# Proof of Useful Work for Autonomous Vehicles: Literature Review

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*— The advent of technology has ignited a profound transformation in various facets of daily life, reshaping how we communicate, entertain, work, and, notably, traverse the world. Among the pioneering developments, Autonomous Vehicles (AVs) stand out as a paradigm shift in the realm of transportation. This literature review embarks on a thorough exploration of the evolving research landscape concerning the integration of blockchain technology in Autonomous Vehicles. With a keen focus on addressing the challenges inherent in AV deployment and operation, this review delves into the promising applications of blockchain, particularly emphasizing the role of the innovative consensus mechanism known as Proof of Useful Work (PoUW).**

**In this comprehensive examination, we delve into the multifaceted intersections of blockchain and AVs, scrutinizing how decentralized, transparent, and secure data communication could redefine the landscape of autonomous transportation. The investigation not only identifies the limitations of traditional consensus mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS), but also highlights the unique challenges faced by AVs, including data security, processing speed, storage efficiency, information accuracy, and the dynamic mobility of vehicles.**

**As technology propels us into an era where autonomous mobility becomes increasingly prevalent, the need for robust, secure, and efficient systems becomes imperative. This literature review navigates through the promising avenues presented by the integration of PoUW in the AV sector. By aligning the computational efforts expended in blockchain networks with real-world problem-solving, PoUW emerges as a catalyst for revolutionizing data management, computational efficiency, and communication protocols within the AV ecosystem.**

**The synthesis of insights from existing literature not only outlines the current state of blockchain applications in AVs but also underscores the potential of PoUW in surmounting the challenges faced by both technologies. This exploration sets the stage for a nuanced understanding of how blockchain, particularly PoUW, can contribute to the enhanced operational efficiency, safety, and sustainability of the rapidly evolving landscape of autonomous vehicles.**

***Keywords*— Blockchain, Cryptography, PoS, PoUW, PBFT, Consensus Mechanisms, Bitcoin, Driverless cars, Autonomous vehicles, Security***

## I. INTRODUCTION

The emergence of AVs marks a new era in transportation, promising increased safety, efficiency, and convenience. However, the deployment and operation of AVs pose unique challenges, particularly regarding secure data communication, integrity, and privacy. Blockchain technology, known for its decentralization, transparency, and security features, presents a promising solution to these challenges, enabling secure and reliable vehicular communications and data exchanges [12],[13]. However, the adoption of blockchain in the AV sector is contingent upon choosing a suitable consensus mechanism which ensures the integrity and trustworthiness of transactions within the blockchain network. Table I enumerates frequently used acronyms throughout the paper.

Table I. Acronyms

| Acronym | Description |
|---|---|
| AVs | Autonomous Vehicles |
| CAVs | Connected and Autonomous Vehicles. |
| DPoS | Delegated Proof of Stake |
| GPS | Global Positioning System |
| IoT | Internet of Things |
| PoW | Proof of Work |
| PoS | Proof of Stake |
| PBFT | Practical Byzantine Fault Tolerance |
| PoUW | Proof of Useful Work |
| LiDAR | Light Detection and Ranging |
| ITS | Intelligent Transportation System |
| RSUs | Road Side Units |

Traditionally, blockchain networks have relied on consensus mechanisms like PoW and PoS to validate transactions and secure the network. PoW, utilized by Bitcoin, requires participants to solve computationally intensive puzzles to add new blocks to the blockchain, ensuring security at the expense of significant energy consumption [14]. While effective in mitigating security threats, this mechanism has been criticized for its environmental impact and tendency to centralize mining power among participants with significant computational resources. PoS, on the other hand, selects validators in proportion to their holdings and staked assets in the network, offering a more energy-efficient alternative to PoW. Despite its advantages, PoS raises concerns regarding wealth concentration and introduces security vulnerabilities, such as the "nothing at stake" problem [4].

In response to the limitations of PoW and PoS, PoUW emerges as an innovative consensus mechanism that aims to repurpose the computational efforts expended in blockchain networks towards solving practical, real-world problems. Unlike its predecessors, PoUW aligns the mining process with beneficial computational tasks, effectively addressing the inefficiencies and environmental concerns associated with PoW and the equity issues posed by PoS. PoUW secures the blockchain and contributes to societal advancements by utilizing the network's computational resources for meaningful purposes.

The integration of PoUW in the AV sector offers a compelling avenue for leveraging blockchain technology. By implementing PoUW, AV systems could benefit from enhanced computational efficiency, where the validation process simultaneously supports data processing and analysis crucial for vehicle operations. This approach facilitates advanced navigation algorithms, real-time traffic management, and predictive maintenance models, significantly enhancing autonomous vehicles' safety, reliability, and efficiency [3],[11].

This paper explores the potential of PoUW in revolutionizing the AV domain, addressing the challenges of secure data handling, processing speed, storage accuracy, and the overall enhancement of AV technologies. By examining current blockchain applications in AVs and identifying the limitations of traditional consensus mechanisms, the investigation highlights how PoUW can overcome these challenges. The exploration focuses on the feasibility, benefits, and implementation strategies of PoUW in the AV ecosystem, considering its contribution to data management, computational efficiency, and the advancement of AVs.

In conclusion, adopting PoUW within the AV sector represents a significant shift towards more sustainable, efficient, and equitable blockchain applications. By prioritizing useful computational work, PoUW addresses key challenges associated with traditional consensus mechanisms and opens new avenues for applying blockchain technology in autonomous vehicles. The findings of this exploration could pave the way for enhanced operational efficiency and safety in the AV domain, redefining the role of blockchain in automotive technology. The rest of the paper is organized into four chapters,

- Technical Background
- Review of AV’s main challenges
- Blockchain and AVs
- Conclusion

## II. Technical Background

### A. Autonomous Vehicles

AVs, often referred to as self-driving cars, represent a ground-breaking technological advancement in the realm of transportation. These vehicles operate without direct human input, relying on a sophisticated combination of technologies to navigate and make decisions. Key components of AVs include a number of sensors like LiDAR, radar, and cameras, enabling them to perceive and interpret their surroundings in real-time. Machine learning algorithms play a pivotal role in enabling AVs to recognize and understand complex scenarios, while high-definition mapping and precise localization technologies are crucial for accurate navigation. Furthermore, the advent of vehicular communication allows AVs to exchange information with each other and with infrastructure, enhancing safety and efficiency on the roads [13]. While tremendous progress has been made in the development of AVs, several challenges remain, particularly in the domain of communication systems.

The interaction between different AVs and communication with base stations is a critical area of ongoing research. Ensuring seamless communication is paramount for coordinated traffic management, enhanced safety protocols, and effective decision-making. Despite notable strides, the full potential of this facet of AV technology is yet to be fully explored and optimized.

### B. Blockchain and Traditional Consensus Mechanisms

Blockchain is a distributed ledger technology that was developed in 1991 by Haber and Stornetta (1991)[22]. Seventeen years later, In 2008, Nakamoto introduced the term "blockchain" in the whitepaper outlining the technology behind the Bitcoin cryptocurrency [21].

Presently, nearly every industry recognizes various applicable use cases for blockchain technology, offering simplification of business processes in areas such as trading, finance, shipping, IoT, healthcare, supply chain and of course, autonomous vehicles domain. The blockchain functions as a distributed data structure comprising interconnected nodes, referred to as blocks, where each node, except the genesis node, has a parent node. Consequently, it forms an ever-expanding chain of connected nodes. The characteristics inherent in blockchain, such as immutability, traceability, verifiability, transparency, and decentralization, make it highly suitable for diverse business applications. Every node within the blockchain incorporates a cryptographically secure hash value containing references to its parent node's hash and so forth, ensuring immutability. Even the slightest alteration in any block reverberates throughout the entire connected chain, making it easily detectable. Due to the interconnected nature of all nodes to their parent, this data structure provides complete traceability back to the initial transaction node. Additionally, each transaction is timestamped and cryptographically signed using a private key, enabling straightforward verification through public key infrastructure methods[22]. Similarly, transparency is achieved through the public ledger, where all transactions are accessible and verifiable by anyone.

Consensus mechanisms play a pivotal role in maintaining the integrity and security of blockchain networks. Various consensus algorithms have emerged to facilitate agreement among distributed nodes on the validity of transactions. Notable mechanisms include PoW, PoS, DPoS, PBFT, and a few others. While these mechanisms offer distinct advantages, they are not without challenges. Proof of Work, as utilized in Bitcoin, consumes significant computational power and energy, raising environmental concerns. Proof of Stake faces challenges related to the concentration of power in the hands of a few stakeholders. Delegated Proof of Stake introduces centralization risks through delegated authority. Practical Byzantine Fault Tolerance may struggle with scalability in large networks.

Continuous research and development in the field of consensus mechanisms reflects the dynamic nature of the blockchain ecosystem. Exploration of novel consensus algorithms to address the limitations and challenges posed by existing methods is an evolving process. An example of such an innovation is the Proof of Useful Work algorithm. PoUW represents an ongoing effort to create more sustainable and efficient consensus mechanisms.

### C. Proof of Useful Work (PoUW)

PoUW is a consensus mechanism that stands out for its unique approach in the world of blockchain. Unlike traditional PoW, where computations are energy-intensive and often seen as wasteful, PoUW focuses on performing tasks that are genuinely beneficial. In PoUW, participants showcase their efforts by engaging in activities that contribute to real-world applications or scientific research. Imagine a scenario where, instead of solving complex mathematical puzzles with no real-world value, the energy and computational resources are directed towards meaningful tasks. These tasks could include finding the best route for the autonomous vehicles using Orthogonal Vectors, 3SUM, All-Pairs Shortest Path algorithm, or similar [2]. By doing so, PoUW not only contributes towards securing the blockchain network but also ensures that the computational power is used for purposes that bring tangible benefits to various fields.

One of the significant advantages of PoUW is its positive impact on sustainability. Traditional PoW systems often face criticism for their environmental footprint due to high energy consumption. PoUW, by contrast, aligns with the concept of "useful" work, potentially reducing the carbon footprint associated with consensus mechanisms.

## III. Review of AV's main challenges

Navigating the real-world deployment of autonomous vehicles brings forth a multitude of challenges, predominantly due to the extensive generation and transmission of data. These intricacies of AVs, armed with diverse sensors like cameras, GPS, Lidar, and Radar, pose challenges in crucial areas. Data security becomes paramount as vast amounts of sensitive information are collected and transmitted. Real-time processing speed is essential to meet the instantaneous demands of AV systems, while securely optimizing storage efficiency becomes critical for managing the huge volume of generated data. Ensuring information accuracy and addressing the high mobility of vehicles further complicate the landscape. These challenges collectively underscore the need for innovative solutions which can provide data management, processing, and security to realize the full potential of AVs in real-world scenarios.

### A. Data Security

Ensuring data security in the autonomous vehicles domain poses a significant challenge due to the vast amount of sensitive information generated and processed by these vehicles. In the contemporary ITS, vehicles are furnished with various sensors like cameras, GPS, Lidar, and Radar, capturing substantial data, including geolocation information. CAVs leverage the data acquired from onboard sensors or external sources like RSUs and fellow vehicles. This information interpretation empowers CAVs to navigate complex driving scenarios, facilitating real-time decision-making and thereby enhancing the efficiency and safety of the transportation system [23]. With the constant exchange of data between sensors, onboard computers, and external networks, protecting against potential cyber threats becomes paramount. Threats such as unauthorized access, data interception, or manipulation could compromise the safety and functionality of autonomous vehicles. Striking a balance between connectivity and security measures becomes crucial to safeguarding passengers and maintaining the trust necessary for the widespread adoption of driverless car technologies. As the industry advances, addressing these data security challenges becomes integral to shaping a secure and resilient autonomous future.

In [5], Dargahi et al. correctly pointed out that Autonomous vehicles collect and consume an extensive volume of data, sharing it both among themselves and with the infrastructure. Typically, the gathered data encompasses sensitive details regarding users and the surrounding environment. Consequently, safeguarding data and ensuring privacy stands out as primary challenges within this sector[5][23]. Furthermore, security of data during transmission as well as at rest is also critical, therefore employing end to end encryption and data encryption at rest is of equal importance. Implementing robust encryption mechanisms to secure data transmission between sensors, in-vehicle systems, and external networks is paramount. This ensures that even if data is intercepted, it remains unintelligible without the appropriate decryption keys.

### B. Data Processing Speed

In the realm of autonomous vehicles or driverless cars, one of the significant challenges revolves around data processing speed. These advanced vehicles are equipped with an array of sensors, including cameras, LiDAR, radar, and more, generating vast amounts of data in real-time. The rapid and efficient processing of this data is crucial for ensuring the timely and accurate decision-making required for safe navigation and interaction with the surrounding environment.

The challenge lies in developing and implementing computing systems with the capability to handle the massive influx of data promptly. Achieving low-latency processing is essential to enable the vehicle's perception and decision-making functions to respond swiftly to dynamic road conditions, unforeseen obstacles, and other critical factors.

In [24], Mollah et al. suggested that instead of relying on cloud infrastructure, edge computing conducts computational processing and data storage in close proximity to the data source, i.e., AVs itself, addressing locally collected information processed locally. This approach by edge computing provides advantages such as location-awareness, low-latency, and real-time applications and services. Additionally, it offers bandwidth savings by avoiding the need to transfer data to a remotely situated cloud computing node [24]. However, they have also highlighted that the distributed nature of edge computing paradigm also introduces security and privacy challenges.

### C. Data Storage Challenges

AVs are equipped with an array of sensors, including cameras, LiDAR, radar, and GPS, producing massive datasets that require efficient and secure storage solutions. The challenge lies not only in managing the continuous influx of real-time data but also in preserving historical data for purposes such as training machine learning models and post-incident analysis. Storage systems must meet the rigorous demands of AVs, providing high-speed read and write capabilities while ensuring high availability, fault tolerance and data integrity. Additionally, the need for onboard storage in AVs necessitates compact yet high-capacity solutions. Addressing these challenges involves developing advanced storage architectures, exploring edge computing for local processing and distributed storage, and implementing robust data compression and encryption techniques to optimize storage efficiency and safeguard sensitive information.

### D. Information Accuracy

In the context of AVs, ensuring data accuracy stands out as a critical challenge. AVs heavily rely on precise and up-to-date data to navigate, make decisions, and operate safely. The accuracy of data, encompassing information from sensors, maps, and environmental inputs, directly influences the AV's ability to interpret its surroundings and respond appropriately. Challenges arise from the dynamic nature of the driving environment, as real-time changes in road conditions, traffic patterns, and unexpected obstacles demand accurate and instantaneous data processing. Trustworthiness and effectiveness of the information is critical therefore any kind of alteration of data, whether intentionally or unintentionally, can introduce errors, compromise integrity, and disrupt the normal functioning of the AVs. False or corrupted data may result in faulty decision-making, life-endangering risks, security vulnerabilities, and a loss of trust in the AVs. The importance of maintaining data accuracy and integrity becomes paramount in applications where human safety is directly impacted.

### E. High Mobility of the Vehicles

Another potential challenge in AVs is due to the nature of subject i.e. vehicles, Vehicles moves on variable speed and have diversity in their mobility profiles hence they could pose challenges in the communication and processing of data. Unlike stationary IoT devices, both manually operated and AVs are dynamic entities constantly in motion on roads. The varied speeds at which these vehicles operate introduce a layer of complexity, especially for manually driven vehicles, creating a diverse mobility landscape within the AVs domain. Vehicles equipped with computational and communication resources strive to establish and maintain stable connections with numerous peers. The challenge intensifies as these vehicles navigate through different speeds and trajectories, making it difficult to ensure consistent and reliable communication channels. Dedicated communication channels face difficulties in accommodating the dynamic and diverse mobility patterns inherent in the transportation. As a result, The high mobility characteristics of vehicles not only impact communication stability but also give rise to additional challenges. These challenges necessitate innovative solutions in communication protocols, network architectures, and resource allocation strategies to ensure seamless and reliable connectivity [24].

The potential of blockchain technology emerges as a crucial catalyst in addressing the challenges faced by autonomous vehicles in dynamic day-to-day scenarios. The reliance on accurate and secure data for real-time decision-making makes blockchain an essential player in the evolving landscape of autonomous transportation. Despite encountering unique hurdles, the promise of blockchain lies in its potential to revolutionize data management and security for AVs operating within the complexities of the real-world environment.

## IV. BLOCKCHAIN AND AVS

Integrating blockchain technology into Autonomous Vehicle ecosystems presents a unique set of challenges and opportunities. Among the various blockchain consensus mechanisms, PoUW emerges as a particularly compelling solution for AVs, offering distinct advantages over traditional mechanisms such as PoW, PoS, and PBFT. This assertion is grounded in an analysis of existing literature, including studies that highlight the efficiency, security, and scalability of blockchain applications within the AV domain [1],[3],[4],[5],[6].

Proof of work, the first consensus mechanism introduced by Bitcoin, secures blockchain networks through computational effort. However, its application in AV systems is limited due to its high energy consumption and low transaction throughput, making it impractical for real-time AV data processing and decision-making needs [4]. Conversely, PoS offers a more energy-efficient alternative by allocating mining power based on the proportion of coins held by a miner. While PoS improves the energy inefficiency of PoW and offers better scalability. Furthermore, PoS often centralizes decision-making power in the hands of a few stakeholders, which may not be suitable for the decentralized and distributed nature of autonomous vehicles. Decentralized decision-making is crucial for the agility and adaptability required in AV environments. On a similar note, dependence on a small number of stakeholders to validate transactions raises security concerns as well. In the AV domain, where safety and security are paramount, a consensus mechanism susceptible to centralization may pose risks.

On the other hand, PBFT, which is designed to achieve consensus even in the presence of malicious nodes, emphasizes fault tolerance and is well-suited for permissioned blockchain networks where participants are known and trusted. This mechanism ensures high transaction throughput and low latency, attributes beneficial for AV communications. In permissionless or public blockchain networks, where nodes can join or leave freely, PBFT may not be suitable due to its assumption of a fixed set of nodes. Similar to PoS, PBFT also lacks on account of operational complexity and the necessity for a relatively centralized set of validators, which might not align with the decentralized ethos of blockchain applications aimed at AVs, potentially limiting its broader adoption [5]. Another significant limitation of PBFT lies in its substantial demand for network resources, particularly due to communication overheads, which are essential for achieving consensus among nodes. The PBFT algorithm requires multiple rounds of communication and voting among nodes, resulting in heightened latency. In situations where maintaining low-latency is imperative, especially in real-time applications like AVs, PBFT may not be the most appropriate selection. Furthermore, it is known to perform sub-optimally and could be a performance bottleneck when dealing with a high number of peers [25]. This can limit its suitability for environments having large numbers of peers with constrained resources, such as autonomous vehicles, edge devices, or base stations with limited bandwidth.

In contrast, PoUW stands out by addressing blockchain's security and consensus and harnessing computational efforts for solving real-world problems. The novelty of this mechanism lies in its ability to direct the enormous computational resources of blockchain mining towards productive and beneficial tasks, such as data processing for AVs, environmental modelling, or even biomedical research [14]. For AV systems, this means that the computational work expended for blockchain consensus could simultaneously contribute to the processing of vehicular data, optimization of traffic flows, or enhancement of navigational algorithms, thereby directly supporting the operational goals of AVs [6].

The integration of PoUW within AV systems aligns with the emerging needs for secure, decentralized data sharing and processing platforms. Unlike PoW and PoS, PoUW offers a dual benefit, securing the blockchain network while contributing to societal and technological advancements. This dual functionality addresses critical aspects of AV technology, including data integrity, real-time processing requirements, and the need for decentralized, trustless communication among vehicles and infrastructure [7].

Furthermore, the adaptability of PoUW to AV technology is evidenced by its flexibility in selecting useful work tasks that are directly relevant to the AV domain. This adaptability ensures that the computational power dedicated to blockchain consensus directly benefits the AV ecosystem, optimizing resources and fostering innovations in vehicular technologies [1],[6]. Moreover, the potential for PoUW to contribute to environmental sustainability by repurposing energy consumption towards beneficial computations presents a compelling argument against the energy-intensive nature of PoW [6].

## V. Conclusion

In conclusion, this literature review has undertaken a comprehensive exploration of the intersection between blockchain technology, with a particular emphasis on the Proof of Useful Work consensus mechanism, and the realm of Autonomous Vehicles. The emergence of AVs has ushered in a new era in transportation, promising increased safety, efficiency, and convenience. However, the deployment and operation of AVs pose unique challenges, ranging from data security to processing speed, storage efficiency, information accuracy, and the high mobility characteristics of vehicles.

Traditional consensus mechanisms, such as PoW and PoS, while effective in securing blockchain networks, have limitations that make them less suitable for the dynamic and decentralized nature of the AV domain. In response to these challenges, PoUW has emerged as an innovative solution, redirecting computational efforts towards meaningful and beneficial tasks. This unique approach not only addresses the environmental concerns associated with PoW but also provides a dual functionality of securing the blockchain network while contributing to real-world problem-solving.

The integration of PoUW in the AV sector presents a compelling avenue for enhancing computational efficiency, data management, and overall advancements in autonomous vehicles. By leveraging the computational power dedicated to blockchain consensus for tasks directly relevant to AV operations, such as data processing for navigation algorithms or traffic optimization, PoUW aligns with the evolving needs of the AV ecosystem.

While challenges persist in the AV domain, ranging from data security to the dynamic nature of vehicle mobility, this literature review underscores the potential of PoUW in overcoming these obstacles. The findings of this exploration advocate for a paradigm shift towards more sustainable, efficient, and equitable blockchain applications in the AV sector. The adaptable nature of PoUW, coupled with its positive impact on sustainability, positions it as a promising solution for the intricate challenges faced by AVs.

As autonomous mobility continues to reshape the future of transportation, the insights gained from this review contribute to the ongoing discourse on the role of blockchain technology, specifically PoUW, in enhancing the operational efficiency, safety, and reliability of AVs. This exploration serves as a foundation for future research endeavors, encouraging further innovation and development at the intersection of blockchain and autonomous vehicles. Ultimately, the integration of PoUW offers a transformative pathway towards realizing the full potential of autonomous vehicles in a connected and secure mobility landscape.

To summarise, a comparison table provided in Table II offers a comprehensive resource for further understanding the nuanced distinctions between these consensus mechanisms and their applicability to the complex challenges of AVs.

TABLE II. Comparison of consensus mechanisms for AVs use-case

| **Feature/Consensus Mechanism** | **PoW** | **PoS** | **PBFT** | **PoUW** |
|---|---|---|---|---|
| Application in Avs scenarios | Limited due to high computational requirements [4] | Moderately suited, with adjustments for AV systems [3] | Highly suited for AVs needing quick consensus [5] | Highly applicable, especially for computational tasks in AVs [1],[6] |
| Efficiency | Low, due to energy-intensive mining process [4] | Higher than PoW, as it eliminates mining [3] | High, optimized for low-latency networks [5] | High, repurposes computational power for useful tasks [1],[6] |
| Security | High, with significant computational cost [4] | Variable, dependent on stake concentration [3] | High, designed for fault tolerance [5] | Dependent on the usefulness and verification of tasks [7] |
| Scalability | Challenged by block time and size [4] | Better than PoW due to flexible validation [3] | Good in permissioned networks, challenging in public ones [5] | Potentially high, if useful tasks are scalable [7] |
| Energy Consumption | Very high, due to complex puzzle solving [4] | Lower, more energy-efficient [3] | Moderate, depends on the network size [5] | Lower than PoW, varies with tasks [6] |
| Adaptability in AV Technology | Low, primarily designed for cryptocurrency mining [4] | Moderate, with potential for integration [3] | High, especially in controlled AV environments [5] | Very high, particularly when tasks align with AV objectives [1],[6] |

## References


[1] Baldominos, Alejandro, and Yago Saez. (2019) "*Coin.AI: A Proof-of-Useful-Work Scheme for Blockchain-Based Distributed Deep Learning*", Entropy 21, no. 8. p. 723. Available at: https://doi.org/10.3390/e21080723

[2] Ball, Marshall, Alon Rosen, Manuel Sabin, and Prashant Nalini Vasudevan. (2017) "*Proofs of Useful Work*", Cryptology ePrint Archive. Available at: https://eprint.iacr.org/2017/203 (Accessed: 1 February 2024)

[3] Biswas, Anushka, and Hwang-Cheng Wang. (2023) "*Autonomous Vehicles Enabled by the Integration of IoT, Edge Intelligence, 5G, and Blockchain*". Sensors 2023, p. 23(4). Available at: https://doi.org/10.3390/s23041963

[4] Bouraga, Sarah. (2021) "*A Taxonomy of Blockchain Consensus Protocols: A Survey and Classification Framework*". Expert Systems with Applications. Available at: https://doi.org/10.1016/j.eswa.2020.114384

[5] Dargahi, Tooska, Hossein Ahmadvand, Mansour Naser Alraja, and Chia-Mu Yu. (2022) "*Integration of Blockchain with Connected and Autonomous Vehicles: Vision and Challenge*". Journal of Data and Information Quality 14, no. 1, p.1–10. Available at: https://doi.org/10.1145/3460003

[6] Davidovic, Tatjana, Milan Todorovic, Dusan Ramljak, Tatjana Jaksic Kruger, Luka Matijevic, Djordje Jovanovic, and Dragan Urosevic. (2022) "*COCP: Blockchain Proof-of-Useful-Work Leveraging Real-Life Applications*". In 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA), 107–10. San Antonio, TX, USA: IEEE, 2022. Available at: https://doi.org/10.1109/BCCA55292.2022.9922117

[7] Dong, Zhongli, Young Choon Lee, and Albert Y. Zomaya. (2019) "*Proofware: Proof of Useful Work Blockchain Consensus Protocol for Decentralized Applications*". arXiv, 21 March 2019. Available at: http://arxiv.org/abs/1903.09276. (Accessed: 1 February 2024)

[8] Dragos, Cojocaru. (2022) "*Proof of Useful Work Based on Matrix Computation*". In 2022 24th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), 108–16. Hagenberg / Linz, Austria: IEEE, 2022. Available at: https://doi.org/10.1109/SYNASC57785.2022.00026

[9] Du, Yao, Cyril Leung, Zehua Wang, and Victor C.M. Leung. (2022) "*Accelerating Blockchain-Enabled Distributed Machine Learning by Proof of Useful Work*". In 2022 IEEE/ACM 30th International Symposium on Quality of Service (IWQoS), 1–10. Oslo, Norway. Available at: https://doi.org/10.1109/IWQoS54832.2022.9812927

[10] Gupta, Rajesh, Aparna Kumari, and Sudeep Tanwar. (2021) "*A Taxonomy of Blockchain Envisioned Edge-as-a-connected Autonomous Vehicles*". Transactions on Emerging Telecommunications Technologies 32, no. 6: e4009. Available at: https://doi.org/10.1002/ett.4009

[11] Haouari, Mohamed, Mariem Mhiri, Mazen El-Masri, and Karim Al-Yafi. (2022) "*A Novel Proof of Useful Work for a Blockchain Storing Transportation Transactions*". Information Processing & Management 59, no. 1.102749. Available at: https://doi.org/10.1016/j.ipm.2021.102749

[12] Ignatious, Henry Alexander, Hesham-El- Sayed, and Manzoor Khan. (2022) "*An Overview of Sensors in Autonomous Vehicles*". Procedia Computer Science 198, p. 736–41. Available at: https://doi.org/10.1016/j.procs.2021.12.315

[13] Jain, Saurabh, Neelu Jyothi Ahuja, P. Srikanth, Kishor Vinayak Bhadane, Bharathram Nagaiah, Adarsh Kumar, and Charalambos Konstantinou. (2021) "*Blockchain and Autonomous Vehicles: Recent Advances and Future Directions*". IEEE Access 9, p. 130264–328. Available at: https://doi.org/10.1109/ACCESS.2021.3113649

[14] Li, Boyang, Changhao Chenli, Xiaowei Xu, Taeho Jung, and Yiyu Shi. (2019) "*Exploiting Computation Power of Blockchain for Biomedical Image Segmentation*". 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), p. 2802–11. Long Beach, CA, USA: IEEE. Available at: https://doi.org/10.1109/CVPRW.2019.00339

[15] Lihu, Andrei, Jincheng Du, Igor Barjaktarevic, Patrick Gerzanics, and Mark Harvilla. (2020) "*A Proof of Useful Work for Artificial Intelligence on the Blockchain*". arXiv, Available at: http://arxiv.org/abs/2001.09244. (Accessed: 1 February 2024)

[16] Ma, Dongning, Sizhe Zhang, and Xun Jiao. (2022) "*HDCoin: A Proof-of-Useful-Work Based Blockchain for Hyperdimensional Computing*". arXiv, Available at: http://arxiv.org/abs/2202.02964 (Accessed: 1 February 2024).

[17] Ma, Zhijie, Qinglin Zhao, Jianwen Yuan, Xiaobo Zhou, and Li Feng. (2020) "Fork Probability Analysis of PoUW Consensus Mechanism". In 2020 IEEE International Conference on Smart Internet of Things (SmartIoT), 333–37. Beijing, China: IEEE, 2020. Available at: https://doi.org/10.1109/SmartIoT49966.2020.00060

[18] Maleš, Uroš, Dušan Ramljak, Tatjana Jakšić Krüger, Tatjana Davidović, Dragutin Ostojić, and Abhay Haridas. (2023) "Controlling the Difficulty of Combinatorial Optimization Problems for Fair Proof-of-Useful-Work-Based Blockchain Consensus Protocol". Symmetry 15, no. 1, p. 140. Available at: https://doi.org/10.3390/sym15010140

[19] Rathee, Sharma, Iqbal, Aloqaily, Jaglan, and Kumar. (2019) "A Blockchain Framework for Securing Connected and Autonomous Vehicles". Sensors 19, no. 14, p. 3165. Available at: https://doi.org/10.3390/s19143165

[20] Todorović, Milan, Luka Matijević, Dušan Ramljak, Tatjana Davidović, Dragan Urošević, Tatjana Jakšić Krüger, and Đorđe Jovanović. (2022) "*Proof-of-Useful-Work: BlockChain Mining by Solving Real-Life Optimization Problems*". Symmetry 14, no. 9, p. 1831. Available at: https://doi.org/10.3390/sym14091831

[21] Nakamoto, S. (2008) "*Bitcoin: A peer-to-peer electronic cash system*", Decentralized Business Review, p. 21260. Available at: https://assets.pubpub.org/d8wct41f/31611263538139.pdf (Accessed: 1 February 2024).

[22] Haber, S. and Stornetta, W.S. (1991) "*How to Time-Stamp a Digital Document*", Advances in Cryptology-CRYPTO' 90. CRYPTO 1990. Lecture Notes in Computer Science, 537, pp. 437-455. Available at: https://doi.org/10.1007/3-540-38424-3_32

[23] Tooska Dargahi, Hossein Ahmadvand, Mansour Naser Alraja,Chia-Mu Yu (2021) "*Integration of Blockchain with Connected and Autonomous Vehicles: Vision and Challenge*", Journal of Data and Information QualityVolume 14 Issue 1 Article No. 5, pp 1–10, Available at: https://doi.org/10.1145/3460003

[24] M. B. Mollah et al., (2020) "*Blockchain for the Internet of Vehicles Towards Intelligent Transportation Systems: A Survey*" IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4157-4185, Available at: http://dx.doi.org/10.1109/JIOT.2020.3028368

[25] H. Sukhwani, J. M. Martínez, X. Chang, K. S. Trivedi and A. Rindos, (2017) "*Performance Modeling of PBFT Consensus*

*Process for Permissioned Blockchain Network (Hyperledger Fabric)*" IEEE 36th Symposium on Reliable Distributed Systems (SRDS), Hong Kong, China, 2017, pp. 253-255, Available at: http://dx.doi.org/10.1109/SRDS.2017.36