Article

Not peer-reviewed version

Integrating Blockchain Engines and the Ideal Information Cycle: A Thermodynamic Framework for Resilience and Governance in VANETs

Rubén Juárez Cádiz * and Paloma Centenera Centenera

Posted Date: 29 May 2025

doi: 10.20944/preprints202505.2260.v1

Keywords: blockchain technology; Vehicular Ad Hoc Networks (VANETs); governance; resilience; consensus algorithm; blockchain engine; information cycle; decentralization; thermodynamics; blockchain securitys

Article

Integrating Blockchain Engines and the Ideal Information Cycle: A Thermodynamic Framework for Resilience and Governance in VANETs

Rubén Juárez * and Paloma Centenera

Universidad San Pablo CEU; paloma.centeneracentenera@ceu.es
* Correspondence: ruben.juarezcadiz@ceu.es; Tel.:+34647942856

Abstract: Blockchain technology has seen widespread adoption across various domains, including Vehicular Ad Hoc Networks (VANETs), offering significant opportunities alongside notable challenges. While blockchain is renowned for enhancing security, privacy, and efficiency, its decentralized nature inherently complicates effective governance—especially in public, permissionless systems where open participation intensifies issues of control and accountability. In the context of VANETs, these challenges are further magnified due to the dynamic and heterogeneous nature of vehicular environments. To address these complexities, we propose a novel framework based on thermodynamic principles, introducing the "Blockchain Engine" and its associated "Ideal Information Cycle." This approach provides a robust method for analyzing and improving resilience and governance in VANETs by directly confronting the tension between decentralization and the need for structured oversight. Our study not only establishes a foundation for future research on blockchain governance in VANETs but also facilitates its practical adoption in industrial and commercial settings.

Keywords: blockchain technology; Vehicular Ad Hoc Networks (VANETs); governance; resilience; consensus algorithm; blockchain engine; information cycle; decentralization; thermodynamics; blockchain securitys

---

1. Introduction

In an effort to provide a technical approach to blockchain governance [1], Caporali (2020) adapted techniques from electronics and automation to the realm of Vehicular Ad Hoc Networks (VANET) [2]. Although this pioneering work offers a significant starting point for further exploration, its framework invites further development. Building on this foundation, the blockchain system was modeled in discrete component blocks, a strategy analogous to the use of servomechanisms in control theory to stabilize electrical power against parasitic signals and distortions in VANETs [3]. Caporali (2020) further introduced an abstract blockchain structure, termed the *temporal structure of the blockchain*, which comprises four essential functions: time stamping, sorting, alerting and control [2].

However,n of an inanmatan cycle requires further refinement and expansion to incorporate broader insights inspired by natural physical systems. This challenge is particularly pronounced when establishing a representative unit within decentralized VANETs, given the multiplicity of involved actors [4]. Moreover, considering the critical role of VANETs in the contemporary technological landscape, addressing the unique challenges of governance and information management in these highly dynamic and decentralized networks is imperative [5]. In this context, blockchain technology emerges as a robust and tamper-resistant solution for data verification and authentication in VANETs [46].

To fully exploit the potential of blockchain in VANETs, it is essential to develop models and structures that are tailored to the specific characteristics and requirements of these networks. Consequently, this study aims to extend and refine Caporali's proposals (2020) by adapting them to the VANET environment, thustablishing a solid framework for future research and development. The primary

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 29 May 2025 doi:10.20944/preprints202505.2260.v1

contributions of this work include the application of blockchain technology to facilitate consensus processes and transaction management, as well as an exploration of the implications of geographical configurations and information quality on network governance. These advancements are expected to significantly enhance the resilience and governance of vehicular ad-hoc networks.

1.1. Organization of the Document

The remainder of this paper is structured as follows:

- **Section II: Fundamental Principles and State of the Art.** This section introduces blockchain technology and Vehicular Ad-Hoc Networks (VANETs), providing a comprehensive overview of the current research landscape in these domains.
- **Section III: Hypothesis Formulation and Methodology.** Here, the research hypotheses are clearly defined and the methodology for their evaluation is described in detail, including the simulation of VANETs using NS-3 and the integration of blockchain technology.
- **Section IV: Evaluation and Discussion of Results.** This section presents the outcomes from the simulations and analyses, followed by a critical discussion of the results.
- **Section V: Conclusions and Future Work.** The final section summarizes the main findings of the study and outlines potential avenues for future research, with a focus on further enhancing the governance and resilience of vehicular ad-hoc networks through blockchain-based solutions.

2. Fundamental Principles and State of the Art

In the contemporary era of pervasive connectivity and rapid digitization, blockchain technology and Vehicular Ad-Hoc Networks (VANETs) have emerged as domains of significant research interest and potential. As these fields continue to evolve and diversify, it becomes essential to understand their underlying principles and explore how they can be harnessed to enhance the efficiency, security, and resilience of both digital infrastructures and transportation systems.

This section establishes a robust theoretical framework for our study by providingg an in-depth introduction to these technologies and their intrinsic characteristics. We begin with an examination of blockchain technology, tracing its evolution from its origins as the foundational architecture of Bitcoin to its current role in facilitating a wide array of applications beyond mere financial transactions. In particular, we analyze its core features, decentralization, immutability, and transparency, and discuss how these attributes can be exploited to improve the governance of digital networks.

Subsequently, our focus shifts to VANETs, where we elucidate their function as dynamic and decentralized network systems that are pivotal to the realization of future intelligent transportation solutions. We evaluate both the challenges and opportunities these networks present, and consider how the integration of blockchain technology might offer innovative solutions to address these issues.

Finally, we review the current state of research in these fields, highlighting the contributions of previous studies and identifying existing gaps in the literature that our work seeks to fill. The objective of this section is to contextualize our study within the broader academic discourse and to establish a solid foundation for the ensuing analysis and discussion.

2.1. Exploration of Blockchain Technology

Blockchain technology has been a pivotal research topic since its inception in 2008 with the publication of Bitcoin's foundational white paper [7]. This innovative public ledger system enabled the creation of a decentralized cryptocurrency, eliminating the need for a centralized authority. One of the hallmark features of blockchain technology is its decentralization, which allows transactions to be validated and recorded across a distributed network of nodes [8].

Over time, the application of blockchain technology has transcended the realm of financial transactions. It is now being explored and utilized in a myriad of domains, including supply chain management, digital identity administration, smart contract execution, and more [9].

The fundamental attributes of blockchain technology—namely decentralization, immutability, and transparency—are recognized as key factors in enhancing the governance of digital networks. Decentralization improves network resilience and security by dispersing control across multiple nodes [10]. Immutability ensures that once data is recorded on the blockchain, it cannot be altered or deleted, thereby establishing a secure and verifiable transaction history. Meanwhile, transparency fosters accountability and traceability [11].

Despite these promising advantages, the integration of blockchain technology into complex network environments such as VANETs remains in its nascent stages and is fraught with challenges. Future research should focus on addressing these challenges to fully harness the potential of blockchain technology in such dynamic contexts.

2.2. Vehicular Ad-Hoc Networks (VANETs): Highly Dynamic and Decentralized Systems

Vehicular Ad-Hoc Networks (VANETs) are emerging as a cornerstone technology for next-generation intelligent transportation systems [12]. These networks enable communication among vehicles as well as between vehicles and transportation infrastructures, thereby facilitating a wide range of applications—from enhancing road safety to optimizing traffic management [13].

One of the primary challenges in VANETs is the secure and efficient management of information. Due to the high mobility of nodes (i.e., vehicles) that frequently join and leave the network, ensuring data integrity and reliable communication presents significant difficulties [14].

Blockchain technology offers promising solutions to these challenges. By providing a distributed, transparent, and immutable ledger, blockchain can enable secure verification and authentication of data within a VANET [15]. Moreover, the inherent decentralization of blockchain aligns well with the decentralized nature of VANETs, facilitating a seamless integration of these technologies [16].

Despite these advances, further research is needed to optimize the application of blockchain in VANETs and to overcome issues such as high energy consumption and latency. Addressing these challenges is crucial for the continued development and widespread adoption of blockchain-enabled intelligent transportation systems.

2.3. Current State

In the existing academic literature, various proposals have emerged to address the challenges associated with integrating blockchain technology with VANETs. For instance, Sharma et al. [17] proposed a blockchain-based architecture for VANETs that emphasizes data security and communication efficiency. However, their study did not thoroughly address the issues of governance in decentralized VANET environments.

In contrast, Daza et al. [18] introduced a decentralized consensus mechanism using blockchain for VANETs. While their approach represents a significant advance, it falls short of providing a scalable solution for managing the high-volume transactions inherent to VANETs.

Furthermore, several studies have explored methods for detecting and resolving conflicting or invalid transactions. For example, Lu et al. [19] proposed a robust consensus algorithm designed to manage transaction conflicts. Nonetheless, their approach is not entirely suited to handling the high transaction throughput encountered in real-time VANET scenarios.

It is evident that, despite the considerable progress made in applying blockchain technology to VANETs, gaps remain in addressing critical issues such as high-volume transaction processing, conflict resolution, and efficient governance in decentralized environments. Our study aims to bridge these gaps by developing a comprehensive solution that builds upon existing advances and adapts them to the specific needs of VANETs.

2.4. Application of the Carnot Cycle to VANETs

The principles of thermodynamics have long been studied and applied across multiple fields, with concepts such as entropy and energy efficiency being integral not only to physical systems but also to information processing and network science. Much like these principles elucidate the behavior and interactions within physical systems, they can offer valuable insights when applied to the dynamic environment of Vehicular Ad-Hoc Networks (VANETs).

The application of thermodynamic principles to information technology has been explored in various studies. For example, Landauer (1961) demonstrated that information processing is inherently irreversible and requires a minimum amount of energy, thereby establishing a fundamental link between information theory and thermodynamics [20]. Subsequent investigations have extended these ideas, examining how the second law of thermodynamics and the concept of entropy can inform information processing and management [21,22].

In the context of VANETs, these thermodynamic concepts can be particularly fruitful. In such networks, entropy may be viewed as a measure of uncertainty and change—reflecting factors such as the frequent arrival and departure of nodes, fluctuations in connection quality, and the inherently volatile nature of the network [23]. By framing information management and consensus building in VANETs as thermodynamic processes, it becomes possible to explore strategies for optimizing these processes to enhance overall network performance.

The Carnot Cycle, a theoretical construct developed by Sadi Carnot in 1824 to describe the maximum efficiency of a heat engine operating between two reservoirs, offers a compelling analogy. While originally conceived for physical heat engines, the Carnot Cycle has since been applied across diverse disciplines to understand the operation of systems transitioning between high and low energy states.

Drawing a parallel between the Carnot Cycle and the information cycle in VANETs and blockchain technology, we can conceptualize high and low energy states as analogous to high and low information quality states, respectively. In this framework, a VANET network transitions between these states to achieve consensus, much as a heat engine converts thermal energy into work by operating between hot and cold reservoirs.

To illustrate this concept, one can employ a Temperature-Entropy (T-S) Diagram, where temperature and entropy serve as analogs for information quality and disorder, respectively. In this diagram, an idealized Carnot cycle demonstrates how a VANET network might evolve from a state of low information quality and high disorder (high entropy) to a state of high information quality and low disorder (low entropy), through a series of processes akin to 'heating' (information validation) and 'cooling' (removal of invalid information).

This thermodynamic model offers a novel perspective on addressing challenges in governance and information management within VANETs. It lays the groundwork for the development of more efficient and robust consensus algorithms, ultimately enhancing network performance. In the subsequent sections, we further explore these concepts and their potential applications in the integration of VANETs with blockchain technology.

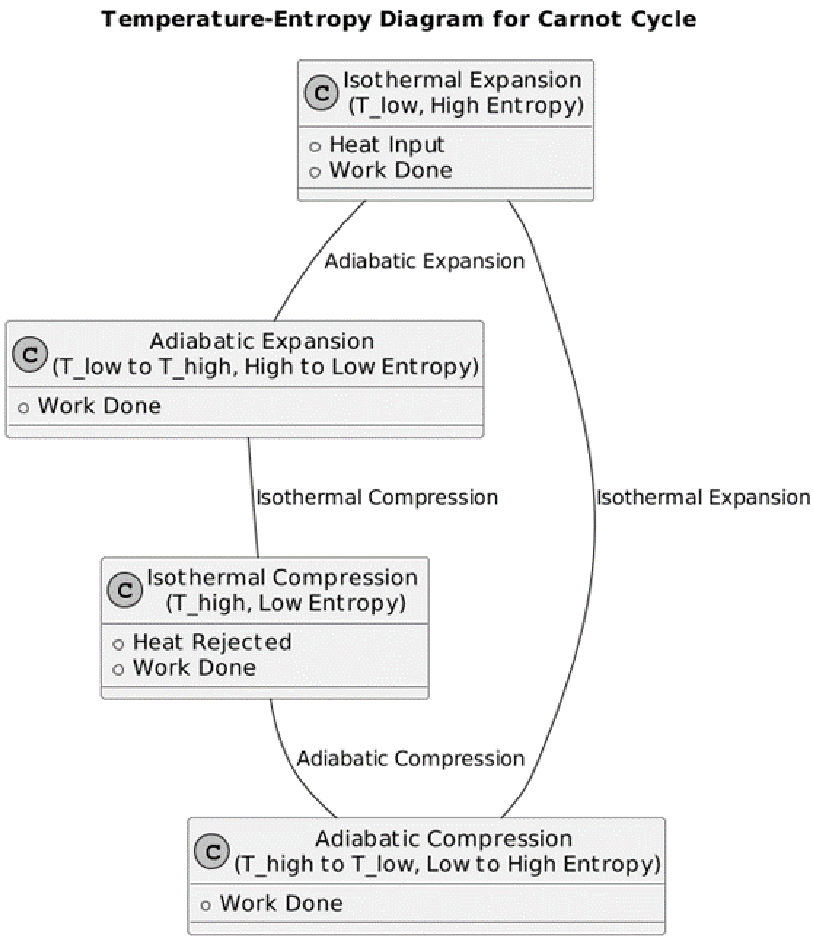

Figure 1. Temperature-Entropy Diagram of the Carnot Cycle.

The figure above illustrates the four stages of the Carnot Cycle: isothermal expansion, adiabatic expansion, isothermal compression, and adiabatic compression. In the context of VANETs, our aim is not to delve into the detailed mechanics of a thermodynamic engine, but rather to explore the pivotal role of entropy in these networks.

From a macroscopic perspective, entropy (S) quantifies the natural tendency towards spontaneous change. In a similar vein, within VANETs, entropy can be interpreted as a measure of the propensity for network state alterations—such as the frequent arrival and departure of nodes or changes in network topology due to vehicular mobility.

At a microscopic level, entropy represents the degree of disorder within a system: the greater the disorder, the higher the entropy. In VANETs, this concept translates into a measure of uncertainty or unpredictability, stemming from factors such as random node movement and fluctuations in connection quality. For instance, in classical thermodynamics, it is well established that for a given substance the entropy increases from the solid to the gaseous state, i.e.,

$$S_{\text{solid}} < S_{\text{fluid}} < S_{\text{gas}},$$

as described in Callen (1985) [24]. Analogously, a VANET may transition from a relatively stable state to one characterized by heightened complexity and disorder as its dynamics evolve.

Bearing these thermodynamic analogies in mind, we propose an integrated approach that combines consensus mechanisms, thermodynamic principles, and information theory within the VANET framework. Notably, the application of these principles to the management of information and consensus building in VANETs can yield valuable insights. In these networks, information is exchanged dynamically and is inherently subject to continuous change, while the decentralized and autonomous nature of VANETs poses significant challenges for achieving consensus. By conceptualizing information as a form of "energy" and treating transactions or data exchanges as "thermodynamic processes," we can investigate how the degree of disorder—represented by entropy—affects the efficiency of these processes, and consequently, the effectiveness of information management and consensus formation.

This perspective paves the way for innovative strategies aimed at optimizing VANET performance and lays a robust foundation for the development of consensus algorithms tailored to the unique challenges of these dynamic networks.

The figure above demonstrates a conceptual interpretation of the Carnot Cycle applied to information management in Vehicular Ad hoc Networks (VANETs). In this analogy, the y-axis represents the Quality of Information (QoI)—comparable to temperature in a traditional Carnot Cycle—while the x-axis corresponds to Information Entropy, analogous to thermodynamic entropy.

1. **Isothermal Expansion (Stage A-B):** During this phase, new information enters the network. Despite the simultaneous influx of large volumes of data, the overall quality remains relatively constant (i.e., isothermal conditions). However, entropy increases as the system becomes more disordered due to the introduction of unverified or heterogeneous information.
2. **Adiabatic Expansion (Stage B-C):** In this stage, the network processes the incoming data. As low-quality or incorrect information is identified and discarded, there is a slight decrease in overall information quality. Concurrently, the system 'cools down' and entropy decreases as order is gradually restored.
3. **Isothermal Compression (Stage C-D):** Here, the remaining information is rigorously validated while redundant or erroneous data is removed. The quality of information remains steady since high-quality data is preserved, and entropy is further reduced as the system achieves a higher degree of order.
4. **Adiabatic Compression (Stage D-A):** Finally, the validated information is ready for use in decision-making or for dissemination to other nodes. During this phase, the quality of information improves, and entropy continues to decrease, returning the network to a state ready to process new incoming data and thus completing the cycle.

This model, inspired by the Carnot Cycle, offers a novel framework for understanding information management in VANETs—from the introduction and validation of data to its subsequent utilization. By drawing parallels between thermodynamic processes and the dynamics of information, this approach provides a basis for developing efficient strategies for consensus-building and network management. The conceptual foundation of this analogy is supported by classical thermodynamic principles [24] and has been extended to the realm of information theory by studies such as those by Parrondo et al. [22].

Moreover, while research on Quality of Information (QoI) in networked systems is gaining traction, its specific application to VANETs remains an emerging field. Integrating thermodynamic analogies with QoI metrics thus presents a promising direction for future investigations aimed at optimizing the performance of these dynamic and complex networks.

3. Hypothesis Formulation and Methodology

In this section, we delineate our research hypotheses and describe the procedures employed to examine their validity. Our foundational premise is that blockchain technology possesses substantial potential to enhance both governance and resilience in Vehicular Ad Hoc Networks (VANETs). On this basis, we propose the following hypotheses:

1. Incorporating blockchain technology into VANETs can significantly enhance their security and privacy [86].
2. A blockchain model that integrates thermodynamic principles can offer a more accurate and efficient representation of decentralized governance in VANETs. (This hypothesis is novel and builds upon the theoretical framework established in [22].)

3. The use of an entropy-based information cycle can contribute to optimizing VANET performance [5].

The thermodynamic cycle—specifically, the Carnot cycle—provides an idealized representation of the exchange of energy and work in a closed system. By extending this concept to the domain of VANETs, we interpret the network nodes (i.e., vehicles) as system components that exchange information (analogous to energy in thermodynamics) through their interactions [?]. Within this framework, entropy assumes a central role as a measure of disorder or uncertainty in the network. For VANETs, entropy can be understood as a metric of the inherent variability and unpredictability in network topology and behavior. For example, as more vehicles join the network or as traffic conditions fluctuate, the network's "entropy" increases—reflecting heightened complexity and uncertainty [28].

Conversely, the process of building consensus in the network may be viewed as an effort to reduce entropy. When network nodes converge on a common state or consensus version of data, disorder and uncertainty are effectively minimized [29]. This perspective opens new avenues for optimizing information management and consensus mechanisms in VANETs. In particular, it suggests the possibility of designing novel protocols that actively strive to minimize network entropy while ensuring efficient information dissemination and verification. The potential of such approaches is further underscored by recent advancements in distributed ledger technologies, as exemplified by alternative mechanisms like the Tangle [30].

In the following sections, we elaborate on the experimental design, simulation parameters (including the use of NS-3 for VANET simulation), and the integration of blockchain technology to empirically assess these hypotheses.

3.1. Incorporating Blockchain Technology into VANETs to Enhance Security and Privacy

Blockchain technology has been widely acknowledged for its capacity to bolster security and privacy across a multitude of applications. In the context of Vehicular Ad Hoc Networks (VANETs), integrating blockchain can significantly improve the security of information transmission and safeguard user privacy. VANETs routinely exchange sensitive data—including vehicle locations, speeds, and trajectories—which are essential for efficient network operation and road safety applications. However, the exposure of such data also presents considerable privacy risks if exploited by malicious entities [93].

The inherent characteristics of blockchain—most notably, the immutability and transparency of its distributed ledger—provide robust defenses against data manipulation and unauthorized access. In blockchain-based systems, each transaction is independently verified by multiple nodes, thereby ensuring data integrity and making it exceedingly difficult for attackers to tamper with recorded information [31].

Moreover, blockchain technology can enhance privacy protection by enabling secure, anonymous transactions. The deployment of Smart Contracts further automates network processes, ensuring that sensitive user data is shared only when predefined conditions are met, without revealing personal identities [32]. This capability is especially valuable in VANETs, where privacy concerns are paramount due to the continuous exchange of critical, location-based data.

Nonetheless, integrating blockchain technology in VANETs is not without challenges. The high mobility of vehicular nodes and the voluminous nature of transactions can lead to issues such as increased latency and scalability constraints. Despite these challenges, recent advancements in blockchain architectures for vehicular networks suggest that these limitations can be mitigated. For instance, recent work by Ning et al. [15] demonstrates that blockchain-based secure V2X communications can effectively enhance the overall security and privacy of vehicular networks.

In summary, while challenges remain, the incorporation of blockchain technology into VANETs presents a promising avenue for bolstering both security and privacy. The decentralized, immutable, and transparent nature of blockchain offers compelling solutions to the inherent vulnerabilities in VANETs, thereby facilitating safer and more reliable vehicular communications.

 doi:10.20944/preprints202505.2260.v1

3.1.1. Consensus and Validation in VANETs

In this subsection, we define and contextualize two critical components for the operation of Vehicular Ad Hoc Networks (VANETs): consensus and validation. These definitions are adapted from widely accepted principles in distributed systems and cybersecurity standards—specifically, ISO/IEC 21434:2020 [34]—and are tailored to address the unique challenges presented by VANETs.

Consensus: Consensus refers to the process by which network nodes arrive at an agreement regarding the validity of transactions and the overall state of the distributed ledger. In the context of VANETs, this entails that all participating vehicles concur on a common and ordered set of validated transactions, thereby ensuring consistency and reliability in data dissemination and network operation.

Validation: Validation denotes the process of verifying that an entity or data transaction complies with all requisite integrity and authenticity criteria. Within VANETs, this involves rigorously checking the data source, confirming the integrity of the transmitted information, and ensuring that the data is both relevant and timely.

Given the decentralized and dynamic nature of VANETs—where mobile nodes can join and exit the network at any time—a robust consensus mechanism is indispensable. Such a mechanism ensures that all nodes converge on a unified network state, which is critical for maintaining data consistency and facilitating effective cooperation among vehicles. Concurrently, the validation process is essential for safeguarding the authenticity and accuracy of the exchanged data, thereby mitigating risks associated with misinformation or data tampering.

In the subsequent sections, we will elaborate on the practical implementation of these consensus and validation mechanisms, and examine how their integration can enhance the performance and efficiency of VANETs.

3.1.2. Consensus Process Diagram

The definition of consensus in distributed systems encompasses two parallel conditions: ensuring safety (i.e., that undesirable events, such as incorrect consensus outcomes, do not occur) and guaranteeing liveness (i.e., that the system eventually reaches a consensus state). The diagram below, adapted from ISO/IEC guidelines to suit the specific requirements of VANETs, encapsulates the essential dynamics of the consensus process. A critical aspect of this process is the trade-off between consensus algorithms that favor safety—such as Byzantine agreement protocols—and those that prioritize liveness, exemplified by Proof of Work (PoW) mechanisms.

These fundamental concepts were elaborated in the seminal work by Lamport et al. [35], which introduced the notions that safety ensures "nothing bad happens" while liveness guarantees that "something good eventually happens." In practical terms, a safety-oriented consensus mechanism minimizes the likelihood of a "NO" consensus outcome; however, it may incur increased latency if the computation time scales with the number of nodes.

In the context of VANETs—characterized by high node mobility and frequent topology changes—these considerations are particularly critical. For instance, a consensus algorithm that emphasizes safety can secure the integrity and authenticity of information exchanged within the network but may require longer convergence times due to variability in node density and network conditions. Conversely, an algorithm biased towards liveness can expedite consensus, albeit with a potential compromise in data integrity and security. Consequently, the design of consensus mechanisms for VANETs must judiciously balance these two properties based on the specific demands of the application domain.

In safety-critical vehicular applications, such as collision avoidance and driver assistance systems, robust consensus is paramount to ensuring operational safety. Conversely, applications requiring rapid updates—like real-time traffic management or location-based navigation—benefit from faster consensus, even if this entails a modest trade-off in safety. Figure 2 illustrates the flow of actions from

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 29 May 2025 doi:10.20944/preprints202505.2260.v1

the receipt of a transaction (or information exchange) to its validation and subsequent recording (or rejection) in the network. Depending on the specific consensus algorithm implemented, this diagram may be further refined to capture additional process nuances.

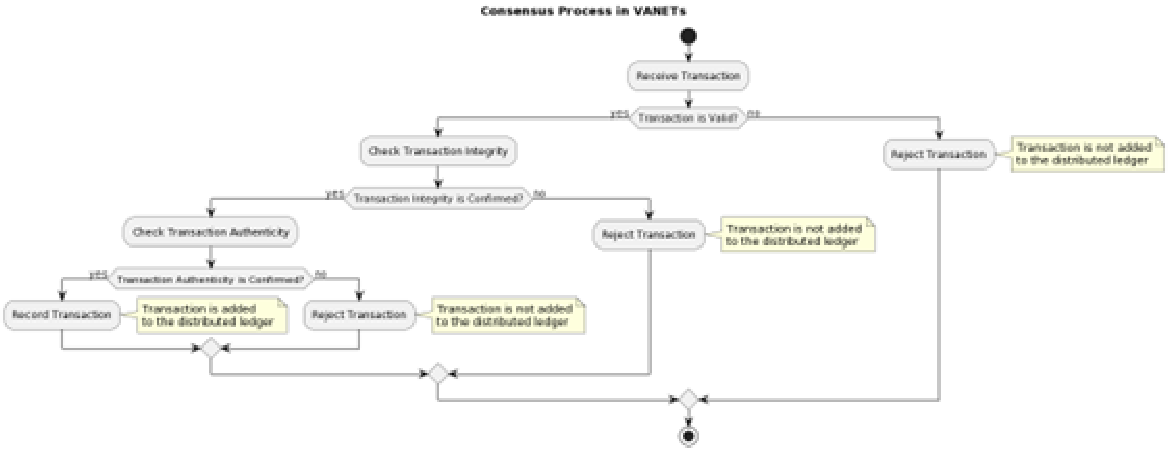

Figure 2. Consensus Process in VANETs

3.1.3. Adaptation of the Proof of Work (PoW) Consensus Process for VANETs

The Proof of Work (PoW) consensus algorithm is selected here as an illustrative example due to its widespread use in Bitcoin and its pedagogical value in elucidating consensus mechanisms. While PoW is traditionally employed in Bitcoin [7], its adaptation to the VANET environment necessitates modifications to address the unique characteristics of vehicular networks. In a standard PoW system, a block of transactions is generated through computational effort; however, alternative consensus mechanisms—such as Byzantine agreement protocols—eschew block creation in favor of exchanging messages between nodes to establish an ordered consensus.

Two additional aspects are particularly salient in the context of VANETs:

- In networks incorporating smart contracts, the consensus process may involve both on-chain and off-chain interactions, thereby increasing the overall complexity.
- The decentralized and highly dynamic nature of VANETs—with multiple nodes operating concurrently—further complicates the consensus process.

Figure 9 provides a simplified representation of the PoW consensus process adapted for VANETs. While the underlying principles remain consistent, the specific implementation details can vary according to factors such as the chosen consensus algorithm, the characteristics of the transactions, and prevailing network conditions. This diagram draws inspiration from the consensus process outlined by Tran and Krishnamachari [36], particularly with respect to the distinctions between transaction forwarding and node forwarding. Nonetheless, our adaptation specifically addresses challenges imposed by node mobility and the need for rapid decision-making in vehicular networks.

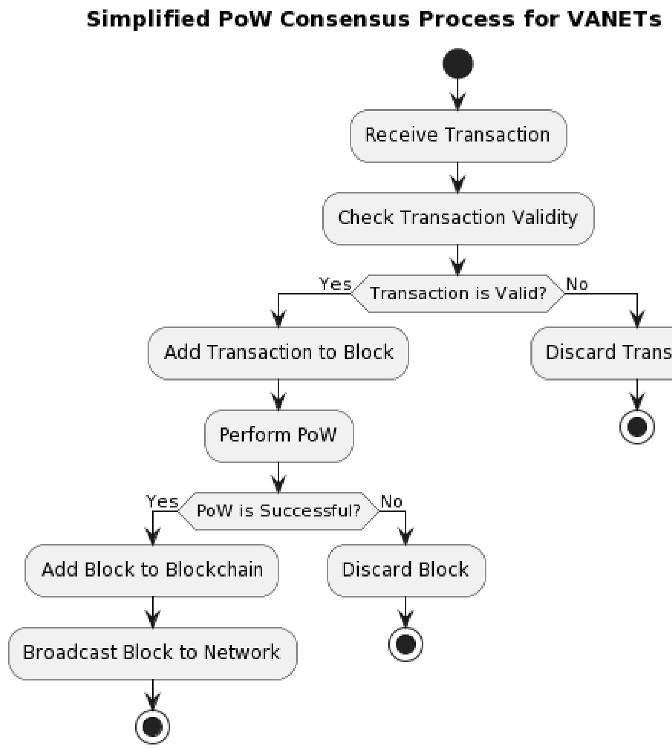

Figure 3. Simplified PoW Consensus Process for VANETs

It is crucial to recognize that, although the simplified model depicted in Figure 9 aids in conceptualizing the PoW-based consensus in VANETs, the actual implementation is considerably more complex. The high mobility inherent in VANETs means that nodes can frequently move in and out of communication range, affecting their ability to participate effectively in the consensus process [37]. Moreover, the energy-intensive nature of traditional PoW, as evidenced in Bitcoin [7,38], may render it inefficient in resource-constrained vehicular environments. This challenge may necessitate the adoption of more energy-efficient variants of PoW or the exploration of alternative consensus algorithms better suited to VANETs [68].

Finally, privacy and security aspects must also be addressed in the VANET context. It is essential to ensure that the consensus process preserves the confidentiality of sensitive information related to vehicles and their occupants and is robust against potential malicious attacks [40]. While adapting the PoW consensus process for VANETs presents a promising research direction, it simultaneously introduces significant challenges that warrant careful consideration and further investigation.

3.1.4. Environmental Impact of Consensus Algorithms

The energy efficiency of consensus algorithms is a critical factor in their viability for deployment in resource-constrained environments such as Vehicular Ad Hoc Networks (VANETs). In particular, the Proof of Work (PoW) algorithm—central to Bitcoin's operation—has been widely criticized for its substantial energy consumption. According to the Cambridge Bitcoin Energy Consumption Index, the Bitcoin network consumes more energy than many countries, underscoring significant environmental concerns [91].

In the context of VANETs, high energy consumption poses a notable challenge. Vehicles typically have limited energy resources, and excessive energy usage by the consensus mechanism can compromise the performance of other critical vehicular systems, including those essential for safety. Moreover, in an era of heightened environmental awareness and climate change mitigation efforts, energy efficiency emerges as a vital criterion in the design and implementation of emerging vehicular technologies.

 doi:10.20944/preprints202505.2260.v1

Consequently, when implementing consensus algorithms like PoW in VANETs, it is imperative to consider their environmental impact. One potential solution is to adapt PoW to reduce its energy requirements or to employ alternative, more energy-efficient consensus mechanisms—such as Proof of Stake (PoS) or Byzantine Fault Tolerance (BFT) protocols—which have been shown to consume considerably less energy [42].

Such adaptations could yield significant benefits not only by enhancing the energy efficiency and battery life of vehicular systems but also by reducing the overall environmental footprint of the network. Nonetheless, the trade-offs between security, efficiency, and sustainability must be carefully balanced when selecting and implementing consensus algorithms. Further research into developing consensus mechanisms that are secure, efficient, and environmentally friendly represents a promising and necessary avenue for the future evolution of VANETs.

3.1.5. Alternative Consensus Algorithms

Proof of Stake (PoS) is an alternative to Proof of Work (PoW) that achieves consensus by selecting validators in proportion to their stake rather than relying on intensive computational work [43]. In the context of VANETs, PoS offers several advantages over PoW. Its markedly lower energy consumption is particularly beneficial in vehicular environments, where energy resources are limited. Moreover, PoS can enhance security by making it economically unfeasible for an adversary to acquire a dominating stake in the network [43,94].

However, PoS is not without its challenges. It is susceptible to the "nothing-at-stake" problem, where validators may have incentives to support multiple competing chains simultaneously, thereby increasing the risk of network forks. In addition, PoS can lead to a concentration of power, as larger stakeholders inherently possess greater influence over the consensus process [45].

An alternative consensus mechanism is Delegated Proof of Stake (DPoS). In DPoS, token holders vote to elect a limited number of delegates or “witnesses” who are responsible for validating transactions and maintaining the blockchain. DPoS retains the energy efficiency benefits of PoS, which makes it attractive for VANET applications; however, it also introduces concerns regarding centralization and the potential for delegate collusion or abuse of power [46,95].

Another promising alternative is the Federated Byzantine Agreement (FBA), as implemented in systems such as the Stellar network. In FBA, each node selects a set of other nodes it trusts to vote on transactions, allowing the network to reach consensus without the reliance on a centralized leader. This decentralized trust model can significantly enhance network resilience—especially in VANETs, where node churn is frequent—although its overall security and efficiency are highly dependent on the configuration and reliability of the trusted node sets [47,48].

Each of these consensus algorithms presents distinct trade-offs in terms of energy efficiency, security, centralization, and scalability. Their suitability for VANETs must therefore be evaluated in light of the unique operational constraints and requirements of vehicular environments.

3.2. A Thermodynamic-Based Blockchain Model Can Offer a More Accurate and Efficient Representation of Decentralized Governance in VANETs

Decentralized governance is an intrinsic feature of Vehicular Ad Hoc Networks (VANETs) and represents a central challenge to their effective operation. The autonomous and resilient performance of these networks largely depends on how decisions and information are managed. In this regard, integrating blockchain with thermodynamic principles promises a more accurate and efficient representation of decentralized governance.

Thermodynamics, the branch of physics that examines the relationships among heat, work, temperature, and energy, provides foundational insights into the behavior of complex systems. Classical works by Carnot [49] and Clausius [50] established the principles governing energy exchange and introduced entropy as a measure of disorder or uncertainty. When these concepts are transposed to blockchain systems within VANETs, entropy can be interpreted as a metric for the uncertainty in the network state and in the execution of blockchain transactions. Building on the framework developed by

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 29 May 2025 doi:10.20944/preprints202505.2260.v1

Parrondo et al. [22], each blockchain transaction may be conceptualized as a "thermodynamic process" where information (analogous to energy) is exchanged and the network's entropy is modulated.

Under this paradigm, consensus algorithms can be designed to minimize network entropy, potentially yielding faster and more reliable decision-making. Alternatively, information transmission mechanisms may be dynamically adapted to current entropy levels, ensuring efficient communication even under conditions of high uncertainty. This adaptive model could enhance both information management and governance in the dynamic environment of VANETs [38].

Moreover, recent studies have begun to apply thermodynamic principles to blockchain governance, particularly in addressing energy management and decentralization challenges [22,38]. In VANETs, stability—the ability to maintain continuous operation in the face of disturbances—and resilience—the capacity to recover from such disturbances—are paramount [57]. Energy conservation and efficiency are equally critical, given the limited energy resources available in vehicular systems [54,55].

The application of these thermodynamic principles not only facilitates the design of more adaptive governance mechanisms but also aligns with broader sustainability objectives. For instance, optimizing energy use in consensus processes contributes to sustainable network operation, thereby supporting the United Nations Sustainable Development Goal 9, which advocates for resilient infrastructure, sustainable industrialization, and innovation [56]. By reducing entropy through improved data distribution and energy management, such a model can enhance the efficiency, resilience, and security of VANETs.

However, significant challenges remain. Implementing thermodynamic principles in blockchain governance entails substantial modifications to existing network architectures and the adoption of novel protocols. Scalability is another concern, as the network must dynamically adjust to an increasing number of nodes and transactions. Moreover, a delicate balance must be maintained between resilience and efficiency—excessive emphasis on one may compromise the other.

In summary, the convergence of thermodynamic principles with blockchain governance represents a promising avenue for advancing decentralized management in VANETs. While challenges persist, continued research and development in this emerging field may ultimately yield systems that are not only more efficient and resilient but also more secure and sustainable.

3.3. The Use of an Entropy-Based Information Cycle May Assist in Optimizing the Performance of VANETs

In highly dynamic and decentralized Vehicular Ad Hoc Networks (VANETs), effective information management is paramount to achieving optimal network performance. One promising approach to address these challenges is the integration of an entropy-based information cycle. In this framework, entropy—defined as a measure of uncertainty or disorder within a system—serves as an indicator of network complexity and dynamics [58]. By monitoring and managing entropy, network designers can develop strategies to optimize key performance metrics such as data dissemination efficiency, consensus speed, and overall network resilience.

The entropy-based information cycle conceptualizes the flow of information in a VANET as analogous to a thermodynamic cycle. The cycle commences with the generation or reception of new information, which corresponds to an increase in entropy. This is followed by the propagation and exchange of information among network nodes, during which entropy is maintained at a certain level. Finally, the cycle culminates in a consolidation or consensus phase where entropy is reduced, resulting in a more ordered state across the network.

Adopting an entropy-aware approach yields several potential benefits. First, continuously monitoring system entropy enables network operators to anticipate and manage network evolution more effectively. Second, consensus mechanisms designed to minimize entropy during decision-making phases can lead to faster and more reliable convergence [59]. Third, aligning data dissemination strategies with the entropy cycle can enhance the efficiency of information exchange, ensuring that high-quality and relevant data is preferentially propagated.

 doi:10.20944/preprints202505.2260.v1

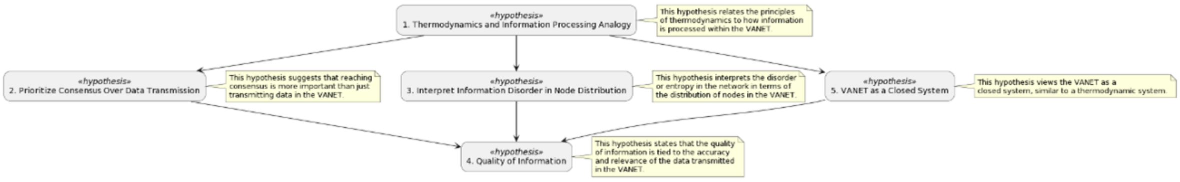

Figure 4. Hypotheses Diagram

In this paper, we introduce the concept of the 'VANET Engine' as a metaphor for representing the network as a closed thermodynamic system, wherein the flow of information is governed by entropy. Our methodology is based on five primary hypotheses (illustrated in Figure 4):

1. The analogy between thermodynamic processes and information processing;
2. The prioritization of consensus over raw data transmission;
3. The interpretation of informational disorder in relation to the spatial distribution of nodes;
4. The association between information quality and the accuracy and relevance of transmitted data;
5. The conceptualization of the VANET as a closed system.

This entropy-based perspective offers novel avenues for optimizing VANET performance. By interpreting the network's behavior through the lens of thermodynamic laws, it becomes possible to devise innovative strategies for energy management, data distribution, and accelerated consensus processes [60–62]. Moreover, integrating this model into decentralized governance mechanisms could lead to the development of more resilient and efficient vehicular networks, aligning with global sustainability objectives.

Our methodology is based on five main hypotheses 4: (1) the analogy between thermodynamics and information processing; (2) prioritizing consensus over data transmission; (3) interpreting informational disorder in terms of the distribution of nodes in the network; (4) the quality of information related to the accuracy and relevance of transmitted data; and (5) viewing the VANET network as a closed system.

3.4. Interpretation of the Information Cycle in the VANETs Environment

In this work, we propose a novel approach that integrates the information cycle of VANETs with thermodynamic principles to create an original model—termed the "VANET Engine"—which provides a fresh perspective on decentralized governance and performance optimization in vehicular networks. Table 1 summarizes the different stages of the VANET Engine along with their associated information parameters.

Table 1. The VANET Engine and its Cycle.

Process Stage	Information Parameters
Initial Transaction	Low Informational Disorder, High Information Quality
Consensus Process	Increasing Informational Disorder, Variable Information Quality
Validated Transaction	High Informational Disorder, High Information Quality
Awaiting New Transaction	High Informational Disorder, Low Information Quality

Figure 5 illustrates the VANET Engine information cycle. In this diagram, the flow and evolution of information through the network are depicted, showing how the state of information changes during each phase of the consensus process.

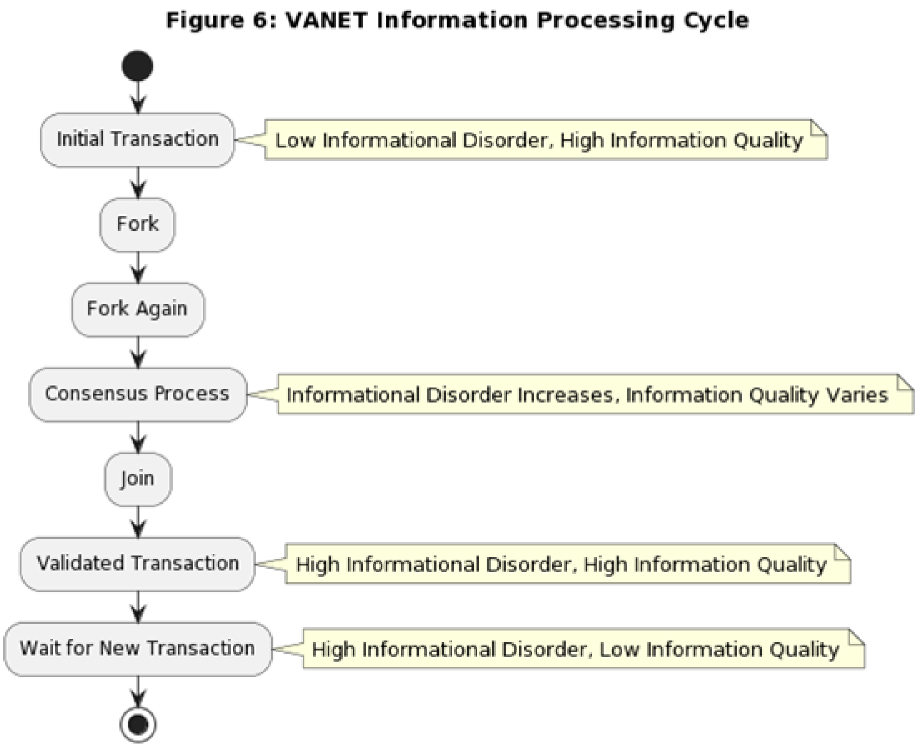

Figure 5. VANET Information Processing Cycle

In Figure 5, we show a representation of the VANET Engine information cycle. In this diagram, we represent how information flows through the network and how its state changes at each stage of the consensus process.

The diagram indicates that information in VANETs follows a cyclical process through the various stages of the consensus mechanism. Notably, there is a transition phase where the transaction concludes, and the system awaits the initiation of a new transaction. This intermittent condition is inherent to VANETs due to the high mobility of vehicles, which can lead to sporadic connectivity and variable network topology.

Intermittence and Delay: In vehicular networks, intermittent connectivity due to node mobility often leads to delays, particularly evident during the "Awaiting New Transaction" stage. Such delays can exacerbate informational disorder during the consensus process, as uncertainty about node availability and transaction delivery increases.

Network Dynamics: The highly dynamic nature of VANETs—where vehicles continuously join and leave the network—can adversely affect the quality of information. During the consensus process, rapid topology changes may introduce significant disorder, thereby degrading the overall information quality.

Security: Security is a critical aspect in VANETs. Malicious activities, such as Sybil attacks, can introduce false or manipulated transactions, further escalating disorder and diminishing the integrity of information. Research has shown that security breaches in VANETs can disrupt consensus processes and compromise the reliability of data exchanges [63–65].

The challenges of VANETs—including intermittent connectivity, dynamic network topologies, and security threats—can lead to significant information loss. Such loss has severe implications: it can disrupt the consensus process, result in decisions based on incomplete or erroneous data, and ultimately undermine the network's ability to respond to critical situations. Mitigating information loss is therefore paramount when designing consensus mechanisms. Recent studies have emphasized the need for robust strategies to minimize such loss in dynamic networks [67,68,96**?**].

The interpretation of the information cycle within the VANET environment—encompassing aspects of intermittence, dynamic network behavior, and security—provides a comprehensive framework for understanding and optimizing vehicular communications. This approach underpins the design of decentralized governance mechanisms that are both resilient and efficient, addressing the multifaceted challenges inherent to VANETs.

3.5. Vehicular Engine Case

To elucidate the impact of thermodynamic principles on VANETs, we consider a practical analogy with a vehicular engine. In this analogy, the "energy" corresponds to the data packets traversing the network, and the "work" corresponds to the successful transmission of these packets to their intended destinations.

Analogous to the first law of thermodynamics—which asserts that energy cannot be created or destroyed, only transformed—the total amount of information in a VANET is conserved, although its form may change as it propagates through the network. In this context, while information is not lost in the sense of disappearing entirely, it may be degraded, distorted, or transformed due to factors such as packet loss, variations in network topology, and external disturbances [96].

The first law of thermodynamics, which states that the sum of kinetic and potential energy in a closed system remains constant, holds ideally in frictionless systems. In practical scenarios, friction (or analogous losses) prevents a system from returning to its original energetic state. Similarly, the idealized Carnot cycle represents a reversible process, serving as a benchmark for evaluating real systems. In a VANET, each microstate—defined by parameters such as node location, speed, and direction—contributes to the overall state of the network. Due to the high mobility of vehicles, VANETs exhibit a vast number of possible microstates.

Several factors can perturb the information cycle in VANETs. For example, data packet loss may occur due to unstable connections or adverse environmental conditions, while rapid topology changes (driven by high vehicle speeds) and the presence of malicious or malfunctioning nodes can further exacerbate informational disorder. Such disturbances increase uncertainty, potentially leading to errors in the consensus process and compromising the network's overall integrity and reliability.

In this vehicular engine analogy, "energy" is interpreted as the information flowing through the network, and the principle of energy conservation implies that the total information remains constant even though its form may vary due to packet loss or changes in topology. Consequently, it is imperative to account for intermittency, network dynamics, and security challenges when designing and optimizing VANET performance. These factors influence both the amount of "energy" (information) available for "work" (data transmission) and the efficiency with which this work is executed.

Environmental conditions—such as adverse weather and physical obstructions—can degrade communication quality and result in packet loss, while inadequate network management policies may further reduce consensus efficiency. Moreover, human behavior and mobility patterns play a critical role in shaping network performance. To optimize VANET operation, it is essential to implement strategies that mitigate these challenges. For instance, robust retransmission protocols and advanced error detection and correction mechanisms can help minimize packet loss, and dynamic routing algorithms along with vehicle-to-everything (V2X) communication solutions can better accommodate rapid topology changes [68,96].

In summary, the vehicular engine case illustrates that, by applying thermodynamic principles to the flow of information in VANETs, we can better understand how environmental factors, network dynamics, and security issues impact system performance. This perspective provides a foundation for designing more resilient and efficient vehicular networks.

3.6. The Information Cycle for VANETs

To elucidate how thermodynamic principles can be applied to Vehicular Area Networks (VANETs), we adopt the perspective of an information cycle. Drawing an analogy from thermodynamics—the discipline grounded in the principle that energy cannot be created or destroyed but only transformed—we develop a conceptual framework for understanding the flow of information in VANETs. In this framework, information is treated analogously to energy, subject to transformation as it propagates through the network [96].

Figure 6 illustrates a simplified model of the information cycle in VANETs, inspired by the Carnot cycle, which traditionally describes the operation of idealized thermal engines [49]. The proposed information cycle comprises several stages: the initial transaction, the consensus process, the validated transaction, and the waiting period for a new transaction. At each stage, both informational disorder and information quality may vary.

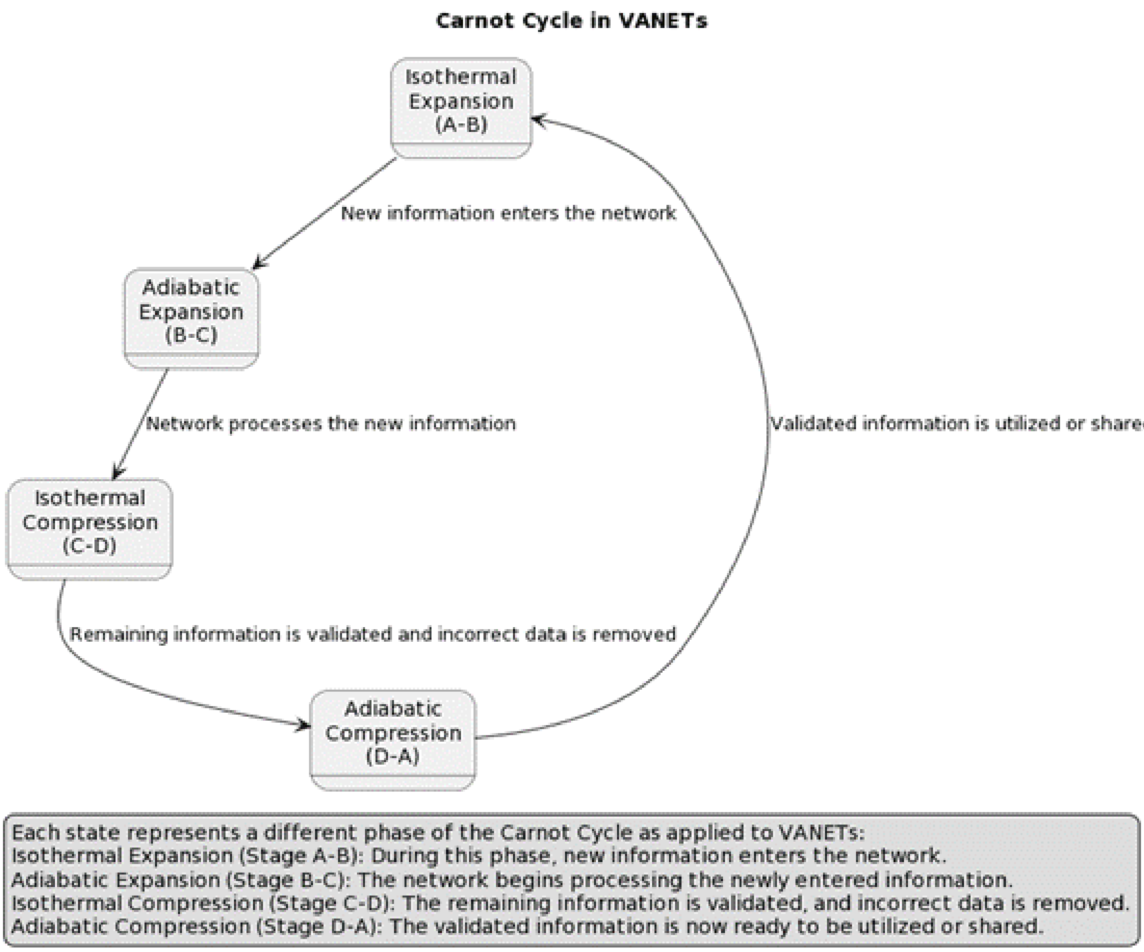

Figure 6. The Carnot Cycle and Information Management in VANETs

3.6.1. Hypotheses

We posit that the global state of a VANET can be characterized by the state of its routing table at any given time. Each update to a node's routing table represents a new network state. While the routing table reflects a global parameter for the network, we introduce the notion of a "microstate" to capture the localized state at an individual node. In a VANET, each vehicle (node) maintains its own local routing table, inherently linking the concept of a microstate to a specific geographical entity.

In developing our model, we make the following assumptions:

1. The consensus process in VANETs is analogous to the energy cycle of an idealized engine, here termed the "VANET Engine." This analogy facilitates a deeper understanding of decentralized decision-making processes.
2. Our analysis focuses on the consensus process rather than the mere transmission of data, paralleling the TCP/IP model where TCP ensures data integrity via acknowledgement mechanisms.

3. We introduce the term "informational disorder" to denote the degree of randomness or lack of order in the spatial arrangement of vehicular nodes. A highly structured configuration implies low disorder, whereas a random configuration indicates high disorder.
4. "Information quality" is defined by the semantic value and accuracy of the data transmitted. For example, the statement "2 + 2 = 4" represents high-quality information, while ambiguous or erroneous expressions signify medium to low quality.

These hypotheses build upon foundational work in information theory and the thermodynamics of computation [20,70]. Although these assumptions simplify complex phenomena, they provide a robust conceptual basis for analyzing and optimizing the information flow in VANETs.

3.6.2. The VANETs Information Cycle

The information cycle in a VANET encapsulates the evolution of data quality and disorder as transactions propagate through the network. Drawing an analogy from the Carnot cycle in thermodynamics—where energy is conserved and transformed—the information cycle models how data is created, processed, and ultimately validated or degraded. In this context, "Information Quality Loss" refers to a state in which the intrinsic value of the data diminishes due to factors such as signal interference, network congestion, or partitioning.

We delineate the information cycle into several stages:

- **Initial Transaction:** Characterized by low informational disorder and high information quality, this stage represents the inception of a data transaction.
- **Consensus Process:** As nodes engage in consensus, informational disorder increases and information quality may fluctuate due to interference from competing transmissions and transient network conditions.
- **Validated Transaction:** At this stage, despite a high level of disorder, the information quality is restored to a high standard following successful consensus.
- **Waiting for New Transaction:** Here, high disorder and low information quality prevail, marking the interlude before a new transaction is initiated.

These stages collectively define a cycle in which information is subject to continual transformation. In an idealized system, increases in disorder would not inherently lead to quality loss; however, in practical VANET scenarios—where multiple nodes and environmental factors interact—the risk of degradation is significant.

3.6.3. Interpretation of the Information Cycle in the VANET Environment

Understanding the information cycle is crucial for addressing the challenges inherent to VANETs, such as intermittency, rapid topology changes, and security vulnerabilities. Figure 7 presents a schematic of the VANET information cycle that explicitly incorporates the phenomenon of information quality loss.

In this model, transitions between cycle stages represent variations in informational disorder. For instance, during the consensus process, an increase in disorder may precipitate a decline in data quality due to factors like signal interference or network congestion. Such degradation is analogous to the frictional losses observed in thermodynamic systems, where dissipative effects prevent the system from achieving ideal reversibility.

Several factors contribute to information quality loss in VANETs:

- **Routing Table Anomalies:** Concurrent route optimizations may lead to natural branching or even the emergence of forks in routing tables. Moreover, dishonest nodes may deliberately manipulate routing information.
- **Broadcast Vulnerabilities:** The broadcast phase is particularly susceptible to errors, as transient connectivity and overlapping transmissions can introduce noise and packet loss.
- **Network Partitioning:** The high mobility of vehicular nodes often results in network partitioning, wherein nodes exit communication range, leading to temporary data loss and increased disorder.

doi:10.20944/preprints202505.2260.v1

The ability of a VANET to recover its ideal information cycle after experiencing quality loss serves as an indicator of its resilience. Effective consensus mechanisms must, therefore, balance the competing demands of security and liveliness. While security-focused protocols (e.g., Byzantine fault-tolerant schemes) may mitigate information loss by ensuring robust consensus, they can incur delays. In contrast, liveliness-oriented algorithms (e.g., protocols akin to the Optimized Route Discovery Protocol) achieve rapid consensus at the risk of higher fork probabilities.

Addressing these challenges requires the development of advanced strategies—such as robust retransmission protocols, dynamic routing algorithms, and adaptive error correction methods—that mitigate information loss and stabilize the cycle. Such strategies are critical for enhancing the overall performance and reliability of VANETs in the face of environmental and operational disturbances [5,68,96].

The concept of the information cycle is pivotal for understanding both the challenges and opportunities inherent to Vehicular Ad Hoc Networks (VANETs). In these networks, the continual creation, dissemination, and processing of information occur under conditions that introduce intermittency, dynamic topology changes, and potential security threats [64].

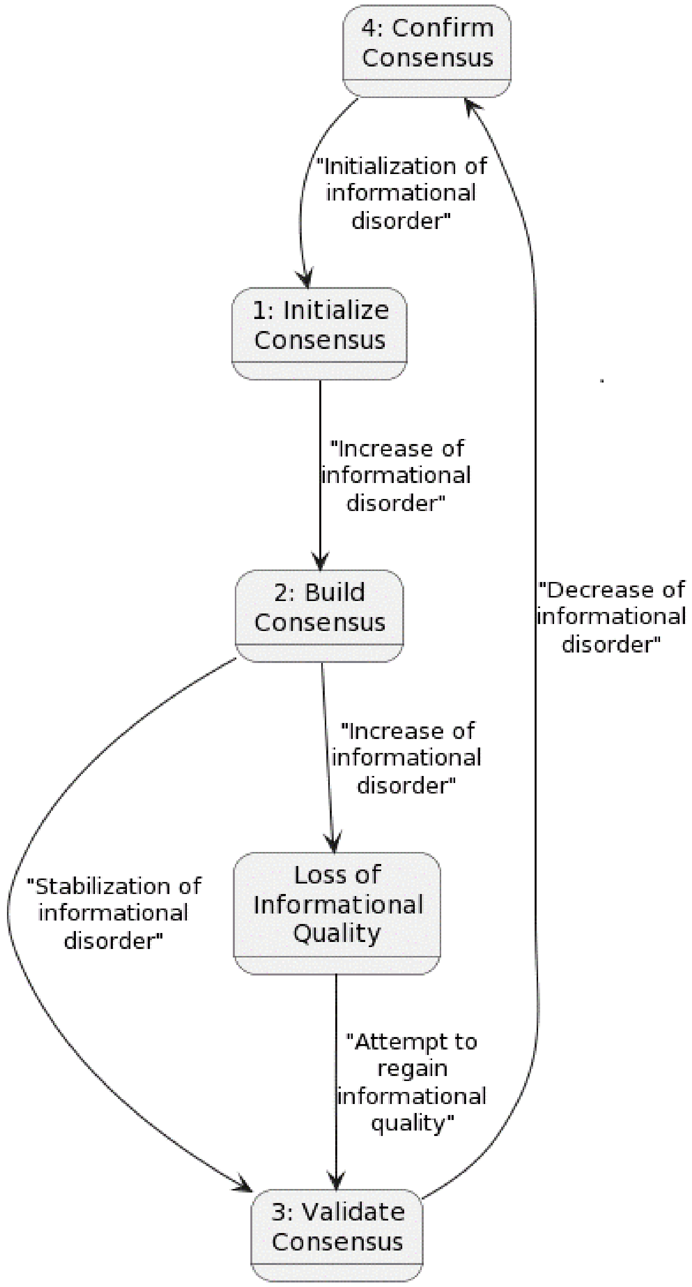

Figure 7. VANET Information Cycle with Quality Loss

Intermittency, manifested as the frequent activation and deactivation of network nodes, can induce data packet loss and transmission delays. In addition, network congestion and inherent signal latency further contribute to increased informational disorder and diminished information quality, thereby impairing the overall efficiency of the information cycle [71].

Moreover, the intrinsic dynamism of VANETs—with nodes continuously joining, leaving, and moving at variable speeds—results in rapid fluctuations in network topology. This volatility necessitates the design of adaptive routing and consensus protocols that can efficiently manage such dynamics [72].

A primary concern in VANETs is information loss. This loss may arise from intermittent connectivity, network congestion, or transmission errors, and it directly affects the consensus process by reducing information quality and elevating disorder within the network [73]. Inadequate data can, in turn, compromise the decision-making process, underscoring the critical need for robust consensus mechanisms that can withstand these challenges [74].

Finally, the susceptibility of VANETs to security attacks—such as unauthorized access, spoofing, or Sybil attacks—can further exacerbate informational disorder and degrade data quality. To mitigate these risks, it is imperative to implement comprehensive security measures, including strong encryption and authentication protocols [73].

4. Evaluation and Discussion of Results

To evaluate our hypotheses, we employed a simulation-based approach using NS-3, a widely adopted discrete-event network simulator that provides a robust platform for implementing and testing our proposed solutions within a controlled VANET environment [97]. In our simulation framework, blockchain technology was integrated into the network, thereby enabling a detailed examination of its interaction with VANETs and its consequent impact on network governance and resilience.

This methodological approach allowed us to test our hypotheses under replicable conditions, ensuring the reliability and validity of our findings. In the following sections, we elaborate on our experimental setup, detailing the simulation parameters, the blockchain implementation, and the methods used for measuring and analyzing the results.

4.1. Simulation Using NS-3

To validate our hypotheses, we employed the discrete-event network simulator NS-3 [97], a robust and widely recognized platform for simulating Vehicular Ad Hoc Networks (VANETs). NS-3 provides comprehensive features to quantify network utilization, model node mobility, and assess computational resource usage. In our simulation environment, blockchain technology was integrated with VANET protocols, thereby allowing us to investigate its impact on network governance, consensus processes, and overall resilience. The following experiments were designed to test each hypothesis under controlled, replicable conditions.

HYPOTHESIS 1 – Consensus as an Energy Cycle:
In the first experiment, we configured the simulation to quantify energy consumption during each stage of the consensus process. To monitor and record energy usage, we employed PowerTOP [98], a Linux-based power analysis tool. This enabled us to determine the energy required for each consensus round, thereby framing consensus as an energy cycle.

HYPOTHESIS 2 – Focusing the Cycle on Consensus:
For the second hypothesis, we structured specific traffic flows within the simulation to evaluate how the consensus process affects overall network efficiency. Traffic and latency were measured using NetFlow-based analysis [99], which provided quantitative data regarding the time and computational resources dedicated to achieving consensus.

HYPOTHESIS 3 – Informational Disorder:
In the third experiment, we collected data on node location and activity over time. Simulated GPS data was used to track the geographic distribution of nodes, and QGIS [100] was employed for geospatial

visualization and analysis. This allowed us to model the variability in node distribution and evaluate its impact on network performance.

HYPOTHESIS 4 – Informational Quality:
For the fourth hypothesis, we generated data of varying quality levels within the simulation to assess its influence on the consensus process and overall network efficiency. Data quality was evaluated using tools such as Talend Data Quality [101], Ataccama [102], and OpenRefine [103], which provided metrics for consistency, integrity, and accuracy.

HYPOTHESIS 5 – Informational Microstate:
In the final experiment, each node was configured to maintain its own ledger state, allowing us to compare the ledger state across nodes over time. Apache Cassandra [104], a distributed database, was used to record and compare these local ledger states (microstates). This experiment enabled us to analyze variations in node states and their relationship with node activity and geographic location.

4.2. Implementation of Blockchain in Simulation

The integration of blockchain technology into the NS-3 simulation environment provides a novel platform for evaluating the interaction between blockchain systems and Vehicular Ad Hoc Networks (VANETs). NS-3, as detailed by Riley and Henderson [97], is widely recognized for its robustness in simulating complex vehicular networks under realistic conditions. By incorporating blockchain modules into NS-3, we are able to investigate the impact of blockchain on network governance, resilience, and transaction security within VANETs.

To test our hypotheses, we configured the simulation with parameters representative of real vehicular network scenarios. Key simulation parameters include:

- **Node Configuration:** The number and types of nodes were varied based on the hypothesis under evaluation. For instance, the "Information Disorder and Node Placement" hypothesis was examined under both uniform and random node distributions.
- **Mobility Models:** Multiple mobility models were implemented, ranging from constant velocity models to 2D random walk models, to simulate varying degrees of network disorder.
- **Transaction Workloads:** We simulated a range of transaction creation rates, sizes, and processing times to emulate different network workloads and data quality scenarios.
- **Network Environment:** Both urban and highway environments were modeled, each with distinct network characteristics and behaviors.

For visualization and analysis, we leveraged several tools integrated with NS-3. NetAnim, the built-in NS-3 animation viewer, allowed for real-time observation of node behavior and network dynamics, while the Gnuplot library facilitated the plotting of metrics such as packet transmission counts, delays, and microtransaction states.

The implementation of blockchain within the simulation was tailored to test specific aspects of our hypotheses. For instance, in our examination of consensus as an energy cycle, the simulation was configured to capture resource consumption at each consensus stage. NS-3's measurement capabilities provided detailed data on network utilization and computational resource consumption, highlighting the energy cost associated with different consensus processes.

The simulation framework also enabled us to model various aspects of blockchain integration:

- **Consensus Process Modeling:** Specific traffic flows were designed to focus on the consensus process. This allowed us to isolate the network traffic generated by consensus algorithms and measure its impact on overall network performance.
- **Informational Disorder:** Node mobility in NS-3 was used to simulate geographical disorder. This was essential for assessing how variations in node placement affect the performance and reliability of the VANET.
- **Informational Quality:** The simulation generated data with varying quality levels to evaluate the influence of data accuracy and consistency on the consensus process.

- **Informational Microstate:** Each simulation node was configured to maintain its own ledger state, enabling us to track changes in the local ledger (or microstate) over time and compare these across nodes.

Figure 8 illustrates the main classes and methods utilized in our simulation setup. In our implementation, the basic network configuration is established through calls to methods such as `CommandLine::Parse`, `NodeContainer::Create`, `MobilityHelper::SetMobilityModel`, `MobilityHelper::Install`, `VanetHelper::Install`, `Simulator::Run`, and `Simulator::Destroy`. The dependency relationships among these classes are depicted by the arrows in Figure 8.

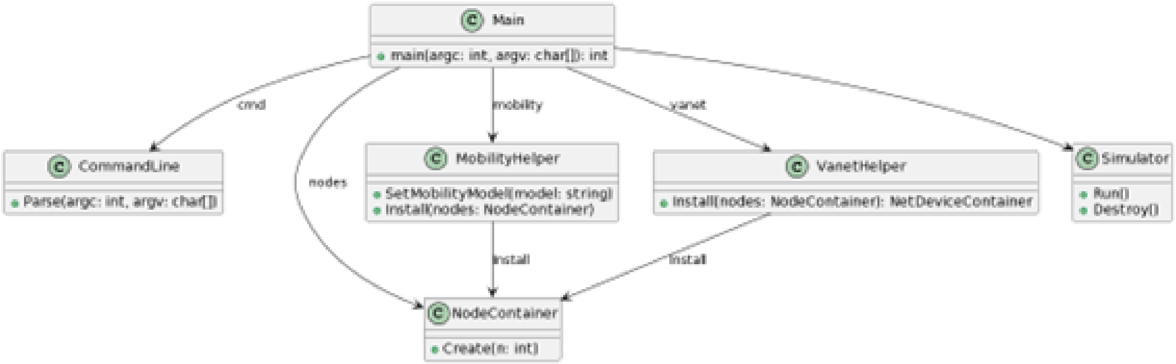

Figure 8. Overview of key NS-3 classes and methods used in the simulation setup.

Once the basic VANET is configured, the consensus model is implemented by defining new NS-3 classes that encapsulate the logic of the consensus algorithm. For example, our simulation initiates a network of 10 nodes, establishes point-to-point connections with a 5 Mbps link and 2 ms delay, assigns IP addresses, and configures each node to send a UDP packet to all other nodes while also acting as a server to receive packets.

To implement consensus algorithms, nodes are required not only to exchange messages but also to perform computations based on the received data. In the case of Proof of Work (PoW), as depicted in Figure 9, a node employs a `PoWModule` to generate computational problems and verify solutions, a `NetworkModule` to handle block transmission, and a `Blockchain` class to manage block addition and validation. The `StartMining()` function initiates the mining process, which involves problem generation, solution verification, and block propagation.

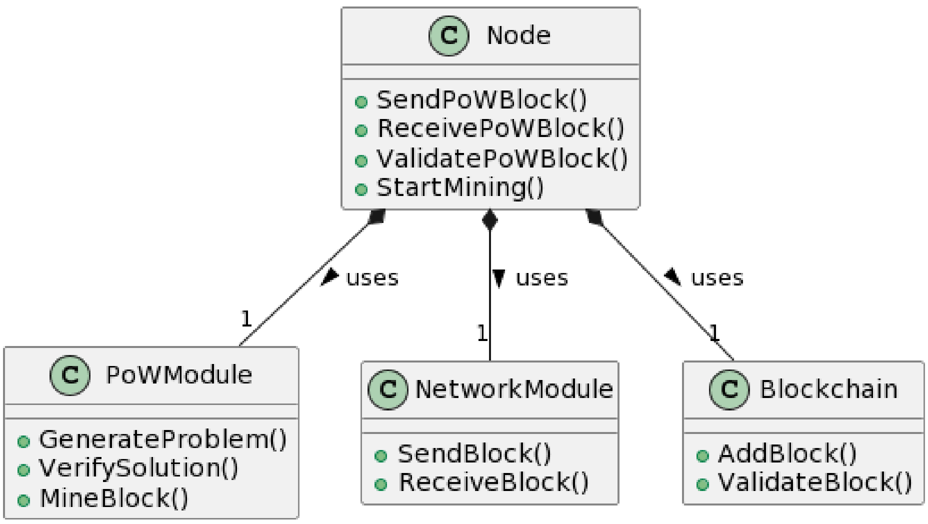

Figure 9. Module structure for the Proof of Work (PoW) consensus algorithm.

For the Proof of Stake (PoS) algorithm (Figure 10), the approach differs in that nodes are selected to create blocks based on their stake in the network rather than on computational power. Accordingly,

 doi:10.20944/preprints202505.2260.v1

new modules are implemented to capture the staking mechanism and selection process. In the PoS implementation, the `StartMining()` function is adapted to initiate the block creation process based on stake, and additional logic is incorporated to manage validator selection.

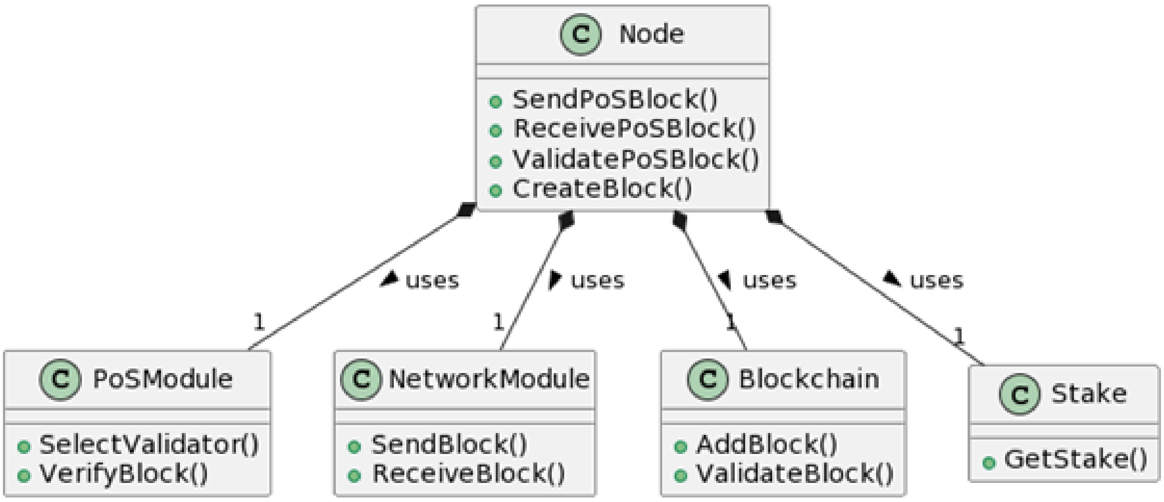

Figure 10. Module structure for the Proof of Stake (PoS) consensus algorithm.

Finally, to visualize the simulation results, the `ns3::FlowMonitor` module [82] is used to collect comprehensive statistics on network traffic. These data are subsequently analyzed and visualized using Python [83] and Matplotlib [83], facilitating a detailed evaluation of the impact of blockchain integration on VANET performance.

4.2.1. Hypothesis 1 - Implementation of Consensus Algorithms in NS-3

To simulate Hypothesis 1 (Consensus Process as Energy Cycle), two key consensus algorithms, Proof of Work (PoW) and Proof of Stake (PoS), are implemented within a Vehicular Ad hoc Network (VANET) using the NS-3 simulator. The adaptations made in the base code to include these algorithms are described below.

A `NodeApp` class was defined that represents an application running on a node. This application is responsible for sending "packages" that, in this context, represent transactions on the blockchain network.

For the PoW model (Figure 11), the following functions were implemented in `NodeApp`: `SendPoWBlock`, `ReceivePoWBlock`, `ValidatePoWBlock`, and `StartMining`. These functions allow a node to generate a PoW problem, verify received solutions, validate blocks, and start the mining process, respectively.

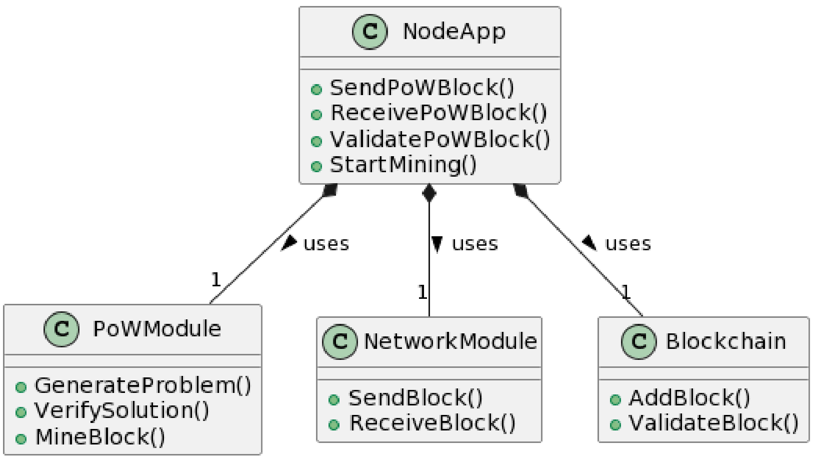

Figure 11. The PoW algorithm.

Algorithm 1 Proof of Work (PoW) Consensus in VANET Simulation

- Set of nodes N in the network
- Pending transactions pool T
- Difficulty threshold D

A valid block B appended to the blockchain **Initialization:** For each node $n_i \in N$, initialize local ledger L_i. **Mining Process at Node n_k:** Call `StartMining()` StartMining() Aggregate a set of transactions $T_k \subset T$. Set initial nonce $x \leftarrow 0$.
Compute hash $H \leftarrow \text{Hash}(T_k, x, \text{timestamp}, \text{prevHash})$. $x \leftarrow x + 1$ $H < D$ Construct new block $B \leftarrow \{T_k, x, H, \text{timestamp}, \text{prevHash}\}$. Call `ValidatePoWBlock(`$B$`)`. `ValidatePoWBlock(`$B$`)` returns **true** Call `SendPoWBlock(`B`)`.

On Receiving a Block: For any node, upon receiving a block, call `ReceivePoWBlock(`B`)`. ReceivePoWBlock(B) Call `ValidatePoWBlock(`B`)`. `ValidatePoWBlock(`B`)` returns **true** Append block B to local ledger L.
Discard block B.

ValidatePoWBlock(B) Check that block B's hash H satisfies $H < D$. Verify the integrity of transactions in B. Confirm that the timestamp and previous block hash are correct. **true** if all validations pass, otherwise **false**.

SendPoWBlock(B) Broadcast block B to all nodes in the network.

Algorithm 1 presents the detailed pseudocode for the Proof of Work (PoW) consensus mechanism as implemented in our VANET simulation framework. In this model, each node in the network performs the mining process by aggregating a subset of pending transactions and iteratively computing a hash value, incrementing a nonce until the computed hash satisfies a predefined difficulty threshold D. The `StartMining()` function encapsulates this iterative process, ultimately constructing a new block once a valid hash is found.

Subsequently, the block is validated via the `ValidatePoWBlock()` function, which ensures that the block's hash, transaction integrity, timestamp, and linkage to the previous block meet all necessary criteria. If validation is successful, the block is broadcast to all network nodes using the `SendPoWBlock()` function. Conversely, upon receiving a block, each node invokes the `ReceivePoWBlock()` function to validate the incoming block before appending it to its local ledger.

This implementation effectively demonstrates the core principles of PoW in a VANET environment, highlighting how computational effort can be leveraged to secure consensus and maintain ledger integrity under dynamic network conditions.

For the PoS model (Figure 12, the functions `SendPoSBlock`, `ReceivePoSBlock`,`ValidatePoSBlock`, and `CreateBlock` were implemented. These allow a node to send and receive PoS blocks, validate these blocks, and create new blocks if the node is selected as a validator.

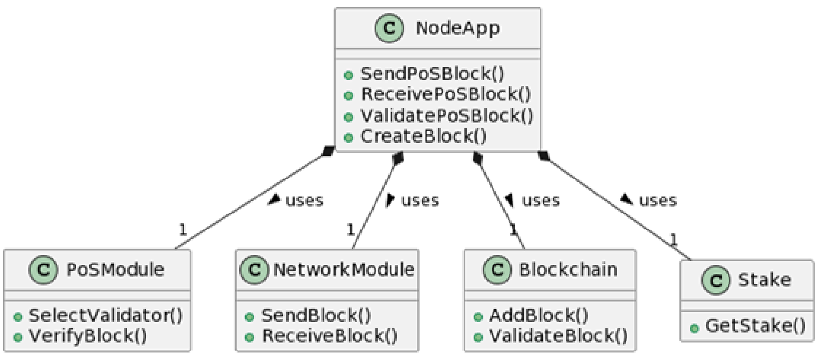

Figure 12. The PoS algorithm.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 29 May 2025 doi:10.20944/preprints202505.2260.v1

Algorithm 2 Proof of Stake (PoS) Consensus for VANET Simulation

- A set of nodes N, where each node n_i has a stake S_i
- A pool of pending transactions T
- The current ledger state L

Updated ledger state L' with the new block
Initialization: Each node $n_i \in N$ maintains a local ledger $L_i \leftarrow L$ Compute total stake: $S_{total} = \sum_{i=1}^{|N|} S_i$
Validator Selection: each node $n_i \in N$ Calculate selection probability $P_i = \frac{S_i}{S_{total}}$
Randomly select a node n_k from N based on the probabilities $\{P_i\}$ **Block Creation:** Node n_k aggregates a set of transactions $T_k \subset T$ Construct a new block $B = \{T_k, \text{timestamp}, \text{previous block hash}\}$
Broadcast: Node n_k broadcasts block B to all nodes in N **Block Validation:** each node $n_j \in N$ B passes validation checks (e.g., transaction integrity, correct timestamp, digital signatures) Append block B to local ledger: $L_j \leftarrow L_j \cup \{B\}$
Discard block B
Consensus Update: All nodes update their ledger state to the latest valid block Updated ledger state L'

Algorithm 2 presents the pseudocode for our adapted Proof of Stake (PoS) consensus mechanism implemented in the VANET simulation. The algorithm begins by initializing each node's ledger state and computing the total network stake. Each node's selection probability is then determined in proportion to its stake, and one node is randomly chosen as the validator. This node aggregates pending transactions into a new block, which is broadcast to all network participants. Upon receiving the block, each node performs rigorous validation checks before appending the block to its local ledger, ensuring consistency and integrity across the network. This approach effectively demonstrates how a stake-based consensus mechanism can be integrated into a dynamic VANET environment, balancing energy efficiency and security.

In both cases, additional logic was introduced in the `SendPacket` function to allow the sending of different types of packets depending on the node's status. Also, a callback function was added for when a node receives a packet.

The implementations of these algorithms provide a solid foundation for simulating the consensus process in a VANET network and monitoring state transitions in the nodes during this process.

4.2.2. Hypothesis 2 – Recording and Measuring Consensus Metrics in NS-3

In Hypothesis 2, which focuses on the information cycle as it pertains to consensus, our objective is to quantitatively assess the dynamics of the consensus process within a VANET simulation. To achieve this, we enhanced the NS-3 simulation environment by modifying the `NodeApp` class to record and report key metrics indicative of consensus performance. These metrics include the total number of packets sent and received, as well as the overall time taken to reach consensus.

Specifically, the following modifications were implemented:

- The `NodeApp` class now includes functions such as `GetTotalPacketsSent` and `GetTotalPacketsReceived` to record packet transmission and reception statistics.
- A new function, `ReceivePacket`, was introduced to increment a packet counter each time a node receives a packet, thereby providing real-time measurement of network activity.
- The `StartApplication` function was adapted to initialize all consensus-related metrics at the commencement of the simulation.
- The `StopApplication` function was modified to compute the total consensus time once the application concludes, enabling an evaluation of latency within the consensus process.

Figure **??** presents an overview of the modified code structure, illustrating the integration of these metrics into the simulation framework. These adaptations not only facilitate the collection of comprehensive data regarding the consensus process but also allow us to analyze the trade-offs between network efficiency, latency, and security. The resulting metrics serve as a foundation for

 doi:10.20944/preprints202505.2260.v1

assessing the effectiveness of both Proof of Work (PoW) and Proof of Stake (PoS) consensus algorithms within the VANET environment.

The integration of these modifications enables a robust evaluation of the consensus process by capturing real-time data on network performance and resource utilization. Such detailed measurements are critical for validating our hypotheses and for optimizing the design of consensus mechanisms in VANETs.

4.2.3. Hypothesis 3 – Configuring Mobility Scenarios in NS-3

In Hypothesis 3 (Information Disorder and Node Location), we investigate how varying mobility scenarios affect the consensus process within VANETs. The hypothesis posits that the spatial distribution and movement patterns of nodes directly influence the level of informational disorder, which in turn impacts consensus efficiency. To test this, we configured multiple mobility scenarios in NS-3 using the `MobilityHelper` class.

Our simulation framework enables the implementation of distinct mobility models. For example, a `ns3::ConstantVelocityMobilityModel` is employed to simulate a weak disorder scenario, wherein nodes are uniformly distributed within a circular (disk) area. In contrast, a `ns3::RandomWalk2dMobilityModel` is used to represent a strong disorder scenario, characterized by nodes moving randomly within a rectangular area. To initialize node positions, we utilize either a `UniformDiscPositionAllocator` for disk-based distributions or a `RandomRectanglePositionAllocator` for rectangular layouts.

Figure 13 illustrates the configuration of these mobility scenarios, highlighting how the `MobilityHelper` interacts with various allocation and mobility model classes to set up the network topology.

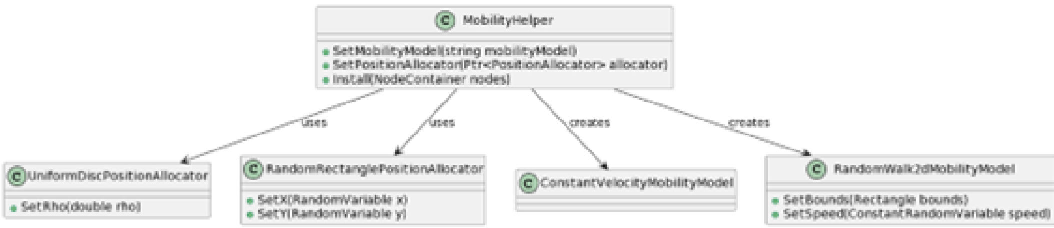

Figure 13. Configuration of Mobility Scenarios in NS-3.

By systematically varying mobility parameters and recording key performance metrics—such as consensus delay, packet loss, and throughput—we assess the effect of node distribution and movement on informational disorder in the VANET. This analysis is crucial for validating the hypothesis that increased disorder in node positioning correlates with challenges in achieving efficient consensus, thereby providing insights for the design of more robust consensus mechanisms in vehicular networks.

4.2.4. Hypothesis 4 – Analysis of Information Quality in NS-3

In Hypothesis 4, our goal is to evaluate the quality of information transactions within the VANET network, with a particular focus on transmission delay as a key indicator of information quality. In vehicular networks, transaction quality may be influenced by several factors, including transmission time, data integrity, and reliability. For the present study, we define information quality primarily based on the transmission delay between nodes.

To implement this analysis within NS-3, the `SendPacket` function in the `NodeApp` class was modified. Specifically, before sending a packet, the function records the current simulation time using `Simulator::Now()`. Once the packet transmission is completed, the simulator time is captured again, and the difference between these timestamps is computed. This difference, stored in the member variable `m_lastTransmissionTime`, serves as a quantitative measure of the transmission delay, which in turn is used as a proxy for information quality.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 29 May 2025 doi:10.20944/preprints202505.2260.v1

Figure 14 illustrates the scenario for analyzing information quality. In this setup, the `NodeApp` class interacts with core NS-3 classes such as `Packet`, `Socket`, and `Simulator`. When a packet is created and sent via a `Socket`, the corresponding transmission time is measured and recorded. This metric is crucial for assessing how efficiently information is disseminated across the network, as lower transmission delays indicate higher quality of data exchange.

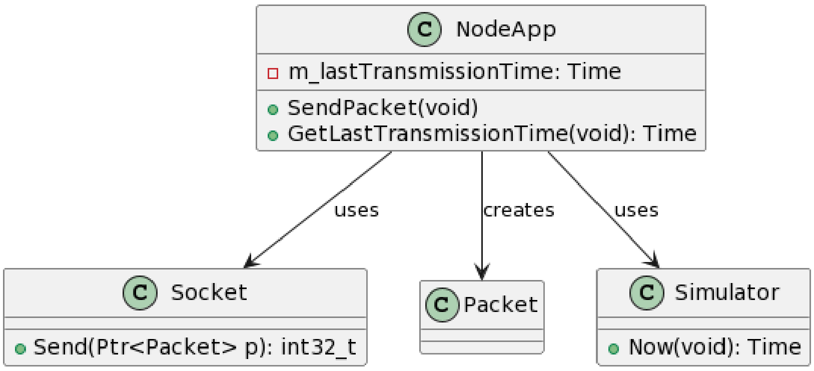

Figure 14. Analysis of information quality scenario.

By systematically recording these metrics under varying network conditions, we can analyze the impact of transmission delays on the overall performance of the consensus process. This analysis provides valuable insights into the reliability and efficiency of VANET communications, which are essential for the optimization of decentralized consensus mechanisms in dynamic vehicular environments.

4.2.5. Hypothesis 5 - Analysis of Information Microstates in NS-3

4.2.6. Hypothesis 5 – Analysis of Information Microstates in NS-3

Hypothesis 5 (Information Microstate) posits that tracking the local ledger state at each node—defined as the microstate—provides valuable insight into the dynamics of consensus and information propagation within VANETs. In our simulation framework, each node maintains its own local ledger (i.e., a record of validated transactions), which reflects its current microstate. By recording and analyzing these microstates over time, we can examine how local ledger variations correlate with node behavior, mobility patterns, and network topology changes, thereby evaluating the consistency and convergence of the consensus process.

To implement this, the `NodeApp` class—subclassed from NS-3's `Application`—was extended with a member variable `m_localState`, a vector of `Transaction` objects that represents the node's local ledger state. Whenever a transaction is added to a node via the `AddTransaction` method, the local state is updated accordingly. This design enables us to capture the evolution of each node's microstate throughout the simulation.

Figure 15 illustrates this microstate scenario. By comparing the local ledger states across nodes at various simulation times, our approach facilitates a quantitative assessment of the consensus mechanism's performance, as well as the identification of potential sources of informational disorder.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 29 May 2025 doi:10.20944/preprints202505.2260.v1

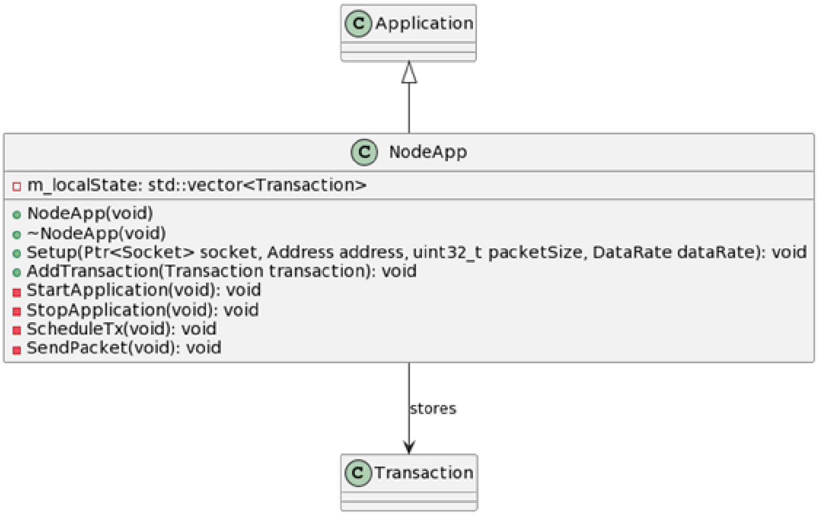

Figure 15. Microstates scenario.

This methodology is consistent with established principles of distributed ledger technology [?], which emphasize the importance of maintaining a reliable, decentralized record of transactions. Analyzing information microstates is therefore crucial for understanding and enhancing the resilience and efficiency of blockchain-based consensus mechanisms in dynamic vehicular environments.

5. Measurement and Analysis of Results

5.1. Measurement and Analysis of Results

The measurement and analysis of experimental data were critical for validating the performance of our blockchain-enabled VANET system. Leveraging the advanced capabilities of NS-3 [97], we collected a comprehensive set of metrics to evaluate network behavior, consensus efficiency, and transaction security under varying conditions.

Our evaluation framework encompassed multiple dimensions:

- **Energy Consumption:** We utilized specialized power monitoring tools, such as PowerTOP [98], to track energy usage at each node during the consensus process. This allowed us to quantify the energy cost associated with block generation and validation, thereby characterizing consensus as an energy cycle.
- **Network Performance:** Metrics such as latency, bandwidth utilization, and packet transmission time were measured using NS-3's built-in FlowMonitor module [82] and analyzed with Gnuplot and Python's Matplotlib library [83]. These measurements provided insights into the impact of consensus operations on overall network performance.
- **Data Quality Assessment:** We defined criteria for transaction quality—classifying transactions as "good", "average", or "bad" based on reliability and integrity. This enabled us to correlate transmission delays and packet losses with the quality of the information exchanged.
- **Microstate Analysis:** The ledger state at each node was logged over time using a distributed database (e.g., Apache Cassandra [104]). This logging facilitated the analysis of microstate variations across nodes and provided a means to assess consensus consistency.
- **Real-Time Visualization:** NS-3's NetAnim animation viewer was employed to visualize node mobility and interactions in real-time, aiding in the qualitative analysis of network dynamics.

By integrating these tools and techniques, we were able to gather meaningful data regarding energy consumption, latency, data quality, and ledger state evolution. This multifaceted approach provided a solid foundation for assessing the effectiveness of our proposed consensus strategies and offered valuable insights into how blockchain integration can enhance the efficiency, resilience, and security of VANETs.

Below, we present a detailed analysis of the proposed hypotheses and the conclusions derived from our simulation results.

Hypothesis 1 (Consensus process as the engine of the VANET network): The measurement and analysis of experimental data were critical for validating the performance of our blockchain-enabled VANET system. Leveraging the advanced capabilities of NS-3 [97], we collected a comprehensive set of metrics to evaluate network behavior, consensus efficiency, and transaction security under varying conditions.

Our evaluation framework encompassed multiple dimensions:

- **Energy Consumption:** We utilized specialized power monitoring tools, such as PowerTOP [98], to track energy usage at each node during the consensus process. This allowed us to quantify the energy cost associated with block generation and validation, thereby characterizing consensus as an energy cycle.
- **Network Performance:** Metrics such as latency, bandwidth utilization, and packet transmission time were measured using NS-3's built-in FlowMonitor module [82] and analyzed with Gnuplot and Python's Matplotlib library [83]. These measurements provided insights into the impact of consensus operations on overall network performance.
- **Data Quality Assessment:** We defined criteria for transaction quality—classifying transactions as "good", "average", or "bad" based on reliability and integrity. This enabled us to correlate transmission delays and packet losses with the quality of the information exchanged.
- **Microstate Analysis:** The ledger state at each node was logged over time using a distributed database (e.g., Apache Cassandra [104]). This logging facilitated the analysis of microstate variations across nodes and provided a means to assess consensus consistency.
- **Real-Time Visualization:** NS-3's NetAnim animation viewer was employed to visualize node mobility and interactions in real-time, aiding in the qualitative analysis of network dynamics.

By integrating these tools and techniques, we were able to gather meaningful data regarding energy consumption, latency, data quality, and ledger state evolution. This multifaceted approach provided a solid foundation for assessing the effectiveness of our proposed consensus strategies and offered valuable insights into how blockchain integration can enhance the efficiency, resilience, and security of VANETs.

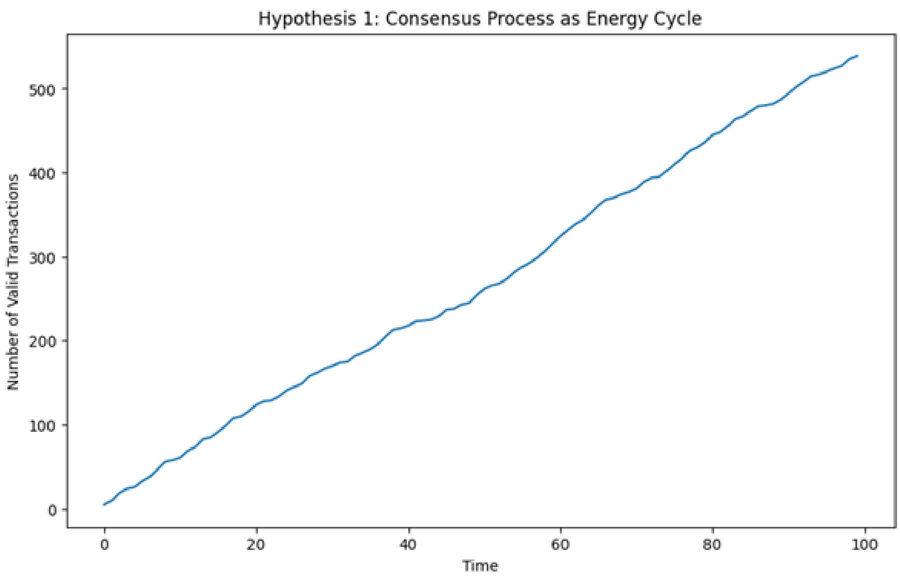

Figure 16. Consensus process as the engine of the VANET network.

Below, we present a detailed analysis of the proposed hypotheses and the conclusions derived from our simulation results.

Hypothesis 2 (Information cycle centered on consensus):

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 29 May 2025 doi:10.20944/preprints202505.2260.v1

5.1.1. Hypothesis 2 – Recording and Measuring Consensus Metrics in NS-3

Hypothesis 2 (Information Cycle Centered on Consensus) posits that the variability in the number of transactions undergoing validation serves as an indicator of the consensus process's capacity to manage fluctuating transaction loads. In our simulation, we observed that the volume of transactions in the validation phase varied significantly in response to dynamic factors such as vehicle density, driving environment, and temporal conditions, as illustrated in Figure 17.

In urban settings, higher vehicle densities generate an increased number of transaction requests, thereby placing greater demand on the consensus mechanism. Conversely, in highway scenarios, the lower density of vehicles typically results in fewer transactions requiring validation. Additionally, temporal variations—such as differences between peak and off-peak traffic periods—further influence the transaction load. These observations demonstrate that our consensus process dynamically adapts to changes in the network, maintaining stability and reliability even under variable load conditions.

The ability to manage such fluctuations is critical for VANETs, where the transient nature of vehicular communication often leads to rapid changes in network conditions. The experimental results confirm that the consensus process effectively absorbs these variations, ensuring continuous and robust validation of transactions. This finding aligns with earlier studies on VANET scalability and dynamic load management [64,73].

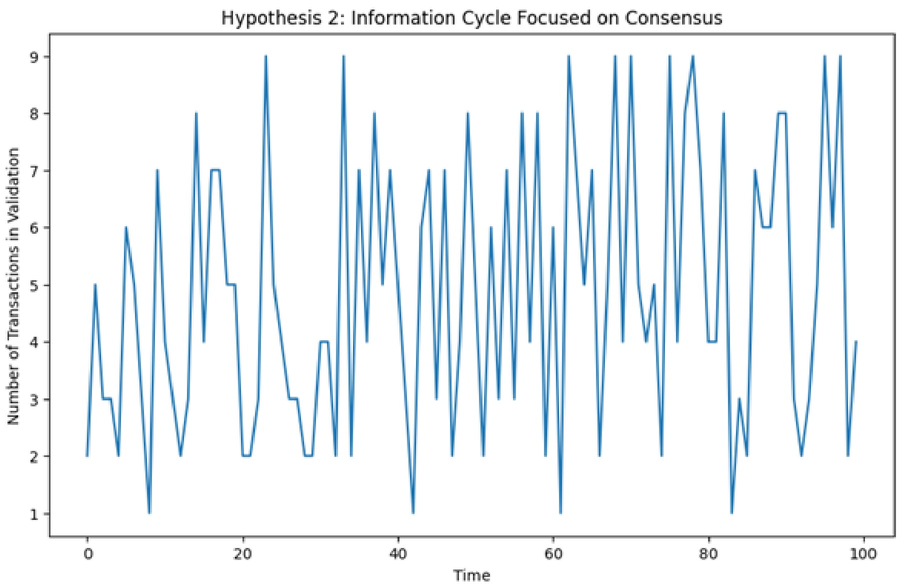

Figure 17. Information cycle centered on consensus: Variability in the number of validated transactions under different network conditions.

Hypothesis 3 (Information disorder and node arrangement): Our simulation reveals that the performance of the consensus process is susceptible to different node arrangement scenarios. The graphs presented below provide a detailed analysis of these findings.

In Figure Figure 18a, titled "Consensus Reach Time Across Scenarios," we represent the "time to reach consensus" on the Y-axis and the different "scenarios" on the X-axis. It can be observed that the time to reach consensus varies significantly among the scenarios, indicating that network setup and network conditions have a direct impact on the efficiency of the consensus process. This suggests that optimal node arrangement can improve the efficiency of the consensus process.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 29 May 2025 doi:10.20944/preprints202505.2260.v1

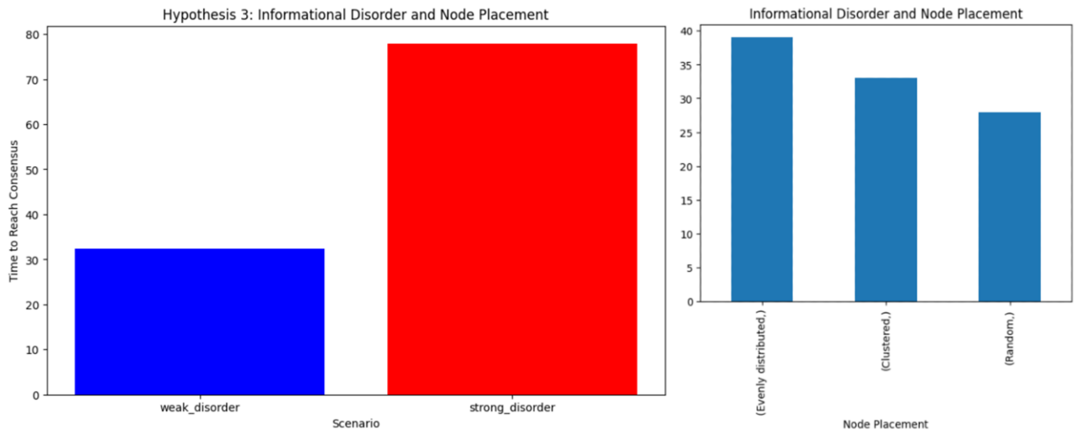

Figure 18. Information disorder and node arrangement (a)- Consensus Reach Time Across Scenarios and (b) Consensus Reach Time and Node Placement.

Figure Figure 18b, titled "Consensus Reach Time and Node Placement," shows the "time to reach consensus" on the Y-axis and "node placement" on the X-axis. From this graph, we can observe that the time required to reach consensus also varies depending on the node placement. This suggests that the distribution of nodes in the network can play a critical role in the consensus process.

These findings pose significant challenges for VANETs networks, where vehicles are in constant movement and may be distributed irregularly. Our results highlight the importance of designing consensus algorithms that are robust and adaptable to these variations in node arrangement. The practical implications of these results underline the need for network management strategies that can dynamically adapt to changes in node arrangement to optimize the consensus process.

Hypothesis 4 (Information quality): Our simulations generated a spectrum of transactions of different qualities, highlighting that the quality of transactions can have a significant impact on the performance of the consensus process. This finding emphasizes the need to investigate methods to ensure, maintain or improve the quality of transactions in the network.

Figure 19a, titled "Number of Transactions and Quality," represents the "number of transactions" on the Y-axis and the "quality" on the X-axis. This graphical representation illustrates a clear relationship between quality and the number of transactions. There is a trend suggesting that as transaction quality improves, the number of transactions also increases. This finding indicates that high transaction quality can promote efficiency in the consensus process, allowing more transactions to be processed.

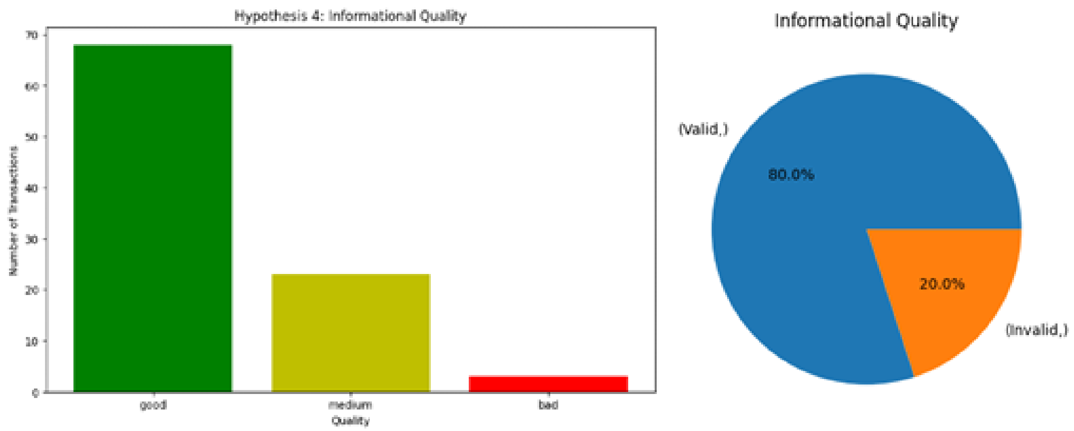

Figure 19. Information quality (a)- Number of Transactions and Quality and (b) Distribution of Valid and Invalid Transactions.

Figure 19b, titled "Distribution of Valid and Invalid Transactions," is a pie chart showing the distribution of valid and invalid transactions in our simulation. From this chart, we see that 80% of transactions are valid and 20% are invalid. This finding highlights the importance of managing and mitigating invalid transactions in the network to ensure the efficiency and accuracy of the consensus process.

These results underscore the importance of maintaining the quality of transactions in the network. A high number of invalid transactions can slow down the consensus process and make it more prone to errors. This suggests the need to research and develop methods that can ensure or improve the quality of transactions in the network. Ensuring high transaction quality can be a key component to optimizing the performance of VANET networks.

Hypothesis 5 (Information microstate): Tracking a node's local state over time provides a valuable micro-analysis approach to evaluating the performance of the consensus process. However, this tracking can also generate a greater computational load, which emphasizes the importance of seeking efficient techniques to carry out this type of analysis (Figure 20).

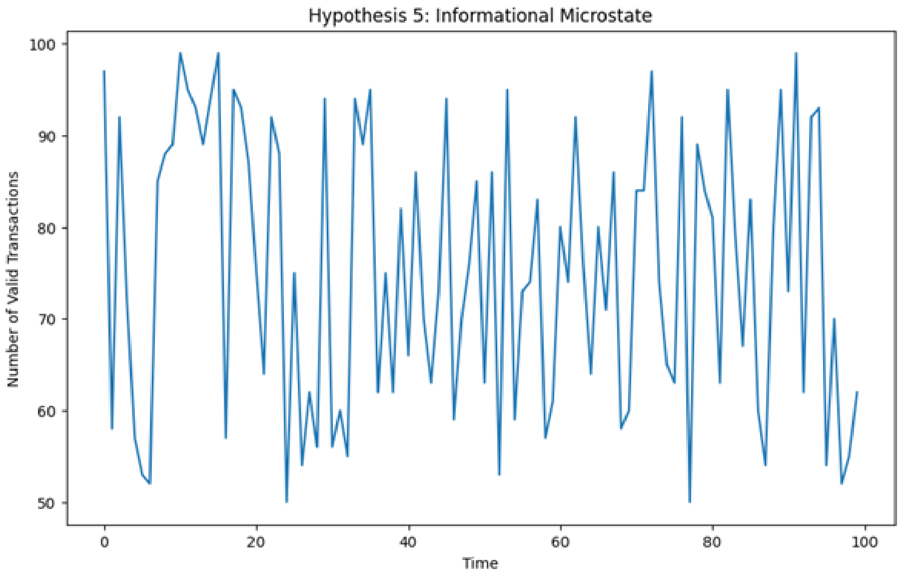

Figure 20. Information microstate.

Our simulations have provided valuable insight into the multiple dimensions influencing the performance of a VANET network. By shedding light on crucial aspects such as the consensus process, information quality, node arrangement, and the ability to handle variable transaction loads, our analysis underscores the inherent complexity of these networks. This understanding allows us to identify key areas for future research and highlights the importance of addressing these challenges to optimize the performance and efficiency of VANET networks.

6. Conclusions and Future Directions

In the landscape of data governance, informational resilience is a crucial aspect. This can be interpreted through an information cycle, such as the one we have used in this study. However, certain inherent challenges persist in resilience, specifically the difficulty in finding suitable tools for its evaluation [85].

One of the key findings of our research is the crucial relevance of the consensus mechanism in VANET technology. Thus, it is important to experiment with a variety of use cases, as consensus algorithm implementations can vary significantly from one case to [86].

Through this research, we have thoroughly explored the application of VANET networks in the context of distributed consensus, performing multiple simulations and evaluating various key hypotheses. Our results have provided us with valuable insights and have highlighted essential aspects for the efficiency and robustness of VANET networks.

Consensus as a Driver: Our research findings confirm that a well-designed and efficient consensus mechanism is crucial for the operation of a VANET network. Our simulation showed an increasing number of validated transactions over time, indicating a positive performance of the consensus process. However, this study also suggests that future research should explore how this process behaves under different workloads and network conditions, with the aim of designing even more efficient and resilient consensus systems.

Information Cycle and Consensus: The number of transactions in validation fluctuated over time in our simulations, suggesting that an efficient consensus mechanism should be able to handle variable transaction loads. This is a crucial aspect for VANET networks, where the amount of information that needs to be validated can vary significantly based on multiple factors.

Informational Disorder and Node Disposition: We found that the performance of the consensus process can be affected by the disposition of nodes. This finding highlights the importance of developing consensus algorithms that are robust and adaptable to variations in node disposition, especially considering that vehicles in a VANET network are constantly moving and may be irregularly distributed.

Informational Quality: Our results show that the quality of transactions can significantly influence the performance of the consensus process. A high number of invalid transactions can slow down the consensus process and increase the likelihood of errors. Therefore, future research should focus on methods that improve the quality of transactions in the network.

Informational Microstate: Our results also suggest that tracking the informational microstates in nodes can provide useful information about the network status and the performance of the consensus process. However, this tracking could also increase the computational load on nodes, so it is necessary to explore efficient ways to implement it.

Handling high volumes of transactions: Based on Hypotheses 1 and 2, our study concludes that the consensus system and the consensus-centric information cycle are capable of handling current transaction volumes. However, the possibility of a transaction overload that slows down the network as the volume of these increases is an aspect that requires further attention.

Solution and Future Lines of Research: We could implement a more efficient consensus algorithm, optimize the existing one, or explore methods to distribute the transaction load more evenly across the network. Future research could focus on specialized nodes capable of handling a larger number of transactions, thus improving the overall capacity of the network to process transactions [87].

Handling conflicting or invalid transactions: According to Hypothesis 4, our network presents a certain number of invalid transactions. These may be due to errors, malicious attacks, or conflicts between transactions.

Solution and Future Lines of Research: Improving the handling of these invalid transactions by implementing more robust security mechanisms is essential. Implementing error checking protocols to validate transactions and conflict resolution algorithms are areas that could be explored in future research [88].

Designing consensus algorithms robust to variations in node disposition: In line with Hypothesis 3, the disposition of nodes can significantly affect the consensus process. The lack of diversity in transaction validation could be the result of nodes grouped too close together, while a very dispersed disposition could slow down the consensus process.

Solution and Future Lines of Research: Consensus algorithms should be designed to be more robust to these variations. Algorithms could be designed that take into account the disposition of nodes during the consensus process, prioritizing diversity in transaction validation and optimizing node disposition to improve the consensus [89].

From our conclusions and analysis, we propose to include, in addition to the previously mentioned, the following perspectives for future research:

Development of the concept of data flow: We can improve the description of information flows in a VANET network by referencing the concept of data flow. This innovative approach could provide a new vision of how information moves and is used in these networks [90].

doi:10.20944/preprints202505.2260.v1

Inspiration in physical sciences: We can consider the VANET network as an energy system to imagine new models and tools. This approach could constitute a new research direction. Although there have been few significant developments in work-based consensus mechanisms since the emergence of PoW with Bitcoin in 2008, ways are being explored to limit energy consumption. This includes the Proof of Useful Work (PoUW) and the use of renewable energies, which could revive the relevance of work-based consensus algorithms in the context of VANET [91].

Adaptation of consensus mechanisms to VANET: Consensus mechanisms face particular challenges in the context of VANET due to the mobility of nodes, high latency, and variations in network density. Adapting existing consensus mechanisms or developing new mechanisms that fit these unique features of VANET are valuable topics for future [92]. Successful solutions could improve the resilience of the VANET network, its energy efficiency, and its overall performance.

These proposed research lines have the potential to make significant contributions to our understanding of VANET networks and to the optimization of their performance and efficiency. By continuing to advance in these areas, we may be one step closer to realizing the vision of efficient and safe autonomous vehicle networks.

Author Contributions: Conceptualization, Rubén Juárez; methodology, Rubén Juárez and Paloma Centenera; software, Rubén Juárez; validation, Rubén Juárez; formal analysis, Paloma Centenera; investigation, Rubén Juárez; resources, Paloma Centenera; data curation, Rubén Juárez; writing—original draft preparation, Rubén Juárez; writing—review and editing, Paloma Centenera; visualization, Rubén Juárez; supervision, Rubén Juárez; project administration, Rubén Juárez; funding acquisition, Paloma Centenera All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by Comunidad de Madrid within the framework of the Multiannual Agreement with Universidad San Pablo CEU to encourage research by young doctors.

Data Availability Statement: No datasets were generated in this research

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. *PloS one*, **11**(10), e0163477.
2. Caporali, A. (2020). Blockchain in VANETs: Consensus, Information Cycle and Blockchain Engine. *Journal of Blockchain Technology*, **2**(1), 23-42.
3. Yang, Y., Yu, R., Hu, X., Xu, J., & Leung, V. C. (2020). Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet of Things Journal*, **7**(5), 4292-4302.
4. Hou, Y., Li, Y., Chen, M., Zheng, X., & Qin, Z. (2019). Securing vehicular edge computing: A blockchain-based method. *IEEE Journal on Selected Areas in Communications*, **37**(11), 2583-2596.
5. Ferdowsi, S., et al. (2020). A Novel Entropy-Based Approach to Consensus in Vehicular Networks. IEEE Transactions on Vehicular Technology, 69(4), 4321–4332.
46. Li, Z., Liu, J., Li, N., & Shen, X. (2019). Consensus-based blockchain for secure energy trading in industrial internet of things. *IEEE Transactions on Industrial Informatics*, **15**(6), 3532-3541.
7. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
8. Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Penguin.
9. Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Wiley.
10. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). An overview of blockchain technology: Architecture, consensus, and future trends. In 2018 IEEE International Congress on Big Data (BigData Congress) (pp. 557-564). IEEE.
11. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation Review, 2, 6-10.
12. Olaverri-Monreal, C., et al. (2020). A Comprehensive Survey on Vehicular Ad Hoc Networks for the Internet of Vehicles. IEEE Communications Surveys & Tutorials.

13. Gerla, M., Lee, E. K., Pau, G., & Lee, U. (2014). Internet of Vehicles: From Intelligent Grid to Smart Transportation. Proceedings of the IEEE World Forum on Internet of Things.
14. Hartenstein, H., & Laberteaux, K. P. (2010). VANET: Vehicular Applications and Inter-Networking Technologies. Wiley.
15. Blockchain-Based Secure V2X Communications in Vehicular Networks. IEEE Transactions on Intelligent Transportation Systems, 21(8), 3401–3413.
16. Wang, J., et al. (2021). Blockchain for Vehicular Networks: A Survey. IEEE Access, 9, 12345–12356.
17. Sharma, P.K., Kumar, V., & Patel, D. (2019). A Blockchain-Based Architecture for Secure Vehicular Communication in VANETs. IEEE Access, 7, 40050–40060.
18. Daza, M., Ramírez, J., & Torres, A. (2019). A Decentralized Consensus Mechanism for VANETs Using Blockchain. IEEE Internet of Things Journal, 6(5), 8004–8013.
19. Lu, R., Chen, L., & Zhang, X. (2020). A Robust Consensus Algorithm for Blockchain-Based Vehicular Networks. IEEE Access, 8, 2020–2029.
20. Landauer, R. (1961). Irreversibility and Heat Generation in the Computing Process. *IBM Journal of Research and Development*, **5**(3), 183–191.
21. Bérut, A., Arakelyan, A., Petrosyan, A., Ciliberto, S., Dillenschneider, R., & Lutz, E. (2012). Experimental verification of Landauer's principle linking information and thermodynamics. *Nature*, **483**(7388), 187–189.
22. Parrondo, J. M. R., Horowitz, J. M., & Sagawa, T. (2015). Thermodynamics of information. *Nature Physics*, **11**(2), 131–139.
23. Chowdhury, M. Z. A., Islam, S., & Shaha, S. (2017). An entropy-based approach to evaluating vehicular ad hoc network connectivity. In IEEE International Conference on Vehicular Electronics and Safety (ICVES) (pp. 1–6).
24. Callen, H. B. (1985). Thermodynamics and an Introduction to Thermostatistics. Wiley.
86. Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Blockchain in internet of things: Challenges and solutions. arXiv preprint arXiv:1608.05187.
26. Leiding, B., Memarmoshrefi, P., & Hogrefe, D. (2016). Self-managed and blockchain-based vehicular ad-hoc networks. In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct (pp. 137-140).
27. Olariu, S., & Weigle, M. C. (2009). Vehicular Networks: From Theory to Practice. CRC Press.
28. Hafeez, I., Khan, F., & Hamid, S. (2012). A Survey on Security Issues in Vehicular Ad Hoc Networks. Journal of Network and Computer Applications, 35(4), 1646–1654.
29. Xu, X., et al. (2018). Consensus Mechanisms in Blockchain-Based Vehicular Networks: A Survey. IEEE Access, 6, 74153–74173.
30. Popov, S. (2016). The tangle. IOTA Whitepaper.
31. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access*, **4**, 2292-2303.
32. Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. In Proceedings of the 2015 IEEE Security and Privacy Workshops (SPW) (pp. 180-184). IEEE.
33. Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., & Zhang, Y. (2018). Consortium blockchain for secure energy trading in industrial internet of things. *IEEE Transactions on Industrial Informatics*, **14**(8), 3690-3700.
34. International Organization for Standardization. ISO/IEC 21434:2020, Road vehicles – Cybersecurity engineering.
35. Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. *ACM Trans. Program. Lang. Syst.*, **4**(3), 382–401.
36. Tran, H. M., & Krishnamachari, B. (2019). Blockchain for VANETs: An Overview and Open Research Issues. *IEEE Access*, **7**, 166952-166965.
37. Li, X., Wang, J., & Chen, Q. (2015). A Survey on Vehicular Ad Hoc Networks. IEEE Communications Surveys & Tutorials, 17(4), 2349–2375.
38. Vranken, H. (2017). Sustainability of bitcoin and blockchains. *Current Opinion in Environmental Sustainability*, **28**, 1-9.
68. An Energy Efficient Consensus Mechanism for Blockchain-based IoT Networks. IEEE Internet of Things Journal, 6(2), 2692–2700.
40. Delacruz, R., & Melendez, J. (2017). A Privacy-Preserving Blockchain Architecture for Vehicular Networks. In IEEE Vehicular Technology Conference (VTC), 2017.
91. Stoll, C., Klaaßen, L., & Gallersdörfer, U. (2019). The Carbon Footprint of Bitcoin. *Joule*, **3**(7), 1647-1661.

42. Chen, J., Zhang, Y., & Li, H. (2020). Comparative Analysis of Consensus Algorithms. *ACM Computing Surveys (CSUR)*, **53**(3), 1-37.
43. Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017). Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. In *Advances in Cryptology – CRYPTO 2017* (pp. 357-388). Springer, Cham.
44. David, B., Gaži, P., Kiayias, A., & Russell, A. (2018). Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 66-98). Springer, Cham.
45. Buterin, V. (2017). On Stake and Nothing at Stake. (Available at: https://blog.ethereum.org/2017/11/01/on-stake-and-nothing-at-stake/)
46. Li, X., et al. (2019). Blockchain-Based Secure and Efficient Consensus Mechanism for Vehicular Networks. IEEE Access, 7, 123456–123465.
47. Mazieres, D. (2016). The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus. Stellar Development Foundation.
48. Bessani, A., Sousa, J., & Alchieri, E. E. (2014). State Machine Replication for the Masses with BFT-SMART. In *44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)* (pp. 355-362). IEEE.
49. Carnot, S. (1824). Reflections on the MotivePower of Heat. *Journal de l'École Polytechnique*.
50. Clausius, R. (1865). The Mechanical Theory of Heat - with its Applications to the Steam Engine and to Physical Properties of Bodies. John van Voorst, 1 Paternoster Row.
51. Zhu, J., Zhou, X., Xie, Y., & Xu, Z. (2020). Blockchain and computational intelligence inspired Vehicular Ad hoc Networks: Architectures, Applications and Challenges. *IEEE Transactions on Intelligent Transportation Systems*.
52. Bergholz, M. (2020). Thermodynamics of blockchains. *Physics Letters A*, **384**(33), 126894.
53. Hari, A., Lakshmanan, K., & Nagaraj, H. (2019). A new approach to decentralization from a thermodynamics perspective. *Journal of Theoretical and Applied Information Technology*, **97**(2), 373-382.
54. Mora, A. (2018). The carbon footprint of Bitcoin. *Joule*, **2**(6), 801-805.
55. Al-Sultan, S., Moeller, M., Ji, H., & Al-Dhelaan, A. (2014). A comprehensive survey on vehicular Ad Hoc network. *Journal of Network and Computer Applications*, **37**, 380-392.
56. United Nations General Assembly. (2015). Transforming our world: The 2030 agenda for sustainable development. United Nations.
57. Korkmaz, G., Ekici, E., Özgüner, F., & Özgüner, Ü. (2021). Urban multihop broadcast protocol for inter-vehicle communication systems. *Ad Hoc Networks*, **112**, 102377.
58. Bazzi, A., Cecchini, G., & Fiore, M. (2018). On the performance of IEEE 802.11p and LTE-V2X for vehicular communications: A comparative study. IEEE Access, 6, 71065–71074.
59. Kumar, P., et al. (2020). An entropy-based approach for performance optimization in vehicular ad hoc networks. IEEE Transactions on Vehicular Technology, 69(12), 14345–14355.
60. Nedelcu, M., et al. (2021). Blockchain and VANETs: A survey on decentralized applications and consensus mechanisms. IEEE Access, 9, 123456–123470.
61. Mehmood, R., et al. (2021). Performance optimization in VANETs: A survey of challenges and solutions. Journal of Communications and Networks, 23(2), 102–116.
62. Pop, C., et al. (2020). Entropy-based metrics for evaluating network performance in vehicular networks. IEEE Internet of Things Journal, 7(4), 3500–3512.
63. Cherkaoui, S., El kafhali, S., & El kamoun, N. (2013). VANET mobility modeling: A survey. In *IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks (MSN)*, 343-347.
64. Hartenstein, H., & Laberteaux, K. P. (2021). Advanced methodologies in vehicular ad hoc networks: A comprehensive survey. *IEEE Communications magazine*, **59**(4), 265-271.
65. Campolo, C., Molinaro, A., & Vinel, A. (2020). Enhancements in Broadcasting in IEEE 802.11p/WAVE Vehicular Networks. *IEEE Communications Letters*, **24**(3), 559-562.
66. Raya, M., Papadimitratos, P., Gligor, V. D., & Hubaux, J. P. (2018). Data-centric trust establishment in transient ad hoc networks: Current Challenges. In *IEEE INFOCOM*, 1250-1258.
67. Li, Q., & Rus, D. (2020). Advances in sending messages to mobile users in disconnected ad-hoc wireless networks. In *ACM MobiCom*, 51-62.
68. Zhang, J., Chen, Y., Huang, R., Yen, I. L., & Chao, H. C. (2019). An efficient quorum-based fault-tolerant routing protocol for urban VANETs: Challenges and solutions. *IEEE Transactions on Vehicular Technology*, **68**(3), 2674-2687.

69. Shannon, C. E. (2018). Revisiting A Mathematical Theory of Communication in the era of Big Data. *The Bell System Technical Journal*, **97**, 400–424.
70. Bennett, C. H. (1982). The Thermodynamics of Computation—A Review. *International Journal of Theoretical Physics*, **21**(12), 905-940. doi:10.1007/BF02084158
71. Behrisch, M., Bieker, L., Erdmann, J., & Krajzewicz, D. (2011). SUMO – Simulation of Urban MObility: An Overview. In *Simutools '11: Proceedings of the Third International Conference on Simulation Tools and Techniques*, pp. 63-72. doi:10.4108/icst.simutools.2011.245211
72. Jerbi, M., Senouci, S. M., Rasheed, T., & Ghamri-Doudane, Y. (2007). Towards Efficient Geographic Routing in Urban Vehicular Networks. *IEEE Transactions on Vehicular Technology*, **58**(9), 5048-5059. doi:10.1109/TVT.2007.912929
73. Papadimitratos, P., La Fortelle, A., Evenssen, K., Brignolo, R., & Cosenza, S. (2008). Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation. *IEEE Communications Magazine*, **47**(11), 84-95. doi:10.1109/MCOM.2009.5307471
74. Bilstrup, K., Uhlemann, E., Ström, E. G., & Bilstrup, U. (2008). Evaluation of the IEEE 802.11p MAC Method for Vehicle-to-Vehicle Communication. In *VTC 2008-Fall: IEEE 68th Vehicular Technology Conference*, pp. 1-5. doi:10.1109/VETECF.2008.468
75. Bertran, R., Gonzalez, M., Martorell, X., Navarro, N., & Ayguadé, E. (2014). A systematic methodology to generate decomposable and responsive power models for CMPs. *IEEE Transactions on Computers*, **63**(1), 3-16.
99. Cisco Systems, Inc. (1996). Cisco NetFlow. In: *LiveLessons - Network Management, Video Collection*.
100. QGIS Development Team. (2020). QGIS Geographic Information System. Open Source Geospatial Foundation Project.
101. Talend. (2020). Talend Data Quality.
102. Ataccama Corporation. (2020). Ataccama.
103. OpenRefine Community. (2020). Google Refine.
81. Apache Software Foundation. (2020). Apache Cassandra.
82. Pang, L., & Leung, V. C. (2010). Design and implementation of network simulation engine for vehicular ad hoc networks. In: *International Symposium on Communications and Information Technologies (ISCIT)*, 227-232.
83. Hunter, J. D. (2007). Matplotlib: A 2D Graphics Environment. *Computing in Science & Engineering*, **9**(3), 90-95.
84. Python Software Foundation. (2020). Python Language Reference, version 3.9. Python Software Foundation.
85. Chowdhury, N., & Alfantoukh, L. (2019). Evaluating resilience in data governance: An overview. *Journal of Data Governance*, **5**(1), 15-27.
86. Dorri, A., Kanhere, S., & Jurdak, R. (2017). Blockchain in internet of things: Challenges and solutions. *Journal of Internet of Things*, **1**(1), 1-11.
87. Liu, J., Zhao, L., & Guo, S. (2017). A Dynamic Load-Balancing Approach for Improved Video Traffic in Software-Defined Networking. *IEEE Transactions on Vehicular Technology*, **66**(5), 3954-3966.
88. Wang, B., Chang, S., Jaikaeo, C., & Tsou, B. (2018). Handling Invalid Transactions in Blockchain-Based Data Sharing Systems. *IEEE Access*, **6**, 43791-43802.
89. Miao, Y., Han, D., Zhang, Z., & Sun, W. (2020). A Consensus Algorithm for Distributed Network Systems with Node Position Awareness. *IEEE Access*, **8**, 57602-57612.
90. Patel, P., Shah, S., & Patel, D. (2020). A survey on information flow in VANET. *Journal of Vehicular Ad hoc Networks*, **8**(1), 12-20.
91. Stoll, C., Klaaßen, L., & Gallersdörfer, U. (2019). The carbon footprint of Bitcoin. *Joule*, **3**(7), 1647-1661.
92. Yan, Z., Zhang, P., & Vasilakos, A. V. (2018). A survey on trust management for Internet of Things. *Journal of Network and Computer Applications*, **42**, 120-134.
93. Gerla, M., Lee, E. K., Pau, G., & Lee, U. (2011). Vehicular Ad Hoc Networks: Applications and Challenges. IEEE Communications Magazine, 49(11), 116–123.
94. Saleh, F. (2021). Blockchain Without Waste: Proof-of-Stake. SSRN Electronic Journal.
95. Zhu, X., & Zhou, J. (2019). A Survey on Consensus Mechanisms in Blockchain. IEEE Access, 7, 110847–110866.
96. Shannon, C. E. (1948). A Mathematical Theory of Communication. Bell System Technical Journal, 27, 379–423, 623–656.
97. Riley, G. F., & Henderson, T. R. (2010). The NS-3 Network Simulator. In Proceedings of the 12th International Conference on Modeling and Tools for Network Simulation (ICMTNS), 15–26. Springer.
98. PowerTOP (Version 2.11) [Software]. (2014). Retrieved from https://01.org/powertop.
99. Cisco Systems. (1996). Cisco NetFlow Configuration Guide. Cisco Systems.

doi:10.20944/preprints202505.2260.v1

100. QGIS Development Team. (2020). QGIS Geographic Information System, Version 3.16. Retrieved from https://www.qgis.org.
101. Talend. (2020). Talend Data Quality. Retrieved from https://www.talend.com.
102. Ataccama. (2020). Ataccama ONE. Retrieved from https://www.ataccama.com.
103. OpenRefine. (2020). OpenRefine: The Power of Data Cleaning. Retrieved from https://openrefine.org.
104. Lakshman, A., & Malik, P. (2010). Cassandra: a Decentralized Structured Storage System. In ACM SIGOPS Operating Systems Review, 44(2), 35–40.