Proof of Useful Work for Autonomous Vehicles

Vinit Saini
MSc in Computing – Blockchain
Dublin City University
Dublin, Ireland
vinit.saini2@mail.dcu.ie

Marcio Vieira
MSc in Computing – Blockchain
Dublin City University
Dublin, Ireland
marcio.vieira3@mail.dcu.ie

***Abstract*— Recent technological advancements have profoundly impacted numerous aspects of our daily lives, fundamentally altering how we connect, engage in leisure activities, perform work, and especially, travel. Autonomous Vehicles (AVs) emerge as a groundbreaking development, marking a significant change in the transportation sector. This research paper comprehensively explores the evolving research area of integrating blockchain technology with AVs. With a specific focus on mitigating challenges associated with AV deployment and operations, the paper examines the promising applications of blockchain in AVs, particularly highlighting the role of the innovative consensus mechanism known as PoUW. By aligning the computational power of blockchain networks with real-world problem-solving tasks, PoUW presents a unique opportunity to revolutionize data management, processing efficiency, and communication protocols within the AV ecosystem. This paper delves into the intricate synergy between blockchain technology and AVs. We explore how the decentralized, transparent, and secure nature of blockchain communication has the potential to revolutionize the landscape of autonomous transportation. The investigation focuses on two key areas: (1)Limitations of Traditional Consensus Mechanisms: we analyze the shortcomings of existing consensus mechanisms like Proof of Work (PoW) and Proof of Stake (PoS) in the context of AVs, and introduce Proof of Useful Work (PoUW); (2)Unique Challenges of AV Integration: we identify the specific challenges faced by integrating blockchain with AVs, including data security, processing speed, storage efficiency, information accuracy, and vehicle dynamic mobility. PoUW addresses these challenges by aligning computational tasks with real-world problem-solving, enhancing overall system efficiency and security.**

This research paper paves the way for a deeper understanding of how blockchain, particularly PoUW-based blockchains, can contribute to improved operational efficiency, safety, and sustainability in the rapidly developing field of autonomous vehicles.

Keywords—Blockchain, BaaS, Consensus Mechanisms, PoUW, Driverless cars, Autonomous vehicles, Security, Privacy, Data integrity, V2X communication

I. INTRODUCTION

The emergence AVs promises a revolution in transportation, offering enhanced safety, efficiency, and convenience. However, deploying and operating AVs presents unique challenges related to secure data communication, data integrity, and user privacy. Blockchain technology, renowned for its decentralized, transparent, and secure nature, has emerged as a potential solution [12, 13]. Yet, successful integration hinges on selecting a suitable consensus mechanism to ensure transaction integrity and network trust.

Table I Acronyms

Acronym	Description
AVs	Autonomous Vehicles
CAVs	Connected and Autonomous Vehicles
DPoS	Delegated Proof of Stake
GNSS	Global Navigation Satellite System
IoT	Internet of Things
IMU	Inertial Measurement Unit
LiDAR	Light Detection and Ranging
ITS	Intelligent Transportation System
PoS	Proof of Stake
PoW	Proof of Work
PoUW	Proof of Useful Work
RSUs	Road Side Units

Traditional blockchain applications like Bitcoin rely on consensus mechanisms such as Proof of Work (PoW) for security and transaction validation. However, PoW's security comes at a high cost, significant energy consumption due to its computationally intensive mining processes. While Proof of Stake (PoS) offers a more energy-efficient alternative, it raises concerns about wealth concentration and the "nothing at stake" problem, where validators may have less incentive to uphold network security due to minimal penalties for misbehavior [4].

Our research introduces a novel application of PoUW in the AV domain, departing from traditional PoW and PoS mechanisms. Existing research, as exemplified by works from Gupta et al. [7] and Dargahi et al. [6], primarily explores these mechanisms within the context of AV security and data integrity using blockchain technology [1, 2, 3]. Our approach emphasizes the efficient processing and validation of AV data through PoUW, contrasting the existing focus on security aspects [4, 6]. Furthermore, we aim to leverage PoUW's computational power for storage and advanced analysis of AV data, extending the scope beyond existing studies like those by Ball et al. [1] and Dong et al. [2].

Our proposal aligns with pioneering explorations of PoUW in decentralized systems, as discussed by Rathee et al. [8]. However, we take it a step further by applying it specifically to the AV ecosystem. This approach promises to bring more sustainable and efficient data processing and management practices to AV systems, going beyond

conventional blockchain applications in this field [4, 5]. By doing so, we aim to contribute new insights and extend the boundaries set by current research, such as the work by Baldominos and Saez [4] and the study on PoUW for AI on blockchain by Lihu et al. [5].

A. Research questions

This research investigates two key questions:

- How can PoUW be efficiently implemented in AVs, considering data handling, collection, processing speed, and storage accuracy?
- How does the application of PoUW contribute to the enhancement of the AVs domain?

This paper is structured as follow. Section II presents related work, Section III outlines the research methodology, Section IV presents performance evaluation, Section V presents results and analysis. The last section draws the conclusion and suggests future research directions.

II. Related Work

Our research builds upon existing work in AVs and blockchain technology, with a specific focus on applying PoUW to address communication network challenges in the AV domain. This existing work is summarized in this section.

A. Existing Work on AV Technology

As identified in our research, AV technology can be broadly divided into two key areas: individual vehicles and communication networks [13].

- Individual AVs: Significant advancements have been made in equipping individual vehicles with LiDAR, radar, camera sensors, and sophisticated machine learning algorithms for real-time navigation and complex environment recognition [1, 2]. High-definition maps and precise geological data further enhance their navigational capabilities [1, 2].
- Communication Networks: Communication networks facilitate data exchange between AVs and non-participating actors (data stores, Roadside Units (RSUs), GNSS systems, data processing units, and Intelligent Transport Systems) for improved safety and traffic efficiency [13]. However, current communication networks face challenges related to performance, scalability, and data security, making them vulnerable to breaches and modifications [13].

B. Blockchain and Security in AVs

Researchers have explored the potential of blockchain technology to address security concerns in AVs [1, 2, 3, 6]. These studies highlight the benefits of blockchain's decentralized, transparent, and secure nature for data communication and integrity within AV systems [12, 13]. However, the selection of a suitable consensus mechanism is crucial for ensuring the network's trustworthiness and transaction validation efficiency [4].

C. Limitations of Traditional Consensus Mechanisms

Traditional consensus mechanisms like PoW and PoS face limitations restricting their suitability for real-time data processing within AV communication networks.

- High Energy Consumption and Processing Delays: PoW's reliance on computationally intensive mining processes leads to significant energy usage, a critical concern for resource-constrained environments like AV networks. Additionally, these complex calculations can introduce delays in transaction processing, potentially impacting the real-time data exchange crucial for AV operations.
- Centralization and Security Concerns: PoS raises concerns about potential centralization of power with those holding the most staked tokens. Furthermore, the "nothing at stake" problem suggests validators with minimal penalties for misbehavior might have less incentive to maintain network security, compromising its integrity.
- Scalability Limitations: Both PoW and existing PoS implementations might struggle to handle the high volume and real-time nature of data generated by AV sensors, potentially leading to processing bottlenecks and hindering the network's ability to scale effectively as the number of AVs increases.

D. Our Contribution: PoUW for AV Communication Networks

This research introduces a novel application of PoUW in the AVs domain. By aligning the mining process with real-world problem-solving, PoUW offers a departure from traditional consensus mechanisms like PoW and PoS. We aim to harness PoUW’s computational power for efficient data processing, validation, and potential storage within the AV ecosystem. This approach addresses the limitations of existing methods, such as high energy consumption, scalability issues, and security concerns associated with PoW and PoS. Ultimately, we seek to contribute to the advancement of AV technology by improving data management practices and enhancing overall system performance.

III. Research Methodology

Our research investigated the feasibility and potential benefits of integrating PoUW into the communication network infrastructure of AVs. We focused on evaluating PoUW's capabilities for real-time data processing and analysis, considering the high-volume nature of sensor data generated by AVs. The steps followed in the research methodology are outlined next.

A. Data Collection. Carla Simulator

We utilized the CARLA simulator, a popular open-source platform for developing, testing, and training algorithms for Autonomous vehicles. This simulator provided a controlled environment to simulate real-world traffic scenarios

involving multiple AVs. These AVs were equipped with various sensors to mimic real-world data collection, including:

- *LiDAR*: 3D point cloud information about the surrounding environment.
- *GNSS*: Navigation and positioning data.
- *Radar*: Range and velocity information about nearby objects.
- *Cameras*: Visual information about the driving scene.
- *Collision Detector*: Registers an event each time the parent actor collides with something in the world.
- *IMU (Inertial Measurement Unit):* Provides measures that an accelerometer, gyroscope, and compass would retrieve.
- *Obstacle Detector*: Registers an event whenever the parent actor encounters an obstacle ahead.
- *Lane Invasion Detector*: Registers an event each time its parent crosses a lane marking.

Sensor data from the simulated AVs formed the core dataset for our investigation, encompassing real-time information about the AVs' surroundings.

Future work could explore enriching the data feed with parameters like weather forecasts to better reflect real-world driving conditions. CARLA's camera APIs offer advanced functionalities such as segmentation, which could be explored to extract detailed environmental information from the simulated world scene. Due to resource constraints, this research prioritized core sensors like LiDAR and radar, leaving the exploration of additional environmental information for future studies.

B. Data Processing and Streaming

Given the high volume and real-time nature of the sensor data, we opted not to store all data directly on the blockchain due to its scalability limitations. Blockchain technology is not currently optimized for persisting large datasets. Instead, we focused on utilizing the blockchain for data validation and integrity purposes. We have a side application that stores the processed data in an InfluxDB instance, which is a time-series database, planned for future use. To achieve this, we implemented a real-time data processing pipeline:

- *Data Filtering*: The raw sensor data stream was filtered to extract critical information essential for ensuring data integrity and facilitating real-time decision-making for AV operations. This filtering process aimed to identify and extract key data points without compromising the overall functionality of the AV system.

- *Data Preprocessing*: The extracted data points underwent preprocessing steps to ensure uniformity and compatibility with the PoUW blockchain infrastructure.

- *Data Streaming*: The preprocessed data stream was then routed to a backend application deployed on Flux powered by PoUW using RESTful APIs.

C. Backend Server and Monitoring

Real-time data processing and communication with the PoUW blockchain occurred through a backend application deployed on the Flux blockchain infrastructure, leveraging the inherent scalability and flexibility of blockchain nodes. The backend server application performed the following tasks:

- *Data Transmission*: The server hosted on the Flux blockchain received filtered and sanitized data streams from the CARLA simulator and processed them using the underlying PoUW blockchain network.

- *Performance Monitoring*: We employed New Relic, a cloud-based software solution, to monitor the performance of the backend server. This allowed us to track key metrics such as API performance, network latency, data processing times, error rates, and potential bottlenecks. This monitoring complemented the server resource utilization metrics readily available through the Flux infrastructure, providing a comprehensive view of system performance.

- *Data Visualization*: New Relic's dashboard feature enabled us to visualize the real-time data stream and create performance metrics from the raw data. This visualization facilitated the analysis and identification of trends within the data.

D. PoUW Blockchain Integration

The backend server application is hosted on the Flux blockchain infrastructure, which utilizes the PoUW consensus mechanism. During the data validation process, the computational power expended by the PoUW network was directed toward solving real-world problems, aligning with the core principles of PoUW. This integration allowed us to assess the suitability of PoUW for handling and processing the critical data points extracted from the AV sensor data stream.

E. Evaluation and Analysis

We evaluated the system's performance across several key metrics to assess the feasibility of integrating PoUW into AV communication networks:

- *Transaction Speed*: We measured the time taken for the dAPP deployed on the PoUW blockchain to process and validate data transmissions, ensuring it met the real-time requirements of AV operations. This analysis considered the impact of data filtering and preprocessing on transaction speed compared to the raw data volume.

- *Node Utilization*: We assessed the capability of blockchain nodes within the network to analyze the data sets, aiming to determine if the nodes could effectively handle the data validation workload while maintaining efficient network operation.

- *Efficiency*: We analyzed the compatibility of the AV system with the PoUW blockchain in terms of overall efficiency, maintainability, and ease of use for potential future implementations. This included evaluating the

scalability of the cloud server infrastructure and the potential need for further data filtering or optimization.

Additionally, we analyzed the processing efficiency of PoUW, particularly its ability to handle and analyze the data stream in real-time. This evaluation aimed to determine if the PoUW consensus mechanism could efficiently validate the data without introducing significant delays that could impact AV operations.

F. Prototype and Documentation

Throughout the research process, we meticulously documented the design, development, and testing phases of our PoUW integration with the AV communication network. This comprehensive documentation serves as a valuable prototype and case study for future research and development efforts exploring PoUW applications in the AV domain. It includes detailed information on the data filtering and preprocessing techniques employed, the configuration and performance of the cloud-based server infrastructure, the integration process with the Flux blockchain network, and the evaluation methods and results obtained during the research.

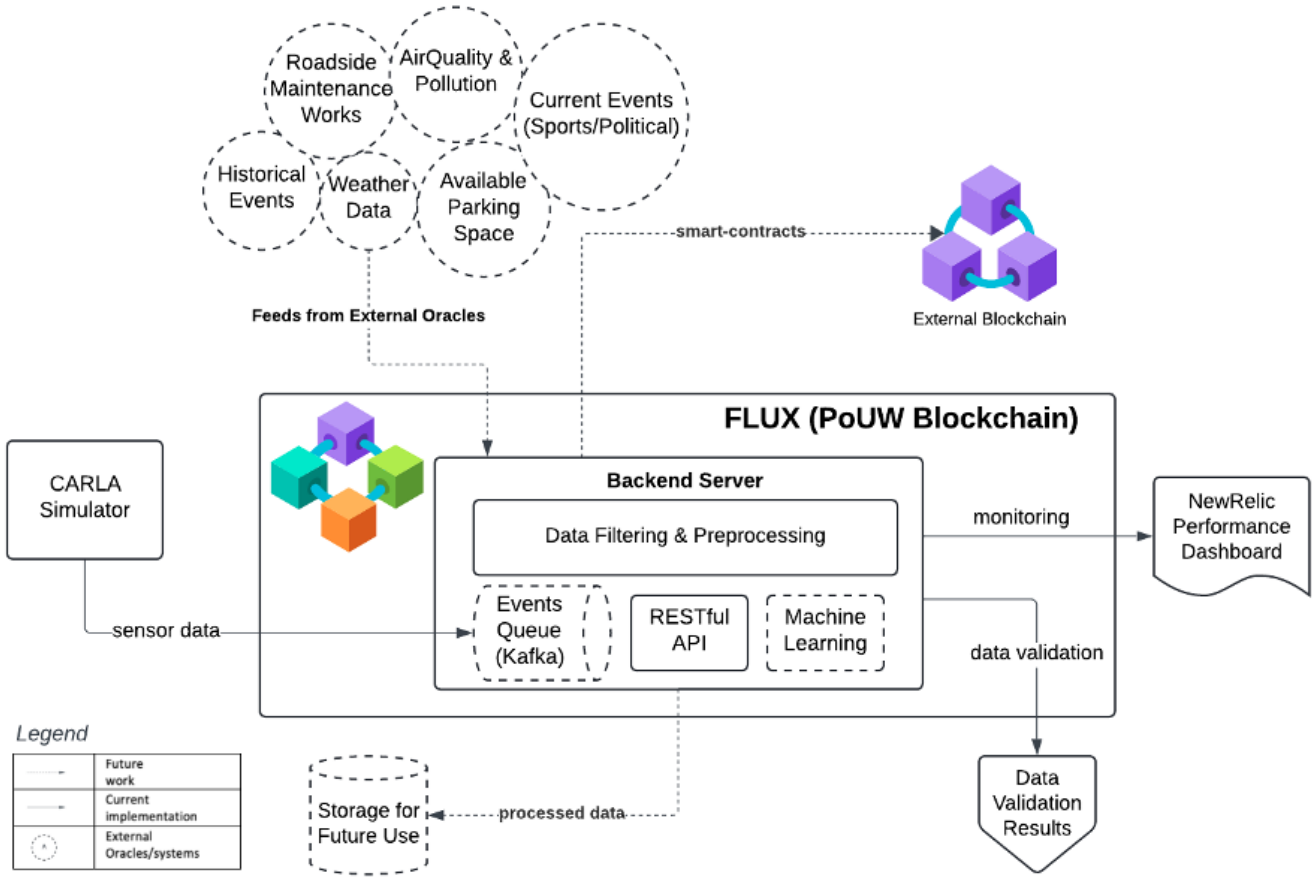


Figure 1 System Diagram

IV. Performance Evaluation

Evaluating the performance of our PoUW integration with the AV communication network was crucial to assess its feasibility and identify potential areas for improvement. We focused on key performance metrics to gain insights into the system's efficiency, scalability, and suitability for real-time AV operations.

A. Transaction Speed and Latency:

We measured the time taken for the backend application running on the Flux infrastructure with the PoUW blockchain to process and validate data transmissions, a metric referred to as transaction speed. This is critical for ensuring the system can handle the real-time data demands of AVs. Additionally, we analyzed network latency, which refers to the time delay experienced during data transmission between the backend servers running on the PoUW blockchain nodes. Both transaction speed and latency need to be sufficiently low to avoid impacting real-time decision-making for AVs. The detailed results are presented in Table V in the appendix.

B. Resource Utilisation

We evaluated the resource utilization of the backend server deployed on the Flux infrastructure, including metrics such as CPU usage, memory consumption, and storage utilization. Analyzing these metrics helped us assess the server's capacity to handle the data processing workload and identify potential bottlenecks. Additionally, we considered the resource utilization of the PoUW blockchain nodes themselves. The Flux infrastructure provides data on node

resource usage, which can inform future decisions about network scaling and optimization.

C. Data Processing Efficiency:

We evaluated the efficiency of the PoUW consensus mechanism in processing the filtered data stream, focusing on the time taken for the blockchain to validate the data and the overall throughput achieved. Efficient data processing capability is essential for ensuring the system can handle the high volume of data generated by AV sensors without introducing significant delays.

D. Error Rate and Bottleneck Identification:

- We monitored the system for potential errors that could occur during data transmission or processing. Analyzing the error rate helped us identify areas for improvement and ensure data integrity within the network.
- We utilized New Relic to monitor key metrics and identify potential bottlenecks within the backend server or the data processing pipeline. By addressing these bottlenecks, we could optimize the system's performance and ensure efficient data flow.

E. Scalability Analysis:

We conducted initial scalability tests by increasing the number of simulated AVs and the complexity of the scenarios within the CARLA simulator. This approach allowed us to assess the system's ability to handle a growing data volume and more demanding processing requirements. Based on these tests, we evaluated the need for further optimization strategies, such as improvements in data filtering or exploring alternative blockchain platforms designed for high-throughput data processing.

By analyzing these performance metrics, we gained valuable insights into the strengths and limitations of our PoUW integration. This information is crucial for informing future research and development efforts toward a robust and scalable communication network infrastructure for autonomous vehicles.

V. Results and Analysis

Our research focused on integrating PoUW into the AV communication network. However, other consensus mechanisms also exist, each with its own advantages and disadvantages. Here, we compare PoUW with PoW and Ethereum's PoS to highlight the suitability of PoUW for AV communication networks.

A. Proof of Work (PoW):

PoW is a mature and well-established consensus mechanism offering a high level of security and decentralization. However, PoW requires significant computational power, leading to high energy consumption and scalability limitations. This high energy usage makes PoW less suitable for resource-constrained environments like AV communication networks.

B. Ethereum (PoS):

PoS offers significant strengths, including faster transaction speeds and lower energy consumption compared to PoW. However, it also has notable weaknesses, such as concerns about centralization since those with the most staked tokens wield greater influence over the network. Additionally, PoS might introduce the "nothing at stake" problem, where validators have less incentive to maintain network security due to lower penalties for misbehavior.

C. Proof of Useful Work (PoUW):

PoUW leverages the computational power used for mining towards solving real-world problems, making it more energy-efficient compared to PoW. It also offers a secure and decentralized network suitable for real-time data processing and validation within the AV communication network. For example, Flux provides an innovative solution to use shared computational resources. However, PoUW is a relatively new concept, and its long-term security and stability require further research. Additionally, optimizing data filtering and choosing the appropriate "useful work" tasks for the PoUW network are ongoing areas of development.

Table II PoUW vs PoS

Feature	PoUW	Ethereum (PoS)
Energy Consumption	Lower than PoW, utilizes computational power for "useful work"	Lower than PoW, but higher than PoUW
Security	Secure and decentralized	Potential concerns about centralization
Scalability	Potentially more scalable than PoW due to lower energy consumption	Faster transaction speeds than PoW, but scalability limitations exist
Suitability for AVs	Well-suited for real-time data processing and validation	May be suitable, but security concerns and potential centralization require further exploration

Our research suggests that PoUW offers a promising alternative to traditional PoW and might be better suited for AV communication networks due to its lower energy consumption and focus on real-world problem-solving tasks. However, both PoUW and PoS require further research and development for optimal performance within the context of AV network security and scalability.

VI. Conclusion

This research investigated the feasibility of integrating PoUW into the communication network infrastructure of AVs. We focused on evaluating PoUW's capabilities for real-time data processing and analysis, considering the high-volume nature of sensor data generated by AVs.

A. Key Findings:

- Our findings indicate that PoUW holds promise for real-time data validation within AV communication networks. The system successfully processed and validated filtered data streams extracted from sensor data in the CARLA simulator.

- Utilizing a cloud-based server and the Flux blockchain infrastructure allowed for scalable data processing and communication. However, the initial deployment on the Flux network highlighted the need for further optimization strategies, particularly regarding data filtering techniques, to handle a larger number of AVs and more complex scenarios.

- The performance evaluation emphasized the importance of transaction speed, resource utilization, data processing efficiency, and error identification. By analyzing these metrics, we gained valuable insights into the system's strengths and limitations.

B. Future Work:

Future research directions include refining the data filtering process to minimize the data volume transmitted to the PoUW blockchain, thereby optimizing resource utilization on the blockchain network. Techniques like edge computing could be explored to perform initial data filtering closer to the AVs themselves. Additionally, investigating alternative blockchain platforms specifically designed for handling high-throughput data streams could be beneficial. Platforms that utilize sharding or other scalability solutions might be better suited for large-scale AV communication networks with a significant number of vehicles. Expanding the test scenarios within the CARLA simulator is also crucial. By including more traffic, non-AV actors, a higher number of AVs, and diverse sensor data, we can achieve a more realistic evaluation of PoUW's performance under complex real-world conditions.

This research contributes to the ongoing exploration of secure and efficient communication networks for autonomous vehicles. By demonstrating the potential of PoUW for real-time data processing and validation, we pave the way for further investigation and development in this field. The successful integration of PoUW could revolutionize AV communication networks, ensuring data integrity and enabling the secure and efficient exchange of critical information essential for safe and reliable autonomous vehicle operation.

VII. REFERENCES

[1] Rathee, Sharma, Iqbal, Aloqaily, Jaglan, and Kumar, ‘A Blockchain Framework for Securing Connected and Autonomous Vehicles’, Sensors, vol. 19, no. 14, p. 3165, Jul. 2019, doi: 10.3390/s19143165.

[2] M. Haouari, M. Mhiri, M. El-Masri, and K. Al-Yafi, ‘A novel proof of useful work for a blockchain storing transportation transactions’, Information Processing & Management, vol. 59, no. 1, p. 102749, Jan. 2022, doi: 10.1016/j.ipm.2021.102749.

[3] A. Lihu, J. Du, I. Barjaktarevic, P. Gerzanics, and M. Harvilla, ‘A Proof of Useful Work for Artificial Intelligence on the Blockchain’. arXiv, Jan. 24, 2020. Accessed: Feb. 02, 2024. [Online]. Available: http://arxiv.org/abs/2001.09244

[4] S. Bouraga, ‘A taxonomy of blockchain consensus protocols: A survey and classification framework’, Expert Systems with Applications, vol. 168, p. 114384, Apr. 2021, doi: 10.1016/j.eswa.2020.114384.

[5] R. Gupta, A. Kumari, and S. Tanwar, ‘A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles’, Trans Emerging Tel Tech, vol. 32, no. 6, p. e4009, Jun. 2021, doi: 10.1002/ett.4009.

[6] Y. Du, C. Leung, Z. Wang, and V. C. M. Leung, ‘Accelerating Blockchain-enabled Distributed Machine Learning by Proof of Useful Work’, in 2022 IEEE/ACM 30th International Symposium on Quality of Service (IWQoS), Oslo, Norway: IEEE, Jun. 2022, pp. 1–10. doi: 10.1109/IWQoS54832.2022.9812927.

[7] H. A. Ignatious, H.-E.- Sayed, and M. Khan, ‘An overview of sensors in Autonomous Vehicles’, Procedia Computer Science, vol. 198, pp. 736–741, 2022, doi: 10.1016/j.procs.2021.12.315.

[8] A. Biswas and H.-C. Wang, ‘Autonomous Vehicles Enabled by the Integration of IoT, Edge Intelligence, 5G, and Blockchain’, Sensors, vol. 23, no. 4, p. 1963, Feb. 2023, doi: 10.3390/s23041963.

[9] S. Jain et al., ‘Blockchain and Autonomous Vehicles: Recent Advances and Future Directions’, IEEE Access, vol. 9, pp. 130264–130328, 2021, doi: 10.1109/ACCESS.2021.3113649.

[10] T. Davidovic et al., ‘COCP: Blockchain Proof-of-Useful-Work Leveraging Real-Life Applications’, in 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA), San Antonio, TX, USA: IEEE, Sep. 2022, pp. 107–110. doi: 10.1109/BCCA55292.2022.9922117.

[11] A. Baldominos and Y. Saez, ‘Coin.AI: A Proof-of-Useful-Work Scheme for Blockchain-Based Distributed Deep Learning’, Entropy, vol. 21, no. 8, p. 723, Jul. 2019, doi: 10.3390/e21080723.

[12] U. Maleš, D. Ramljak, T. Jakšić Krüger, T. Davidović, D. Ostojić, and A. Haridas, ‘Controlling the Difficulty of Combinatorial Optimization Problems for Fair Proof-of-Useful-Work-Based Blockchain Consensus Protocol’, Symmetry, vol. 15, no. 1, p. 140, Jan. 2023, doi: 10.3390/sym15010140.

[13] B. Li, C. Chenli, X. Xu, T. Jung, and Y. Shi, ‘Exploiting Computation Power of Blockchain for Biomedical Image Segmentation’, in 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Long Beach, CA, USA: IEEE, Jun. 2019, pp. 2802–2811. doi: 10.1109/CVPRW.2019.00339.

[14] Z. Ma, Q. Zhao, J. Yuan, X. Zhou, and L. Feng, ‘Fork Probability Analysis of PoUW Consensus Mechanism’, in 2020 IEEE International Conference on Smart Internet of Things (SmartIoT), Beijing, China: IEEE, Aug. 2020, pp. 333–337. doi: 10.1109/SmartIoT49966.2020.00060.

[15] D. Ma, S. Zhang, and X. Jiao, ‘HDCoin: A Proof-of-Useful-Work Based Blockchain for Hyperdimensional Computing’. arXiv, Feb. 07, 2022. Accessed: Feb. 02, 2024. [Online]. Available: http://arxiv.org/abs/2202.02964

[16] T. Dargahi, H. Ahmadvand, M. N. Alraja, and C.-M. Yu, ‘Integration of Blockchain with Connected and Autonomous Vehicles: Vision and Challenge’, J. Data and Information Quality, vol. 14, no. 1, pp. 1–10, Mar. 2022, doi: 10.1145/3460003.

[17] ‘Introducing Ofelimos: a proof-of-useful-work consensus protocol - IOHK Blog’, IOHK. Accessed: Jul. 12, 2024. [Online]. Available: https://iohk.io/en/blog/posts/2022/08/16/introducing-ofelimos-a-proof-of-useful-work-consensus-protocol/

[18] A. Perritaz and D. Wittock, ‘Proof of Useful Work - Litepaper’.

[19] C. Dragos, ‘Proof of Useful Work Based on Matrix Computation’, in 2022 24th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), Hagenberg / Linz, Austria: IEEE, Sep. 2022, pp. 108–116. doi: 10.1109/SYNASC57785.2022.00026.

[20] M. Todorović et al., ‘Proof-of-Useful-Work: BlockChain Mining by Solving Real-Life Optimization Problems’, Symmetry, vol. 14, no. 9, p. 1831, Sep. 2022, doi: 10.3390/sym14091831.

[21] M. Ball, A. Rosen, M. Sabin, and P. N. Vasudevan, ‘Proofs of Useful Work’. 2017. Accessed: Feb. 02, 2024. [Online]. Available: https://eprint.iacr.org/2017/203

[22] Z. Dong, Y. C. Lee, and A. Y. Zomaya, ‘Proofware: Proof of Useful Work Blockchain Consensus Protocol for Decentralized Applications’.

arXiv, Mar. 21, 2019. Accessed: Feb. 02, 2024. [Online]. Available: http://arxiv.org/abs/1903.09276

VIII. Appendix

Following are the Test run results retrieved from the running system.

A. TestRun-1 Scenario with 50 AVs for 1 hr on 3 node flux cluster

Table III Flux nodes specs - TestRun-1

Flux Nodes	vCPU Core	Memory (MBs)
Node 1	1	600
Node 2	1	600
Node 3	1	600

We conducted a test simulating 50 autonomous vehicles (AVs) for a one-hour duration on a 3-node Flux cluster. The cluster configuration consisted of 1 vCPU core and 600MB of memory per node. The scenario ran successfully for the entire hour with no reported errors. CPU utilization and memory consumption remained consistent throughout the test, indicating stable resource usage.

Additionally, the New Relic charts associated with this test run below, depict the system's throughput and transaction statistics for the entire duration. These charts can be further analyzed to gain more insights into the system's performance under these specific conditions.

This passage highlights the successful execution of the test, emphasizes the lack of errors and stable resource usage, and acknowledges the availability of performance data for further analysis.

Table IV Transaction speed and average latency sorted.

Transactions (APIs called)	Total time	Avg	Min	Max	Median	95th %	99th %	Apdex	Error rate	Throughput	Total count
:download_data	<0.01 %	3.85 ms	0 ms	6.16 ms	4.08 ms	6.16 ms	6.16 ms	1	0%	0.02 rpm	3.00
:index	0.02%	2.69 ms	0 ms	5.79 ms	1.94 ms	5.79 ms	5.79 ms	1	0%	0.07 rpm	11
:post_sensor_obstacle_data	16.41%	2.15 ms	0 ms	23.5 ms	2.02 ms	3.01 ms	4.67 ms	1	0%	89 rpm	13.2k
:post_sensor_collision_data	16.60%	2.15 ms	0 ms	15.3 ms	2.02 ms	3.01 ms	4.85 ms	1	0%	90 rpm	13.4k
:post_sensor_lane_invasion_data	16.67%	2.15 ms	0 ms	16.9 ms	2.02 ms	3.01 ms	4.73 ms	1	0%	90 rpm	13.4k
:post_sensor_radar_data	16.45%	2.15 ms	0 ms	19.9 ms	2.02 ms	3.01 ms	4.73 ms	1	0%	89 rpm	13.2k
:get_usage	1.59%	1.54 ms	0 ms	8.15 ms	1.27 ms	3.4 ms	4.3 ms	1	0%	12 rpm	1.78k
:post_sensor_imu_data	11.68%	1.5 ms	0 ms	15.8 ms	1.43 ms	2.09 ms	2.88 ms	1	0%	91 rpm	13.5k
:post_sensor_gnss_data	11.40%	1.48 ms	0 ms	21.8 ms	1.41 ms	2.06 ms	2.82 ms	1	0%	89 rpm	13.3k
app:Flask.handle_http_exception	<0.01 %	1.42 ms	0 ms	2.13 ms	1.27 ms	2.13 ms	2.13 ms	1	0%	0.05 rpm	7.00
:get_counters	9.17%	1.38 ms	0 ms	20 ms	1.29 ms	1.93 ms	3.16 ms	1	0%	77 rpm	11.5k

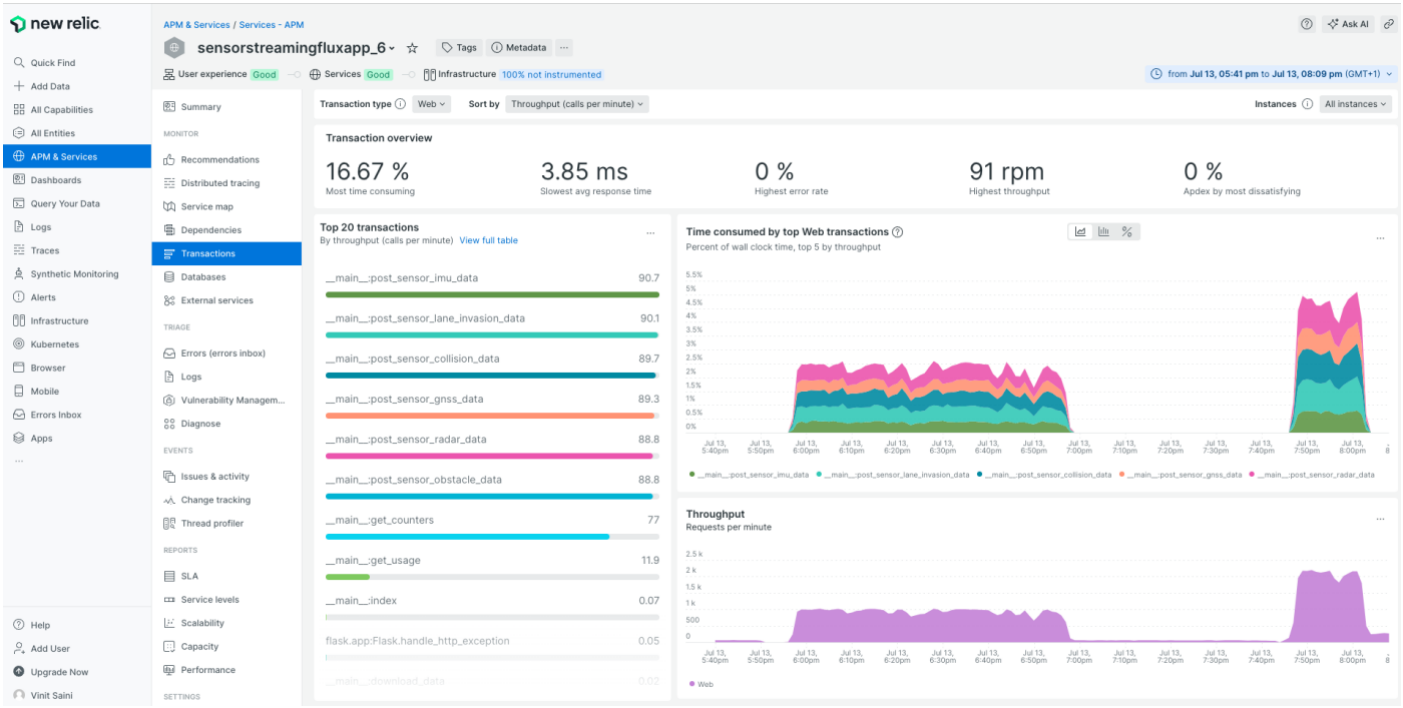


Figure 2 NewRelic chart - APIs transaction time

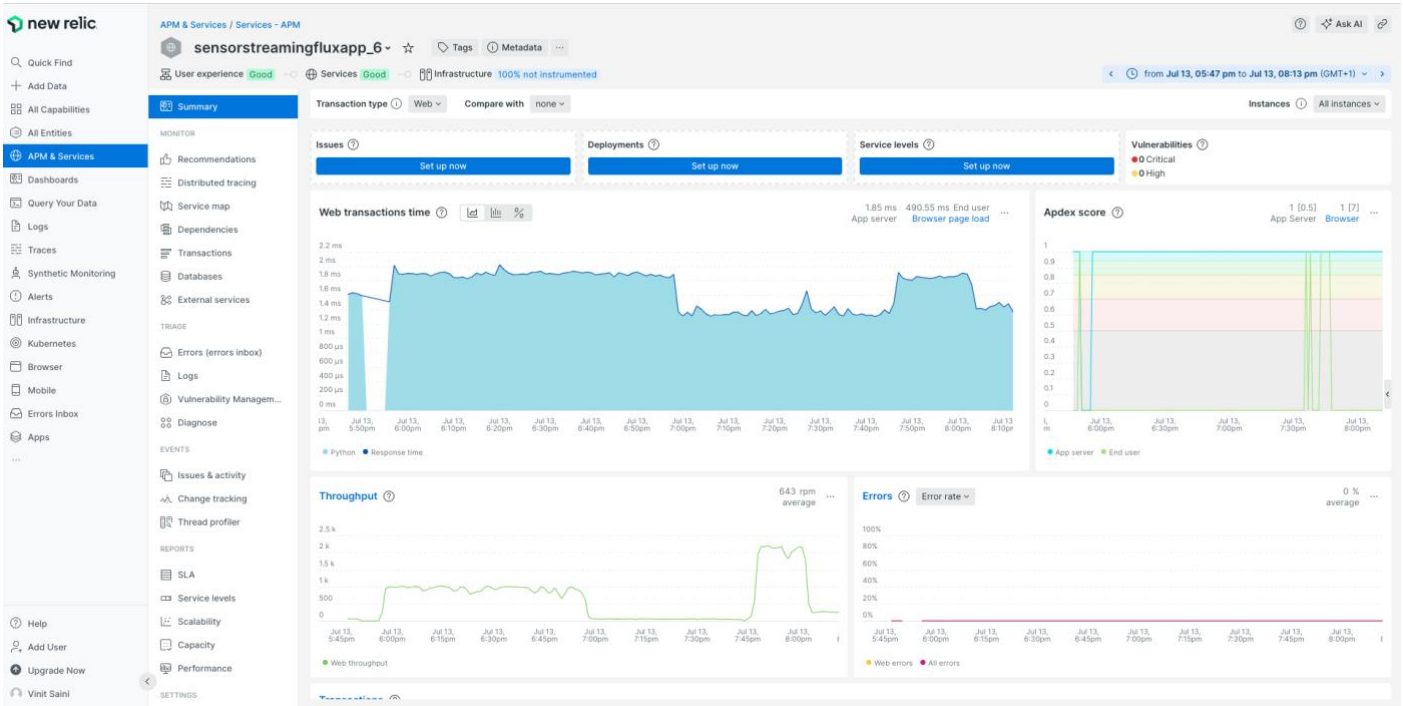
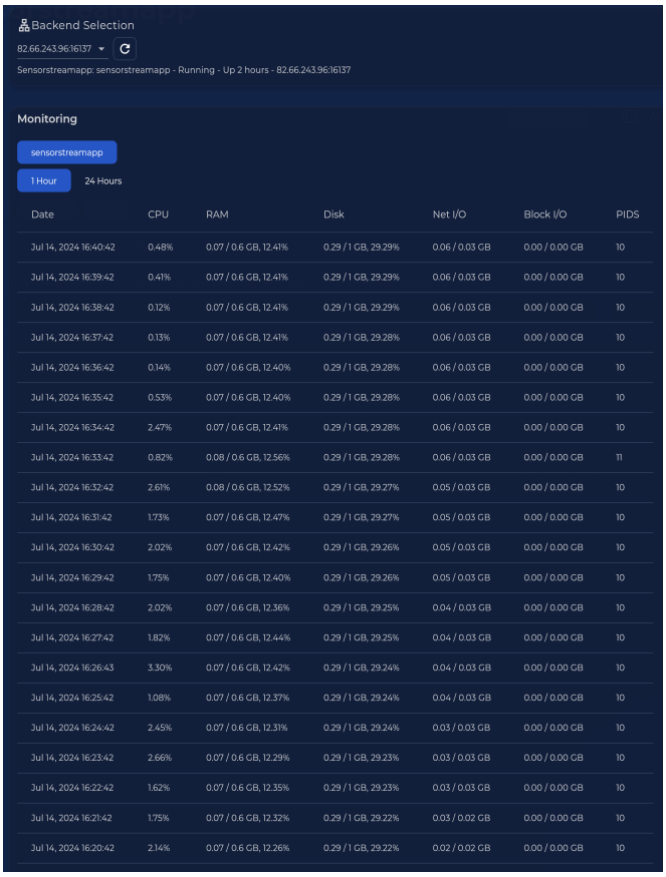


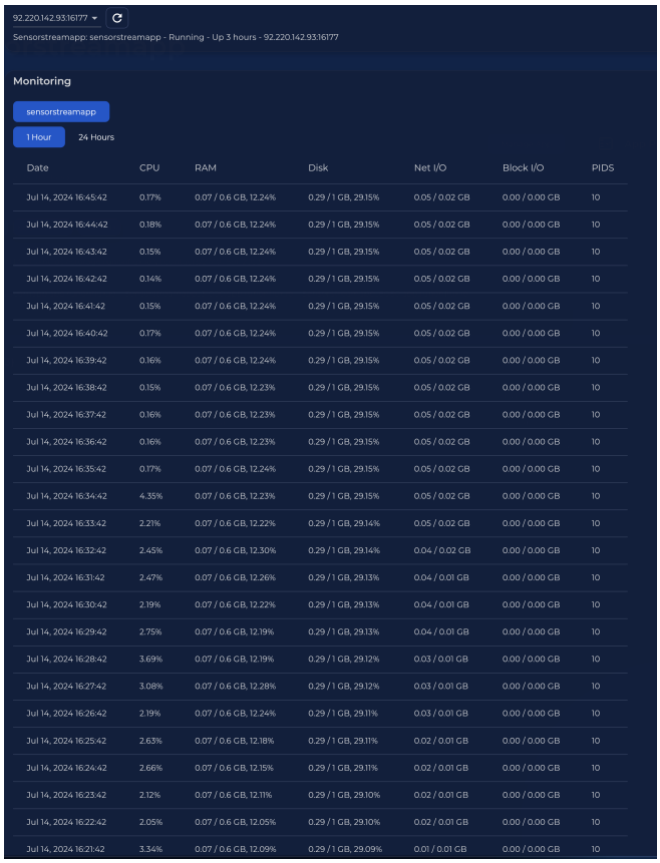
Figure 3 NewRelic chart - APIs Throughput

The following screenshots show the Infrastructure metrics resource usage from 3 containers in the cluster.



Date	CPU	RAM	Disk	Net I/O	Block I/O	PIDS
Jul 14, 2024 16:40:42	0.48%	0.07 / 0.6 GB, 12.41%	0.29 / 1 GB, 29.29%	0.06 / 0.03 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:39:42	0.41%	0.07 / 0.6 GB, 12.41%	0.29 / 1 GB, 29.29%	0.06 / 0.03 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:38:42	0.12%	0.07 / 0.6 GB, 12.41%	0.29 / 1 GB, 29.29%	0.06 / 0.03 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:37:42	0.13%	0.07 / 0.6 GB, 12.41%	0.29 / 1 GB, 29.28%	0.06 / 0.03 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:36:42	0.14%	0.07 / 0.6 GB, 12.40%	0.29 / 1 GB, 29.28%	0.06 / 0.03 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:35:42	0.53%	0.07 / 0.6 GB, 12.40%	0.29 / 1 GB, 29.28%	0.06 / 0.03 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:34:42	2.47%	0.07 / 0.6 GB, 12.41%	0.29 / 1 GB, 29.28%	0.06 / 0.03 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:33:42	0.82%	0.08 / 0.6 GB, 12.56%	0.29 / 1 GB, 29.28%	0.06 / 0.03 GB	0.00 / 0.00 GB	11
Jul 14, 2024 16:32:42	2.61%	0.08 / 0.6 GB, 12.52%	0.29 / 1 GB, 29.27%	0.05 / 0.03 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:31:42	1.73%	0.07 / 0.6 GB, 12.47%	0.29 / 1 GB, 29.27%	0.05 / 0.03 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:30:42	2.02%	0.07 / 0.6 GB, 12.42%	0.29 / 1 GB, 29.26%	0.05 / 0.03 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:29:42	1.75%	0.07 / 0.6 GB, 12.40%	0.29 / 1 GB, 29.26%	0.05 / 0.03 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:28:42	2.02%	0.07 / 0.6 GB, 12.36%	0.29 / 1 GB, 29.25%	0.04 / 0.03 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:27:42	1.82%	0.07 / 0.6 GB, 12.44%	0.29 / 1 GB, 29.25%	0.04 / 0.03 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:26:43	3.30%	0.07 / 0.6 GB, 12.42%	0.29 / 1 GB, 29.24%	0.04 / 0.03 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:25:42	1.08%	0.07 / 0.6 GB, 12.37%	0.29 / 1 GB, 29.24%	0.04 / 0.03 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:24:42	2.45%	0.07 / 0.6 GB, 12.31%	0.29 / 1 GB, 29.24%	0.03 / 0.03 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:23:42	2.66%	0.07 / 0.6 GB, 12.29%	0.29 / 1 GB, 29.23%	0.03 / 0.03 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:22:42	1.62%	0.07 / 0.6 GB, 12.35%	0.29 / 1 GB, 29.23%	0.03 / 0.03 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:21:42	1.75%	0.07 / 0.6 GB, 12.32%	0.29 / 1 GB, 29.22%	0.03 / 0.02 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:20:42	2.14%	0.07 / 0.6 GB, 12.26%	0.29 / 1 GB, 29.22%	0.02 / 0.02 GB	0.00 / 0.00 GB	10

Figure 4 Node 1 Resources Utilization



Date	CPU	RAM	Disk	Net I/O	Block I/O	PIDS
Jul 14, 2024 16:45:42	0.17%	0.07 / 0.6 GB, 12.24%	0.29 / 1 GB, 29.15%	0.05 / 0.02 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:44:42	0.18%	0.07 / 0.6 GB, 12.24%	0.29 / 1 GB, 29.15%	0.05 / 0.02 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:43:42	0.15%	0.07 / 0.6 GB, 12.24%	0.29 / 1 GB, 29.15%	0.05 / 0.02 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:42:42	0.14%	0.07 / 0.6 GB, 12.24%	0.29 / 1 GB, 29.15%	0.05 / 0.02 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:41:42	0.15%	0.07 / 0.6 GB, 12.24%	0.29 / 1 GB, 29.15%	0.05 / 0.02 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:40:42	0.17%	0.07 / 0.6 GB, 12.24%	0.29 / 1 GB, 29.15%	0.05 / 0.02 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:39:42	0.16%	0.07 / 0.6 GB, 12.24%	0.29 / 1 GB, 29.15%	0.05 / 0.02 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:38:42	0.15%	0.07 / 0.6 GB, 12.23%	0.29 / 1 GB, 29.15%	0.05 / 0.02 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:37:42	0.16%	0.07 / 0.6 GB, 12.23%	0.29 / 1 GB, 29.15%	0.05 / 0.02 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:36:42	0.16%	0.07 / 0.6 GB, 12.23%	0.29 / 1 GB, 29.15%	0.05 / 0.02 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:35:42	0.17%	0.07 / 0.6 GB, 12.24%	0.29 / 1 GB, 29.15%	0.05 / 0.02 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:34:42	4.35%	0.07 / 0.6 GB, 12.23%	0.29 / 1 GB, 29.15%	0.05 / 0.02 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:33:42	2.21%	0.07 / 0.6 GB, 12.22%	0.29 / 1 GB, 29.14%	0.05 / 0.02 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:32:42	2.45%	0.07 / 0.6 GB, 12.30%	0.29 / 1 GB, 29.14%	0.04 / 0.02 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:31:42	2.47%	0.07 / 0.6 GB, 12.26%	0.29 / 1 GB, 29.13%	0.04 / 0.01 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:30:42	2.19%	0.07 / 0.6 GB, 12.22%	0.29 / 1 GB, 29.13%	0.04 / 0.01 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:29:42	2.75%	0.07 / 0.6 GB, 12.19%	0.29 / 1 GB, 29.13%	0.04 / 0.01 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:28:42	3.69%	0.07 / 0.6 GB, 12.19%	0.29 / 1 GB, 29.12%	0.03 / 0.01 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:27:42	3.08%	0.07 / 0.6 GB, 12.28%	0.29 / 1 GB, 29.12%	0.03 / 0.01 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:26:42	2.19%	0.07 / 0.6 GB, 12.24%	0.29 / 1 GB, 29.11%	0.03 / 0.01 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:25:42	2.63%	0.07 / 0.6 GB, 12.18%	0.29 / 1 GB, 29.11%	0.02 / 0.01 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:24:42	2.66%	0.07 / 0.6 GB, 12.15%	0.29 / 1 GB, 29.11%	0.02 / 0.01 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:23:42	2.12%	0.07 / 0.6 GB, 12.11%	0.29 / 1 GB, 29.10%	0.02 / 0.01 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:22:42	2.05%	0.07 / 0.6 GB, 12.05%	0.29 / 1 GB, 29.10%	0.02 / 0.01 GB	0.00 / 0.00 GB	10
Jul 14, 2024 16:21:42	3.34%	0.07 / 0.6 GB, 12.09%	0.29 / 1 GB, 29.09%	0.01 / 0.01 GB	0.00 / 0.00 GB	10

Figure 5 Node 2 Resources Utilization

Figure 6 Node 3 Resources Utilization

B. TestRun-2 Scenario with 100 AVs for 15 mins on 3 node flux cluster

Table V Flux nodes specs - TestRun-2

Flux Nodes	vCPU Core	Memory (MBs)
Node 1	1	600
Node 2	1	600
Node 3	1	600

We conducted a test simulating a larger scenario with 100 autonomous vehicles (AVs) for 15 minutes. This test utilized a 3-node Flux cluster, with each node having 1 CPU core and approximately 600MB of memory. While the test ran for 15 minutes, the "Failure statistics" metric revealed a high error rate.

This suggests that the cluster's underlying resources might not have been sufficient to handle the demands of this more intensive test. The combination of a larger number of simulated AVs and a shorter timeframe likely placed a greater strain on the cluster's processing power and memory capacity. Further investigation is needed to determine the specific resource limitations that contributed to the errors.

Figure 7 Application Request Response Throughput

Failures Statistics

# Failures	Method	Name	Message
3	POST	/sensor/collision/data	TimeoutError(110, 'Connection timed out')
9	POST	/sensor/collision/data	RemoteDisconnected('Remote end closed connection without response')
10	POST	/sensor/gnss/data	RemoteDisconnected('Remote end closed connection without response')
8	POST	/sensor/gnss/data	TimeoutError(110, 'Connection timed out')
3	POST	/sensor/imu/data	TimeoutError(110, 'Connection timed out')
10	POST	/sensor/imu/data	RemoteDisconnected('Remote end closed connection without response')
13	POST	/sensor/lane_invasion/data	RemoteDisconnected('Remote end closed connection without response')
6	POST	/sensor/lane_invasion/data	TimeoutError(110, 'Connection timed out')
4	POST	/sensor/obstacle/data	TimeoutError(110, 'Connection timed out')
20	POST	/sensor/obstacle/data	RemoteDisconnected('Remote end closed connection without response')
4	POST	/sensor/radar/data	TimeoutError(110, 'Connection timed out')
8	POST	/sensor/radar/data	RemoteDisconnected('Remote end closed connection without response')
2	POST	/sensor/radar/data	OSError(113, 'No route to host')

Figure 8 API Endpoints Error Stats

Request Statistics

Type	Name	# Requests	# Fails	Median (ms)	Average (ms)	Min (ms)	Max (ms)	Average size (bytes)	Current RPS	Current Failures/s
POST	/sensor/collision/data	4546	12	130	232.35	2	130315	46.88	5.1	0
POST	/sensor/gnss/data	4591	18	130	385.02	5	131090	46.82	4.8	0
POST	/sensor/imu/data	4611	13	130	229.56	5	130663	46.87	5.1	0
POST	/sensor/lane_invasion/data	4564	19	130	318.61	6	131158	46.8	4.7	0
POST	/sensor/obstacle/data	4571	24	130	259.81	1	130562	46.75	5.8	0
POST	/sensor/radar/data	4515	14	130	260.79	6	130623	46.85	5.8	0
	Aggregated	27398	100	130	281.1	1	131158	46.83	31.3	0

Figure 9 API Endpoints Requests Stats

Response Time Statistics

Method	Name	50%ile (ms)	60%ile (ms)	70%ile (ms)	80%ile (ms)	90%ile (ms)	95%ile (ms)	99%ile (ms)	100%ile (ms)
POST	/sensor/collision/data	130	140	180	190	190	290	450	130000
POST	/sensor/gnss/data	130	130	180	180	190	300	430	131000
POST	/sensor/imu/data	130	130	180	180	190	290	450	131000
POST	/sensor/lane_invasion/data	130	130	180	190	190	300	490	131000
POST	/sensor/obstacle/data	130	130	180	180	190	300	420	131000
POST	/sensor/radar/data	130	130	180	180	190	300	460	131000
	Aggregated	130	130	180	180	190	300	450	131000

Figure 10 API Endpoints Response Stats

Figure 11 Carla Scene Screenshot

The following links provide further information about the concepts and tools used in this research, and these resources offer valuable insights into the technologies and methodologies applied.

CARLA Simulator

- CARLA Simulator: Used for testing the PoUW integration within the AV communication network.

Proof of Useful Work (PoUW)

- PoUW Litepaper: Offers a concise explanation of the Proof of Useful Work (PoUW) consensus mechanism.
- Proof of Useful Work vs. Other Mechanisms: Discusses the advantages of PoUW compared to other consensus mechanisms.
- PoUW: A Game Changer for Blockchain: Explains the potential impact of PoUW on the future of blockchain technology.
- Project Pai PoUW Overview: Provides information about the PoUW implementation by Project Pai.
- Project Pai PoUW GitHub Repository: Links to the Project Pai PoUW code repository on GitHub.

Flux Blockchain Infrastructure

- Flux PoUW Documentation: Provides comprehensive documentation for the PoUW implementation within the Flux infrastructure.
- Flux Website: The official website of the Flux project, offering general information about the blockchain platform.
- Flux Wiki: A collaborative knowledge base containing technical details and tutorials related to Flux.
- Flux GitHub Repository: The official Flux project repository on GitHub, contains the blockchain platform's source code.