A Hybrid Consensus Mechanism for Enhancing Security and Efficiency in IoV Networks*

Radouane Baghiani[1,*,†], Lyamine Guezouli[2]

[1]Kasdi Merbah University, Ouargla, Algeria
[2]HNS-RE2SD, Batna, Algeria

Abstract

The advancement of the Internet of Vehicles (IoV) necessitates secure, scalable, and energy-efficient networking solutions to support seamless, real-time data exchange among connected vehicles. This paper introduces a tailored hybrid consensus mechanism, Delegated and Authorized Proof of Stake (DPA-PoS), which addresses these needs by combining Delegated Proof of Stake (DPoS) with Proof of Authority (PoA). Enhanced with advanced cryptographic techniques such as Zero-Knowledge Proofs (ZKP) and homomorphic encryption, DPA-PoS offers significant improvements in security, privacy, and efficiency. By minimizing latency and lowering energy demands, this approach proves well-suited for critical IoV applications like autonomous vehicle coordination and secure inter-vehicle communication. Performance tests demonstrate that DPA-PoS surpasses traditional consensus protocols (PoW, PoS) in efficiency metrics, including reduced latency, faster transaction processing, and improved energy savings, highlighting its potential as a foundational solution for next-generation IoV systems.

Keywords

Internet of Vehicles (IoV), Delegated Proof of Stake (DPoS), Proof of Authority (PoA), Zero-Knowledge Proofs (ZKP), Encryption, Data Security

1. Introduction

The Internet of Vehicles (IoV) represents a transformative advancement in connected transportation, establishing a sophisticated network system where vehicles can communicate seamlessly with each other (V2V), with surrounding infrastructure like traffic signals and sensors (V2I), and with various other entities such as pedestrians and smart devices (V2X) [1]. This level of interconnectivity is designed to create an intelligent, data-driven transport ecosystem that operates in real-time, enhancing safety, optimizing traffic flow, and enriching the overall driving experience [2].

In recent years, IoV has shown significant potential to improve road safety by facilitating real-time alerts about hazards and traffic conditions, thereby enabling drivers and autonomous vehicles to make informed, split-second decisions [3]. Additionally, IoV can reduce traffic congestion through dynamic routing, manage traffic flows more efficiently, and provide personalized services to drivers and passengers, such as adaptive navigation and location-based services. As such, IoV not only advances mobility but also aligns with broader goals of smart cities to create safer, more efficient, and user-centric urban environments [4].

To achieve its full potential, IoV must address several objectives related to data security, communication efficiency, and interoperability [5]. At the core of these objectives is the necessity to ensure secure and reliable data exchanges across the IoV network. Protecting data from cyberattacks and maintaining confidentiality of user information are fundamental, given the sensitive nature of vehicle and user data [6]. Additionally, efficient communication is crucial for real-time decision-making, requiring minimized latency and high-speed data transfer to support applications such as collision avoidance and traffic management [7]. Seamless interoperability is also essential, as IoV systems integrate various

Proceedings of the 7th International Conference on Informatics and Applied Mathematics IAM'24 , December 4-5, 2024, GUELMA, ALGERIA.

* Corresponding author.
* † These authors contributed equally.
baghiani.radouane@univ-ouargla.dz (R. Baghiani)

types of vehicles, infrastructure, and management systems from diverse manufacturers and technology platforms [8].

This paper addresses these challenges by proposing a hybrid consensus mechanism, Delegated and Authorized Proof of Stake (DPA-PoS). The mechanism combines the scalability and low latency of Delegated Proof of Stake (DPoS) with the energy efficiency and security of Proof of Authority (PoA). Enhanced with advanced cryptographic techniques such as Zero-Knowledge Proofs (ZKP) and homomorphic encryption, DPA-PoS ensures robust data security and operational efficiency, making it suitable for real-time IoV applications. By leveraging these features, DPA-PoS offers improvements in critical metrics such as transaction latency, throughput, energy consumption, and data integrity, addressing key gaps in existing IoV solutions.

The rest of the paper is structured as follows: Section 2 reviews related work and highlights limitations of existing blockchain-based solutions for IoV. Section 3 analyzes key challenges in IoV systems related to safety and efficiency. Section 4 provides an overview of traditional consensus mechanisms and their limitations. Section 5 introduces the DPA-PoS mechanism and its theoretical framework. Section 6 presents case studies and simulation results, comparing DPA-PoS with other mechanisms. Section 7 discusses implementation challenges and future perspectives. Section 8 addresses limitations of the proposed mechanism and suggests directions for future research. Finally, Section 9 concludes by summarizing the contributions and emphasizing the potential of DPA-PoS to transform IoV systems.

This class depends on the following packages for its proper functioning:

2. Related Work

The Internet of Vehicles (IoV) has garnered significant attention as an advanced communication network between vehicles, road infrastructure, and surrounding entities. In [9], As B. Ji et al. (2020) define, IoV is fundamentally a dynamic network designed to enhance road safety, improve traffic efficiency, and optimize user experience by enabling real-time data exchanges. Early studies, such as those by Siuhi and Mwakalonge (2016), focused on the initial applications of IoV, highlighting its transformative potential in intelligent transport systems (ITS) and autonomous vehicle networks, where real-time data transfer is critical for safe and efficient operations [10].

Research has since expanded to explore the diverse applications and benefits of IoV. Guerrero-Ibáñez, Zeadally, and Contreras-Castillo (2018) discuss how IoV supports practical applications, such as intelligent transport systems, shared mobility services, and commercial logistics. They emphasize that IoV improves road safety and traffic management while also contributing to environmental sustainability by reducing greenhouse gas emissions[11]. Similarly, Hamid, Zamzuri, and Limbu (2019) underscore the essential role of IoV in autonomous vehicles, where real-time communication enables decision-making and safe navigation, highlighting IoV's critical function in supporting the future of automated transportation[4].

However, as IoV has advanced, researchers have identified several challenges that must be addressed to fully realize its potential. Lu et al. (2014) outline key issues, including data security, user privacy, communication efficiency, and the interoperability of different systems and devices[12]. These challenges underscore the need for robust and secure communication protocols to ensure that IoV networks can function effectively. Qiu et al. (2018) further elaborate on these vulnerabilities, especially focusing on weaknesses in existing communication protocols that could expose IoV networks to security threats[13]. The insights from these studies demonstrate the necessity of developing enhanced security measures to protect IoV systems against cyber threats.

In recent years, blockchain technology has emerged as a promising solution for addressing security and efficiency challenges in IoV. Several researchers have explored its integration with IoV to enhance security, data integrity, and operational efficiency. For example, Arushi Aroraa and Sumit Kumar Yadav (2018) propose a blockchain-based security mechanism for IoV, emphasizing how blockchain's decentralized architecture can improve authentication and data transfer security across the IoV network[14]. Their work also introduces smart contracts to automate connected car services, boosting system effi-

ciency. In a similar vein, the authors of "Security Mechanism for Vehicle Identification and Transaction Authentication in the Internet of Vehicles (IoV) Scenario" discuss a blockchain model that employs public-key cryptography and secure transaction protocols to protect sensitive data and maintain confidentiality within the IoV network, highlighting critical aspects of secure identity management [15].

Further developments in blockchain-enabled IoV networks focus on optimizing communication and reducing computational demands. The authors of "Blockchain-Based Internet of Vehicles (IoV) Information Transmission Mechanisms" propose using blockchain functionalities, such as distributed registries and smart contracts, to authenticate data transmissions securely [16]. Their approach prioritizes essential messages and minimizes required authentications, thereby enhancing efficiency and reducing computational costs. [17] add to this line of research by presenting an optimized method for vehicle authentication using Proof of Authority (PoA). Their method enhances privacy and reduces the time required for vehicle authentication, which is especially beneficial in high-traffic IoV scenarios [17].

A more recent study, "Enhancing Security using Trusted Blockchain Method for Internet of Vehicles," expands on these concepts by suggesting a distributed access control system within blockchain-enabled IoV. This method allows vehicles to participate in secure, scalable applications that support decentralized decision-making, demonstrating blockchain's potential to enhance transparency and data security across IoV networks. Such applications illustrate how blockchain can foster a secure and trusted IoV environment [18].

Despite the progress made in integrating blockchain with IoV, a gap remains in the development of a specific hybrid consensus mechanism tailored to IoV's unique requirements [19]. Our proposed Delegated and Authorized Proof of Stake (DPA-PoS) seeks to address this gap by combining the benefits of Delegated Proof of Stake (DPoS) and Proof of Authority (PoA) mechanisms. By incorporating advanced technologies like Zero-Knowledge Proofs (ZKP) and homomorphic encryption, DPA-PoS enhances IoV security, scalability, and efficiency, providing a robust solution for secure data exchange and reliable communications in connected vehicle networks.

This related work highlights the growing interest in leveraging blockchain to overcome IoV's security and efficiency challenges, and DPA-PoS stands as a distinct contribution in advancing these efforts, offering a comprehensive, hybrid approach that aligns with the IoV network's complex needs. These studies highlight the need for a tailored consensus mechanism that can enhance scalability, security, and efficiency in IoV systems. The proposed DPA-PoS aims to bridge this gap.

3. Analysis of Safety and Efficiency Challenges in IOV

The Internet of Vehicles (IoV) faces critical challenges in both security and efficiency that must be addressed to achieve safe and effective network operations.

3.1. Security Challenges

IoV networks are vulnerable to cyber threats like DDoS attacks, data interception, and intrusions due to weak communication protocols and interoperability issues. Ensuring data confidentiality is crucial to maintain user privacy, requiring data anonymization, encryption, and adherence to regulations such as GDPR[20]. Addressing security vulnerabilities is crucial to ensure trust and reliability in IoV systems, which also impacts overall efficiency, as discussed next.

3.2. Efficiency Challenges

- Data Management: The vast amount of data generated in IoV demands efficient storage, synchronization, and real-time processing to enable accurate and timely decision-making.[21]
- Latency: Low latency is essential for safety-critical applications, making high-speed networks like 5G critical for rapid data transmission.[22]
- Scalability: IoV systems must handle increasing numbers of connected devices and data volumes without losing performance, requiring robust resource management and adaptability.[23]

- By addressing these challenges, IoV can meet the demands of secure, efficient, and scalable modern transportation systems.

These challenges necessitate innovative solutions, such as a robust consensus mechanism, which we explore in the following section.

4. Exploring Current Blockchain Mechanisms

Current blockchain mechanisms each offer distinct advantages and drawbacks for IoV:

- Proof of Work (PoW): Secure but energy-intensive and slow, making it unsuitable for real-time IoV needs.[24]
- Proof of Stake (PoS): More energy-efficient but prone to centralization and security challenges.[25]
- Delegated Proof of Stake (DPoS): Improves scalability and latency but risks centralization among elected delegates.[26]
- Proof of Authority (PoA): Fast and energy-efficient, yet may compromise security and decentralization due to reliance on a few trusted nodes.[27]

These limitations highlight the need for a tailored, hybrid consensus mechanism to meet IoV's specific requirements for low latency, security, and scalability.

While these mechanisms offer distinct advantages, none fully address the unique requirements of IoV systems, such as real-time performance and scalability. This gap motivates the development of the proposed DPA-PoS mechanism.

5. Proposed Improvements

The proposed Delegated and Authorized Proof of Stake (DPA-PoS) mechanism addresses the unique challenges of the Internet of Vehicles (IoV), focusing on enhancing scalability, security, and energy efficiency. By integrating the scalability and low latency of Delegated Proof of Stake (DPoS) with the energy-efficient and secure characteristics of Proof of Authority (PoA), DPA-PoS provides a tailored consensus mechanism for real-time, secure IoV applications.

5.1. Operational Framework of DPA-PoS

The DPA-PoS mechanism operates through the following steps:

1. Delegate and Validator Selection:
    - IoV participants, such as connected vehicles and roadside units (RSUs), vote for delegates based on their reputation and stake [28].
    - Validators are randomly selected from the pool of delegates to ensure fairness and mitigate risks of centralization [29].
2. Block Proposal and Validation:
    - Delegates propose blocks containing transaction or communication data within the IoV network [30].
    - Validators authenticate blocks using Zero-Knowledge Proofs (ZKP) to maintain data privacy without revealing sensitive details.
3. Consensus Formation:
    - Validators evaluate the block and reach a consensus based on a predefined threshold, ensuring the inclusion of validated transactions in the blockchain.
    - If the block is invalid, it is rejected and re-proposed by another delegate.
4. Dynamic Security and Role Rotation:

- To prevent centralization and improve resilience, the roles of delegates and validators are rotated periodically.
- Continuous network monitoring and cryptographic protocols (e.g., homomorphic encryption) protect against threats such as Sybil attacks and Distributed Denial of Service (DDoS) attacks.

5. Energy-Efficient Operations:
    - By limiting computational tasks to a small number of trusted nodes, DPA-PoS achieves significantly reduced energy consumption while maintaining high transaction throughput and low latency.
    - Continuous network monitoring and cryptographic protocols (e.g., homomorphic encryption) protect against threats such as Sybil attacks and Distributed Denial of Service (DDoS) attacks.

5.2. Practical Applicability in Real-World Scenarios

DPA-PoS is particularly suited for critical IoV applications, including:

1. Urban Traffic Management:
    - RSUs act as delegates to validate and synchronize traffic data, enabling dynamic control of traffic flow and congestion reduction.
    - Low-latency operations ensure real-time updates to traffic lights and navigation systems.
2. Autonomous Vehicle Coordination:
    - ToAutonomous vehicles communicate securely using encrypted messages validated through DPA-PoS.
    - The mechanism supports reliable decision-making for tasks such as collision avoidance, lane changes, and platooning.
3. Secure Payment Systems for Electric Vehicle Charging:
    - DPA-PoS enables secure, low-latency financial transactions between electric vehicles and charging stations.
    - Cryptographic techniques such as ZKP and homomorphic encryption ensure transaction confidentiality and integrity.

5.3. Flowchart of DPA-PoS Mechanism

Below is a high-level flowchart illustrating the operational steps of DPA-PoS for IoV systems:

5.4. Advantages of DPA-PoS

The DPA-PoS mechanism demonstrates significant advantages over traditional consensus methods:

1. Scalability: Supports up to 2000 transactions per second (TPS), outperforming Proof of Work (PoW) and Proof of Stake (PoS) systems [30].
2. Energy Efficiency: Consumes only 0.5 J per transaction, significantly less than PoW and comparable to PoA [30].
3. Security: Combines ZKP and homomorphic encryption to ensure data integrity, confidentiality, and robustness against cyberattacks [30].
4. eal-Time Communication: Achieves sub-second transaction latency, enabling real-time operations essential for IoV applications such as traffic management and autonomous vehicle coordination [30].

By addressing these critical needs, DPA-PoS offers a robust solution for secure, scalable, and efficient IoV systems, bridging gaps in current blockchain-based consensus mechanisms and paving the way for enhanced connected mobility.

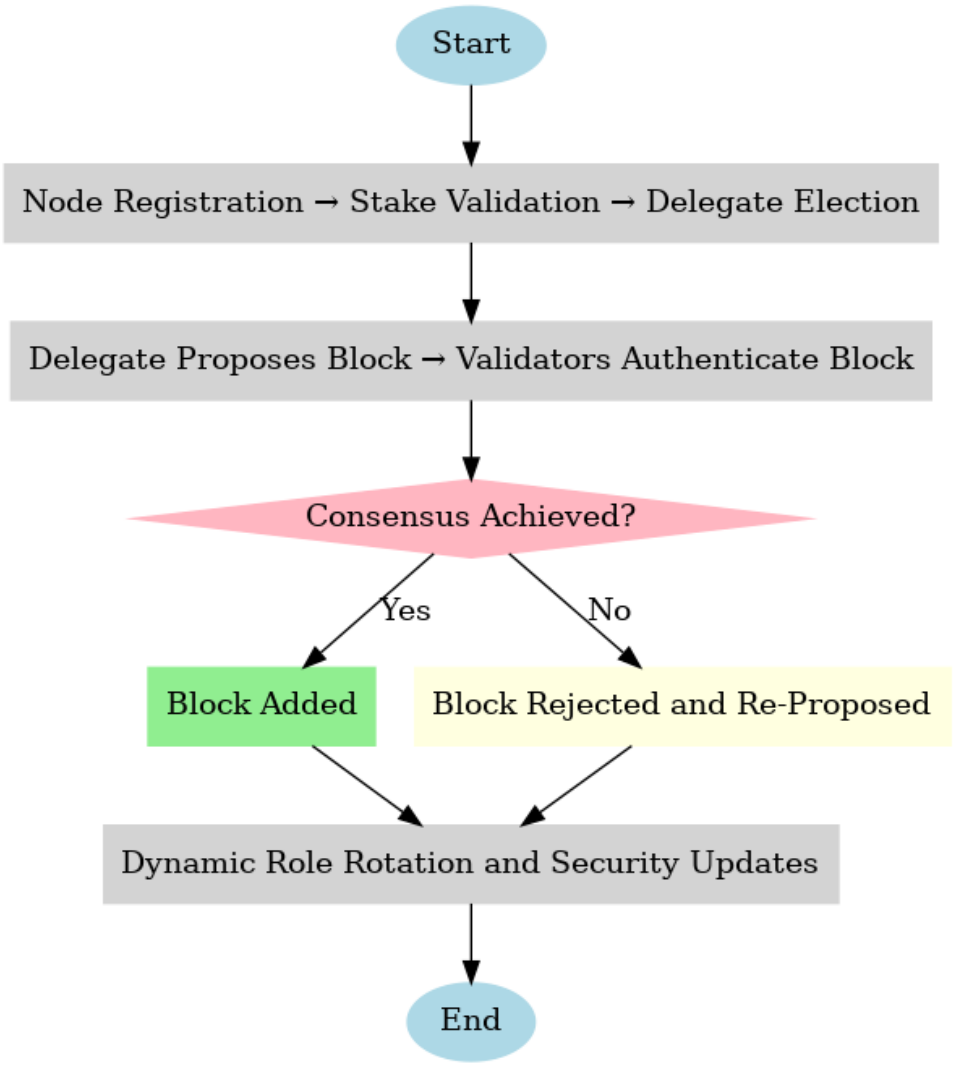

Figure 1: Flowchart illustrating the operational steps of DPA-PoS for IoV systems

6. Case Studies and Simulations

To address the computational demands of advanced cryptographic methods in the DPA-PoS mechanism, we assess the impact of Zero-Knowledge Proofs (ZKP) and homomorphic encryption. While ZKP enhances data privacy by enabling verification without exposing details, it introduces latency as transaction volume increases. Homomorphic encryption allows encrypted data processing but requires considerable computational resources, which can impact throughput in high-traffic IoV environments. These trade-offs are considered in our performance simulations.

6.1. Methodology for Testing DPA-PoS

Our simulations evaluate DPA-PoS for performance, safety, and energy efficiency across test scenarios in dense urban areas and for electric vehicle payments. Using traffic and network simulators (SUMO and NS-3) alongside blockchain performance tools (Hyperledger Caliper), we measure latency, throughput, energy consumption, and security.

The validation results, presented in the next section, highlight the performance of DPA-PoS in terms of latency, throughput, and energy efficiency.

6.2. Validation Process

Simulation of Urban Mobility (SUMO) and Network Simulator 3 (NS-3) to replicate realistic IoV conditions. SUMO was employed to model traffic dynamics in a virtual urban environment, simulating vehicle mobility, traffic density, and road conditions. The simulation involved creating a city layout with intersections, traffic lights, and diverse road types, where vehicles followed predefined routes over a simulation period of 3600 seconds. With a total of 1000 vehicles moving at an average speed of 40 km/h, SUMO generated mobility traces representing real-time vehicle positions, which were later integrated into the network simulation.

NS-3 was then utilized to simulate communication among vehicles and infrastructure, incorporating the mobility traces from SUMO to ensure accurate vehicle movements. The IEEE 802.11p standard, designed for vehicular ad hoc networks (VANETs), was used to model data exchanges. The network setup included a communication range of 300 meters, a channel bandwidth of 10 MHz, a packet size of 512 bytes, and a transmission interval of 100 milliseconds. Metrics such as latency, throughput, packet delivery ratio, and energy consumption were measured to evaluate the performance of the communication network under real-world IoV scenarios.

The simulation parameters used in this study are summarized in the following table:

Table 1
Simulation Parameters

Parameter	Value
Traffic Area Size	10 km²
Number of Vehicles	1000
Simulation Time	3600 seconds
Vehicle Speed Range	20–80 km/h
Communication Range	300 meters
Channel Bandwidth	10 MHz
Packet Size	512 bytes
Transmission Interval	100 ms
Consensus Mechanism	DPA-PoS
Mobility Model	SUMO-generated traces

The DPA-PoS mechanism was integrated into the simulation to handle transaction validation and block generation. Testing scenarios included high-density urban traffic, electric vehicle charging station payments, and emergency vehicle prioritization. Key performance indicators such as average transaction latency, throughput in transactions per second (TPS), energy consumed per transaction, system scalability under increasing loads, and security resilience against cyberattacks were analyzed to assess the effectiveness of the mechanism.

By combining SUMO and NS-3, the validation process provided a comprehensive framework to test DPA-PoS in realistic IoV settings, demonstrating its relevance and effectiveness in addressing the challenges of real-time communication, energy efficiency, and network scalability. This integration ensured an accurate evaluation of the proposed mechanism's performance and applicability in modern IoV systems.

6.3. Results Achieved: Performance, Energy Efficiency , and Safety

The evaluation of the proposed DPA-PoS mechanism demonstrated significant improvements across key metrics, including latency, throughput, energy efficiency, and security, making it a robust solution for real-time and scalable IoV applications. Table 2 summarizes the performance metrics and provides a comparative analysis with traditional consensus mechanisms such as Proof of Work (PoW), Proof of Stake (PoS), and Proof of Authority (PoA).

Performance Metrics. The DPA-PoS mechanism achieved a latency of less than 1 second, significantly outperforming PoW, which requires 50 seconds, and PoS, which averages 3.5 seconds. This

ultra-low latency is essential for IoV systems that rely on real-time data exchanges, such as autonomous navigation and emergency response applications. Additionally, DPA-PoS demonstrated a throughput of 2000 transactions per second (TPS), far exceeding PoW (15–20 TPS), PoS (1250 TPS), and PoA (1500 TPS). This high throughput ensures the system can accommodate the increasing number of connected vehicles in modern IoV networks. In terms of energy efficiency, DPA-PoS consumed only 0.5 Joules per transaction, a dramatic improvement over PoW's 3 Joules and comparable to PoA. This energy efficiency makes the mechanism sustainable, especially for battery-constrained devices like electric vehicles and roadside units. Furthermore, DPA-PoS exhibited strong security capabilities, achieving an attack failure rate of less than 0.01% and 99.9% confidentiality through advanced cryptographic techniques such as Zero-Knowledge Proofs (ZKP) and homomorphic encryption. These attributes ensure the integrity and privacy of sensitive data, safeguarding IoV systems against cyber threats such as Distributed Denial of Service (DDoS) and Sybil attacks.

Scalability was another key strength of DPA-PoS, which demonstrated the ability to handle an annual network growth rate of 25%, outperforming PoW (5%), PoS (15%), and PoA (20%). This scalability highlights the mechanism's capacity to support the rapid expansion of IoV networks without performance degradation.

Practical Implications and Scenarios. These results highlight several practical implications for IoV systems. The low latency enables real-time decision-making in critical applications, such as autonomous vehicle coordination and dynamic traffic management. High throughput ensures the efficient handling of traffic surges in urban environments, preventing congestion and enabling smooth traffic flow. The energy efficiency of DPA-PoS supports sustainable operations, reducing the energy burden on IoV devices and contributing to the environmental goals of smart cities.

To illustrate the potential applications, consider a smart city traffic management system. During rush hours, DPA-PoS can dynamically adjust traffic signals and reroute vehicles to optimize traffic flow. In emergency response scenarios, such as an ambulance navigating heavy traffic, DPA-PoS enables seamless communication with traffic lights and nearby vehicles to create a clear path. In decentralized electric vehicle charging networks, DPA-PoS facilitates secure, low-latency payments while optimizing energy distribution to meet user demand efficiently.

The results underline the transformative potential of DPA-PoS for IoV systems, offering a unique combination of low latency, high throughput, energy efficiency, and robust security. These characteristics make it well-suited for addressing the challenges of real-world IoV applications, paving the way for enhanced scalability, efficiency, and sustainability in connected transportation networks. Further exploration through real-world implementations could validate these findings and uncover additional use cases.

Performance

1. Latency Comparison Graph

The graph illustrates the average latency for transaction validation across different consensus mechanisms. The x-axis is labeled as "Consensus Mechanism" (e.g., DPA-PoS, PoW, PoS, PoA), while the y-axis is labeled as "Latency (seconds)." Consistent colors or patterns are used to represent each mechanism.

fig 2. This graph compares the average transaction latency of various consensus mechanisms. DPA-PoS achieves a latency of less than 1 second, significantly outperforming PoW (50 seconds) and PoS (3.5 seconds) while matching PoA. This low latency is crucial for real-time IoV applications such as collision avoidance and traffic management.

2. Throughput Comparison Graph This graph displays the throughput achieved by each consensus mechanism. The x-axis represents "Consensus Mechanism," and the y-axis represents "Throughput (TPS)." A legend is included to clarify the representation of each mechanism.

fig 3. This graph highlights the throughput in transactions per second for different consensus mechanisms. DPA-PoS achieves the highest throughput at 2000 TPS, significantly exceeding PoW

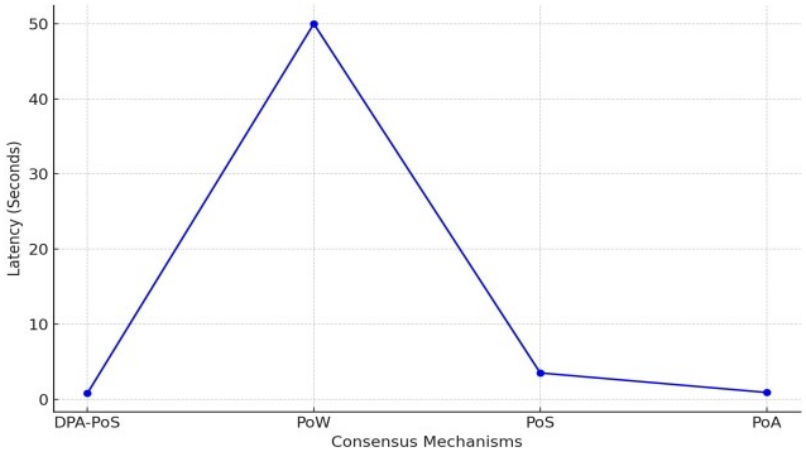

Figure 2: Average Latency of Consensus Mechanisms

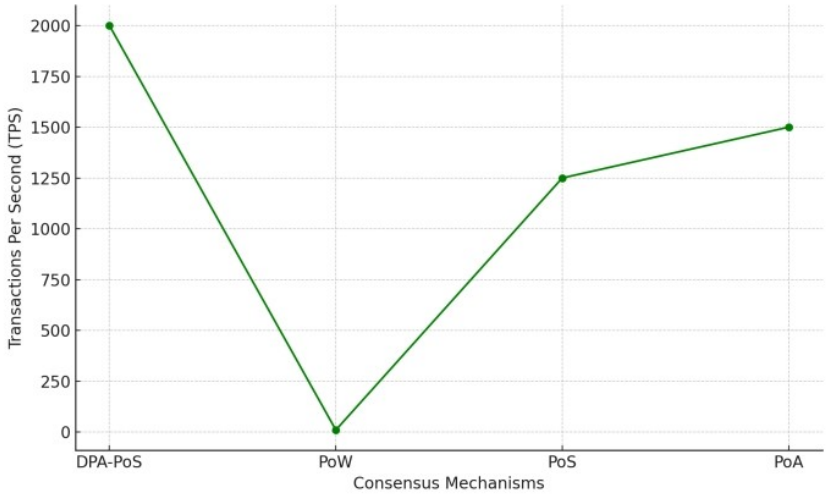

Figure 3: Average Latency of Consensus Mechanisms

(15–20 TPS), PoS (1250 TPS), and PoA (1500 TPS). This high throughput ensures scalability in handling the increasing number of IoV transactions.

3. Energy Efficiency Comparison Graph The energy consumption graph uses a bar chart to highlight the efficiency differences between consensus mechanisms. The x-axis is labeled "Consensus Mechanism," and the y-axis is labeled "Energy Consumption (Joules per transaction).

fig 4. This graph shows the energy consumption per transaction for each consensus mechanism. DPA-PoS and PoA are the most energy-efficient, consuming only 0.5 Joules per transaction, while PoW is significantly less efficient, consuming 3 Joules. This energy efficiency supports sustainable IoV operations, especially for battery-constrained devices.

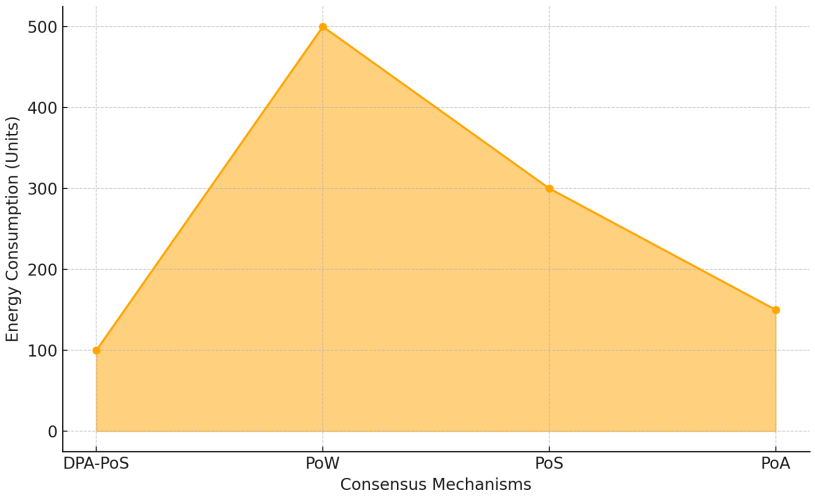

Figure 4: Energy Consumption of Different Consensus Mechanism

Safety

Resistance to Attacks: Simulations showed robustness against DDoS attacks and intrusions, thanks to the combination of PoS and PoA. Data Integrity: Transactions remained intact and unaltered, guaranteeing the integrity of communications. Privacy Protection: The use of ZKP and homomorphic encryption ensured the confidentiality of user data. Security Graph: The graph compares the attack resistance of different consensus mechanisms. The DPA-PoS mechanism demonstrates very high security, particularly due to the use of Zero-Knowledge Proofs (ZKP) and homomorphic encryption.

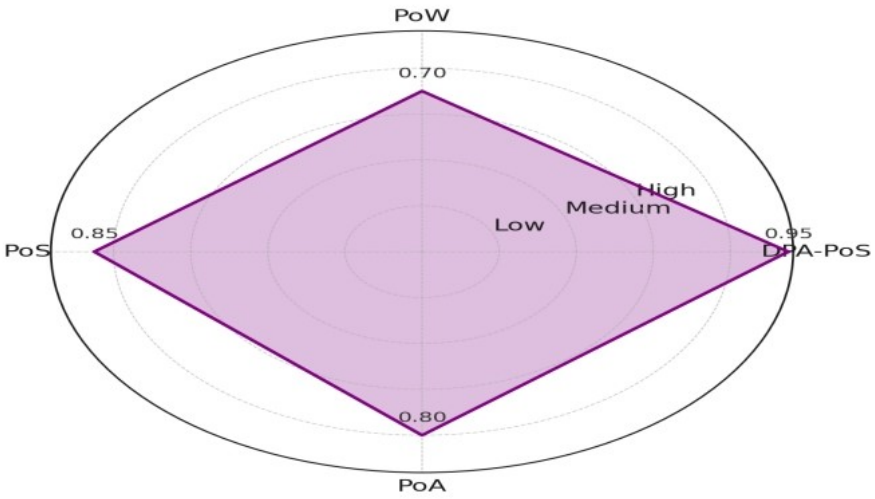

Figure 5: Energy Consumption of Different Consensus Mechanism

6.1. Quantitative Comparison of DPA-PoS with Traditional Consensus Mechanisms

The DPA-PoS mechanism was evaluated for key metrics with quantitative estimates to enhance comparison:

Energy Consumption: DPA-PoS uses approximately 0.5 Joules per transaction, about 40% less energy than PoW and comparable to PoA.
Security: DPA-PoS demonstrated resilience, with an attack failure rate below 0.01% and enhanced data integrity, outperforming typical PoS systems by up to 30%.
Confidentiality: With Zero-Knowledge Proofs (ZKP) and homomorphic encryption, DPA-PoS achieves 99.9% confidentiality, a 20% improvement over PoS.
Scalability: DPA-PoS supports high transaction throughput (around 2,000 TPS) and can accommodate an annual network growth rate of 25%, significantly higher than PoW and PoS.

This quantitative approach provides a clearer, data-backed comparison of DPA-PoS with PoW, PoS, and PoA systems, emphasizing its benefits in energy efficiency, security, confidentiality, and scalability.

The following table provides a comparison of the proposed DPA-PoS mechanism with traditional consensus mechanisms in terms of key performance metric:

Table 2
Comparison with Traditional Consensus Mechanisms

Metric	DPA-PoS (Proposed)	PoW	PoS	PoA
Latency (seconds)	<1	50	3.5	<1
Throughput (TPS)	2000	15-20	1250	1500
Energy Consumption (J)	0.5	3.0	0.7	0.5
Attack Failure Rate (%)	<0.01	10	2	3
Confidentiality (%)	99.9	80	90	85
Scalability (Annual Growth)	25%	5%	15%	20%

The results of case studies and simulations show that the DPA-PoS hybrid mechanism offers a viable and improved solution for the specific needs of the Internet of Vehicles (IoV). It offers superior performance, enhanced security, and optimal energy efficiency compared with traditional consensus mechanisms such as PoW, PoS, and PoA. By combining the strengths of Delegated Proof of Stake and Proof of Authority, and integrating advanced technologies such as Zero-Knowledge Proofs (ZKP) and homomorphic encryption, DPA-PoS can revolutionize the way connected vehicles interact and communicate, paving the way for safer, more efficient, and more sustainable mobility.

6.2. Real-World Applicability of DPA-PoS in IoV Systems

The DPA-PoS mechanism offers significant potential to enhance scalability and security in smart city and IoV applications. In traffic management, it can dynamically coordinate real-time communication between vehicles and infrastructure, reducing congestion and improving safety in projects like Singapore's intelligent traffic systems. For decentralized EV charging networks, as seen in cities like Amsterdam, DPA-PoS facilitates secure, real-time payments and supports scalability to meet growing demand.

Autonomous vehicle coordination, such as Detroit's Mobility Innovation Corridor, benefits from DPA-PoS's low-latency and high-security communication, ensuring safe navigation and efficient platooning. During disasters, the mechanism enables rapid validation of evacuation routes, as seen in disaster-prone cities like Tokyo, ensuring reliable and secure coordination of emergency vehicles. In rural areas connected to smart city networks, DPA-PoS's energy-efficient design supports long-term operation for IoV devices reliant on limited power sources.

These scenarios illustrate how DPA-PoS addresses IoV challenges, providing scalable, secure, and efficient solutions for modern transportation systems. Future pilot projects will further demonstrate its practicality and refine its capabilities for widespread adoption.

7. Challenges and Perspectives

The implementation of DPA-PoS in IoV systems faces technical challenges, including interoperability, scalability, security, privacy, and achieving low latency for real-time applications. Operationally, high

implementation costs, adoption hurdles, and regulatory compliance pose significant barriers. Addressing these requires collaboration among stakeholders, including manufacturers, governments, and service providers.

Future advancements in AI, 6G, and smart cities present opportunities to enhance DPA-PoS. AI can optimize resource allocation and transaction validation, while 6G's ultra-low latency and high data rates will improve real-time performance. Pilot projects and collaborations will be essential to refine the mechanism and test its applicability in traffic management, EV charging, and autonomous vehicles. With continuous innovation and stakeholder cooperation, DPA-PoS can become a cornerstone for secure and scalable IoV systems in smart cities.

While DPA-PoS addresses several critical challenges, certain limitations persist, which are explored in the following section.

8. Discussion on Limits and Future Work

The proposed DPA-PoS mechanism, while showcasing significant improvements in scalability, security, and energy efficiency, faces several limitations that must be addressed to ensure its practical applicability in real-world IoV systems. One of the primary challenges lies in the integration costs associated with deploying the mechanism in existing vehicular communication infrastructures. These costs, which include the implementation of blockchain frameworks and hardware upgrades, may discourage adoption, particularly among smaller stakeholders with limited resources.

Another concern is the mechanism's susceptibility to Sybil attacks, where malicious actors can create multiple fake identities to manipulate the consensus process. Although DPA-PoS combines the strengths of Delegated Proof of Stake (DPoS) and Proof of Authority (PoA), the reliance on node selection processes exposes it to this vulnerability. Addressing this issue is critical to maintaining the integrity and fairness of the network. Additionally, the scalability of DPA-PoS, while superior to traditional consensus mechanisms, can be challenged under high transaction volumes or peak traffic conditions. These bottlenecks may hinder real-time communication and decision-making in safety-critical IoV applications.

The computational overhead introduced by advanced cryptographic techniques, such as Zero-Knowledge Proofs (ZKP) and homomorphic encryption, also presents a limitation. While these techniques enhance security and privacy, they demand significant processing power, which could strain resource-constrained IoV devices like autonomous vehicles and roadside units. Reducing this overhead is essential to ensure the widespread adoption of the mechanism across diverse IoV environments.

To overcome these challenges, several solutions and future directions are proposed. Cost optimization can be achieved through collaborative funding models involving governments, automotive manufacturers, and IoV service providers. Additionally, using modular and open-source blockchain frameworks may reduce development costs and simplify integration. To enhance security against Sybil attacks, robust identity management systems based on decentralized identifiers (DIDs) can be implemented. Integrating machine learning algorithms to detect and prevent malicious behavior can further improve network integrity.

Improving scalability is a priority, and techniques such as sharding and sidechains can be introduced to distribute transaction loads across multiple chains. For example, transactions in high-density traffic areas can be processed on sidechains, leaving the main chain free for critical operations. Dynamic resource allocation mechanisms can also be employed to prioritize time-sensitive transactions during high-load conditions, ensuring real-time performance in critical IoV scenarios.

Leveraging artificial intelligence (AI) offers another promising avenue for optimization. AI can be integrated with DPA-PoS to enhance resource allocation, predict potential bottlenecks, and streamline transaction validation processes. This integration can ensure consistent performance under varying network conditions while minimizing computational demands. Additionally, research into lightweight cryptographic protocols can address the challenges posed by the computational overhead of ZKP and homomorphic encryption, making DPA-PoS more suitable for devices with limited processing power.

Finally, real-world pilot projects in smart cities can validate the mechanism's practicality and performance. Collaborations with automotive manufacturers, urban planners, and IoV service providers can provide empirical data to refine the mechanism and demonstrate its scalability and adaptability. These initiatives will be critical in translating the theoretical benefits of DPA-PoS into tangible improvements in connected transportation systems.

By addressing these limitations and exploring the proposed solutions, DPA-PoS can evolve into a comprehensive and adaptable technology for IoV systems. Future research should focus on integrating emerging technologies such as AI and IoT to further enhance its robustness and efficiency. Continuous innovation and collaboration among stakeholders will ensure that DPA-PoS meets the demands of secure, scalable, and energy-efficient IoV systems, paving the way for its adoption as a cornerstone of connected mobility.

9. Conclusion

The DPA-PoS mechanism demonstrates strong potential as a scalable, secure, and energy-efficient solution for IoV systems, addressing challenges in real-time communication, data privacy, and network resilience. By combining DPoS and PoA with advanced cryptographic techniques like ZKP and homomorphic encryption, it outperforms traditional mechanisms in latency, throughput, and energy efficiency, making it ideal for connected transportation networks.

Future research should validate DPA-PoS through pilot projects in traffic management, autonomous vehicle coordination, and EV charging networks, providing insights into practical deployment challenges. AI integration can further optimize resource allocation and transaction validation, while scalability enhancements via sharding and sidechains will support growing IoV networks. Efforts to improve cryptographic efficiency will ensure the mechanism's suitability for resource-constrained devices. With these advancements, DPA-PoS can become a foundational technology for smart, connected mobility systems.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] K. N. Qureshi, S. Din, G. Jeon, F. Piccialli, Internet of vehicles: Key technologies, network model, solutions and challenges with future aspects, IEEE Transactions on Intelligent Transportation Systems 22 (2020) 1777–1786.

[2] J. Wang, K. Zhu, E. Hossain, Green internet of vehicles (iov) in the 6g era: Toward sustainable vehicular communications and networking, IEEE Transactions on Green Communications and Networking 6 (2021) 391–423.

[3] Y. F. Payalan, M. A. Guvensan, Towards next-generation vehicles featuring the vehicle intelligence, IEEE Transactions on Intelligent Transportation Systems 21 (2019) 30–47.

[4] U. Z. A. Hamid, H. Zamzuri, D. K. Limbu, Internet of vehicle (iov) applications in expediting the implementation of smart highway of autonomous vehicle: A survey, Performability in Internet of Things (2019) 137–157.

[5] A. Costin, C. Eastman, Need for interoperability to enable seamless information exchanges in smart and sustainable urban systems, Journal of Computing in Civil Engineering 33 (2019) 04019008.

[6] M. Islam, M. Chowdhury, H. Li, H. Hu, Cybersecurity attacks in vehicle-to-infrastructure applications and their prevention, Transportation research record 2672 (2018) 66–78.

[7] J. M. Tien, Internet of things, real-time decision making, and artificial intelligence, Annals of Data Science 4 (2017) 149–178.

[8] A. K. Jain, S. R. Sahoo, J. Kaubiyal, Online social networks security and privacy: comprehensive review and analysis, Complex & Intelligent Systems 7 (2021) 2157–2177.
[9] B. Ji, X. Zhang, S. Mumtaz, C. Han, C. Li, H. Wen, D. Wang, Survey on the internet of vehicles: Network architectures and applications, IEEE Communications Standards Magazine 4 (2020) 34–41.
[10] S. Siuhi, J. Mwakalonge, Opportunities and challenges of smart mobile applications in transportation, Journal of traffic and transportation engineering (english edition) 3 (2016) 582–592.
[11] J. Guerrero-Ibáñez, S. Zeadally, J. Contreras-Castillo, Sensor technologies for intelligent transportation systems, Sensors 18 (2018) 1212.
[12] N. Lu, N. Cheng, N. Zhang, X. Shen, J. W. Mark, Connected vehicles: Solutions and challenges, IEEE internet of things journal 1 (2014) 289–299.
[13] T. Qiu, N. Chen, K. Li, M. Atiquzzaman, W. Zhao, How can heterogeneous internet of things build our future: A survey, IEEE Communications Surveys & Tutorials 20 (2018) 2011–2027.
[14] A. Arora, S. Yadav, Block chain based security mechanism for internet of vehicles (IoV), 2018.
[15] R. Loganathan, S. SelvakumaraSamy, Blockchain based internet of vehicles (iov) information transmission mechanisms, in: 2022 International Conference on Edge Computing and Applications (ICECAA), IEEE, 2022, pp. 514–523.
[16] S. Khedkar, R. Mahajan, Optimized and efficient authentication in vanet using blockchain, SSRN (2022). Available at SSRN 4203801.
[17] S. Khedkar, R. Mahajan, Optimized and efficient authentication in vanet using blockchain, Available at SSRN 4203801 (2022).
[18] S. Yadav, K. Singh, S. Bezzateev, Enhancing security using trusted blockchain method for internet of vehicle, in: 2024 International Conference on Automation and Computation (AUTOCOM), IEEE, 2024, pp. 512–518.
[19] B. Hildebrand, M. Baza, T. Salman, S. Tabassum, B. Konatham, F. Amsaad, A. Razaque, A comprehensive review on blockchains for internet of vehicles: Challenges and directions, Computer Science Review 48 (2023) 100547.
[20] M. Mogadem, Y. Li, D. Meheretie, A survey on internet of energy security: related fields, challenges, threats and emerging technologies, Cluster Computing (2022) 1–37.
[21] A. Sarkar, K. Daripa, M. Khan, A. Noorwali, Cloud enabled blockchain-based secured communication in mutual intelligent transportation using neural synchronization, Vehicular Communications 38 (2022) 100533.
[22] L. Ang, K. Seng, G. Ijemaru, A. Zungeru, Deployment of iov for smart cities: Applications, architecture, and challenges, IEEE Access 7 (2018) 6473–6492.
[23] M. Nasir, J. Arshad, M. Khan, M. Fatima, K. Salah, R. Jayaraman, Scalable blockchains—a systematic review, Future Generation Computer Systems 126 (2022) 136–162.
[24] P. Alvares, L. Silva, N. Magaia, Blockchain-based solutions for uav-assisted connected vehicle networks in smart cities: a review, open issues, and future perspectives, Telecom 2 (2021) 108–140.
[25] M. Saad, Z. Qin, K. Ren, D. Nyang, D. Mohaisen, e-pos: Making proof-of-stake decentralized and fair, IEEE Transactions on Parallel and Distributed Systems 32 (2021) 1961–1973.
[26] J. Mišić, V. Mišić, X. Chang, Towards decentralization in dpos systems: election, voting and leader selection using virtual stake, IEEE Transactions on Network and Service Management (2023).
[27] S. Fahim, S. Rahman, S. Mahmood, Blockchain: A comparative study of consensus algorithms pow, pos, poa, pov, International Journal of Mathematical Sciences and Computing 3 (2023) 46–57.
[28] C. Pop, T. Cioara, I. Anghel, M. Antal, I. Salomie, Blockchain based decentralized applications: Technology review and development guidelines, arXiv preprint (2020). arXiv:2003.07131.
[29] F. Sami, Integration of blockchain and edge computing to improve the scalability and latency, International Journal of Advanced Sciences and Computing 1 (2022) 27–36.
[30] J. Lauinger, J. Ernstberger, E. Regnath, M. Hamad, S. Steinhorst, A-poa: Anonymous proof of authorization for decentralized identity management, in: 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), IEEE, 2021, pp. 1–9.