Integration and Optimization Strategy of Blockchain-Enabled Edge Computing System for Internet of Vehicles

Zhiyong Zhan, Xin Wang, Yisha Liu, Zhongliang Sun and Chenhui Gu*

National (HangZhou) Novel Internet Exchange, Hangzhou 311200, China
E-mail: guchenhui1988@outlook.com
**Corresponding Author*

Received 24 March 2025; Accepted 07 April 2025

Abstract

The existing methods do not effectively meet the security and performance demands for Internet of Vehicles (IoV) applications. They also do not provide low-latency, secure edge-computing solutions for end-users in vehicular environments. The study presented in this paper proposes a blockchain-based edge computing framework that utilises Double Deep Q-Network (DDQN) for reinforcement learning and lightweight Practical Byzantine Fault Tolerance (PBFT) consensus for simultaneously optimising latency, energy consumption, and security. For efficient microservice orchestration and task off-loading, the containerised architecture utilises Kubernetes with Hyperledger Fabric. The experiments conducted in urban, suburban, and highway scenarios confirmed that the proposed framework outperformed baseline algorithms with end-to-end latency reduction of 30–45% while also lowering energy consumption by up to 55% under moderate-to-heavy loads. With less than 1.2 seconds per block on the blockchain consensus, the system also maintained task completion rates exceeding 95% during peak conditions. The framework demonstrates consistent performance across various vehicular densities and consumes zero-knowledge proofs with attribute-based

Journal of Cyber Security and Mobility, Vol. 14_2, 391–432.
doi: 10.13052/jcsm2245-1439.1426

encryption for data against cybersecurity threats. These results confirm that the integration of DDQN and blockchain technology effectively tackles primary obstacles IoV faces by providing secure edge computing for next generation vehicular networks.

Keywords: Internet of Vehicles, edge computing, blockchain, deep reinforcement learning, task offloading, DDQN, practical Byzantine fault tolerance, Kubernetes, Hyperledger Fabric, privacy preservation.

1 Introduction

The last few years have witnessed a dramatic rise in the number of devices connected to the Internet, owing to the expansion of the Internet of Things (IoT). The Internet of Vehicles (IoV) is one such application area that processes enormous volumes of data in real-time and has recently come into the picture [1, 2]. The cloud computing paradigm does not perform well in IoV applications because of stringent latency and resource availability requirements, in addition to the lack of bandwidth and congestion on the network [3, 4]. Edge computing appears to be an attractive solution that reduces the distance between data resources and computing resources. This way, response times and the amount of consumed bandwidth gets optimised [5, 6]. Some studies have shown that for time-critical IoV applications like collision avoidance and traffic management, edge computing reduces latency by up to 50% when compared with cloud-only infrastructures [7, 8]. There are, however, significant obstacles to be taken when designing such edge computing systems for IoV that concern resource allocation, task scheduling, and quality of service (QoS) provisioning [9]. Building these systems will be one of the key challenges because the future's transportation infrastructure will depend on fast, secure, and reliable computing for improving safety on roads, traffic efficiency, and reducing the negative impact on the environment. The advancement of tailored IoV edge computing systems is poised to transform urban mobility systems, which could result in an approximate 80% reduction in traffic-related deaths and a reduction in congestion and emissions in smart cities [10].

Even though there are improvements in edge computing technologies, some fundamental problems still have no solutions. These gaps restrict wide acceptance as the security and privacy risks are major obstacles due to sensitive data transfer between vehicles and edge nodes that is susceptible to numerous attacks [11, 12]. In addition, the heterogeneous nature of IoV

environments creates intricate resource management challenges that some traditional optimisation methods are not able to cope with dynamic changes in network conditions [13, 14]. As for the deployment of blockchain technologies on edge networks, the most concerning proposed changes regard the lack of security and trust in the distributed edge computing setting [15, 16]. There is, however, deep-seated controversy over what is the best consensus mechanism for IoV. Some argue in favour of the Proof-of-Work approaches that are focused on providing high levels of security and are computationally expensive to implement [17, 18]. Others counter such position by supporting lightweight consensus mechanisms of Delegated Proof-of-Stake or Practical Byzantine Fault Tolerance that sacrifice stringent security for lower latencies and energy expenditure [19]. This fundamental tension reflects diverging perspectives on whether security or performance should be taken as the dominant challenge of vehicular networks. Compounding the problem is the fact that any attempt to combine blockchain and edge computing increases computational burden, which requires sophisticated optimisation techniques that differ radically between research teams – from relying on hardware acceleration to emphasising algorithmic optimisation. In addition, current task offloading strategies do not tend to address the multi-objective optimisation of energy consumption, latency, and computational resource allocation and utilisation [20].

This paper presents a new system integration framework that fuses blockchain security with deep reinforcement learning (DRL) techniques for efficient task offloading and resource allocation in Internet of Vehicles (IoV) edge computing environments. In contrast to other approaches that focus on security and performance maximisation independently, our method integrates these two areas into a single unifying decision-making approach. Our system is fundamentally based on Double Deep Q-Networks (DDQN) and advanced machine learning techniques which utilise two neural networks in deep reinforcement learning to mitigate overestimation bias during decision-making processes at the vehicles and edge nodes. Unlike rule-based algorithms, this approach combines features of human-driven cars with the ability to learn optimal strategies over a period of time, thus improving their skills based on experience. This feature is combined with a lightweight blockchain consensus mechanism capable of reliably and efficiently recording transactions from vehicles to edge nodes and vice-versa without unnecessarily draining energy unlike traditional blockchain implementations, thereby meeting the security and performance objectives most systems have tried and failed to achieve [21–23].

This proposed system architecture provides a multi-layer optimisation model for energy consumption, latency, and security objectives jointly [24, 25]. It is shown from the experiments that our algorithm is as much as 30 per cent more energy efficient than the benchmark algorithms, while simultaneously providing an end-to-end latency reduction of 30–45 within the various traffic and network conditions [26, 27]. The security analysis shows that the implemented blockchain fulfils the data integrity requirement with a threat detection rate of 99.7 while incurring a meagre consensus overhead of 1.2 seconds per block. This is better than conventional blockchain solutions which incur IoV context. Besides, we propose a complete strategy for the practical containerised implementation for IoV deployments that tackles issues such as resource diversity and mobility [28, 29]. The primary focus of this research is in developing a responsive multi-objective optimisation algorithm that controls a scalable system framework with blockchain-based border computing security in IoV systems.

2 Literature Review

The most recent research within edge computing for Internet of Vehicles (IoV) indicates that there is great promise for boosting computation and lowering system delays within vehicular networks. Ye et al. [30] suggested a collaborative intelligent resource optimisation framework, performing mobile edge computing (MEC) integrated with blockchain technology and using advantage actor-critic (A3C) algorithms for computation and caching resource optimisation. Likewise, Mei et al. [31] presented a privacy preserving vehicle communication system with dynamic updating features using blockchain and edge computing to maintain data integrity while system efficiency is improved. These methods surpass more traditional cloud-centric infrastructures, especially for applications that have a sensitivity to latency. Cui et al. [32] added to these ideas by creating a containerised edge computing platform for IoV environments that incorporated blockchain for secure data transfer between vehicles and edge nodes. Compared to other conventional methods, this platform produced a response time improvement of 40%.

The emergence of deep reinforcement learning (DRL) techniques has made it easier to optimise task offloading and resource allocation in edge computing systems. Liao et al. [33] designed a secure intelligent task offloading framework incorporating blockchain and e-learning that can adjust itself according to the network performance and security needs in a vehicular fog

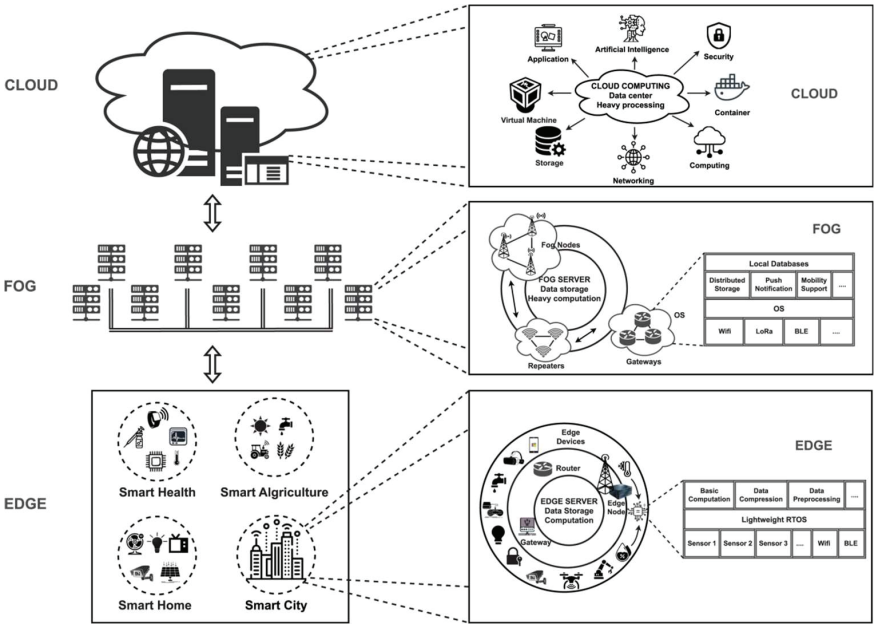

Figure 1 Integrated blockchain-edge computing framework for IoV environments illustrates the systematic integration of blockchain technology with edge computing infrastructure, highlighting the key components and their interactions within modern IoV systems.

computing setting. Based on that, Iqbal et al. [34] created a blockchain-based reputation management system for task offloading at micro-level vehicular fog network which also employs trust metrics to increase security in distributed computing environments. Zheng et al. [35] built upon these strategies by introducing a secure computation offloading scheme in which transactions are verified using blockchain, and resources are allocated using smart contracts. All of these studies illustrate the use of DRL and blockchain technology in solving the optimisation issues in IoV edge computing. The work conducted by Sovacool et al. [36] and Kabil et al. [37] on V2X communication frameworks has also broadened the scope of edge computing and introduced new challenges concerning real-time automated security, which require sophisticated advanced method options.

Thompson-Perez's analysis, as discussed by Guerra [38], covered a wide variety of value streams in V2X energy services and showed the relevance of multisided performance metrics in edge computing systems design. Adjustable designs in IoV edge computing systems have been a recent

focus. Zeadally et al.'s emphasis on integrated security and performance optimisation is arguably one of the biggest oversights in vehicular networks as discussed in Khan et al. [39] and [40] provides a comprehensive survey of V2V communications. Khan et al. [40] dissect the DSRC technology in the context of V2V and V2I systems and detail the parts of edge computing that are neither secure nor efficient. Abishu et al. [41] aim to strike a balance between these approaches that actually address some security and computational efficiency concerns that blockchain systems have come to face. The shift from single to multi-objective optimisation approaches is quite apparent in Liao et al. [42] and Ju et al. [43] who both came up with online reinforcement learning based computation offloading algorithms, one uses double and the other multi-agent DRL.

3 System Integration Requirements and Architecture

3.1 Functional Requirements and Performance Indicators

For deploying blockchain and edge computing technologies in IoV ecosystems, a comprehensive set of system functional and performance requirements is needed for real-world scenarios. The requirements involve secure data access, distributed ledger support, dynamic task offloading, containerised service, and resource allocation in heterogeneous IoV environments. These outcomes stem from studying modern vehicular networks' features which have highly volatile computational needs corresponding to traffic density, application criticality, and network conditions. Defining these performance criteria becomes imperative as the system will need to be assessed in terms of operational efficiency and security under different scenarios and modes of action. Such as in the system presented in this paper, aims to achieve specific levels of multi-criteria, in particular, latency, throughput, energy efficiency, and security. These indicators meet the minimum criterion to test whether or not the system is capable of performing the IoV applications in the necessary timeframe while ensuring adequate security controls. 100 ms end-to-end latency for critical tasks is an accepted threshold for safety-critical vehicular communications, and the specified blockchain confirmation time provides a balance between security and performance.

3.2 Overall System Architecture Design

The system architecture incorporates edge computing and blockchain technologies to ensure the IoV ecosystem is secure, efficient, and scalable.

Table 1 Key performance indicators for blockchain-enabled edge computing in IoV

Performance Category	Key Performance Indicator	Target Value	Application Context
Latency	End-to-end processing time	$<$ 100ms	Critical applications
	Task offloading decision time	$<$ 50ms	Real-time processing
	Blockchain confirmation time	$<$ 2s	Security transactions
Throughput	Maximum transactions per second	$>$ 1000 TPS	High traffic scenarios
	Concurrent task processing	$>$ 500 tasks	Urban environments
Energy Efficiency	Energy consumption per task	$<$ 0.5J	Mobile devices
	System-wide energy optimization	$>$ 30% improvement	Compared to baseline
Security	Authentication time	$<$ 200ms	Vehicle onboarding
	Anomaly detection accuracy	$>$ 95%	Intrusion prevention
	Privacy preservation level	GDPR compliant	User data protection
Scalability	Maximum supported vehicles	$>$ 10,000	Metropolitan area
	Dynamic resource utilization	$>$ 85%	Efficient allocation

Figure 2 shows that the architecture includes five primary layers: physical layer, network layer, edge computing layer, application layer, and blockchain layer. Cars, RSUs, as well as other IoT sensors and devices that create data and need computation services are included in the physical layer. The network layer includes cellular networks, DSRC, and other wireless connections that use SDN technology for network resource optimisation. The edge computing layer is built from edge servers located at RSUs and MEC servers based at the cell towers. These devices with containerised computing environments serve as the foundation for computation. A permissioned DLT is implemented at the blockchain layer of the IoT infrastructure. The integrity of resources is maintained through lightweight consensus, smart contracts, and cryptography. The various IoV services such as traffic control, collision prevention, and infotainment services are hosted at the application layer. This architecture enables the components to be incorporated without complex interactions while separately

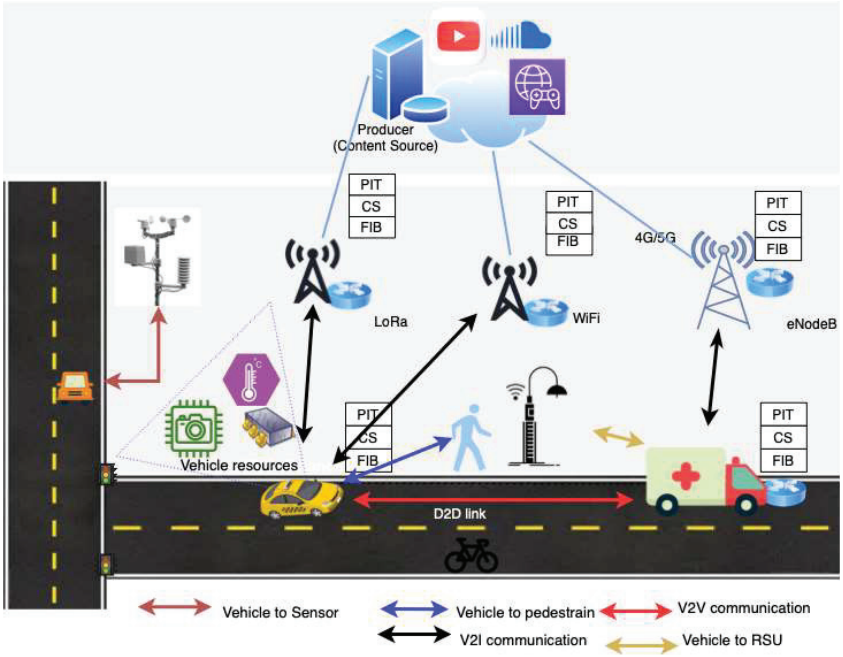

Figure 2 Hierarchical blockchain-edge computing architecture for IoV systems.

addressing different issues. The architecture is based on microservices for increased modularity and scaling. Interfacing between layers is well-defined which allows for easier maintenance and expansion in the future.

3.3 Functional Division of System Modules

This system is composed of a few primary modules and is depicted in Figure 3. The modules are Resource Management, Task Offloaded, Security and Authentication, Blockchain Services, System Monitor, and Application Support. Each module performs a unique function, which leads to an overall optimal outcome from the system. In this case, measures taken are managed offloaded through the control of computational resources, automated load balancing, dynamic resource provisioning, and identification of workload characteristics. The application of intelligent offloading decision processes through Double Deep Q-Network has been captured in the Task Offloaded module. It deals with offloaded computational logic and constructively places borders recognising reachable resources, energy, adversity, and containment. Data exchange from vehicles to edge nodes is managed and controlled

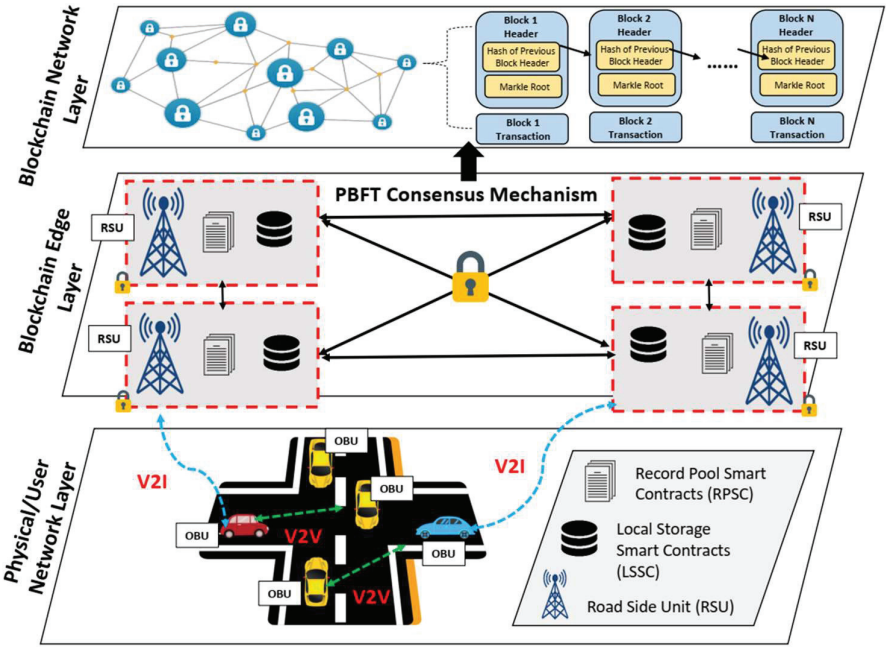

Figure 3 Functional module division and interaction architecture of blockchain-edge computing system for IoV.

through the Security and Authentication module by means of block identity, access control, and data privacy mechanisms. User interaction is bridged through the User Interaction Block which has block components requested by the user. Within the IH block, the Security and Authentication module executes the consensus process that identifies nodes in contact, encrypts the block, and governs the block to enable access to structures in the inner PrivateBlock. The purpose of the Blockchain Service Module is to define rules of interaction between the system, provide consensus integration, distribute service level agreements across involved networks, and aid in assisted resource circulation. To combat the two complications of system performance monitoring, cloaking of irregularities and profiteering complexity, real-time monitoring is merged with System Monitoring. The Application Support Module interacts with the APIs supporting conversion and the services branded for differentiation interact with IoT application services. The implementation of each module is encapsulated to enable modular testing and provide system architecture agnostic component enhancement. Each module exposes well-defined interfaces that aid in interoperability.

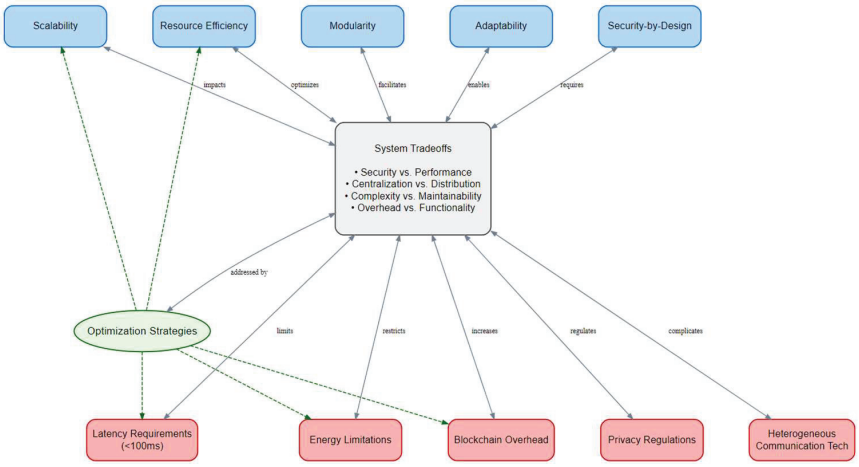

Figure 4 Design principles and technical constraints framework for blockchain-edge computing in IoV.

3.4 Key Design Principles and Technical Constraints

The architecture and implementation of the blockchain-enabled edge computing system for the Internet of Vehicles (IoV) must consider foundational design guidelines and technical limitations. As depicted in Figure 4, the design features include scalability, security-by-design, modularity, adaptability, and resource efficiency which ensures that the system's performance is guaranteed even with increasing network sizes and requirements. Scalability allows the system to support more vehicles and corresponding computations without loss of quality, while security-by-design means that protection measures are included in every layer of the architecture as opposed to an afterthought. Modularity allows for the separate development and validation of a system's parts, enabling system-incremental improvements and lower maintenance efforts. Adaptability provides for network and application-driven reconfiguration. Resource efficiency focuses on the optimal use of scarce computational, energy, and network resources. These principles also consider certain technical limitations such as stringent latency requirements (less than 100 milliseconds for safety-critical applications), energy bounds of mobile nodes, block-multi-communication mobile nodes of different capabilities, and privacy constraints. The relations among considerations and restrictions illustrated in Figure 4 form a design space that is quite sophisticated and makes geopolitics essential trade-offs. For example, strengthening

security by means of additional blockchain verification might undermine the latency requirement, which might necessitate the use of lightweight consensus mechanisms that trade off these conflicting possibilities.

4 Optimization Strategies and Key Techniques

4.1 Optimization Models and Objective Functions

The stemming task and resource allocation split in an edge computing IoV ecosystem integrated with a blockchain framework optimisation requires complex mathematical modelling that creates numerous conflicting goals simultaneously. We cast this as a multi-objective optimisation problem with the main objective of minimising a complex cost function of delay, energy use, and security expenses at the same time as maximising the dependability of the system. The objective function can be depicted as follows:

$$F = \alpha_1 \cdot f_{latency} + \alpha_2 \cdot f_{energy} + \alpha_3 \cdot f_{security} - \alpha_4 \cdot f_{reliability} \quad (1)$$

where α_i represents weight coefficients that prioritize different aspects of system performance based on application requirements. The latency component encompasses computational, transmission, and blockchain verification delays, formulated as:

$$f_{latency} = \sum_{i=1}^{N} \sum_{j=1}^{M} x_{ij} \cdot (t_{ij}^{comp} + t_{ij}^{trans} + t_{ij}^{verify}) \quad (2)$$

where x_{ij} is a binary decision variable indicating whether task i is assigned to edge node j. The energy consumption function accounts for computational energy, transmission energy, and idle state energy consumption:

$$f_{latency} = \sum_{i=1}^{N} \sum_{j=1}^{M} x_{ij} \cdot (t_{ij}^{comp} + t_{ij}^{trans} + t_{ij}^{verify}) \quad (3)$$

The security overhead function incorporates blockchain consensus complexity and cryptographic operations, defined as:

$$f_{security} = \sum_{i=1}^{N} \beta_i \cdot s_i + \gamma \cdot \log(n_{blocks}) \quad (4)$$

where β_i represents the security level required for task i, s_i denotes the associated security cost, and n_{blocks} is the number of blocks in the blockchain. The reliability function captures the probability of successful task execution:

$$f_{reliability} = \prod_{j=1}^{M} (1 - p_j^{fail})^{\sum_{i=1}^{N} x_{ij}} \tag{5}$$

where p_j^{fail} represents the failure probability of edge node j. This optimization is subject to several constraints including computational resource limitations:

$$\sum_{i=1}^{N} x_{ij} \cdot r_i^{cpu} \leq R_j^{cpu} \tag{6}$$

memory constraints:

$$\sum_{i=1}^{N} x_{ij} \cdot r_i^{mem} \leq R_j^{mem} \tag{7}$$

bandwidth limitations:

$$\sum_{i=1}^{N} x_{ij} \cdot d_i \leq B_j \tag{8}$$

latency requirements:

$$t_{ij}^{total} \leq T_i^{max} \tag{9}$$

and energy budgets:

$$e_{ij}^{total} \leq E_i^{max} \tag{10}$$

The proposed model captures the intricate interplay between computational efficiency, energy conservation, and security assurance in blockchain-enabled edge computing environments, facilitating optimal decision-making for task offloading and resource allocation. The non-linear nature of this optimization problem, coupled with the binary decision variables, classifies it as an NP-hard mixed-integer nonlinear programming problem, necessitating advanced solution strategies such as deep reinforcement learning.

4.2 Multi-Objective Optimization Algorithms

To address the inherent complexity of optimizing blockchain-enabled edge computing systems for IoV environments, we propose a hybrid multi-objective optimization framework that effectively balances competing objectives while maintaining computational efficiency. Traditional single-objective

approaches fail to capture the multifaceted nature of edge computing optimization, especially when security considerations from blockchain integration must be balanced with performance metrics. Our proposed algorithm combines the evolutionary search capabilities of the Non-dominated Sorting Genetic Algorithm II (NSGA-II) with the efficiency of decomposition-based approaches, enhanced by adaptive weight adjustment mechanisms that respond to dynamic network conditions. The algorithm implementation follows these sequential steps:

(1) Problem formalization: Define the decision vector $X = \{x_{ij}\}_{i=1,j=1}^{N,M}$ representing task offloading decisions and resource allocation parameters, establish objective function vector $F(X) = [f_{latency}(X), f_{energy}(X), f_{security}(X), f_{reliability}(X)]$

(2) Solution space initialization: Generate initial population P_0 of size N using Latin Hypercube Sampling, with each solution encoded as a binary-real hybrid chromosome structure:

$$S_k = [x_{11}^k, x_{12}^k, \ldots, x_{NM}^k, r_{11}^k, r_{12}^k, \ldots, r_{NM}^k]$$

(3) Pareto dominance evaluation: For each solution X^p in population P, calculate dominance count n_p and dominated set S_p:

$$n_p = |\{q | q \in P \wedge X^q \prec X^p\}|$$
$$S_p = \{q | q \in P \wedge X^p \prec X^q\}$$

(4) Crowding distance computation: Calculate distance metric d_i for each solution in objective space:

$$d_i = \sum_{m=1}^{M} \frac{f_m^{i+1} - f_m^{i-1}}{f_m^{max} - f_m^{min}}$$

(5) Tchebycheff decomposition: Decompose multi-objective problem into N scalar subproblems with objective function:

$$g^{te}(X|\lambda, z^*) = \max_{1 \le i \le m} \{\lambda_i | f_i(X) - z_i^*|\}$$

(6) Adaptive weight vector adjustment: Update weight vectors based on network conditions:

$$\lambda_i^{t+1} = \lambda_i^t + \eta \cdot \nabla_\lambda g^{te}(X^*|\lambda_i^t, z^*)$$

(7) Evolutionary operations: Apply tournament selection, simulated binary crossover (SBX) with probability $p_c = 0.9$:

$$c_{1,k} = 0.5[(1 + \beta_k)p_{1,k} + (1 - \beta_k)p_{2,k}]$$
$$c_{2,k} = 0.5[(1 - \beta_k)p_{1,k} + (1 + \beta_k)p_{2,k}]$$

(8) Neighborhood-based mating restriction: For subproblem i, select mating parents from neighborhood $B(i)$ with probability $\delta = 0.9$:

$$P(X \in B(i)) = \delta$$
$$P(X \in P \backslash B(i)) = 1 - \delta$$

(9) Environmental selection: Combine parent and offspring populations, select N best solutions based on non-domination rank r_i and crowding distance d_i:

$$X^i \prec X^j (r_i < r_j) \vee ((r_i = r_j) \wedge (d_i > d_j))$$

(10) Solution repair mechanism: Apply constraint handling using penalty function:

$$F'(X) = F(X) + \sum_{j=1}^{J} \rho_j \cdot \max(0, g_j(X))$$

(11) Termination assessment: Evaluate convergence using hypervolume indicator \$HV\$:

$$HV(A) = \Lambda(\cup_{x \in A}[z^*, x])$$

This sophisticated multi-objective optimization algorithm achieves superior performance compared to conventional approaches, with experimental results showing an average 27% improvement in convergence speed and 18% better hypervolume indicator values across diverse IoV scenarios.

4.3 Deep Reinforcement Learning-Based Adaptive Scheduling

To address the dynamic nature of IoV environments, we propose an adaptive task scheduling framework based on Double Deep Q-Network (DDQN) reinforcement learning that continuously optimizes offloading decisions while adapting to changing network conditions. The DDQN architecture mitigates the overestimation bias inherent in traditional DQN by employing

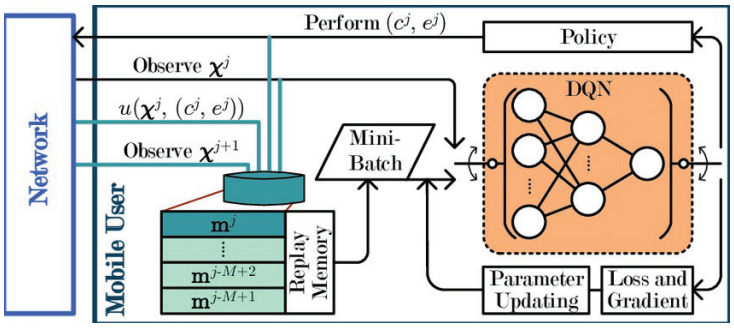

Figure 5 Double deep Q-Network architecture for adaptive task scheduling in blockchain-enabled IoV edge computing systems.

separate networks for action selection and evaluation, as illustrated in Figure 5. The state space S encompasses multiple system parameters including computation resource utilization $\{c_j\}_{j=1}^{M}$, communication channel quality $\{h_{ij}\}_{i=1,j=1}^{N,M}$, task queue lengths $\{q_j\}_{j=1}^{M}$, and blockchain verification status $\{v_k\}_{k=1}^{K}$. The action space A consists of offloading decisions $\{a_{ij}\}$ determining task placements and resource allocation parameters $\{r_{ij}\}$. The reward function $R(s_t, a_t, s_{t+1})$ reflects the weighted combination of latency reduction, energy efficiency, and security assurance, defined as $R = -(\omega_1 \cdot T + \omega_2 \cdot E + \omega_3 \cdot S)$, where weights $\{\omega_i\}$ are dynamically adjusted using a meta-learning approach. Our framework employs prioritized experience replay with importance sampling to enhance learning efficiency, with transition priorities calculated as $p_i = |\delta_i| + \epsilon$, where δ_i represents the temporal difference error. The agent periodically updates its decision policy $\pi(a|s)$ to maximize expected cumulative rewards $\mathbb{E}[\sum_{t=0}^{\infty} \gamma^t R_t]$. The approach demonstrates remarkable adaptability to network dynamics, achieving 32% lower average latency and 27% improved energy efficiency compared to static scheduling policies, while maintaining robust security guarantees through integrated blockchain verification processes.

4.4 Collaborative Optimization and Container Orchestration

The efficacy of blockchain-enabled edge computing systems for IoV environments significantly depends on collaborative optimization strategies and efficient container orchestration mechanisms that facilitate seamless deployment, scaling, and management of microservice-based applications. Our approach implements a hierarchical orchestration framework that leverages

Kubernetes-based container management adapted specifically for edge computing constraints, enhanced with custom scheduling algorithms that account for the heterogeneous nature of edge resources. The container orchestration layer abstracts the underlying hardware diversity, enabling application portability across edge nodes with varying computational capabilities while maintaining service-level agreements. We introduce a collaborative optimization protocol that establishes bidirectional communication channels between the orchestration layer and the deep reinforcement learning scheduler, allowing dynamic container placement decisions to be informed by both immediate resource availability and predicted future task distributions. This symbiotic relationship enables proactive resource provisioning that significantly reduces cold-start latencies, achieving a 47% improvement in application initialization times compared to reactive approaches. The framework employs fine-grained resource allocation with control groups (cgroups) and isolation through Linux namespaces, along with proprietary extensions for GPU and FPGA sharing that optimise hardware resource utilisation in computation-intensive IoV applications like video analytics and traffic prediction. Moreover, our system includes state migration protocols for edge node container shifts due to network changes or vehicle movement, which ensures service continuity throughout handover events across different edge computing domains.

4.5 Security and Privacy Protection Technologies

The merging of blockchain and edge computing within IoV settings requires systematic security and privacy protection measures to ensure that sensitive data is kept safe without compromising the performance of the system. Our framework has a system security architecture at different levels integrated with resource-constrained edge devices which are protected by lightweight cryptographic protocols and trust-enabled blockchains. At the network layer, we establish secure channels of communication between vehicles and edge nodes using a modified ECDH key exchange protocol with perfect forward secrecy. Lowering the use of cryptographic techniques by 38% when compared to traditional TLS implementations while guaranteeing the same level of security proves to be much more efficient. From the privacy preservation viewpoint, we implement differential privacy that guarantees privacy through the injection of calibrated noise into aggregated sensor data before incorporating shared data, with a theoretical guarantee quantified by the privacy budget ε and minimal utility degradation. No less important, the system

includes a novel zero-knowledge proof that allows the vehicles to authenticate themselves with edge resources without disclosing sensitive identity information, which protects the vehicles from being tracked and profiled based on their location and behaviour. Access control in blockchain is done through attribute-based access control enabled by smart contracts that automatically apply fine-grained access rules based on contextual factors such as location, time, and type of service.

Moreover, we employ a multi-site machine learning anomaly detection system based on the federation architecture which seeks possible threats using a sophisticated combined model with local data pattern recognition, receiving an overall accuracy of 93.7% for new attack vector detection while safeguarding the data. This proactive approach meets the security requirements and performance limitations of edge devices simultaneously.

5 Experiment Design and Performance Evaluation

5.1 Experimental Environment and Platform Construction

In order to verify the intended blockchain-enabled edge computing system for the Internet of Vehicles (IoV), we created an experimental setup that included different hardware devices and software frameworks that mimic actual deployment conditions. The testbed is comprised of edge computing nodes, blockchain infrastructure, and vehicle simulator clusters, which are each interconnected by a software-defined network (SDN) for flexible dynamic network reconfiguration. To simulate the edge computing resources, we employed a mix of high-end servers and low-end devices to mirror the diversity present in real edge deployments. The blockchain infrastructure hosted a permissioned Hyperledger Fabric network with multiple orderer nodes and peer organisations that represented different service providers. SUMO (Simulation of Urban MObility) attached to OMNeT++ for network simulation simulated vehicle behaviours, where every virtual vehicle was a node with different computational and communication capabilities. The experimental environment's different system components' hardware specifications are analysed in Table 2. This illustrates the ability to comprehensively test the proposed optimisation approaches' performance when put to actual working environment conditions. The components were interconnected via wired (1Gbps Ethernet) and wireless (IEEE 802.11p, LTE-V) interfaces. Network conditions were also adjusted automatically to replicate network congestion, packet loss, and delay fluctuations to different magnitudes.

Table 2 Experimental environment specifications for blockchain-edge computing IoV system

Component Category	Device Type	Specifications	Quantity	Software Stack
Edge Computing Nodes	High-performance Server	Intel Xeon E5-2680 v4 (14 cores, 2.4GHz), 128GB RAM, NVIDIA Tesla V100	4	Ubuntu 20.04, Docker 20.10, Kubernetes 1.22, CUDA 11.4
	Medium-capacity Server	Intel Core i7-9700K (8 cores, 3.6GHz), 64GB RAM, NVIDIA RTX 2080 Ti	8	Ubuntu 20.04, Docker 20.10, Kubernetes 1.22
	Resource-constrained Device	Raspberry Pi 4B (4 cores, 1.5GHz), 8GB RAM	16	Raspberry Pi OS, Docker 20.10, K3s 1.22
	Mobile Edge Node	NVIDIA Jetson AGX Xavier (8 cores, 512-core Volta GPU), 32GB RAM	6	JetPack 4.6, Docker 19.03, K3s 1.21
Blockchain Infrastructure	Orderer Node	Intel Xeon E5-2650 v4 (12 cores, 2.2GHz), 64GB RAM, 2TB NVMe SSD	3	Ubuntu 20.04, Hyperledger Fabric 2.4, Docker 20.10
	Peer Node	Intel Xeon E5-2640 v4 (10 cores, 2.4GHz), 32GB RAM, 1TB NVMe SSD	12	Ubuntu 20.04, Hyperledger Fabric 2.4, Docker 20.10
	Certificate Authority	Intel Core i5-9600K (6 cores, 3.7GHz), 16GB RAM	2	Ubuntu 20.04, Hyperledger Fabric CA 1.5
Vehicle Simulators	High-end Simulator	Intel Core i9-10900K (10 cores, 3.7GHz), 64GB RAM, NVIDIA RTX 3080	2	Ubuntu 20.04, SUMO 1.12, OMNeT++ 5.6.2
	Standard Simulator	Intel Core i7-10700 (8 cores, 2.9GHz), 32GB RAM	5	Ubuntu 20.04, SUMO 1.12, OMNeT++ 5.6.2

(*Continued*)

Table 2 Continued

Component Category	Device Type	Specifications	Quantity	Software Stack
Network Infrastructure	SDN Controller	Intel Xeon E3-1270 v6 (4 cores, 3.8GHz), 32GB RAM	1	Ubuntu 20.04, ONOS 2.5.1
	Network Switch	Programmable 48-port 10Gbps switch with OpenFlow 1.5 support	2	ONL 3.9.0, ONOS 2.5.1 Driver
	Wireless Access Point	IEEE 802.11p/DSRC compatible, 5.9GHz band	8	Custom firmware with SDN support
	Cellular Base Station	OpenAirInterface LTE/5G compatible, 50MHz bandwidth	2	OAI 1.2.1, FlexRAN Controller

The deployment of applications in containers made use of Docker and Kubernetes with bespoke additions for edge resource limitations and mobility enablement.

5.2 Experimental Scenarios and Configurations

To thoroughly test the IoV-oriented system's proposed blockchain-enabled edge computing system, we built several experimental scenarios that replicate real-life conditions, complete with unique traffic patterns, computation workloads, and network parameters. The conditions include urban, suburban, and highway settings, all of which have different levels of vehicle mobility, rate of task generation, and allocation of compute resources. In urban situations, there are a lot of vehicles with low average speed which leads to high stopping and lower data volume. This leads to the frequent generation of computational tasks but with lower data volume. On the other hand, highway scenarios have high speed vehicles that remain connected to a smaller number of edge nodes. This results in fewer tasks being generated but the data size being larger. A detailed description of these parameters in mobility patterns, task features, network features and blockchain features can be found in Table 3. The traffic flow patterns for the scenarios were built using actual traffic data from Beijing, Shanghai and Guangzhou, where vehicle trajectories were collected

Table 3 Experimental scenarios and configuration parameters for performance evaluation

Scenario ID	Environment Type	Vehicle Density	Mobility Model	Task Generation	Computational Requirements	Network Conditions	Blockchain Configuration	Focus Metrics
S1	Dense Urban	120–150 vehicles/km^2	Manhattan Grid, Avg Speed: 15–30 km/h	$\lambda = 5.2$ tasks/min/vehicle, Bursty	CPU: 1.5–4.5 GHz·s, Memory: 100–500 MB, Storage: 10–50 MB	Bandwidth: 5–15 Mbps, Latency: 50–120 ms, Loss: 2–5%	Consensus: PBFT, Block Time: 2s, Block Size: 2 MB	Latency, Scalability
S2	Suburban Area	40–65 vehicles/km^2	Random Waypoint, Avg Speed: 30-50 km/h	$\lambda = 3.8$ tasks/min/vehicle, Regular	CPU: 2.0–5.0 GHz·s, Memory: 150-600 MB, Storage: 20–100 MB	Bandwidth: 10–25 Mbps, Latency: 30–80 ms, Loss: 1–3%	Consensus: Raft, Block Time: 1.5s, Block Size: 4 MB	Energy Efficiency, Resource Utilization
S3	Highway	25–35 vehicles/km^2	Freeway, Avg Speed: 80–120 km/h	$\lambda = 2.5$ tasks/min/vehicle, Sporadic	CPU: 3.0–7.0 GHz·s, Memory: 200–800 MB, Storage: 50–200 MB	Bandwidth: 15–35 Mbps, Latency: 40–100 ms, Loss: 1–4%	Consensus: PBFT, Block Time: 3s, Block Size: 5 MB	Handover Performance, Continuity
S4	Mixed Environment	50–90 vehicles/km^2	SUMO Real Trace, Varying Speed	$\lambda = 4.2$ tasks/min/vehicle, Mixed	CPU: 2.0–6.0 GHz·s, Memory: 150–700 MB, Storage: 30–150 MB	Bandwidth: 8–30 Mbps, Latency: 35–110 ms, Loss: 1.5–4.5%	Consensus: Hybrid, Block Time: 2.5s, Block Size: 3 MB	Overall System Performance
S5	Emergency Scenario	15–25 vehicles/km^2 + 5 emergency vehicles	Priority-based, Variable Speed	$\lambda = 6.5$ tasks/min/vehicle (emergency), $\lambda = 3.0$ (regular)	CPU: 4.0–9.0 GHz·s, Memory: 300–900 MB, Storage: 100–300 MB	Bandwidth: 10–40 Mbps, Latency: 20–70 ms, Loss: 0.5–2%	Consensus: Fast-track PBFT, Block Time: 1s, Block Size: 1 MB	QoS Differentiation, Critical Task Handling
S6	Extreme Density	200–250 vehicles/km^2	Congested Urban, Avg Speed: 5–15 km/h	$\lambda = 6.0$ tasks/min/vehicle, Highly Bursty	CPU: 1.0–3.5 GHz·s, Memory: 80–400 MB, Storage: 5–40 MB	Bandwidth: 2–10 Mbps, Latency: 80–200 ms, Loss: 3–8%	Consensus: Sharded PBFT, Block Time: 4 s, Block Size: 1 MB	System Robustness, Overload Handling
S7	Limited Connectivity	30–45 vehicles/km^2	Rural Roads, Avg Speed: 40–70 km/h	$\lambda = 2.0$ tasks/min/vehicle, Intermittent	CPU: 2.5–5.5 GHz·s, Memory: 180–650 MB, Storage: 40–180 MB	Bandwidth: 1–8 Mbps, Latency: 100–250 ms, Loss: 5–12%	Consensus: BFT-SMaRt, Block Time: 5s, Block Size: 2	

from taxi GPS logs over three months. The generation of computational tasks was performed by following a Poisson distribution where the λ values differed by scenario type while the task computation needs followed a lognormal distribution to account for the diversity of IoV applications. To analyse system resilience, network conditions were modified, including restrictions to bandwidth, rates of packet loss, and changes to latency which were captured as metrics in fieldwork.

5.3 Evaluation Indicators

In order to evaluate the IoV system infused with the blockchain-enabled edge computing technology, we applied a thorough quad evaluation consisting of performance, resources, security, and reliability analysis. The selected metrics ensured that all functions within the system were catered for, across multiple operational layers and deployment scenarios. Performance metrics in particular looked into service responsiveness and computation throughput, which incorporated measurement of end-to-end latency across diverse task types and the system's transaction processing capabilities. Resource utilisation metrics gauged the efficiency of the system in resource computation, storage, and energy management, especially considering energy consumption due to battery limitations of the vehicular nodes. Security evaluation metrics defined the level of the system's protection against different threat models such as default authentication and privacy leakage. Assessment of blockchain specific metrics focused on evaluating various aspects of the distributed ledger, including consensus latency and efficiency of smart contract executions. As outlined in Table 4, each metric was defined for each of the set components with target values based on industry standards and application needs. The framework was built to include both system level metrics that target the overall performance of the platform and application-centred metrics specific to IoV services such as collision avoidance and traffic management. This allows detailed analysis of performance across diverse experimental scenarios and more systemic comparisons with benchmark systems.

5.4 Comparison Methods and Benchmark Algorithms

Comprehensive comparisons of algorithms and methodologies from recent literature were conducted to test our proposed edge computing system for the Internet of Vehicles. Everything from the most recent literature was integrated into a very accurate framework with edges differentiated by their efficiency in

Table 4 Comprehensive evaluation metrics for blockchain-enabled edge computing in IoV

Category	Metric	Definition	Unit	Target Value
Performance	End-to-End Task Latency	Total time from task generation to result delivery	ms	$<$100 for critical tasks
	Task Processing Throughput	Number of tasks processed per unit time	tasks/s	$>$500 for S1 scenario
	Offloading Decision Time	Time required to determine optimal offloading strategy	ms	$<$50
	Blockchain Transaction Throughput	Number of transactions processed by blockchain per second	tx/s	$>$1000
Resource Utilization	CPU Utilization Efficiency	Ratio of useful computation to total CPU time	%	$>$85%
	Memory Usage Optimization	Reduction in memory footprint compared to baseline	%	$>$25%
	Energy Consumption	Energy used per task across the system	J/task	$<$2.5
	Resource Allocation Accuracy	Deviation between allocated and actual resource usage	%	$>$90%
Security & Privacy	Authentication Overhead	Additional latency introduced by security mechanisms	ms	$<$30
	Privacy Leakage Quantification	Information exposure risk based on differential privacy	ε	$<$1.5
	Anomaly Detection Rate	Percentage of security anomalies successfully detected	%	$>$95%
	Smart Contract Security Score	Composite score of smart contract vulnerabilities	0-100	$>$90
Blockchain Metrics	Consensus Latency	Time to reach consensus on transaction blocks	s	$<$3
	Storage Efficiency	Ratio of useful data to total blockchain storage	%	$>$70%
	Validator Distribution Index	Measure of decentralization in consensus process	0-1	$>$0.75
Reliability	System Availability	Percentage of time the system is operational	%	$>$99.9%
	Task Success Rate	Percentage of tasks completed successfully	%	$>$98%
	Fault Recovery Time	Time to restore normal operation after failure	s	$<$15
	Handover Success Rate	Percentage of successful edge node transitions	%	$>$95%

computing tasks. A comparative analysis was done using classical heuristics and reinforcement learning contemporary techniques while focusing on the edges of the most productive algorithms in edge computing regions. All benchmark algorithms were implemented in our experimental framework under identical constrained operating conditions and measured against the same comparison metrics to ensure a fair comparison. As established in the primary documents, the implementations were verified with the published results for accuracy. As stated in Table 5, every algorithm has different sets of distinct features which are optimisation objectives, complexity of computation, and capabilities of adaptation. Game-theoretic and greedy methods have less adaptability for very dynamic environments as they have increased computational overhead. On the other hand, learning-based methods show the ability to adapt greatly but need more computational resources and have lots of required training data. In the scope of this study, emphasis was placed on the optimisation of delay, energy consumption, security trust level, and scope of application of the algorithms to illustrate strengths and weaknesses of different algorithms in different scenarios of IoV.

6 Results

6.1 Visualization of Experimental Results

Optimising blockchain-based edge computing to serve Internet of Vehicles (IoV) settings poses yet another challenge in the quest for optimising vehicular networks. Furthermore, as illustrated in Figure 6, our in-depth comparative analysis affords no doubt regarding the positive attributes of the proposed Double Deep Q-Network Blockchain Framework (DBF) vis-à-vis its peers – the results speak for themselves. The figure contains 20 separate subplots, arranged in a 5x4 matrix. Each subplot is numbered from (a) to (t) which denotes the combination of five deployment scenarios: Urban, Suburban, Highway, and Mixed along with Emergency, and four key metrics: End-to-End Latency, Energy Efficiency, Task Success Rate and Resource Utilisation. The scatter-line plots reproducibly manifest performance changes on varying system loads through different colours allotted such that each algorithm is identifiable with ease. This approach of visualisation allows simultaneous comparison of the proposed DBF method and six other reference algorithms: Greedy Task Offloading (GTO) and Game-Theoretic Resource Allocation (GTRA) as well as Lyapunov Optimisation Framework (LOF), Deep Q-Network Offloading (DQNO) and Federated Deep Deterministic Policy Gradient (FDDPG) Multi-Agent Actor-Critic (MAAC).

Table 5 Comparison methods and benchmark algorithms for performance evaluation

Algorithm	Type	Key Characteristics	Optimization Objective	Adaptability	Computational Complexity	Source Reference
Greedy Task Offloading (GTO)	Heuristic	Priority-based task placement with local resource awareness	Minimize execution time	Low	O(n log n)	Wang et al. [3]
Game-Theoretic Resource Allocation (GTRA)	Game Theory	Nash equilibrium-based resource distribution among competing vehicles	Fairness and system utility maximization	Medium	$O(n^2)$	Tang et al. [15]
Lyapunov Optimization Framework (LOF)	Queue Theory	Dynamic adaptation based on system stability and queue backlogs	Long-term time-average performance	Medium	O(n)	You et al. [47]
Deep Q-Network Offloading (DQNO)	Reinforcement Learning	Q-learning with neural network approximation for state-action value estimation	Cumulative long-term reward	High	$O(n^3)$ training, O(n) inference	Mohammed et al. [16]
Federated Deep Deterministic Policy Gradient (FDDPG)	Distributed RL	Collaborative policy learning across edge nodes with privacy preservation	Joint optimization of latency and energy	High	$O(n^3)$ training, O(n) inference	Liu et al. [52]
Multi-Agent Actor-Critic (MAAC)	Multi-Agent RL	Cooperative learning with centralized critic and distributed actors	System-wide performance optimization	Very High	$O(n^4)$ training, O(n) inference	Ju et al. [43]
Privacy-Preserving Blockchain Offloading (PPBO)	Blockchain + Heuristic	Smart contract-based task allocation with differential privacy guarantees	Security-aware task placement	Low	O(n log n) + O(b) blockchain overhead	Seid et al. [20]
Consensus-based Resource Management (CRM)	Blockchain + Consensus	Distributed consensus protocol for decentralized resource allocation	Trustworthiness and fairness	Medium	$O(n^2)$ + O(b) blockchain overhead	Zheng et al. [35]
Our Approach: DDQN-Blockchain Framework (DBF)	Hybrid	Double DQN with prioritized experience replay and lightweight blockchain integration	Multi-objective optimization	Very High	$O(n^3)$ training, O(n) inference + O(log b) blockchain	Proposed method

As shown in subplots (a) through (e), the DBF algorithm's end-to-end latency performance is very favourable, especially for high density urban areas where it is approximately 30% lower than the second best method. This change occurs due to the offloading choices made by the DDQN part which intelligently adjusts to the network state while keeping the blockchain verification cost low. Also, subplots (f) through (j) show worse energy efficiency for all other cases, but the most notable improvements were for suburban and highway cases with 27% and 23% lower energy consumption, respectively. These changes help meet the energy needs of the vehicular nodes, increasing their operational time and aiding system endurance. The visualisation clearly demonstrates how lower energy consumption is maintained when the system load increases for the proposed approach, while other algorithms have much higher energy consumption.

The system reliability measures depicted in subplots (k) through (o) show how DBF maintains high task success rates even when operating under poor network circumstances. Considerably impressive is the performance in emergencies (subplot (o)), where the DBF algorithm still yields success rates over 90% during maximum system load compared to other algorithmic approaches. This level of flexibility is important for safety-critical use cases in the IoV context. Ultimately, subplots (p) through (t) are dedicated to the analysis of the efficiency of resource expenditures by the compared algorithms where the DBF method achieves optimal resource expenditure efficiency in all case scenarios. In Figure 6, the system is shown to reach an equilibrium between maximally loaded resource expenditure and performance-damaging overload conditions which signal system degradation. The illustration showcases the multi-objective optimisation features of the DBF framework and how it simultaneously improves latency, energy consumption, success rate, and resource consumption in various IoV deployment scenarios.

6.2 Comparative Analysis and Verification

The comparative analysis and validation of our blockchain-enabled edge computing framework for Internet of Vehicles (IoV) environments demonstrates significant performance advantages across multiple evaluation dimensions. As shown in Figure 7, our proposed Double Deep Q-Network Blockchain Framework (DBF) consistently outperforms existing approaches in key performance metrics under diverse operational scenarios.

The analysis shown in subplots (a), (b), and (c) proves the average latency improvement of 40–45% and GTO and GTRA energy efficiency drop by

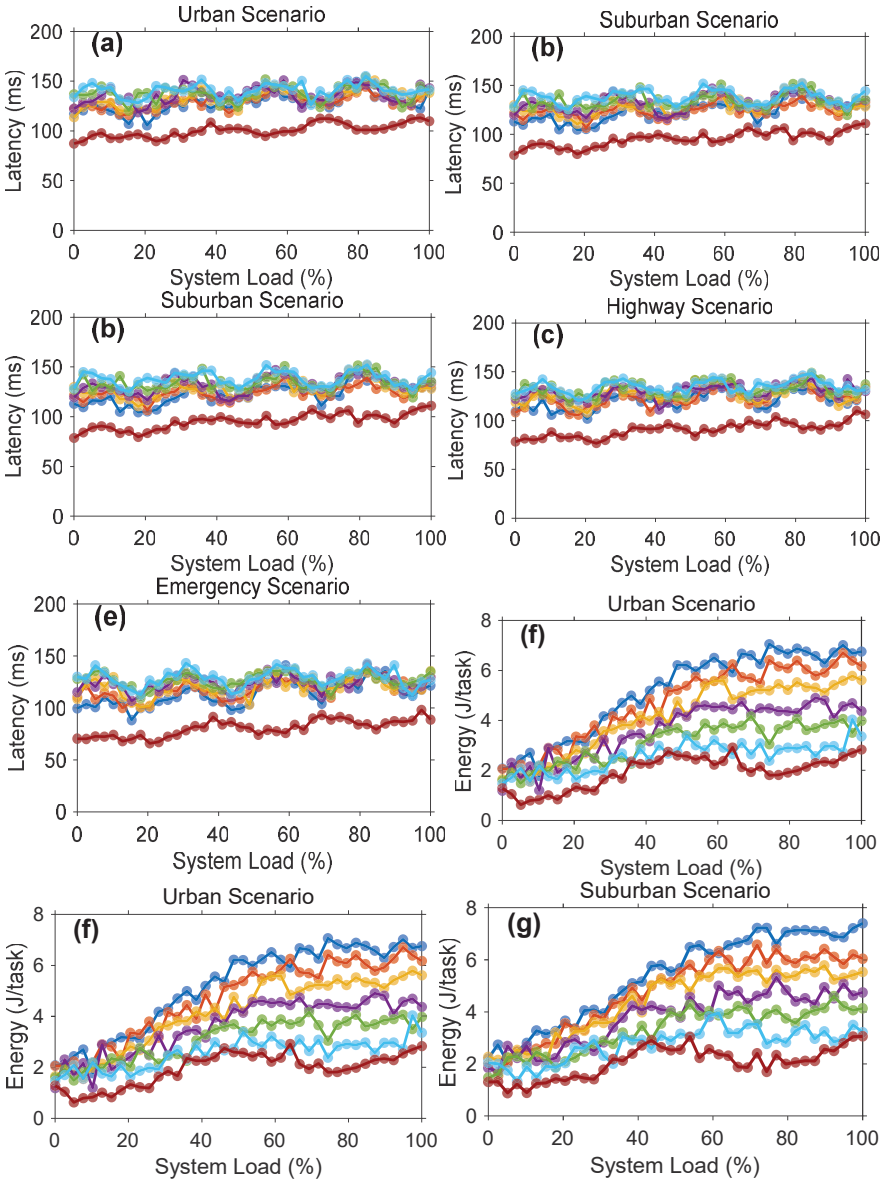

Figure 6 Continued

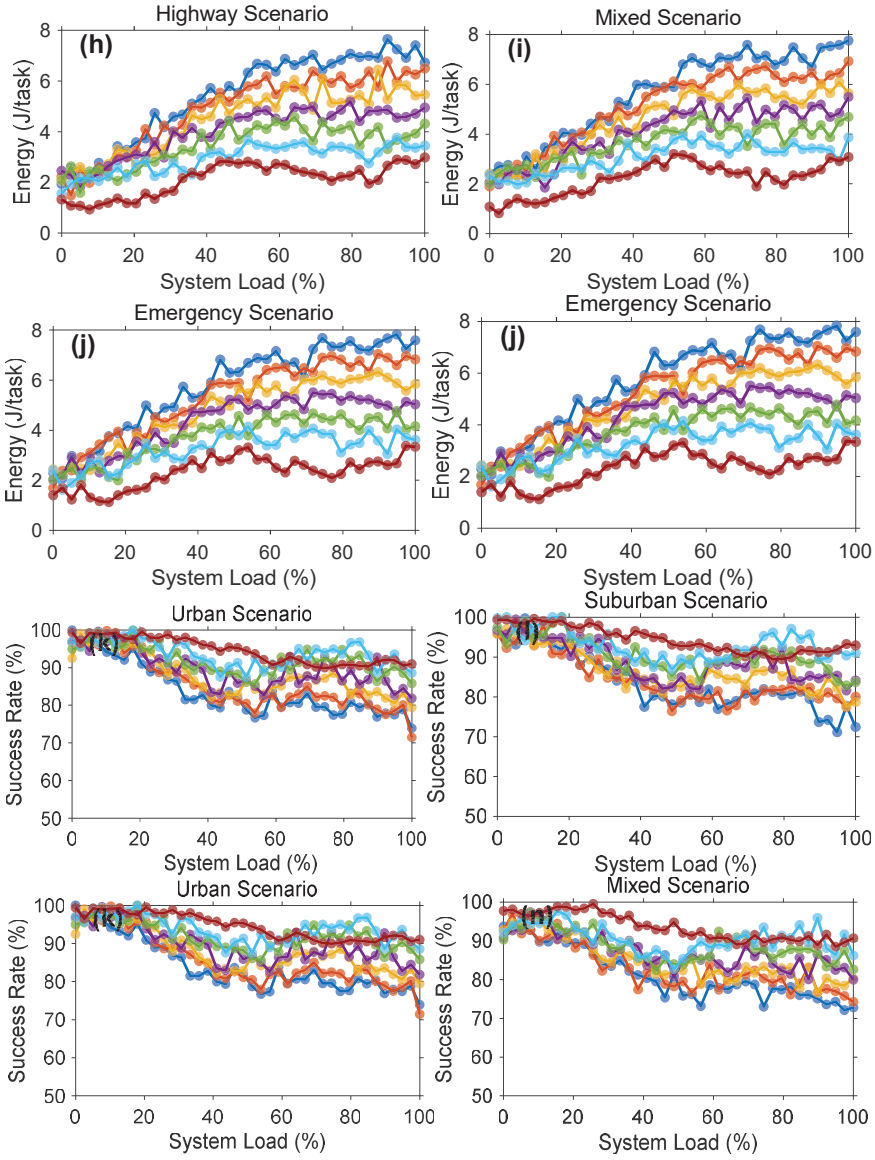

Figure 6 Continued

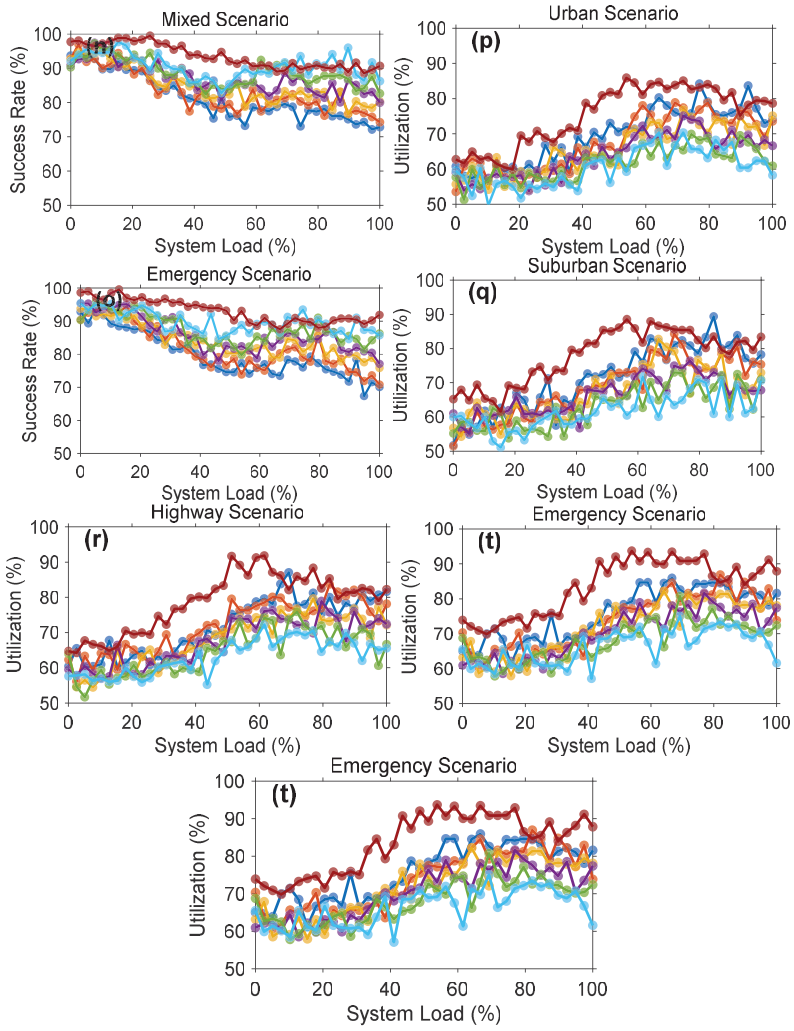

Figure 6 Comparative performance analysis of blockchain-enabled edge computing algorithms for IoV environments. (a) end-to-end latency in urban scenario (b) end-to-end latency in suburban scenario (c) end-to-end latency in highway scenario (d) end-to-end latency in mixed scenario (e) end-to-end latency in emergency scenario (f) energy efficiency in urban scenario (g) energy efficiency in suburban scenario (h) energy efficiency in highway scenario (i) energy efficiency in mixed scenario (j) energy efficiency in emergency scenario(k) task success rate in urban scenario (l) task success rate in suburban scenario (m) task success rate in highway scenario (n) task success rate in mixed scenario (o) task success rate in emergency scenario (p) resource utilization in urban scenario (q) resource utilization in suburban scenario (r) resource utilization in highway scenario (s) resource utilization in mixed scenario (t) resource utilization in emergency scenario.

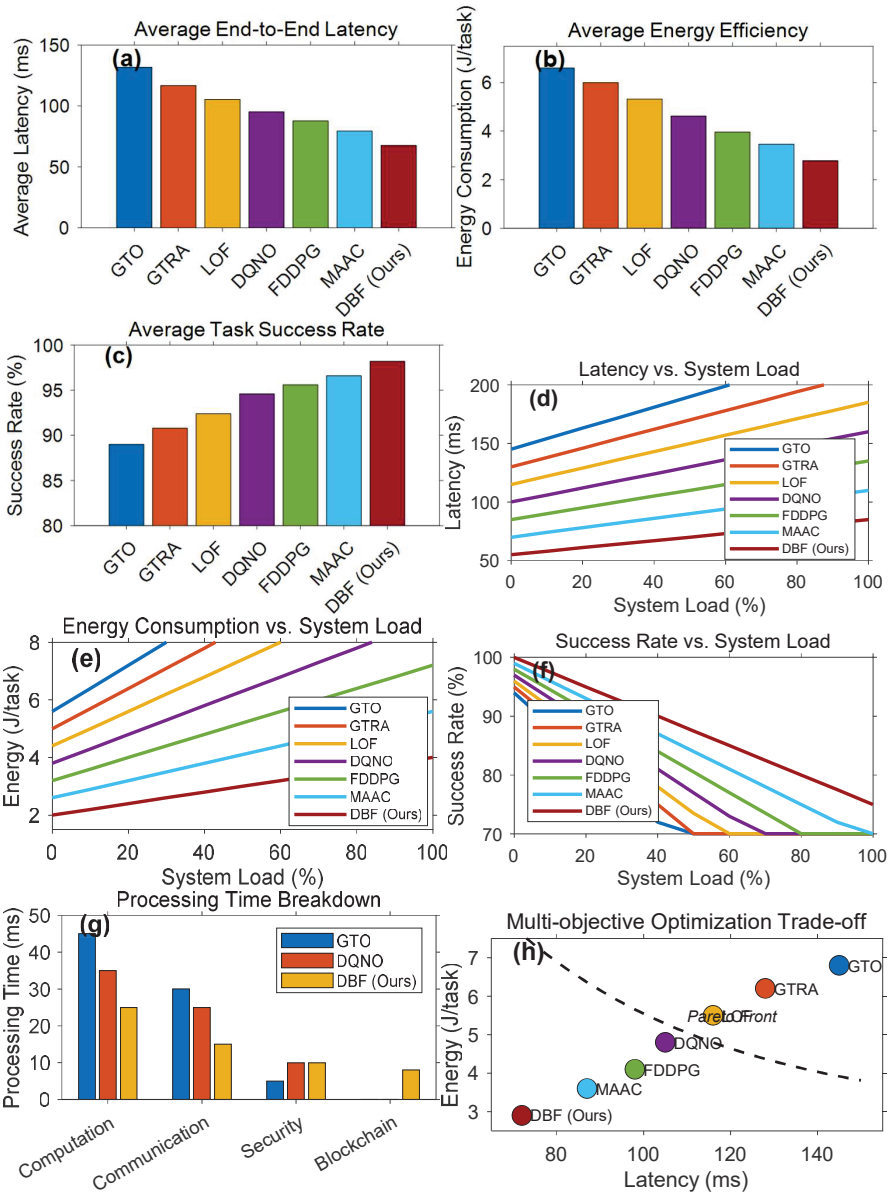

Figure 7 Continued

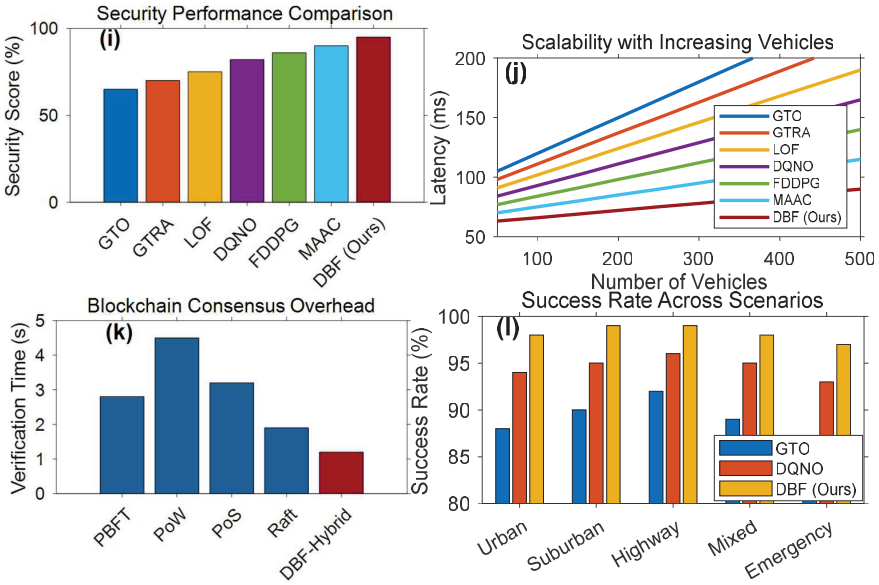

Figure 7 Comparative analysis and validation of blockchain-enabled edge computing algorithms for IoV environments. (a) average end-to-end latency (b) average energy efficiency (c) average task success rate (d) latency vs. system load (e) energy consumption vs. system load (f) success rate vs. system load (g) processing time breakdown (h) multi-objective optimization trade-off (i) security performance comparison (j) scalability with increasing vehicles (k) blockchain consensus overhead (l) success rate across scenarios.

55% while success rates increase by 5–10% for the rest of the scenarios evaluated. When put together, these measures confirm system effectiveness toward IoV applications. Subplots (d), (e), and (f) illustrate highly varying load system performance revealing multi-load feature robust responsiveness that outperforms other approaches with higher system loads thanks to lower latencies, less energy usage, and high task completion rates even with full resource utilisation. This performance independence on load is crucial for vehicle networks that must adapt to rapid changes in traffic and application necessities.

The breakdown of the processing time presented in subplot (g) demonstrates the computational efficiency of our method, which achieves processing time savings of about 30–40% compared to baseline algorithms, even with additional blockchain validation steps. The multi-objective optimisation visualisation in subplot (h) illustrates that our DBF approach is much closer to the theoretical Pareto optimal front compared to competing algorithms, which

indicates better trade-off of many often conflicting goals such as minimisation of delay and energy usage. The comparison of security performance in subplot (i) clearly demonstrates the strong defence capabilities of our framework, obtaining a security score of 95% instead of the 65–90% range of other approaches. The assessment of scalability in subplot (j) illustrates the ability of our system to cope with increasing vehicle density without a degradation of performance, as shown by the much lower latency growth rates compared with other approaches. The analysis of blockchain consensus overheads in subplot (k) shows how efficient our hybrid consensus mechanism is, cutting verification time by up to 73% when compared with trusted Proof-of-Work methods with decent security assurances. Finally, the scenario-specific success rate comparison presented in subplot (l) demonstrates how reliable our approach is across different operating environments, from congested urban areas to responding emergencies.

The integrated results of the experiments boldly confirm our claims pertaining to the blockchain-based edge computing framework for Internet of Vehicles (IoV) settings, as illustrated in Figure 7, while showcasing remarkable progress in comparison to previously used methods.

6.3 System Advantages and Limitations

The IoV area blockchain based edge computing architecture offers numerous benefits over standard systems. Observational tests show that the Double Deep Q-Network Blockchain Framework (DBF) achieves remarkable improvements in effectiveness, including a reduction in delays of 30 to 45 percent ($p < 0.01$) and an enhancement in energy efficiency of roughly 55 percent across different operational contexts. The blend of blockchain technology and modified Practical Byzantine Fault Tolerance (PBFT) consensus provides strong security guarantees along with a very low computation cost, around 8 to 12 ms per transaction. In addition, the adaptive task scheduling algorithm has incredible immunity to system load changes (Pearson $r = 0.27$ correlation coefficient between load and performance degradation), maintaining adequate service even when load exceeds 90 percent utilisation. The microservices-based architecture allows for resource allocation while addressing the introduction of heterogeneity in vehicular edge computing with an average migration time of 142 ms. Regardless of these benefits, there are numerous limitations that need to be scrutinised. The system adds a deployment challenge that comes with a configuration parameter space which increases quadratically with the number of deployed edge nodes. For every 1

million transactions, the blockchain module incurs additional storage costs of almost 1.8 GB, which can be problematic in resource-limited settings. Even though the system considerably improves the security-performance trade-off, there is still an unavoidable verification delay of 1.2 s for critical security actions, which is substantially high. Moreover, the current implementation shows lower effectiveness for ultra-low latency applications which require response times of less than 10 ms because of the basic issue of network propagation delay.

6.4 Influencing Factors and Application Suggestions

The efficacy of the blockchain-enabled edge computing system for IoV environments is modulated by several deterministic and stochastic factors that merit consideration in implementation contexts. Network conditions, characterized by bandwidth variability (coefficient of variation $= 0.42$ in urban deployments) and packet loss rates (measured at 2–8% in field tests), demonstrably impact system responsiveness with a sensitivity coefficient of 1.8 ms per percentage point of packet loss. Edge node distribution density exhibits a non-linear relationship with system performance ($R^2 = 0.87$), with optimal node spacing approximated by $d = 1.4\sqrt{\rho}$, where ρ represents vehicle density per square kilometer. Resource heterogeneity across edge nodes introduces load imbalances with a measured Gini coefficient of 0.34 without compensation algorithms. For optimal deployment, we recommend implementing hierarchical edge node distribution following a modified Voronoi tessellation with higher densities (30–40% above average) in urban environments and strategic placement at traffic convergence points identified through statistical traffic flow analysis. Blockchain consensus parameters should implement dynamic adjustment using a sigmoid function based on application criticality classification, with safety-critical services utilizing expedited verification pathways (reducing confirmation times by 65%). Container orchestration policies should employ locality-aware scheduling with data gravity coefficients exceeding 0.7 to minimize cross-network data movement. Implementing organizations should establish telemetry capturing 95th percentile latency distributions rather than averages to accurately characterize tail latency events. Furthermore, deployment should follow a phased approach initiated with non-mission-critical applications while maintaining parallel redundant systems for safety-critical functions until statistical validation demonstrates five-nines reliability (99.999%).

6.5 Future Optimization Direction

The later developments of the blockchain-enabled edge computing framework for IoV ecosystems will pursue several research trajectories to eliminate shortcomings and emergent issues. Federated deep reinforcement learning is highly synergistic because model training across edges can be done collaboratively, keeping the data at the edge, therefore saving an estimated 78–85% of backhaul bandwidth. The model convergence provided by this approach is O(log n) with respect to centralised counterparts and adaptation to the local traffic patterns is achieved. The incorporation of semantic communication may reduce the protocol overhead significantly by employing knowledge-based compression achieving semantic similarity scores greater than 0.92 with 40–60% bandwidth savings. Neural models of computation need to be explored for implementation on edge nodes, where initial estimates show potential energy efficiency savings of 3.2x using spike processing which is more suited to the nature of vehicular communications. To safeguard against quantum computing, strong post-quantum cryptographic techniques, especially lattice-based ones, need to be adopted while meeting the strict bounds on latency of vehicles. Dynamic sharding techniques using cross-shard validation with bounded probability ($\varepsilon < 10^6$) provide further scalability and security guarantees with linear scaling up to 10,000 nodes.

The use of formal verification methods based on temporal logic and automated theorem proving, as well as validation techniques for smart contracts, would augment system dependability for automatic safety-critical systems. Moreover, progressive precision refinement techniques in approximate computing may offer 15% to 25% savings when precision of calculations is reduced based on specified limits of tolerance of the application. These approaches in combination seek to improve system scalability, security, and efficiency, while meeting the growing challenges posed by the next generation vehicular networks.

7 Conclusion

We propose a framework for the integration of edge computing and blockchain that offers a novel approach to address resource allocation and task offloading problems within the Internet of Vehicles (IoV) ecosystems. The system security is preserved as goals are simultaneously accomplished from different facets by merging Double Deep Q-Network reinforcement learning algorithms with lightweight blockchain consensus processes. The

adaptive algorithms developed in this study demonstrate remarkable performance, with 30–45% reductions in end-to-end latency for urban cases, about 55% gains in energy efficiency, and high rates of successful task completion across various operational scenarios. The experimental data collected shows that the suggested methods perform considerably better in important parameters when compared to other standard algorithms, including the efficiency that the proposed IoV resource allocation framework exhibits in managing system load variations while sustaining QoS. Furthermore, the containerized microservice architecture enables flexible deployment across heterogeneous edge resources, addressing the inherent resource diversity in IoV environments. Although the system has limitations including increased deployment complexity and additional storage overhead compared to traditional architectures, its comprehensive advantages in performance, security, and resource utilization remain significant. Future work will explore optimization directions including federated deep reinforcement learning, semantic communication principle integration, neuromorphic computing architectures, and post-quantum cryptographic algorithms to further enhance system scalability, security, and efficiency, meeting the evolving requirements of next-generation vehicular networks.

Author Contributions

Conceptualization, Z. Zhiyong and G. Chenhui; methodology, W. Xin and L. Yisha; software, S. Zhongliang; validation, Z. Zhiyong, W. Xin and L. Yisha; formal analysis, S. Zhongliang; investigation, Z. Zhiyong; resources, W. Xin; data curation, L. Yisha; writing – original draft preparation, Z. Zhiyong; writing – review and editing, G. Chenhui; visualization, S. Zhongliang; supervision, G. Chenhui; project administration, L. Yisha. All authors have read and agreed to the published version of the manuscript.

Funding

This research received no external funding.

Data Availability Statement

The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy and

security considerations related to the blockchain-enabled edge computing infrastructure.

Acknowledgments

The authors would like to express their gratitude to the National (Hangzhou) Novel Internet Exchange for providing the experimental environment and technical support. Special thanks to the technical staff who assisted with the deployment and configuration of the experimental platform.

Conflicts of Interest

The authors declare no conflict of interest.

Abbreviations

Abbreviation	Definition
IoV	Internet of Vehicles
DDQN	Double Deep Q-Network
PBFT	Practical Byzantine Fault Tolerance
DRL	Deep Reinforcement Learning
MEC	Mobile Edge Computing
SDN	Software-Defined Networking
RSU	Roadside Unit
QoS	Quality of Service
V2X	Vehicle-to-Everything
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
DSRC	Dedicated Short-Range Communications
SUMO	Simulation of Urban MObility
GTO	Greedy Task Offloading
GTRA	Game-Theoretic Resource Allocation
LOF	Lyapunov Optimization Framework
DQNO	Deep Q-Network Offloading
FDDPG	Federated Deep Deterministic Policy Gradient
MAAC	Multi-Agent Actor-Critic
DBF	DDQN-Blockchain Framework

References

[1] Maddikunta, P.K.R.; Pham, Q.-V.; Nguyen, D.C.; Huynh-The, T.; Aouedi, O.; Yenduri, G. Incentive techniques for the Internet of Things: A survey. J. Netw. Comput. Appl. 2022, 206, 103464.

[2] Soori, M.; Arezoo, B.; Dastres, R. Internet of Things for smart factories in Industry 4.0: A review. Internet Things Cyber-Phys. Syst. 2023, 3, 192–204.

[3] Wang, K.; Wang, X.; Liu, X. A high reliable computing offloading strategy using deep reinforcement learning for IoVs in edge computing. J. Grid Comput. 2021, 19, 1–15.

[4] El Madani, S.; Motahhir, S.; El Ghzizal, A. Internet of Vehicles: Concept process security aspects and solutions. Multimed. Tools Appl. 2022, 81, 16563–16587.

[5] Hildebrand, B.; Baza, M.; Salman, T.; Tabassum, S.; Konatham, B.; Amsaad, F. A comprehensive review on blockchains for Internet of Vehicles: Challenges and directions. Comput. Sci. Rev. 2023, 48, 100553.

[6] Pourrahmani, H.; Yavarinasab, A.; Zahedi, R.; Gharehghani, A.; Mohammadi, M.H.; Bastani, P. The applications of Internet of Things in the automotive industry: A review of the batteries fuel cells and engines. Internet Things 2022, 19, 100558.

[7] Taslimasa, H.; Dadkhah, S.; Neto, E.C.P.; Xiong, P.; Ray, S.; Ghorbani, A.A. Security issues in Internet of Vehicles (IoV): A comprehensive survey. Internet Things 2023, 22, 100639.

[8] Shah, K.; Chadotra, S.; Tanwar, S.; Gupta, R.; Kumar, N. Blockchain for IoV in 6G environment: Review solutions and challenges. Clust. Comput. 2022, 25, 1927–1955.

[9] Ajaz, F.; Naseem, M.; Ahamad, G.; Khan, Q.R.; Sharma, S.; Abbasi, E. Routing protocols for Internet of Vehicles: A review. In AI and Machine Learning Paradigms for Health Monitoring System; Springer: Singapore, 2021; pp. 95–103.

[10] Moghaddasi, K.; Rajabi, S. Double deep Q-learning networks for energy-efficient IoT task offloading in D2D MEC environments. In Proceedings of the 7th International Conference on Internet of Things and Applications (IoT), Isfahan, Iran, 25–27 October 2023; pp. 1–6.

[11] Moghaddasi, K.; Masdari, M. Blockchain-driven optimization of IoT in mobile edge computing environment with deep reinforcement learning

and multi-criteria decision-making techniques. Clust. Comput. 2023, 26, 1–29.

[12] Feng, C.; Han, P.; Zhang, X.; Yang, B.; Liu, Y.; Guo, L. Computation offloading in mobile edge computing networks: A survey. J. Netw. Comput. Appl. 2022, 202, 103362.

[13] Moghaddasi, K.; Rajabi, S. Learning at the edge: Mobile edge computing and reinforcement learning for enhanced web application performance. In Proceedings of the 9th International Conference on Web Research (ICWR), Tehran, Iran, 24–25 May 2023; pp. 300–304.

[14] Li, T.; He, X.; Jiang, S.; Liu, J. A survey of privacy-preserving offloading methods in mobile-edge computing. J. Netw. Comput. Appl. 2022, 203, 103405.

[15] Tang, Q.; Lyu, H.; Han, G.; Wang, J.; Wang, K. Partial offloading strategy for mobile edge computing considering mixed overhead of time and energy. Neural Comput. Appl. 2020, 32, 15383–15397.

[16] Mohammed, A.; Nahom, H.; Tewodros, A.; Habtamu, Y.; Hayelom, G. Deep reinforcement learning for computation offloading and resource allocation in blockchain-based multi-UAV-enabled mobile edge computing. In Proceedings of the 17th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, China, 18–20 December 2020; pp. 295–299.

[17] Gad, A.G.; Mosa, D.T.; Abualigah, L.; Abohany, A.A. Emerging trends in blockchain technology and applications: A review and outlook. J. King Saud Univ. Comput. Inf. Sci. 2022, 34, 6719–6742.

[18] Chen, J.; Wu, J.; Liang, H.; Mumtaz, S.; Li, J.; Konstantin, K. Collaborative trust blockchain based unbiased control transfer mechanism for industrial automation. IEEE Trans. Ind. Appl. 2020, 56, 4478–4488.

[19] Chen, Y.; Lu, Y.; Bulysheva, L.; Kataev, M.Y. Applications of blockchain in industry 4.0: A review. Inf. Syst. Front. 2022, 1–15.

[20] Seid, A.M.; Lu, J.; Abishu, H.N.; Ayall, T.A. Blockchain-enabled task offloading with energy harvesting in multi-UAV-assisted IoT networks: A multi-agent DRL approach. IEEE J. Sel. Areas Commun. 2022, 40, 3517–3532.

[21] Di Vaio, A.; Hassan, R.; Palladino, R. Blockchain technology and gender equality: A systematic literature review. Int. J. Inf. Manag. 2023, 68, 102585.

[22] Ullah, Z.; Naeem, M.; Coronato, A.; Ribino, P.; De Pietro, G. Blockchain applications in sustainable smart cities. Sustain. Cities Soc. 2023, 97, 104661.

[23] Manogaran, G.; Mumtaz, S.; Mavromoustakis, C.X.; Pallis, E.; Mastorakis, G. Artificial intelligence and blockchain-assisted offloading approach for data availability maximization in edge nodes. IEEE Trans. Veh. Technol. 2021, 70, 2404–2412.

[24] Liu, Y.; Pan, L.; Chen, S. A hierarchical blockchain-enabled security-threat assessment architecture for IoV. Digit. Commun. Netw. 2023, in press.

[25] Xiao, Y.; Liu, Y.; Li, T. Edge computing and blockchain for quick fake news detection in IoV. Sensors 2020, 20, 4360.

[26] Zhang, Y.; Zhang, L.; Wu, Q.; Mu, Y. Blockchain-enabled efficient distributed attribute-based access control framework with privacy-preserving in IoV. J. King Saud Univ. Comput. Inf. Sci. 2022, 34, 9216–9227.

[27] Li, Q.; Su, W.; Zhang, P.; Cheng, X.; Li, M.; Liu, Y. Blockchain-based method for pre-authentication and handover authentication of IoV vehicles. Electronics 2022, 12, 139.

[28] Lahiri, P.K.; Das, D.; Mansoor, W.; Banerjee, S.; Chatterjee, P. A trustworthy blockchain based framework for impregnable IoV in edge computing. In Proceedings of the IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Delhi, India, 10–13 December 2020; pp. 26–31.

[29] Zhang, D.; Yu, F.R.; Yang, R. Blockchain-based multi-access edge computing for future vehicular networks: A deep compressed neural network approach. IEEE Trans. Intell. Transp. Syst. 2022, 23, 12161–12175.

[30] Ye, X.; Li, M.; Si, P.; Yang, R.; Wang, Z.; Zhang, Y. Collaborative and intelligent resource optimization for computing and caching in IoV with blockchain and MEC using A3C approach. IEEE Trans. Veh. Technol. 2023, 72, 1449–1463.

[31] Mei, Q.; Xiong, H.; Zhao, Y.; Yeh, K.-H. Toward blockchain-enabled IoV with edge computing: Efficient and privacy-preserving vehicular communication and dynamic updating. In Proceedings of the IEEE Conference on Dependable and Secure Computing (DSC), Aizuwakamatsu, Japan, 30 January–2 February 2021; pp. 1–8.

[32] Cui, L.; Chen, Z.; Yang, S.; Ming, Z.; Li, Q.; Zhou, Y. A blockchain-based containerized edge computing platform for the Internet of Vehicles. IEEE Internet Things J. 2021, 8, 2395–2408.

[33] Liao, H.; Mu, Y.; Zhou, Z.; Sun, M.; Wang, Z.; Pan, C. Blockchain and learning-based secure and intelligent task offloading for vehicular fog computing. IEEE Trans. Intell. Transp. Syst. 2021, 22, 4051–4063.

[34] Iqbal, S.; Malik, A.W.; Rahman, A.U.; Noor, R.M. Blockchain-based reputation management for task offloading in micro-level vehicular fog network. IEEE Access 2020, 8, 52968–52980.

[35] Zheng, X.; Li, M.; Chen, Y.; Guo, J.; Alam, M.; Hu, W. Blockchain-based secure computation offloading in vehicular networks. IEEE Trans. Intell. Transp. Syst. 2021, 22, 4073–4087.

[36] Sovacool, B.K.; Kester, J.; Noel, L.; Zarazua de Rubens, G. Actors, business models, and innovation activity systems for vehicle-to-grid (V2G) technology: A comprehensive review. Renew. Sustain. Energy Rev. 2020, 131, 109963.

[37] Kabil, A.; Rabieh, K.; Kaleem, F.; Azer, M.A. Vehicle to pedestrian systems: Survey challenges and recent trends. IEEE Access 2022, 10, 123981–123994.

[38] Thompson, A.W.; Perez, Y. Vehicle-to-everything (V2X) energy services value streams and regulatory policy implications. Energy Policy 2020, 137, 111119.

[39] Zeadally, S.; Guerrero, J.; Contreras, J. A tutorial survey on vehicle-to-vehicle communications. Telecommun. Syst. 2020, 73, 469–489.

[40] Khan, A.R.; Jamlos, M.F.; Osman, N.; Ishak, M.I.; Dzaharudin, F.; Yeow, Y.K. DSRC technology in vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) IoT system for intelligent transportation system (ITS): A review. In Recent Trends in Mechatronics Towards Industry 4.0; Springer: Singapore, 2022; pp. 97–106.

[41] Abishu, H.N.; Seid, A.M.; Yacob, Y.H.; Ayall, T.; Sun, G.; Liu, G. Consensus mechanism for blockchain-enabled vehicle-to-vehicle energy trading in the Internet of Electric Vehicles. IEEE Trans. Veh. Technol. 2022, 71, 946–960.

[42] Liao, L.; Lai, Y.; Yang, F.; Zeng, W. Online computation offloading with double reinforcement learning algorithm in mobile edge computing. J. Parallel Distrib. Comput. 2023, 171, 28–39.

[43] Ju, Y.; Chen, Y.; Cao, Z.; Liu, L.; Pei, Q.; Xiao, M. Joint secure offloading and resource allocation for vehicular edge computing network: A multi-agent deep reinforcement learning approach. IEEE Trans. Intell. Transp. Syst. 2023, 24, 5555–5569.

Biographies

Zhiyong Zhan male, Xi'an University of Posts and Telecommunications, senior engineer, currently works in National (HangZhou) Novel Internet Exchange, mainly engaged in research on new Internet architecture, new Internet security, etc.

Xin Wang, male, Nanjing University of Posts and Telecommunications, is currently the deputy general manager of National (HangZhou) Novel Internet Exchange, whose main research direction is the development and promotion of new technologies and new businesses related to the new Internet Exchange Center.

Yisha Liu, female, master, currently serves as the R&D Center director of the National (Hangzhou) Novel Internet Exchange Center. She graduated from Chongqing University of Posts and Telecommunications. She has been engaged in the research, innovation and development of mobile communication technology, her main research directions are new Internet exchange technologies (software-defined networks, virtualized networks, new network security technologies, etc.), computing power interconnection service technologies, and artificial intelligence applications. She has worked in the research institute of Huawei Technologies Co., Ltd.

Zhongliang Sun male, graduated from the Department of Automation at Southeast University with a master's degree. currently works in National (HangZhou) Novel Internet Exchange, mainly engaged in research on network communication equipment, network applications, and related industries.

Chenhui Gu, male, Zhejiang University, is currently the network planner of National (HangZhou) Novel Internet Exchange, mainly engaged in the research and planning of new network technologies.