of disseminated sites in the network.

2) Global Chain: The GC is created and managed by the ECNs of all LC and a public monitor node (MN) established by the supervisory body. It stores information that has an impact on multiple or all road units, such as the vehicle reputation value. Specifically, if the $S_f \geq \theta$, the ECN will encapsulate the message as

$$TX^{GC} =< H(\varphi_f), I, Url, S_f, Sig_{AV}, Sig_M >$$

where $\varphi_f = \{\sigma_f, E_{id}\}$ is the ID of the ECN that encapsulates the transaction, Sig_{ECN} and Sig_{MN} are the signatures of ECNs and MN.

B. Process of Data Sharing

Assuming that the vehicle v senses environmental information and we denote its own control data by f and it needs to share the data to the ECN K, the workflow of the system can be described by the following four steps.

1) *Data collection and uploading*. The process begins with v generating an identification vector σ_f for the data f, where the parameter Url designates the address of K. Following this, v signs σ_f using its private key and transmits it to K along with f.
2) *Data encapsulation and consensus on the LC chain.* Upon receiving the data from v, K begins by quantifying the data's impact range, denoted as S_f, with the assistance of I in σ_f. Following validation of Sig_{AV}, K encapsulates the data in the TX^{LC} format and broadcasts the transaction to the LC. Unlike traditional Proof-of-X (PoX) blockchains, nodes in a DAG-based blockchain do not compete for packing rights. Instead, sites accumulate their own weight based on the number of verifications they receive. Once the accumulated weight surpasses

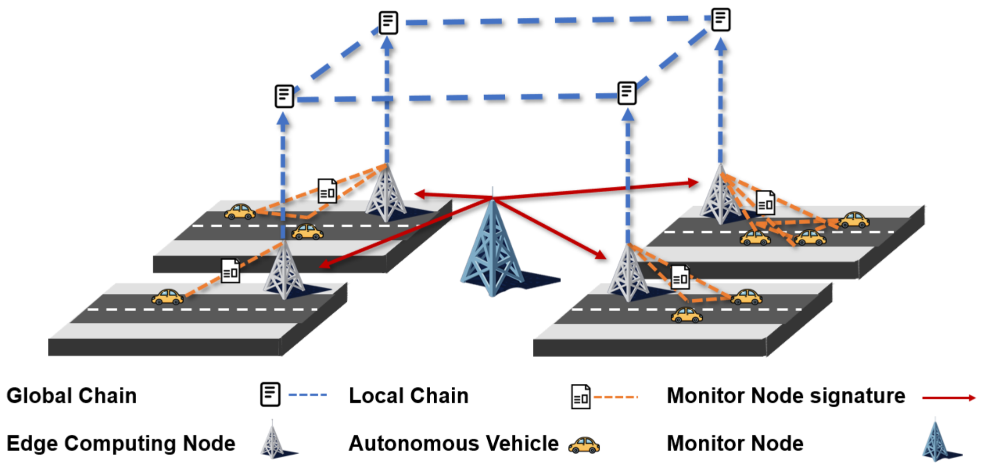

Fig. 1. Hierarchical wireless network framework

a certain threshold, the transaction is automatically confirmed, otherwise it becomes an orphan transaction. This lightweight consensus mechanism helps to avoid unnecessary computational power wastage that arises from the competition for packing rights. In addition to the data from v, in this step, K will also process the data obtained from the scheduling instructions based on the processing of the data uploaded by AV and the data downloaded from the GC chain. These two types of data have the same processing flow as the data shared by AV.

3) *Determining the range of influence.* The ECN will check the data impact range of the TX^{LC} that is globally acknowledged in the LC. If $S_f \leq \theta$, the data will only achieve consensus within LC. Otherwise, the RSU that collects this data will issue a transaction within the GC scope, ensuring the data is recorded across the entire network. When other LCs require this data, the RSU can query the data in GC and issue a new transaction in LC. In this way, data can achieve migration between shards.

4) *Data encapsulation and consensus on GC chains.* Similar to the process in the LC, the ECNs encapsulate the data that requires network-wide dissemination into the TX^{GC} format and broadcast it to the cluster. Notably, all TX^{GC} must undergo verification by a common MN and have the MN's digital signature appended. Now, the data f has been successfully collected from the end-of-pipe and stored network-wide.

III. DAG-based Blockchain with Improved Consensus Mechanism

In some of the most popular DAG-based blockchain instances such as IOTA, it uses PoW for each incoming transaction to verify two previous tips. PoW is resistant to Sybil attacks and 51% attacks but consumes a significant amount of computational resources. VANET could be regarded as a permission network, where malicious behaviours and attacks including Sybil attacks exist but are controllable due to the required registration of each vehicle and the limited amount of edge devices and vehicles. Therefore, we propose a reputation-based optimization on TSA, which makes sites issued by malicious nodes extremely difficult to confirm to achieve network reliability, security and trustworthiness without the expensive mining procedure.

A. Vehicular Reputation Model

The vehicular reputation model serves as a record of a vehicle's historical behavior within VANET. Specifically, the reliability of sites published by a vehicle will be quantitatively assessed by subsequent vehicles chosen to verify the transaction, and this assessment value is employed as the weight for the DAG edges. Considering the feasibility and efficiency of practical operations, this paper selects four parameters: the influence range of a transaction, effective transaction volume, participation degree, and authenticity of messages to establish a reliability score model(Formula (3)).

$$R = ln(\alpha S + \beta V + \gamma C + 1) \times RE \tag{1}$$

where α, β, γ all are non-negative regulators. S represents the influence range of a transaction. The damage of a Byzantine node's attack on the system is directly related to the influence range of the chain it attempts to affect. Therefore, introducing S allows for differentiated penalties for attacks of varying severity. V represents the effective transaction volume of a node, reflecting its historical reputation. C is the participation degree of the node, indicating the frequency with which the node participates in network sites. The introduction of C can increase the cost of malicious behavior and encourage regular nodes to participate in sites more actively. RE represents the reality of the message which is determined by the node's validation results for the transaction. When a malicious node launches an attack, its reliability score decreases. The reliability scores are stored as the edge weight of DAG. Fig. 2 represents the edge-weighted DAG that records the message reliability scores.

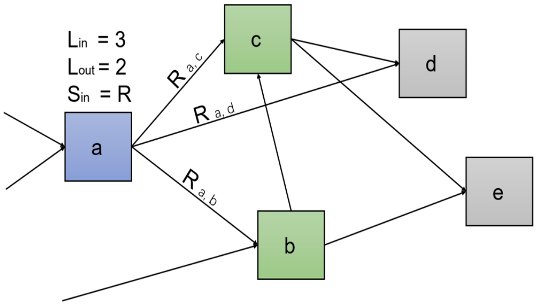

Fig. 2. edge-weighted DAG based on message reliability

Where L_{in} represents the number of incoming edges to a node, and L_{out} represents the number of outgoing edges from a node. A higher L_{in} value indicates that the transaction has been verified more times, indicating a higher acceptance level in the network. In the IOTA protocol, L_{out} is typically set to 2, meaning that a node needs to contribute a certain amount of computational power to validate two previous sites in the network before publishing a new one. S_{in} represents the weighted sum of the incoming edges, which represents the total reliability score obtained by the transaction. In the figure, purple sites ($W_v \geq m$) are confirmed sites, green sites ($W_v \in (1, m)$) are sites that have been selected and validated by subsequent sites in the network, and gray sites ($W_v = 1$) are newly added sites that have not been validated yet. $L_{in} = 3$ indicates that there are three subsequent sites selecting transaction a for validation, and Formula (3) provides the reliability scores $R_{a,b}$, $R_{a,c}$, and$R_{a,d}$ for transaction a. $L_{out} = 2$ means that the transaction follows the publishing rules defined by IOTA. The reliability score of transaction a is R_a. This model vividly illustrates the message on-chain process, DAG network rules, and the vehicle reputation values evolving with message reliability. The ECN dynamically updates the reputation values of nodes by continuously monitoring DAG parameters. The calculation method for reputation values is as follows

$$RU = \sum_{k=1}^{K} \frac{D_k S_k}{L_{in}^{k}} \tag{2}$$

where K denotes the number of all sites posted to the DAG-based blockchain by the vehicle in the current cycle. D_k denotes the amount of data in the messages recorded by the brow exchange. Equation (4) shows that the reputation value gradually increases with the publication of true and reliable messages and compliance with blockchain network rules, or decreases due to the provision of false messages and rule violations. When a node commits a malicious act, the node that subsequently verifies its posted sites will give a low reliability score, resulting in a decrease in reputation value.

B. Improved DAG Structure

In traditional chain-based blockchain structure, the operations could only be executed in a single-thread pipeline. The DAG-based blockchain, is originally proposed to solve scaling and concurrency issues. The graph structure is naturally more capable of concurrent operations, hence making it more suitable to be deployed in VANET scenarios where simultaneous operations are needed. DAG-based blockchain could be formally described as follows [7]:

DAG-based distributed ledger $\mathcal{G} = (\mathcal{E}, \mathcal{V})^{\dagger\ddagger}$, such that
$\mathcal{V} = \{u | u \in \tau \cup \mathcal{B} \cup \epsilon\}$,
$\mathcal{E} = \{(u, v) | u \leftarrow v \wedge (u \neq v) \wedge \{u, v\} \in \mathcal{V}\}$,
$\dagger : \forall u \leftarrow v \nRightarrow v \leftarrow u$,
$\ddagger$: *Assume that* $u_i \in u_1, u_2, \cdots, u_n \subset \mathcal{V}$,
$\forall i, j, \cdots, k \in [1, n-1], i \leq j \leq \cdots \leq k$, *then* $u_k \rightarrow u_i$, $\nexists u_i \rightarrow u_k$.

where "$\leq$" is the partial ordering relation, "$\rightarrow$" represents confirmation or verification from the tail to the head. The two properties are that 1) only one direction exists in the graph ($unidirectional^{\dagger}$), and 2) no loop exists ($acyclic^{\ddagger}$). These two properties guarantee that the nodes in the graph are appended-only and orderable, similar to the single-chain structure. As an underlying data structure, DAG could be integrated with different consensus. For instance, in IOTA [8], each node needs to validate two new sites in the DAG before issuing them. A successor site can only choose to validate a predecessor site.

At any time t, the graph G can be described by the adjacency matrix $M(t)$.

$$M(t) = \begin{bmatrix} m_{1,1} & m_{1,2} & \cdots & m_{1,v} \\ m_{2,1} & m_{2,2} & \cdots & m_{2,v} \\ \vdots & \vdots & \ddots & \vdots \\ m_{v,1} & m_{v,2} & \cdots & m_{v,v} \end{bmatrix}$$

The matrix $M(t)$ describes the DAG-based blockchain with v sites at time t. The adjacency matrix element $m_{i,j}$ represents the connection relationship between the edges at sites i and j, i.e. the direct verification relationship [9]. When $m_{i,j} = 1$, it means that transaction j directly chooses to validate transaction i and there is a directly connected directed edge between them. When $m_{i,j} = 0$, it means that there is no direct selection of the verification relationship between the sites. The mathematical representation of M reflects the fairness of the graph structure. The binary assignment of elements ensures equality between sites but also poses challenges in handling the site released by Byzantine nodes.

Therefore, in the vehicle reputation management mechanism proposed in this paper, the DAG-based blockchain structure is improved to a weighted directed acyclic graph $G < V, E, W_v.W_e >$, where V and E still represent sites and one-way verification relationships between sites. W_v represents the cumulative weight of sites and W_e represents the weight of edges, which is influenced by the vehicle reputation value. The weight assignment matrix $D(t)$ of the graph G is

$$D(t) = \begin{bmatrix} R_{1,1} & R_{1,2} & \cdots & R_{1,v} \\ R_{2,1} & R_{2,2} & \cdots & R_{2,v} \\ \vdots & \vdots & \ddots & \vdots \\ R_{v,1} & R_{v,2} & \cdots & R_{v,v} \end{bmatrix}$$

where the matrix elements $R_{i,j}$ represent the edge weights between site i and j. To calculate the number of times a transaction x has been directly and indirectly selected for validation in the blockchain at moment t, $M(t)$ is multiplied, i.e. $M^a(t)$. Where a is a minimum of 1 denotes the direct validation relationship between sites and a maximum is the number of rounds a transaction has undergone. The adjacency matrix allows for the calculation of the cumulative weights of x at moment t.

$$W_v(x,t) = 1 + \#\{e \in e_i^T \sum_{k=1}^{r} M^r : e \neq 0\} \tag{3}$$

The assignment matrix allows the calculation of the edge weights of x at moment t.

$$W_e(x,t) = e \in e_i^T \sum_{k=1}^{r} D^r (1, ..., 1)^T \tag{4}$$

where r represents the round of network unit time during the transaction.

C. Proof of Reputation Consensus Algorithm

In this section, by combining the reputation model with the weighted DAG structure introduced before, a proof of reputation based biased random walk (PoR-BRW) algorithm is proposed. This ensures that the DAG-based blockchain not only safeguards system security but also conserves computational resources as much as possible. The BRW [10] is a technique that exhibits a preference for selecting and validating tips. This algorithm introduces the bias factor that enhances its adaptability to different scenarios. In the BRW algorithm, a certain number of random walk particles are placed at depth h in the DAG. These particles randomly traverse the directed edges in the direction of tips. The first two tips reached by the particles are selected for transaction validation. During this process, the probability of each step taken by a particle in the random walk is given by:

$$P_{xy} = \frac{e^{\sigma \Delta w_{xy}}}{\sum_{z:z\to x} e^{\alpha \Delta w_{xz}}} \tag{5}$$

where σ is non-negative regulators, Δw is the cumulative weighting difference between tips. To improve the system's resistance to malicious node attacks, this paper introduces the reputation value into BRW thereby distinguishing the probability of a transaction being selected for verification. The improved particle wandering step probability is

$$P_{xy} = \frac{RU_y \cdot e^{\sigma \Delta w_{xy}}}{\sum_{z:z\to x} C_z \cdot e^{\alpha \Delta w_{xz}}} \tag{6}$$

When the parameter σ approaches zero, the particles exhibit a state of complete randomness in their roaming behavior. Consequently, the system achieves the highest level of fairness albeit at the expense of reduced security. On the other hand, when σ assumes a larger value, the particles tend to favor posting sites with high node reputation values, thereby enhancing the system's security. However, it is crucial to exercise caution when selecting a sufficiently large non-negative adjustment factor, as an excessively high value may lead to a substantial increase in the average aggregation factor of the graph. Hence, careful calibration of this parameter is necessary.

IV. Experiments and Results

In this section, the performance of the proposed hierarchical network structure and the consensus mechanism of the improved DAG-based blockchain are numerically simulated and analyzed.

A. Hierarchical Wireless Network Simulation

Fig. 3 illustrates the impact of the network sizes on the consensus time delay of the different blockchain architectures. In this simulation, the GC comprises 10 ECNs, and the number of participating nodes in the 10 LC chains expands from $5/LC$ to $20/LC$. A single-chain blockchain employing the Practical Byzantine Fault Tolerance (PBFT) algorithm [11] is used as a reference for the consensus process. The simulation is based on the following assumptions. Wireless communication links between nodes follow a 5G millimetre-wave path loss model with the parameter given by $PL(d) = 79.2 + 26\log_{10}\left(\frac{d}{d_0}\right) + X_\sigma \sim \mathcal{n}(0, 9.6)$ [12]. The distance between vehicles and RSUs is uniformly distributed within the range of (20, 100) meters. The time overhead for hash computation is parameterized as $C_h = 0.01215$ and the overhead for signature verification is $C_v = 0.00309$. These parameter settings are referenced from the study [13].

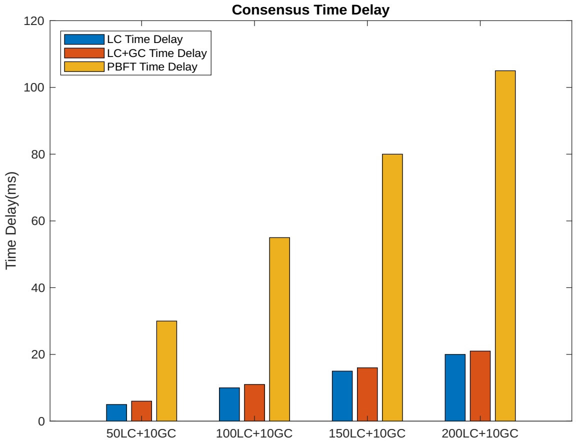

Fig. 3. Consensus time delay comparison

As depicted in Fig. 3, the hierarchical DAG-based blockchain architecture proposed in this paper results in lower consensus time delays. This is attributed to the hierarchical design, which decouples the original large-scale consensus process into multiple small-scale local consensuses for each LC and relies on GC for secondary consensus. Meanwhile, when the total number of nodes is n, the communication complexity of the PBFT algorithm is $O(n^2)$, while that of the IOTA algorithm approaches $O(1)$. Therefore, as the network scale expands, the communication overhead of the DAG-based blockchain will grow significantly slower than that of the blockchain based on the PBFT algorithm. Simulation verifies the advantages of the DAG-based blockchain in terms of consensus time delay.

B. Proof of Reputation Consensus Algorithm Simulation

Fig. 4 presents the simulation of the node reputation mechanism in a DAG-based blockchain, where the line represents real-time reputation values of the vehicles, and the bar chart signifies the cumulative weight of sites published by the nodes. Initially, for the first 25 rounds, nodes are assumed to behave honestly, but then Node B is introduced as a malicious actor by providing false messages in a 50-round transaction simulation. As seen in the figure, the malicious behavior of Node B leads to a marked instability and rapid decline in the vehicle's reputation. Consequently, its sites are less likely to be chosen by nodes publishing subsequent sites. This shows that the reputation mechanism established in this article is sensitive to Byzantine attacks.

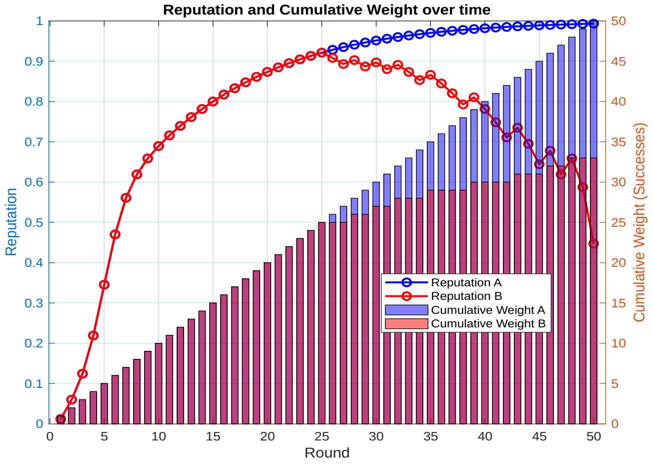

Fig. 4. Reputation and Cumulative Weights

Further, to verify the ability of PoR to resist Byzantine attacks, a DAG-based blockchain maintained by 10 nodes is simulated. Nine of these nodes are set as trusted nodes while node 5 is subjected to a Byzantine attack starting from round 25. The attack causes the sites posted by node 5 to be tampered with and verified as false messages by other nodes. Fig. 5 shows the source of the new sites added to the blockchain in each round. It can be seen that the false message posted by node 5 after the attack will not be validated in the blockchain. The simulation verifies the security of the blockchain based on DAG using the PoR consensus algorithm.

V. Conclusion and Future Work

This paper introduces a hierarchical DAG-based blockchain architecture to be utilised in edge computing-based VANET to solve the security and trust issue. We use DAG-based blockchain to enhance security while adjust simultaneous operations in VANET instead of single-thread chain-based blockchain. To meet the specific power consumption requirement and consider the typical permissioned network model in VANET, we developed a node reputation TSA mechanism to replace the generally utilized PoW consensus. Meanwhile, to improve blockchain efficiency for large-scale information exchange in VANET and reduce system overhead, a hierarchical architecture is designed to disperse the major transactions into LCs. Simulation results demonstrates that the reputation mechanism achieves network security for DAG-based blockchain in VANET.

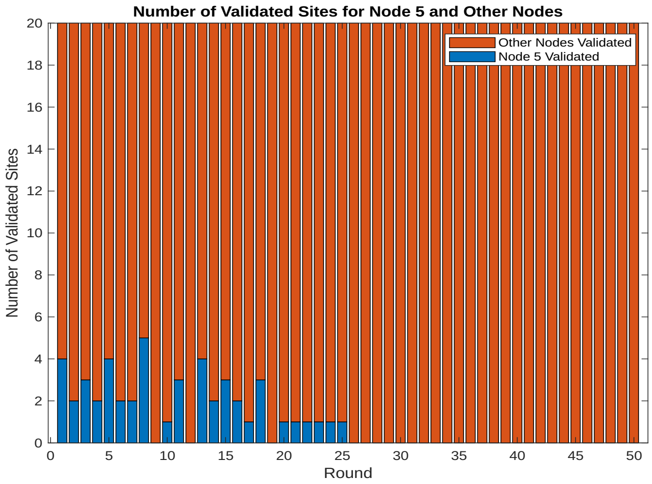

Fig. 5. Reputation and Cumulative Weights

References

[1] B. P. Rimal, D. Pham Van, and M. Maier, "Mobile-edge computing vs. centralized cloud computing in fiber-wireless access networks," in *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2016, pp. 991–996.

[2] L. Liu, C. Chen, Q. Pei, S. Maharjan, and Y. Zhang, "Vehicular edge computing and networking: A survey," *Mobile networks and applications*, vol. 26, pp. 1145–1168, 2021.

[3] S. Matsumoto and R. M. Reischuk, "Ikp: Turning a pki around with decentralized automated incentives," in *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2017, pp. 410–426.

[4] X. Li, Y. Han, J. Gao, and J. Niu, "Secure hierarchical authentication protocol in vanet," *IET Information Security*, vol. 14, no. 1, pp. 99–110, 2020.

[5] L. Li, D. Huang, and C. Zhang, "An efficient dag blockchain architecture for iot," *IEEE Internet of Things Journal*, vol. 10, no. 2, pp. 1286–1296, 2023.

[6] C.-Y. Cheng, H. Liu, L.-T. Hsieh, E. Colbert, and J.-H. Cho, "Attribute-based access control for vehicular edge cloud computing," in *2020 IEEE Cloud Summit*. IEEE, 2020, pp. 18–24.

[7] H. Y. Wu, X. Yang, C. Yue, H.-Y. Paik, and S. S. Kanhere, "Chain or dag? underlying data structures, architectures, topologies and consensus in distributed ledger technology: A review, taxonomy and research issues," *Journal of Systems Architecture*, vol. 131, p. 102720, 2022.

[8] S. Popov, "The tangle," 2018.

[9] W. Yang, X. Dai, J. Xiao, and H. Jin, "Ldv: A lightweight dag-based blockchain for vehicular social networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5749–5759, 2020.

[10] B. Kusmierz, W. Sanders, A. Penzkofer, A. Capossele, and A. Gal, "Properties of the tangle for uniform random and random walk tip selection," in *2019 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2019, pp. 228–236.

[11] M. Castro, B. Liskov *et al.*, "Practical byzantine fault tolerance," in *OSDI*, vol. 99, no. 1999, 1999, pp. 173–186.

[12] M. Mezzavilla, M. Zhang, M. Polese, R. Ford, S. Dutta, S. Rangan, and M. Zorzi, "End-to-end simulation of 5g mmwave networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2237–2263, 2018.

[13] R. Ben Romdhane, H. Hammami, M. Hamdi, and T.-H. Kim, "An efficient and privacy-preserving billing protocol for smart metering," in *International Conference on Advanced Information Networking and Applications*. Springer, 2021, pp. 691–702.