

Article

FlexiChain 3.0: Distributed Ledger Technology Based Intelligent Transportation for Vehicular Digital Asset Exchange in Smart Cities

Ahmad Alkhodair ^{1,†,‡}, Saraju P. Mohanty ^{2,§} and Elias Kougianos ^{3,*} 

¹ University of North Texas; Department of Computer Science and Engineering; Denton; USA; ahmadalkhodair@my.unt.edu

² University of North Texas; Department of Computer Science and Engineering; Denton; USA; saraju.mohanty@unt.edu

³ University of North Texas; Department of Electrical Engineering; Denton; USA; elias.kougianos@unt.edu

* Correspondence: elias.kougianos@unt.edu

Abstract: Due to the enormous amounts of data being generated between users, Intelligent Transportation Systems (ITS) are complex cyber physical systems that necessitate a reliable and safe infrastructure. Internet of Vehicles (IoV) is the term that describes the interconnection for every single node, device, sensor, and actuator that are Internet enabled, whether attached or unattached to vehicles. A single smart vehicle will generate a huge amount of data. Concurrently it needs an instant response to avoid accidents since vehicles are fast moving objects. In this work, we explore Distributed Ledger Technology (DLT) and collect data about consensus algorithms and their applicability to be used in the IoV as the backbone of ITS. Multiple distributed ledger networks are currently in operation. Some are used in finance, or supply-chain, and others for general decentralized applications. Despite the secure and decentralized nature of the blockchain, each of these networks has trade-offs and compromises. Based on the analysis of consensus algorithms, a conclusion has been made to design one that fits the requirements of ITS-IoV. FlexiChain 3.0 is proposed in this work to serve as a Layer0 network for different stakeholders in the IoV. A time analysis has been conducted and shows a capacity of 2.3 transactions per second, which is an acceptable speed to be used in IoV. Moreover, a security analysis was conducted as well and shows high security and high independence of the node number in terms of security level per the number of participants.

Keywords: Blockchain; Distributed Ledger Technology (DLT); Cyber Physical Systems (CPS); Intelligent Transportation (ITS); Vehicle to Vehicle Communication (V2V)

1. Introduction

Citation: Alkhodair, A.; Mohanty, S.P.; Kougianos, E. FlexiChain Based V2V Scenario. *Sensors* **2023**, *1*, 0. <https://doi.org/>

Received:

Revised:

Accepted:

Published:

Copyright: © 2023 by the authors. Submitted to *Sensors* for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Every day, the number of vehicles on the road is increasing, which causes traffic congestion and delays in the transit process for emergency vehicles, such as ambulances, fire trucks and police cars [1]. Transportation solutions that were formerly acceptable have become insufficient in addressing the enormous growth in the number of vehicles over the last two decades, despite significant improvements in infrastructure[2]. ITS integration is more important than ever. ITS is meant to aid in the construction of “smart roads” by decreasing the incidence of traffic jams and increasing the effectiveness of relieving them. Insight into traffic conditions and availability is provided to users. As a result, travel is safer and more pleasant, and less time is spent getting to and from daily destinations. The IoV is a novel concept that evolved from the idea of Vehicular Ad hoc Networks (VANETs) as a result of recent advances in computing and communication technology [3], [4]. For ITS to function, the IoV must first be established. The United States Department of Transportation (DOT) [5] claims that the IoV can help reduce accidents involving sober drivers. Cars can communicate with each other in order to track other cars’ movements and whereabouts [6]. The term IoV is used to describe a system in which vehicles are linked together and can

share and receive information from one another and from other devices. This paves the way for the instantaneous dissemination of data regarding traffic conditions, road hazards, and other elements that might significantly affect travelers' safety and productivity.

With the IoV in place, it is predicted that 79% of such collisions can be prevented through improved coordination and dialogue between vehicles [2]. Bicycles, pedestrians, and roadside infrastructures are all linked together reducing environmental pollution, accident rates, and traffic jams [7][8] [9] by exchanging messages about traffic conditions and information on safety and accidents with a worldwide traffic control system that improves convenience, comfort, and safety. Thus, improvements in public transportation and pedestrian traffic are also possible. Because of Global Positioning Systems (GPS) technology, it is now possible to know where other vehicles are in situations such as blind spots, stoppages on the highway but concealed from view, around a blind corner, or blocked by other vehicles. A vehicle's ability to anticipate and respond to changing driving conditions can provide immediate warning to its owners [10]. When it comes to preventing car accidents, the primary purpose of Vehicle to Vehicle (V2V) communication technology is to help drivers be aware of their surroundings and increase safety at a reasonable cost.

Traditional means of interoperability in the IoV have included cellular networks, satellite communications, and Dedicated Short-Range Communication (DSRC). While these approaches have shown promise, they are not without drawbacks, including security risks and transmission inefficiencies. For example, a smart vehicle is one that can sense its surroundings and operate independently without human intervention [11]. A smart-featured automobile relies on sensors and actuators, complicated algorithms, machine learning systems, and powerful processors. Sensors in various components of the vehicle are used to construct and maintain a map of the vehicle's surroundings. Radar sensors keep an eye out for other vehicles that may be approaching from behind. Traffic lights, road signs, other vehicles, and pedestrians are all detected by video cameras. To determine distances, road boundaries, and lane markers, Lidar sensors bounce light pulses off the car's surroundings [12]. When parking, ultrasonic sensors in the wheels pick up on obstacles like curbs and other vehicles. The car's actuators, which control the car's acceleration, braking, and steering, receive orders from sophisticated software, which interprets the sensory data and maps a route. Predictive modeling and object identification assist the software to navigate traffic regulations and avoid obstructions [13]. All these data are generated from one smart entity, which will create a challenge. Challenges exist to scalability such as scalability in data, scalability in throughput, scalability in power, and scalability in time response.

Smart vehicles are a trend research area for many companies, labs, and researchers due to their anticipated benefits to the quality of life [14]. This type of driving relies partially on machines and is ruled by algorithms and embedded standards and regulation codes which give drivers more tools to enhance their experience. Security and real-time operations are an important factor in such applications, where the impact of any failure will influence lives. Each vehicle will be full of sensors to read the environment and act accordingly. The integration of multiple technologies will burden the central authorities regarding security threats. [15]. Depending on the above, several questions come to mind, such as: how to create secure communication? how to avoid latency? how to reduce centralization? how to reduce power consumption? and how to encourage nodes to act honestly? Such a large, complex CPS has many obstacles to overcome for full deployment such as interference conditions, traffic regulations, and complex V2V communications.

The introduction of the blockchain DLTs, which have altered numerous aspects of our lives, has been one of the most revolutionary developments of the past few decades [16,17]. These innovative methods of data storage and transaction processing have the potential to affect a broad range of industries, including banking, supply chain management, government, healthcare, and ITS [18].

DLT is a group of mechanisms and protocols governed by the consensus mechanism of participants through direct communication in an untrusted environment [19]. DLT has

been proposed to resolve many issues of the current centralized paradigm of intelligent transportation and to provide a secure environment for its operations [20] [21]. ITS-VANETs needs to acquire the characteristics of DLT such as decentralization, immutability, transparency, security, efficiency, and programmability in order to satisfy its requirements as a Complex Cyber Physical System (CCPS) [22]. For example, real-time interaction, scalable architecture, automated operation, low power consumption and security. Increased trust, transparency, and security are just some of the ways in which DLT could change the face of ITS [23]. Certain conditions must be met before DLT-based ITS operations can be put into place. Already existing ledger structures and consensus algorithms need trade-offs in which, sometimes security and privacy are strong but scalability is weak or scalability is high but security is low.

Scalability: the volume of data related to transportation operations is expected to expand, and the system must be able to process a high volume of transactions and nodes. This is not the case in all DLTs. Some lack of scalability such as Bitcoin. The paradigm is a fit for electronic cash systems but will cause an issue in term of scalability and hardware requirements if applied to ITS. Blockchain-Based Secure Data Exchange (BDESCF) ITS is a secure and tamper-proof framework for data exchange and storage. It also prevents replay, Man in the Middle (MiTM) weaknesses, impersonation, data leakage, and unwanted data updating with authentication and privacy measures. BDESCF-ITS integrates smoothly with existing transportation systems. BDESCF-ITS is a strong security mechanism for DLT applications to transportation security and privacy [24]. However, Practical Byzantine Fault Tolerance (PBFT) is suggested to be used in such a framework which will burden the network with the redundancy. Power consuming protocols are part of the scalability problem and need a preexisting level of trust to be initiated. Also, this protocol has a lower degree of decentralization which will change the nature of ITS-VANETs. Another example is interoperability: when it comes to transportation, the DLT system should be compatible with a wide range of systems, technologies, and platforms to ensure that data is shared effectively among all parties involved. With the absence of Layer 0 in the crypto-networks and due to the importance of interoperability to an ITS system, the choice of a certain ledger should be based on the requirement of ITS.

Security and Privacy: data integrity and confidentiality must always be maintained by the system to prevent any unwanted changes or disclosures to private information. Strong encryption, access restriction, and other privacy-protecting measures fall under this category. For example, Ethereum provides strong cryptography and a medium latency which is acceptable. However, with the growth of VANETS, the network will encounter some throughput and routing issues due to time adjustment (used in Bitcoin), and the huge amount of operations which take place in Ethereum to reach agreement. In [25], a blockchain-based Conditional Privacy-Preserving Authentication (BCPPA) protocol employs key derivation and blockchain technology to enhance VANET authentication and privacy. BCPPA utilizes Ethereum smart contracts to secure vehicle communication over VANET. The costly Elliptic Curve Digital Signature Algorithm (ECDSA) can be replaced with a modified version or another Public Key Infrastructure (PKI)-based signature with bulk verification to increase efficiency. Using blockchain technology, the BCPPA protocol provides conditional privacy-preserving authentication and decentralized, tamper-proof VANET communication. Even though smart contracts are hosted in a secure blockchain, limiting the process of securing the communication to a programmable transaction will centralize the process, in addition to the centralization level of Ethereum.

Latency: Traffic management, navigation, and V2V communication are just a few examples of real-time ITS applications that require low latency. Transactions and data exchange on the DLT system must be rapid. The nature of ITS-VANETs is direct and rapid communication. When using a DLT based framework, the latency must be taken into account. In [26], The primary contribution of this work is to propose a secure 5G-ITS through the use of blockchain technology to evaluate trust against potential attacks. To accomplish hierarchical trust evaluations and protect the privacy of users, federated deep learning is

used to evaluate the trust of ITS users and task distributors. In order to guarantee the efficiency and accuracy of trust evaluation, hierarchical incentive mechanisms are also designed to implement reasonable and fair rewards and punishments. Hyperledger is used to implement frameworks and is well known for its power consuming and high resource usage. The nature of DLT based IoV is decentralization while ensuring fairness and decentralization. In [27], a Public, Special, and Supreme framework is presented. The “Public” blockchain server is responsible for service-related data transmission, verification, and storage. It is a shared blockchain server with limited storage capacity. Once the public blockchain’s memory is complete, it will replace its own data within the blockchain. Similarly to the public blockchain server, the “Special” blockchain server displays dynamic features. Specifically, the “Supreme” blockchain server is used to store all network-participating vehicle information. Each data transmission detail of the intelligent vehicle is securely preserved and processed in the supreme blockchain. The nature of the required operation for DLT usage is not satisfy since the three servers reduce the decentralization and increase the vulnerability toward Single Point Failure (SPF).

Consensus Mechanism: security, decentralization, and performance are all factors that should be considered while deciding on a consensus process. It also needs to be secure against attacks like Sybil and 51% attacks, as well as energy efficient. Consensus is the core of any DLT. Most of the challenges faced are based on the consensus algorithm. In [22], a blockchain-enabled vehicular crowd-sensing technology secures 5G Internet of Vehicles user privacy and data safety by securing real-time traffic data. A deep reinforcement learning (DRL) algorithm selects the best active miners and transactions to optimize blockchain security and latency. A two-sided matching-based approach allocates non orthogonal multiple access sub channels to reduce uploading delay for all users. This technology safeguards vehicular crowd-sensing data collecting and user privacy. The consensus algorithm proposed in this work is PBFT, which is known for its high tolerance and security but has overhead computational requirements. [28] proposes the Ethereum-based VNB (VANETs with a Blockchain). The VNB simulates a vehicle on-board unit (OBU), scanning adjacent vehicles, authenticating them, and communicating with blockchain accounts. The VNB correctly distinguished different vehicle types in simulations. Despite its limitations, the proposed VNB offers a promising security and trust architecture for autonomous vehicular networks and ITS in smart cities in the near future. Proof of Work (PoW) and Proof of Stake (PoS) are both used as consensus algorithms. PoW is utilized for its ease and security in determining the correct nonce, while PoS is utilized for its energy efficiency and decentralization prevention. Nonetheless, PoS is susceptible to double-spend attacks. PoW is known for its high security but needs resource-rich nodes, and thus is not suitable for IoV operations. PoS is known for its security and operations efficiency but vulnerable to centralization and routing problems.

Other conditions and criteria such as data quality: information saved and transmitted through the system must be as accurate and trustworthy as possible by excluding any potentially misleading data. Governance: the many participants in the DLT-based ITS ecosystem need a well-defined governance framework that specifies their specific responsibilities and how they will make decisions. Legal and Regulatory Compliance: the system must follow all data protection, privacy, and cybersecurity legislation, both domestically and internationally. Incentive Mechanisms: suitable incentive mechanisms, such as token-based rewards for users and service providers, should be built into the DLT-based ITS to encourage widespread adoption and active involvement. User Experience: the system needs to be simple and straightforward so that those who really utilize the DLT-based ITS services can get about with ease. By meeting these requirements, a DLT-based ITS can contribute to the development of a more productive, secure, and transparent transportation ecosystem, which will benefit users, operators, and regulators. In this paper, we compare multiple blockchain and non-blockchain consensus algorithms and their applicability to serve ITS applications based on the requirement [29]. We propose FlexiChain 3.0 Technology as a platform to host ITS digital assets collections and exchange in V2V, Vehicle to Machine

(V2M), and Vehicle to Human (V2H) transactions. In addition, a detailed security analysis for certain types of attacks between the proposed work and related works is presented.

Figure 1 illustrates the layered structure of employing DLT in intelligent transportation in applications such as auto vehicle driving data training, V2X communication, vehicles' history, and autonomous vehicles.

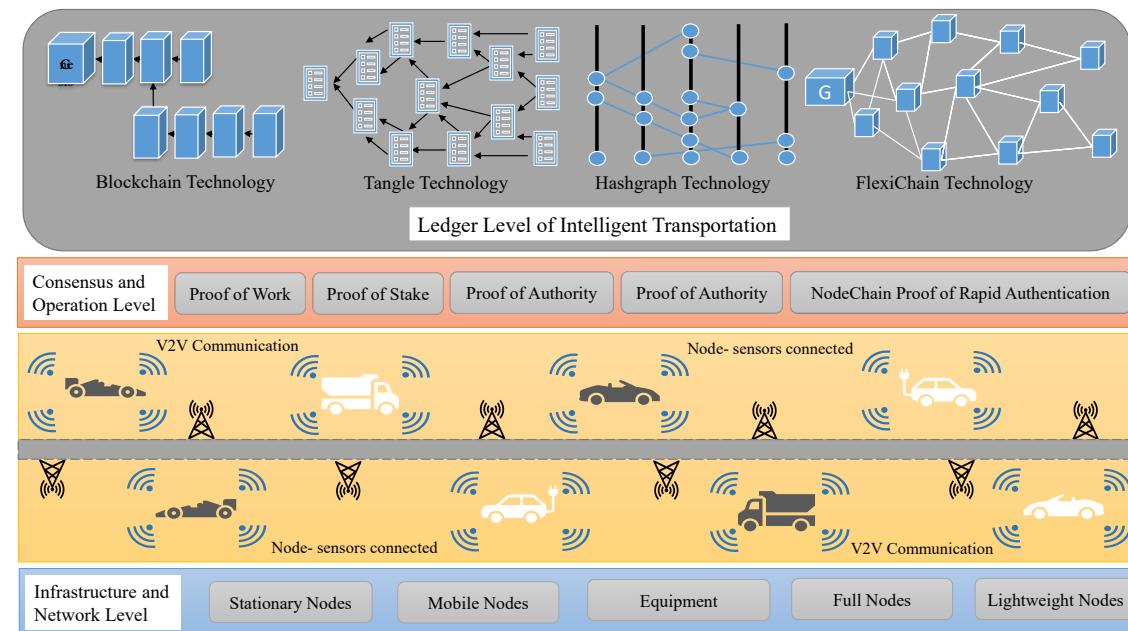


Figure 1. High-Level Depiction of DLT-based ITS.

The rest of the paper is organized as follows: Section 2 summarizes the novel contributions of this paper. Section 3 presents background information and previous related works. Section 4 presents the proposed system. Section 5 provides experimental results. Finally, Section 6 concludes the paper and presents directions for future research.

2. Novel Contributions

In this section, the paper's unique contributions are discussed and the proposed work is highlighted. Data accuracy, instant responses, security, consistency, fault tolerance and privacy are all required for such an ITS-V2X system. Accuracy of any ITS relies on the huge data accumulation and training through an Artificial Intelligence (AI) agent which requires correct information and integrity to produce a useful feedback and directions. Security and privacy are required to keep the operations running smoothly with no fails or undesired events to keep peoples' and nodes' identities secured and private. Consistency is required to ensure that the operations are always on and will not encounter any issues even during an attack such as Distributed Denial of Service (DDoS). Low latency is a need since all operations in ITS require the lowest time to execute. Also, power consumption is a critical factor which should be minimized for sustainable and reliable operations.

2.1. Problem Addressed

With the advancement of technology, vehicles act as a driving computer system recording routes, status, identities, data, and gives feedback to users. Due to this huge amount of data generated from vehicles, a secure platform is desirable. Also, secure channels and fast communication are also required. Due to the amount of data involved, this can be a challenge. Moreover, data training, data exchange, central authority and speed all are challenges to the current paradigm. DLTs are suitable to resolve ITS challenges but must satisfy the desirable requirements for the application. For example, using the blockchain (Bitcoin) Paradigm will not benefit ITS due to its operation that by design has

been targeting an electronic cash system. As another example, the blockchain (Ethereum) paradigm is a very efficient distributed super computer, but the operation is suitable to web applications and financial applications while a few seconds latency will not harm whereas one second latency might cause huge safety and security issues in ITS.

2.2. Solutions Proposed

An exploration of the feasibility for DLT based CPS, such as ITS, is justified since the technology provides a secure platform that could make it practical and effective. An analysis of prior technologies and their consensus algorithms is presented to analyze the need of having a customized or application based designed DLT to satisfy ITS conditions. FlexiChain 3.0 is an upgraded version from our previous work [30] for ITS data collection and trade based ITS proposed to introduce the feasibility of operating a V2V network over FlexiChain technology [17,20,30].

2.3. Significance of the solution

1. The suitability of several technologies to ITS is analyzed.
2. The need of an application-based DLT is introduced
3. Propose a DLT that could satisfy ITS requirements without trade-offs.
4. A novel technology framework, FlexiChain 3.0 is presented as a solution.
5. The novel DLT is designed specifically for ITS as CCPS.

In Table 1, a comparison is given between our previous versions of FlexiChain and the current work. In [30], the work is representing FlexiChain 1.0 which is combining our work with the novel MultiChain Proof of Rapid Authentication [17]. A novel block structure has been proposed with an enrollment process that creates the Accessible Secure Identification List proposed in [20]. In the next version, FlexiChain 2.0, an upgrade was presented on how to generate the file using a combined ledger of NodeChain, and how the file is created and updated, making NodeChain as Layer0 and all other blockchains as Layer1. Moving to the next version, since the proposed work is about a designed distributed ledger for Cyber Physical Systems, FlexiChain 2.0 has been upgraded and modified to fit ITS applications as a complex CPS using a distributed offline vault (NodeChain) which is a manufacturer's predefined trust and which provides a public permissioned ledger. The rest of the table is covering other differences and similarities.

Table 1. Comparative Perspective Between FlexiChain Versions.

Features/Version	FlexiChain 1.0 [30]	FlexiChain 2.0 [31]	FlexiChain 3.0 (Current)
Linked Lists	Genesis Blockchain (independent ledger) DAG based Blocks	Layer0 Ledger Independent NodeChain DAG Based Blockchains	Independent NodeChain Layer0 Ledger DAG based BlockX
Registration	Pre-Installed or Equipped Manufacturer Trusted Modules	Trusted Security Hardware NodeChain (Chain of Narration)	Entry Key Pre-Enrollment Pre-Launched NodeChain Manufacturer Trust
Authentication	ASID Proof of Rapid Authentication	NodeChain Proof of Rapid Authentication	NodeChain Proof of Rapid Authentication
Type of Validation	Authentication (Minerless)	Authentication (Minerless)	Authentication (Full Nodes)
Validators	All Virtual Nodes	All Qualified Nodes	Full Nodes
Security	Digital Signature Hash Function Secure File (ASID) and TPM	Digital Signature, Hash Function Tokenized UID and Hardware Security	Digital Signature Hash Function Tokenized UID from Independent Offline NodeChain
Design Purpose	IoT/CPS Applications	IoT/CPS Applications	Intelligent Transportation

3. Background and Previous Related Work

3.1. Smart Cities

Smart cities have recently generated a lot of attention. The idea of having a smart city that comprises of smart sectors such as smart population, smart administration, smart transportation, smart agriculture, smart grid, smart education, and smart infrastructure is unique but challenging [32]. Due to the attention given to the notion of a smart city, it has been defined in various ways in [33]. Others have presented the current concept of smart city and its future directions [34]. In [35], an extensive overview of smart cities is presented covering a wide range of topics including research aims, research challenges, potential scenarios, and potential project areas [14]. Functional specifications that needed to be known about smart cities have been discussed in [36]. Since the quality of life for each citizen is the most important factor, designing and planning the smart services within a smart city must be done in a way that could facilitate people's lives due to the adoption of information and communication technology (ICT) [37]. In [38], numerous potential and commercial benefits associated with the smart economy and the connection between the economy and citizens are explored. In [39], it is stated that smart government in smart cities is effective only if it offers their residents city services, channels, smart mobile services, and network integration. Environment quality such as air quality, water, trees, waste management, and infrastructure has been discussed in [40–42]. While using all these smart services, enormous amount of data are produced and have to be managed. Big data and the paradigm of Internet of Things (IoT) or CPS might raise some challenges such as security, and privacy issues. In [43], protecting user confidentiality in blockchain-based IoT systems is discussed. The paper focuses on privacy issues presenting examples and cases. In [13], the potential of adopting DLT in smart cities and their applications is investigated. Also, some blockchain paradigms that could be applied to a smart city are discussed.

3.1.1. NEOM

Recently, a new smart city has been introduced to the whole word under the name of "The Line", as part of the huge project of the government of Saudi Arabia's Neom mega city. The city is built over the dessert from the ground up as a smart city taking into account all aspects to provide the optimum quality of life. The city will include a smart infrastructure, and smart supply chain and logistic services. The city is designed with smart energy systems [44,45].

3.2. IoV & VANET

IoV is a concept that extends the IoT to the transportation domain, allowing for seamless connectivity and communication between vehicles, infrastructure, and other smart devices [46]. IoV seeks to develop intelligent transportation systems with enhanced safety, traffic efficiency, and vehicle experience. VANETs serve an essential role in the execution of the IoV vision. The IoV incorporates a wider array of applications, devices, and technologies, whereas VANETs are primarily concerned with V2V and vehicle-to-infrastructure (V2I) communication. The contributions of VANETs to the IoV ecosystem are as follows: Communication: VANETs serve as the communication infrastructure for IoV vehicles. They enable V2V and V2I communication, facilitating real-time data sharing and decision-making. Safety: by enabling vehicles to share information about their position, speed, and orientation, VANETs enables various safety applications, such as collision avoidance and early warning systems, which are integral components of the IoV [47]. VANETs enable vehicles to share traffic information such as congestion levels, road conditions, and detours, which can optimize traffic flow, reduce travel time, and enhance overall transportation efficiency in the context of IoV. Data collection and analysis: VANETs can facilitate the accumulation of vast quantities of data from vehicles and infrastructure that can be used for real-time monitoring, predictive analytics, and decision-making within the IoV ecosystem. VANETs can be incorporated with other IoT systems, such as smart grids and smart cities, allowing for a more comprehensive and interconnected approach to transportation man-

agement and urban planning. VANETs are a crucial component of the IoV, as they provide the communication infrastructure required for vehicles and the infrastructure to exchange data and cooperate. VANETs contribute to the development of safer, more efficient, and environmentally friendly transportation systems within the IoV ecosystem as a whole by facilitating efficient communication between vehicles and roadside infrastructure.

3.3. DLT

DLT is a broad term that encompasses a variety of technologies that facilitate the secure, transparent, and decentralized storage of records across a network of participants [48]. A top-down approach to elucidating DLT would entail deconstructing the concept into its fundamental elements and then building upon them. Here is an in-depth explanation of DLT:

3.3.1. Cryptography:

Several cryptographic techniques and mechanisms are used in DLTs to ensure security, privacy, and data integrity. Some of the key techniques and mechanisms include:

3.3.2. Hash functions:

These are mathematical algorithms that take an input and produce a fixed-size output, called a hash. In DLT, hash functions are used for data integrity, tamper resistance, and generating unique identifiers. Examples of hash functions used in DLT include SHA-256 (used in Bitcoin) and Keccak-256 (used in Ethereum).

3.3.3. Digital signatures:

Digital signatures enable the sender of a message to sign it with their private key, proving authenticity and integrity. In DLT, digital signatures are used for transaction authorization and ownership verification. Commonly used digital signature algorithms in DLT include ECDSA and the Edwards-curve Digital Signature Algorithm (EdDSA).

3.3.4. Public Key Cryptography (PKC):

Also known as asymmetric cryptography, PKC uses a pair of keys, namely a public key and a private key. In DLT, public keys serve as user addresses, while private keys authorize transactions and asset transfers. Examples of PKC used in DLT are the RSA algorithm and Elliptic Curve Cryptography (ECC).

3.3.5. Cryptographic key derivation functions (KDFs):

KDFs are used to generate cryptographic keys from user-provided inputs, such as passwords or passphrases. In DLT, KDFs increase the security of keys, making it harder for attackers to guess or brute-force them. Examples of KDFs used in DLT include scrypt, bcrypt, and Argon2.

3.3.6. Cryptographic consensus mechanisms:

Cryptography plays a role in consensus mechanisms that maintain the integrity and security of the distributed ledger. Examples include PoW, where miners solve cryptographic puzzles to validate transactions and create new blocks, and PoS, where validators are chosen based on their stake in the network.

3.3.7. Privacy-enhancing techniques:

Cryptographic techniques are also used to preserve privacy in DLT. Some examples include:

1. Zero-knowledge proofs (ZKPs): ZKPs enable users to establish the authenticity of a statement without disclosing additional details. Examples of ZKP systems used in DLT are zk-SNARKs (used in Zcash) and zk-STARKs.

2. Confidential transactions: These techniques hide transaction amounts or other sensitive data. Examples include Pedersen commitments and Bulletproofs (used in Monero and Mimblewimble-based protocols).
 355
3. Ring signatures: Ring signatures obscure the sender's identity in a transaction by making it indistinguishable from other users in the same group. An example of a ring signature implementation in DLT is CryptoNote (used in Monero).
 358

These cryptographic techniques and mechanisms form the foundation of security, privacy, and data integrity in DLT systems. As the technology evolves, new cryptographic techniques may be developed and adopted to address emerging challenges and enhance the capabilities of DLT.

3.3.8. Transaction

In DLT, a transaction is an operation or event that involves the transfer or modification of assets, data, or other digital resources within the network. Transactions are the fundamental building blocks of DLT systems, and are used to record and track the history of assets and interactions among network participants, as shown in Figure 2.

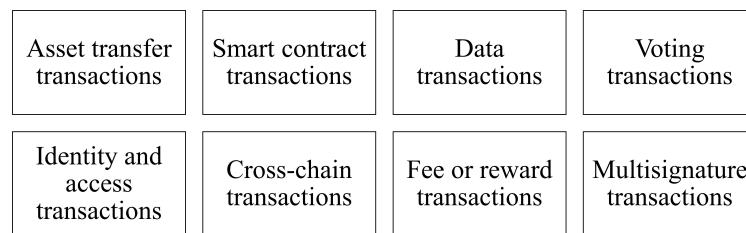


Figure 2. Transaction Types.

3.3.9. Ledger Structure

A DLT's ledger is a data structure that captures transactions and maintains a verifiable record of all network activity. The ledger structure can take various forms, such as a linear blockchain (e.g., Bitcoin, Ethereum) or a Directed Acyclic Graph (DAG), depending on the specific DLT implementation. (e.g., IOTA).

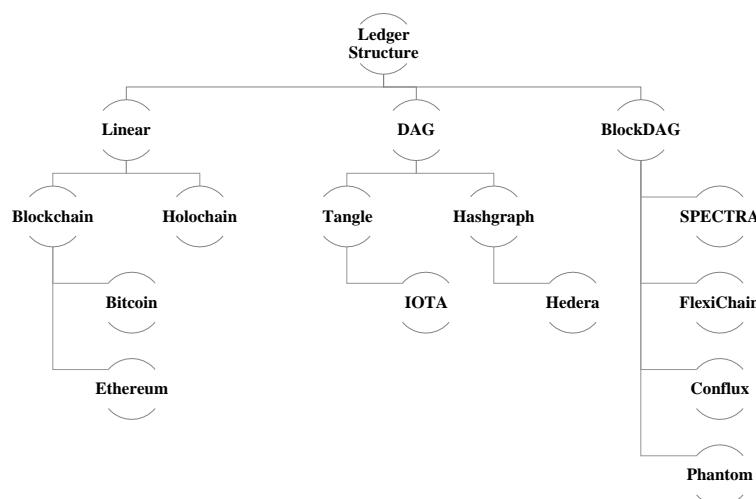


Figure 3. Ledger Structure.

3.3.10. Consensus Algorithms

DLT systems utilize consensus algorithms that enable network members to agree on the validity of transactions for the purpose of maintaining a consistent and secure ledger.

PoW, PoS, and Byzantine Fault Tolerance (BFT) are prevalent consensus mechanisms. Each mechanism has trade-offs regarding security, efficiency, and resource usage. The consensus algorithm is the core of the technology and it is what supports the decentralization nature, increases the security and transparency, and is a key player in network throughput and latency. Table 2 lists some consensus algorithms and their trade-offs.

378
379
380
381
382

Table 2. Comparison of Consensus Algorithms and DLTs.

#	Algorithm/Technology	Pros	Cons
1.	Proof of Work (PoW) [49]	High security, Decentralization	Energy inefficiency, Scalability issues
2.	Proof of Stake (PoS) [50] [51]	Energy efficiency, Faster transactions	Centralization risk, Security concerns
3.	Delegated Proof of Stake (DPoS) [51]	High scalability, Energy efficiency	Centralization risk
4.	Practical Byzantine Fault Tolerance (PBFT) [52]	Fast transactions, High fault tolerance	Limited scalability, Centralization risk
5.	Proof of Authority (PoA) [53]	Fast transactions, Energy efficiency	Centralization risk
6.	Tangle (DAG-based) [54]	Scalability, No transaction fees, Energy efficiency	Vulnerable to spam attacks, Lower security guarantees
7.	Hashgraph [55]	Fast transactions, Fairness, Asynchronous Byzantine Fault Tolerance	Centralization risk, Licensing and patent issues

3.3.11. Nodes and Network Architecture

In a DLT, the ledger is maintained by a network of nodes, or machines, that validate transactions, store the ledger, and communicate with each other. Nodes can have various duties and responsibilities, such as full nodes (which store the entire ledger) and lightweight nodes (which do not store the entire ledger but storing only a subset of the ledger.) The architecture of the network is distributed and decentralized, with no singular point of failure or control.

38
38
4
38
5
38
6
38
7
38
8
38
9

3.3.12. Applications and Use Cases

DLT can be applied to a wide range of industries and use cases, such as finance (cryptocurrencies, remittance, tokenization of assets), supply chain management (provenance tracking, inventory control), healthcare (secure data sharing, patient records), identity management (digital identity, access control), and more.

39
0
391
392
393
394

3.4. DLT-based ITS Related Works

Vehicles become smarter everyday due to the advancement of transportation and communication technology [56]. The blockchain can potentially handle various IoV applications with creative solutions. Most IoV applications are real-time, mobile, and generate and share large amounts of data. In IoV environments, many standard strategies may not work. In addition, increased connectivity may give malevolent actors new attack channels. Blockchain incorporation into the IoV enhances security, privacy, trust, system performance, and automation. Thus, blockchain-like robust technology should be used for flexibility and big data. We list some important incentives for IoV blockchain adoption below. To be considered a “smart city”, a metropolis must have reliable public transportation. Due to the many factors that must be considered to ensure passenger safety, ITS is classified as a Complex Cyber Physical System (CCPS). The term “Internet of Vehicles” refers to the network of vehicles that allows them to share data, conduct analysis, and deliver and receive feedback in a real-time environment [3,4].

39
5
396
397
398
399
400
401
402
403
404
405
406
407
408

The IoV has the potential to become the next decade trend due to advancements in satellite communications, AI and CPS [56,57]. The next decade will see a rise in vehicle automation and intelligence. A small number of initiatives, such as ERTICO ITS Europe and City Verve Manchester, have been launched to aid the development of ITS in smart cities. Depending on the precision of the data and the methods used to regulate traffic, a mountain of information will be generated as the number of vehicles on the road continues to swell. If the operations are conducted using the traditional IoT model, then latency, complexity, and IoV needs will be major obstacles. Compatibility and interoperability across IoV components from different service providers is extremely difficult to guarantee. Data interchange and storage infrastructure must be decentralized, distributed, interoperable, flexible, and scalable to support the growth of IoV and unlock the full potential of ITS. Data security and management, data resource and training, resource sharing, vehicle management, ride sharing, content streaming, traffic control and management, and V2V communication are all areas where DLT could serve as a platform [18].

In [58] a blockchain-based distributed ledger solution for managing data securely within the vehicle edge computing networks using a consortium blockchain was developed. There are two ways in which the use of smart contracts would improve the proposed system. As a first step, the smart contract is utilized to guarantee the integrity of data exchanged between vehicles and the edge computing servers located in vehicles. Second, the smart contract prevents unauthorized disclosure of the data. Hence, vehicles may pick the greatest and most trusted source of high-quality data. The suggested system also includes a mechanism to share data based on its reputation. Taking into account the number of encounters, the timing of occurrences, and the closeness of their trajectories, a three-weight subjective logic model is utilized to manage the reputation of vehicles in a fair and realistic manner. The proposed system can more easily detect vehicles that are maliciously intent on harming others or acting suspiciously with the use of this reputation scheme than with more conventional reputation schemes.

In [59], with the support of a smart contract, physically unclonable functions (PUFs), and a public-key infrastructure, DrivMan was proposed, which is a blockchain-based solution for automobiles that facilitates trust management, data provenance, and privacy via PKI. DrivMan's use of the blockchain allows for distributed trust management even in a partially trusted network. Also, thanks to the PUFs' role in creating a crypto fingerprint for each vehicle, DrivMan can demonstrate the origin of the data. PKI is also used to enable car registration and provide key pairs to automobiles via a Certificate Authority (CA). If necessary, the CA can track down the source of malicious vehicles' certificates and revoke them. The purpose of PKI is to prevent attackers from discovering genuine identities and to safeguard personal information by making it impossible to connect identities to public keys.

The fundamental innovation proposed in [60] is a new method of key negotiation that allows for auditable and verifiable cryptographic signatures. In particular, this strategy aims to address concerns regarding the safety, credibility, and oversight of jointly held information. The approach allows either script-based or static automated key exchange. Because of this, crucial vehicle-to-vehicle communication talks may be completed rapidly and mechanically. Also, the negotiation process prevents a packet-dropping attack from taking place because of its use of preventative measures such as scripts, channels, and scheduling.

Data trading proposed in [61] presents a number of challenges that can be mitigated with the use of the blockchain, including a lack of transparency and traceability as well as the potential for illegal alterations to data. To audit and verify transactions, a group of regional aggregators collaborates like a consortium. To further ensure that societal utility is maximized, data is sold at the optimal price, and individual privacy is safeguarded for both buyers and sellers, an iterative double auction method is employed. More people will share information as a result of this. The system is made more reliable by also factoring in

the price of transferring data. Resource sharing between cars is another application of this technology.

The solutions proposed in [62] are ensuring that bids are transparent and are allowing buyers and sellers to engage in resource trading. A broker is proposed here as a means of maintaining the market for trade. The broker then determines the quantity of resources being traded and devises a price rule to induce truthful bidding from buyers and sellers. An iterative two-sided auction is the process proposed here. Therefore, it is the most fiscally responsible, sensible, and socially beneficial option.

The Device-to-Device Edge Computing and Networks (D2D-ECN) in [63] utilizes blockchain technology, smart contracts, edge computing, and device-to-device connectivity to facilitate asset trade and the distribution of work. When completed, D2D-ECN will serve as a shared environment for developing high-performance and low-latency applications together. This ensures that real-time application scenarios can be handled fast by offloading the computing responsibilities. Swarm intelligence is used to devise a method of work allocation that minimizes both delay and processing time. While addressing the problem of poorly managed resources, it also helps to establish trust between those who supply resource services and those who need them to complete their work. For devices with fewer resources, the proof-of-work consensus technique is replaced with proof-of-reputation. With this setup, only the user with the greatest reputation value can pack resource transactions. The blockchain serves as the repository for the reputation values. Each entity's reputation value is calculated by factoring in both its recent and past achievements. The players are rewarded by a game-theory-based process.

The study in [64] details a blockchain-based system that safeguards the anonymity of automobile drivers when they look for, and reserve parking spots in advance. The usage of blockchain technology is proposed in this proposal as a means of avoiding the drawbacks of centralization. The blockchain cannot function without the cooperation of parking lot owners, even though they may not trust one another. They may include information on parking deals, for instance. Then, the blockchain will serve as a permanent record of all open offers. The private information retrieval (PIR) approach is utilized alongside the blockchain to conceal drivers' whereabouts. When using PIR, drivers can look for parking information in the blockchain without disclosing their intended destination. After receiving a parking offer through the blockchain network, the driver can confirm the reservation with the parking owner in a way that protects their anonymity by using a short, randomizable signature. However, the trusted authority will be able to identify the genuine drivers and take appropriate action, if necessary, because of this signature's short length and randomizability. It is also proposed that drivers have the option of making payments anonymously rather than using conventional card payment systems, which could potentially expose their personal information. A comparative view of these works is presented in Table 3.

4. Proposed FlexiChain 3.0: DLT based V2V

DLT has been proposed as a solution to multiple challenges in various applications. In this section, the DLT will be proposed as a solution to fulfill the requirements of ITS-IoV. DLT has secured operations due to its architecture and distributed form since it relies on the nodes and not a central authority. Also, securing assets and eliminating malicious behavior is proved through some established distributed ledger networks that have been operating for several years. Nodes are independent in distributed networks, but different methods are used to track the updated state of a ledger or a digital asset. The ledger is distributed, which means each node has its own copy which reduces security threats if this technology is used in ITS.

In this paper, it is assumed that trusted manufacturers are producing Trusted Modules which in this case will contain vehicle keys. These entry keys are linked to each other and are contained in a NodeChain Assisted Distributed Offline Vault that unifies and secures the vehicles' identities [20]. Surface Zones are represented in this work as a blockchain for

Table 3. A Comparative Perspective of DLT Based Previous Works

Decentralized Applications (Dapps)	DLT Type	Consensus Algorithm	Resources Requirements	Contributions
Kang et al. 2019 [58]	Consortium Blockchain	Proof of Work (PoW)	High	Blockchain based data management using smart contract
Javaid et al. 2019 [59]	Public Blockchain	Proof of Work	High in RSU, Low in IVs	Blockchain based trust management and data exchange using smart contract
Chen et al. 2019 [61]	Consortium Blockchain	Proof of Work (PoW)	High in Edge Layer, Low in Vehicles Layer	Vehicle data trading blockchain based
Zichichi et al. 2020 [65]	Permissionless DLT	IOTA Proof of Work	Medium/Low	Data Management and services decentralized framework using IOTA as a distributed ledger, Ethereum Virtual Machine smart contracts and distributed database such IPFS
Maffiola et al. 2022 [66]	Consortium Blockchain	Proof of Stake (PoS) & PBFT	Medium	Blockchain data collection framework

each zone, and all blockchains are strongly linked through FlexiChain, which represents Layer0 for all blockchains. 515
516
517
518
519

FlexiChain 3.0 Technology could provide a solid ledger for ITS due to its multiple features that have been designed to target this type of application using multiple blockchains as multiple areas that cars drive through. Each car can operate in every zone due to the flexibility of Layer0 which provides to the network one-time registration. Nodes in this application represent cars, stations, towers, trucks, etc. 520
521
522
523
524
525
526
527
528
529
530

FlexiChain 3.0 is a Layer0 ledger that uses BlockDAG structure to build its ledger. It uses Proof of Rapid Authentication (PoRa) as its consensus algorithm that relies on trusted module authentication and lightweight computation. FlexiChain 3.0 uses NodeChain for its authentication process from which the network security independence increase. NodeChain is an integrated ledger initiated with the network and used to mirror nodes and secure their manufacturers' specification and an agreement reached among stakeholders to add a device to create its correspondent Trusted ID (TUID) which is used in the operations of Layer0 that is represented here as zones. 531
532
533
534
535

4.1. FlexiChain 3.0 Layer0 (Zones)

In this section, the Zones component of the FlexiChain based proposed framework of Peer to Peer (P2P) communication system is explained and illustrated in Figure 4. In this framework, the area of the proposed application is divided into zones each of which has its own blockchain and is connected with Layer0 FlexiChain. Each blockchain has a block type and is defined to all vehicles entry keys (trusted modules). 536
537
538
539
540

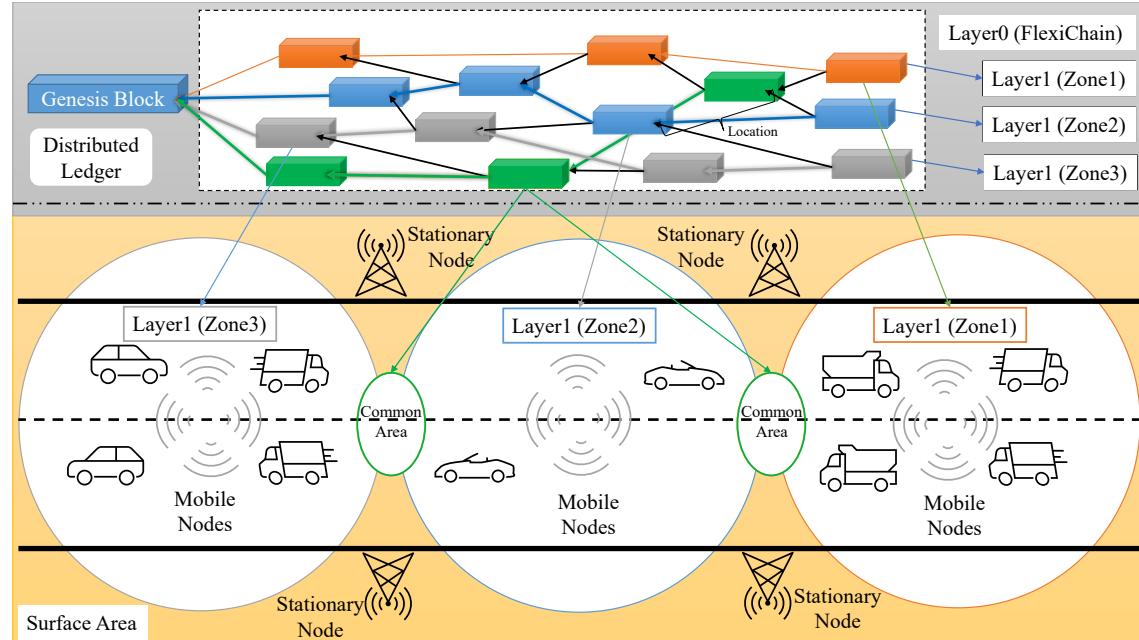


Figure 4. Zones and their Corresponding FlexiChain Ledger.

4.2. Block Types (Digital Assets Collected & Exchanged)

This section shows the contents of each block. All zones have the same block structure, but are labeled differently to append to the location specified. The block contains the header which is the hash value of all comprised data. The source TUID is included to be authenticated. The data are collected from the car or its environment. The distance from the genesis block is based on the location chosen. Minimal distance is used to get the shortest way to genesis if block reduction is needed. Lastly, the chain of narration is used to list all nodes that have confirmed this block to present block authenticity within the FlexiChain. Block content and types are presented in Figure 5.

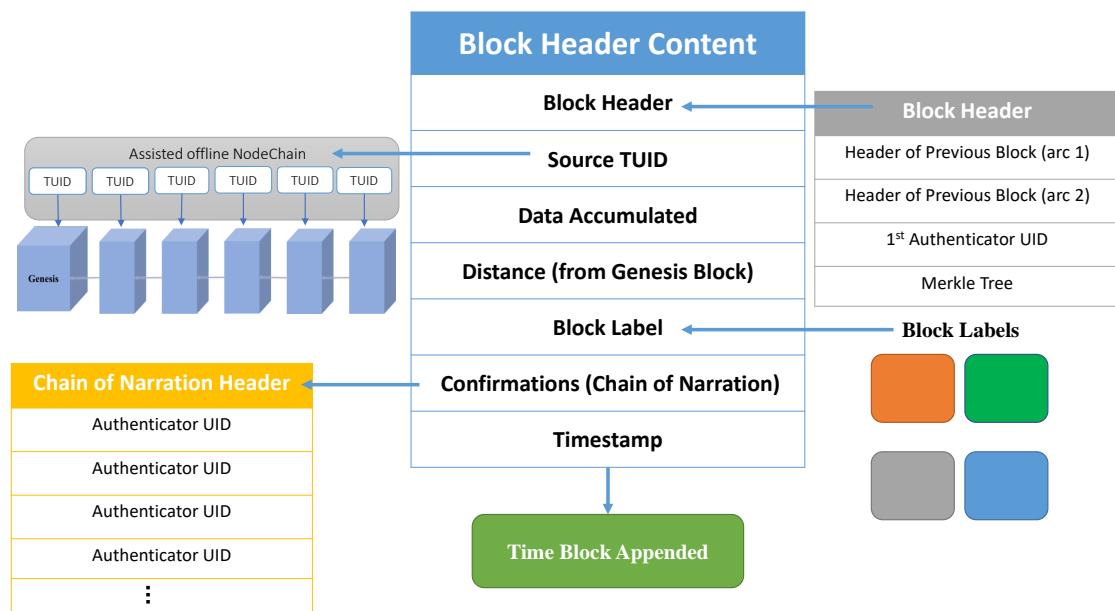


Figure 5. Block Content of Each Zone and its Labels.

4.3. Node Types (V2V Participant Authority Levels)

There are three types of nodes:

536
537
538
539
540
541
542
543
544

545
546

1. The Backup Node (BN) is the network's "cloud", or original node. In NodeChain [20], the first block represents the virtual existence of a backup node. 547
2. Vehicles or fixed Stations are classified as edge node and they are full nodes and have 549
a full ledger. 550
3. CPS and IoT nodes or subscriber nodes are used for data collection and transmission. 551
Since this technology is aiming for restricted nodes, a node that is both IoT and CPS 552
could qualify based on the requirements. These represents sensors and actuators in 553
the proposed framework. 554

4.4. Trusted Modules (Vehicles Entry Keys)

Trusted modules in this proposed framework are the vehicles' entry keys. The keys are manufactured with a built in signature generator, and a copy of the NodeChain which gives each car access to the NodeChain assisted distributed offline vault for rapid authentication. The initial registration process runs through the manufacturers as the stakeholders of the network. The modules provide an extra level of security to compensate the low computation required to append a block. Once this key is inserted to the car or identifies the signal of the car, the data collected by the car sensors and actuators are collected and broadcast to the ledger.

4.5. NodeChain Assisted Distributed Offline Vault (Vehicles Digital Unique Identity Aggregator)

NodeChain [20] is formed and built by the registration process. It has all nodes' TUID and these TUID are a tokenized version of the real UID that is assigned by the manufacturer and registered in the NodeChain, as shown in Figure 6. Only the vehicle's entry keys can be accessed and with its own signature the real UID can matched (Figure 7).

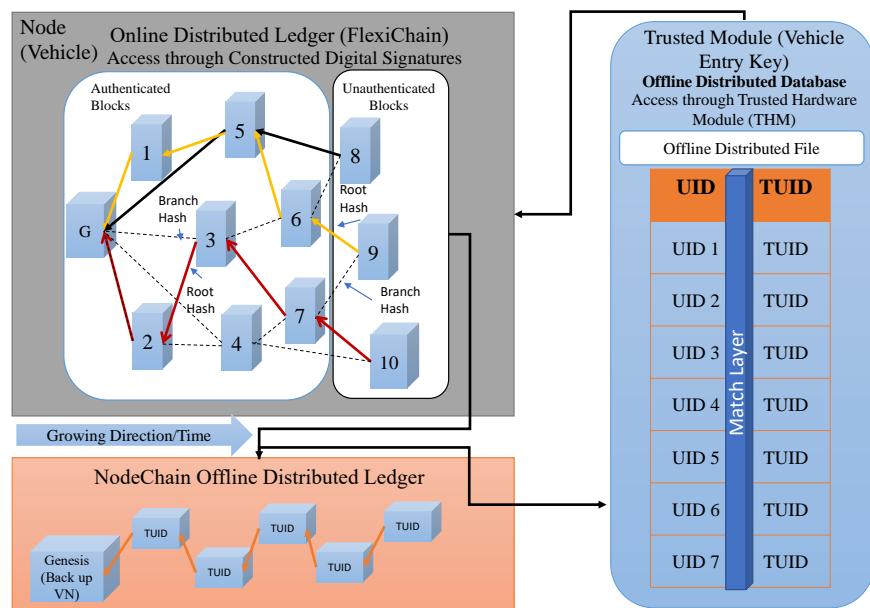


Figure 6. NodeChain Offline Vault.

4.6. NodeChain Proof of Rapid Authentication (Lightweight Consensus)

569

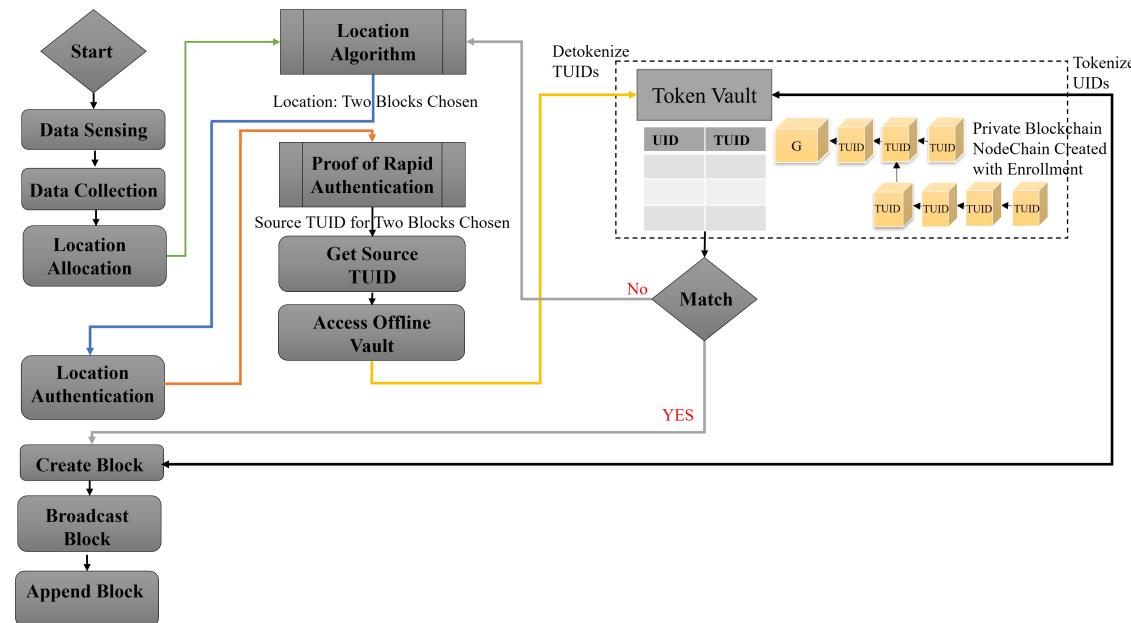


Figure 7. NodeChain Proof of Rapid Authentication.

570

5. Experimental Results

571

5.1. Time Analysis

572

5.1.1. Setup

573

64 nodes of each technology have been created and run for 30 minutes, as detailed in Table 4. Docker containers have been used to host each node and peer with the second node.

574

Table 4. Setup Components.

Number of Nodes	Size of Block	Up Time (s)
64	32 * 1024 bytes	1800

575

Nodes directly send blocks to each other. FlexiChain has been implemented using Python and PostgreSQL and running through docker containers. The network starts by running the BN. The regular nodes join after NodeChain has initialized. The initialization sequence of the network is shown in Figure 8. A performance analysis is shown in Table 5 and a real-time graph of authentication activity is shown in Figure 9.

576

577

578

579

Table 5. FlexiChain Technology Number of Transactions/Second

Nodes	Total Number of Blocks	Trxs/second (Average)
64	4158	2.3

580

5.2. Security And Privacy Analysis

581

FlexiChain Technology is built with CPS applications in mind, therefore security measures are built in at both the hardware and software levels. Researchers may assess the efficacy of the technique by simulating a variety of security threats [16]. Such attacks include corrupting the exchanged data between nodes, implanting incorrect data during communication, and full malicious control over the network authority. The feasibility that each attack can take place will be calculated and compared to each other for each scenario

582

583

584

585

586

587

```

===== Starting Regular Node-1 container =====
25aac22a7908b9e44d16e60b4bbda22763059bc7555bea2f7cbee54a23141e08
===== Regular container started =====

===== Starting Regular Node-2 container =====
dcae1c5ab3146ca31c3da5ce11824e8435b3de8166068f0c6d13d5b80063c46d
===== Regular container started =====

===== Starting Regular Node-3 container =====
ad4725983d0548ac1e7b0483e6b561a33cf13cd657c41d173aec3fb8390e19eb
===== Regular container started =====

===== Starting Regular Node-4 container =====
a5daae0cf49d842a6e89def44c4c075f721868ae9e099815484f6dc3bd12013
===== Regular container started =====

===== Starting Regular Node-5 container =====
1d14ba9c35999d2b46d9ef4ef9ae17db6b3dcc94be663b026b431b3ce7fb7db3
===== Regular container started =====

===== Starting Regular Node-6 container =====
3a7b318f703ba999694d16c05d3fa1754ef65451ac7ce09366755a44d743fe41
===== Regular container started =====

===== Starting Regular Node-7 container =====
fdfc01fa526c8afa5b0d12a0e9b60b2a22288c9c5ca6f34be499f87bec1a1577
===== Regular container started =====

===== Starting Regular Node-60 container =====
cd76abcdfc26e877ed7d8ebb9c6cab9ad1767cd7aeb295cdb3c3f5e78e151fb
===== Regular container started =====

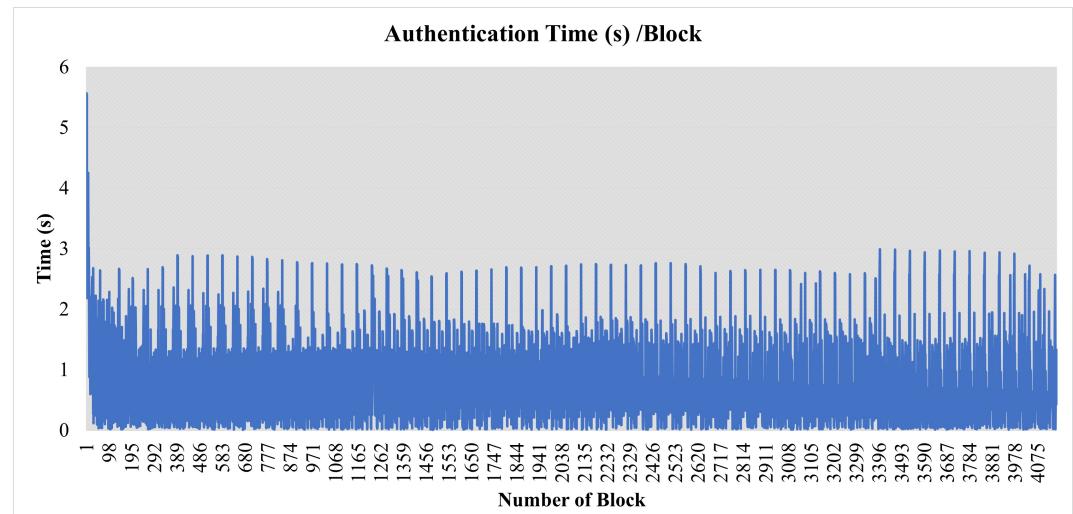
===== Starting Regular Node-61 container =====
d2fb452e9f83e5071a0307edc9d2d8cee62a52e50f2209832cb7af5a365c14
===== Regular container started =====

===== Starting Regular Node-62 container =====
c5b283b4e20132255da9ec1222bc18292b19df110a6f484fa1851b4c9f55b61
===== Regular container started =====

===== Starting Regular Node-63 container =====
970f169650a4fc2745acffb59fc02dc1469144a46336af31c478d653e44773c
===== Regular container started =====

===== Starting Regular Node-64 container =====
6e425e9d2bbd17810f88c590857aecf3e83943dadd45b29d6c6df1b1d3904603
===== Regular container started =====

```

Figure 8. 64 FlexiChain Nodes Registered.**Figure 9.** Nodes Containers on Docker.

[16]. Three scenarios are proposed: traditional central authority, blockchain technology and FlexiChain technology for the listed attacks below:

1. **Attack-1: Data Corruption:** For this attack, the digital assets exchanged among participants will be corrupted.
2. **Attack-2 Implant Incorrect Data:** For this attack, malicious activity by implanting incorrect data takes place while transacting data.
3. **Attack-3: Central Authority Full Malicious Control:** For this attack, maliciously expose the authority database.

5.2.1. Traditional Central Paradigm

The probability of the attacks to occur in the central paradigm ($P(TC)$) is given by:

$$P(TC) = P(A) + P(B) + P(C) \quad (1)$$

$P(A)$ represents attack-1 and can be done by a successful attack over all edge nodes and represented as $\alpha\kappa$. The probability can be calculated by

$$P(A) = \frac{1}{4} \prod_{\kappa=1}^n \alpha\kappa \quad (2)$$

$P(B1)$ represents attack-2 and can be done by a successful attack over the transmission channels between edge nodes and central node represented as $\beta\kappa$. The probability can be calculated by

$$P(B1) = \frac{1}{4} \prod_{\kappa=1}^n \beta\kappa \quad (3)$$

The corresponding transmission channels are also considered in the formula which can be calculated similar to $P(B1)$ and calculated by $P(B2)$.

$$P(B2) = \frac{1}{4} \prod_{\kappa=1}^n \beta\kappa \quad (4)$$

$P(C)$ represents attack-3 and can be done by a successful attack over a central node represented as ρ . The probability can be calculated by

$$P(C) = \frac{1}{4}\omega \quad (5)$$

From Equations 1-4 we obtain the total probability:

$$P(TC) = \frac{1}{4} \prod_{\kappa=1}^n \alpha\kappa + \frac{1}{4} \prod_{\kappa=1}^n \beta\kappa + \frac{1}{4} \prod_{\kappa=1}^n \beta\kappa + \frac{1}{4}\omega \quad (6)$$

This is shown as a function of the number of nodes in Figure 10 along with the parameters of an exponential fit of the data.

5.2.2. Blockchain

The probability of the attacks to occur in the blockchain paradigm is

$$P(BC) = P(A) + P(B) + P(C) \quad (7)$$

$P(A)$ represents attack-1 and can be done by a successful attack over all nodes $\alpha\kappa$ and acquiring nodes' credentials represented as $\theta\kappa$. The probability can be calculated by

$$P(A) = \frac{1}{4} \prod_{\kappa=1}^n \alpha\kappa \times \frac{1}{4} \prod_{\kappa=1}^n \theta\kappa \quad (8)$$

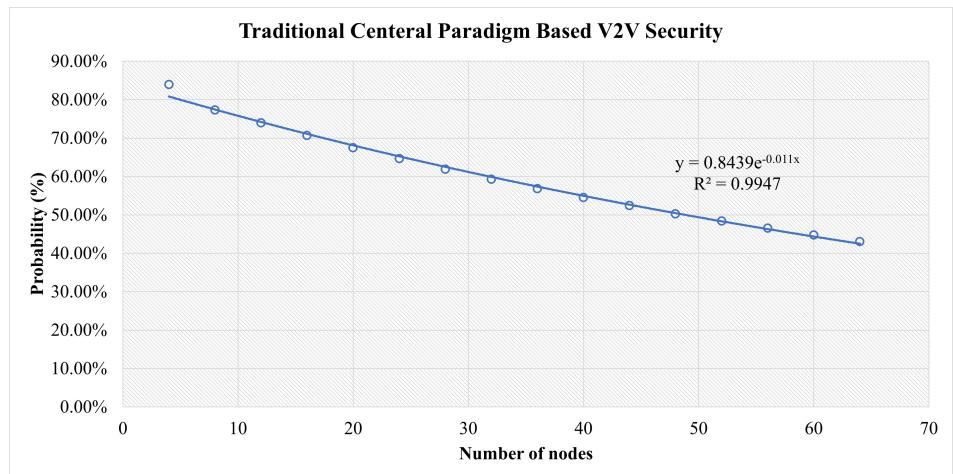


Figure 10. Results for all 3 Categories of Attacks in the Traditional Central Based V2V Scenario

$P(B1)$ represents attack-2 and can be done by a successful attack over nodes and acquiring nodes' credentials represented as $\theta\kappa$. There is $\frac{n \times (n-1)}{2} = a$, which is the number of transmissions channels represented as $\beta\kappa$ can be created by pairs of nodes for n nodes [16]. The probability can be calculated by

$$P(B1) = \frac{1}{4} \prod_{\kappa=1}^a \beta\kappa \times \frac{1}{4} \prod_{\kappa=1}^n \theta\kappa \quad (9)$$

The corresponding transmission channels are also considered in the formula which can be calculated similar to $P(B1)$ and denoted as $P(B2)$.

$$P(B2) = \frac{1}{4} \prod_{\kappa=1}^a \beta\kappa \times \frac{1}{4} \prod_{\kappa=1}^n \theta\kappa \quad (10)$$

$P(C)$ represents attack-3 and can be done by a successful attack over all edge nodes $\rho\kappa$ and acquiring nodes' credentials represented as $\theta\kappa$. There are $\frac{n}{2} = v$, which is the number of mining nodes or validators (edges) that an attacker should control to compromise the ledger. The probability can be calculated by

$$P(C) = \frac{1}{4} \prod_{\kappa=1}^v \rho\kappa \times \frac{1}{4} \prod_{\kappa=1}^n \theta\kappa \quad (11)$$

$$\begin{aligned} P(BC) = & \frac{1}{4} \prod_{\kappa=1}^n \alpha\kappa \times \frac{1}{4} \prod_{\kappa=1}^n \theta\kappa \\ & + \frac{1}{4} \prod_{\kappa=1}^a \beta\kappa \times \frac{1}{4} \prod_{\kappa=1}^n \theta\kappa \\ & + \frac{1}{4} \prod_{\kappa=1}^a \beta\kappa \times \frac{1}{4} \prod_{\kappa=1}^v \rho\kappa \\ & + \frac{1}{4} \prod_{\kappa=1}^v \rho\kappa \times \frac{1}{4} \prod_{\kappa=1}^n \theta\kappa \end{aligned} \quad (12)$$

This is shown as a function of the number of nodes in Figure 11 along with the parameters of an exponential fit of the data.

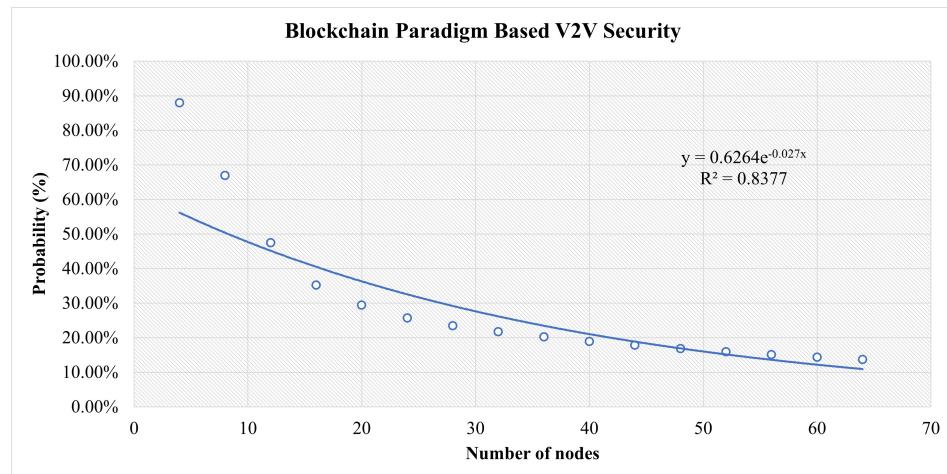


Figure 11. Results for 3 Categories of Attacks in the Blockchain Based Scenario

5.2.3. FlexiChain

The probability of the attacks to occurs in the blockchain paradigm is

$$P(FC) = P(A) + P(B) + P(C) \quad (13)$$

$P(A)$ represents attack-1 and can be done by a successful attack over all nodes $\alpha\kappa$, acquiring nodes' credentials represented as $\theta\kappa$, acquiring trusted attached hardware credentials, and Unique Identification (UID). The probability can be calculated by

$$P(A) = \frac{1}{4} \prod_{\kappa=1}^n \alpha\kappa \times \frac{1}{4} \prod_{\kappa=1}^n \theta\kappa \times \frac{1}{4} \prod_{\kappa=1}^n \phi\kappa \times \frac{1}{4} \prod_{\kappa=1}^n \Phi\kappa \quad (14)$$

$P(B1)$ represents attack-2 and can be done by a successful attack over all nodes $\alpha\kappa$ and acquiring nodes' credentials represented as $\theta\kappa$. There are $\frac{n \times (n-1)}{2} = a$, which is the number of transmissions channels can be created by pairs of nodes for n number of nodes [16]. The probability can be calculated by

$$P(B1) = \frac{1}{4} \prod_{\kappa=1}^a \beta\kappa \times \frac{1}{4} \prod_{\kappa=1}^n \theta\kappa \times \frac{1}{4} \prod_{\kappa=1}^n \phi\kappa \times \frac{1}{4} \prod_{\kappa=1}^n \Phi\kappa \quad (15)$$

The corresponding transmission channels are also considered in the formula which can be calculated similar to $P(B1)$ and denoted as $P(B2)$.

$$P(B2) = \frac{1}{4} \prod_{\kappa=1}^a \beta\kappa \times \frac{1}{4} \prod_{\kappa=1}^n \theta\kappa \times \frac{1}{4} \prod_{\kappa=1}^n \phi\kappa \times \frac{1}{4} \prod_{\kappa=1}^n \Phi\kappa \quad (16)$$

$P(C)$ represents attack-3 and can be done by a successful attack over all nodes $\rho\kappa$ and acquiring nodes' credentials represented as $\theta\kappa$. There are $\frac{n}{2} = v$, which is the number of mining nodes or validators (edges) that an attacker should control to compromise the ledger. The probability can be calculated by

$$P(C) = \frac{1}{4} \prod_{\kappa=1}^v \rho\kappa \times \frac{1}{4} \prod_{\kappa=1}^n \theta\kappa \times \frac{1}{4} \prod_{\kappa=1}^n \phi\kappa \times \frac{1}{4} \prod_{\kappa=1}^n \Phi\kappa \quad (17)$$

$$\begin{aligned}
 P(FC) = & \frac{1}{4} \prod_{\kappa=1}^n \alpha \kappa \times \frac{1}{4} \prod_{\kappa=1}^n \theta \kappa \times \frac{1}{4} \prod_{\kappa=1}^n \phi \kappa \times \frac{1}{4} \prod_{\kappa=1}^n \Phi \kappa \\
 & + \frac{1}{4} \prod_{\kappa=1}^a \beta \kappa \times \frac{1}{4} \prod_{\kappa=1}^n \theta \kappa \times \frac{1}{4} \prod_{\kappa=1}^n \phi \kappa \times \frac{1}{4} \prod_{\kappa=1}^n \Phi \kappa \\
 & + \frac{1}{4} \prod_{\kappa=1}^a \beta \kappa \times \frac{1}{4} \prod_{\kappa=1}^n \theta \kappa \times \frac{1}{4} \prod_{\kappa=1}^n \phi \kappa \times \frac{1}{4} \prod_{\kappa=1}^n \Phi \kappa \\
 & + \frac{1}{4} \prod_{\kappa=1}^v \rho \kappa \times \frac{1}{4} \prod_{\kappa=1}^n \theta \kappa \times \frac{1}{4} \prod_{\kappa=1}^n \phi \kappa \times \frac{1}{4} \prod_{\kappa=1}^n \Phi \kappa
 \end{aligned} \tag{18}$$

This is shown as a function of the number of nodes in Figure 12 along with the parameters of an exponential fit of the data.

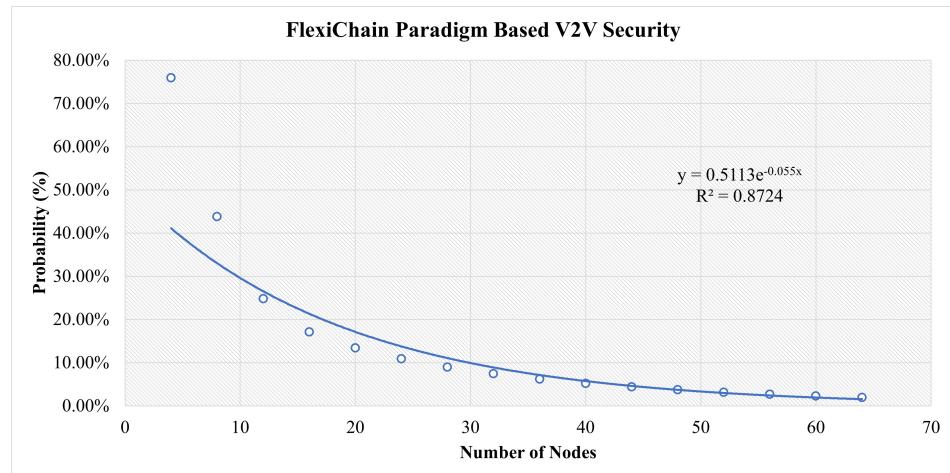


Figure 12. Results for 3 Categories of Attacks in the FlexiChain Based Scenario

5.3. Comparative Analysis of FlexiChain 3.0

A comparative analysis of the three types of DLT examined in this work is given in Table 6.

Table 6. Comparison Between Central Versus Blockchain Versus FlexiChain

Attack Type	Central Based V2V	Blockchain Based V2V	FlexiChain Based V2V
Attack-1 (A)	Equation 2: 1 security factor	Equation 8: 2 security factor	Equation 14: 4 security factors
Attack-2 (B)	Equations 3 & 4: transmission channel between server and edge nodes	Equations 9 & 10: transmission channels combinations between 2 nodes. Creates more channels to be compromised which increased cost for adversary	Equations 15 & 16: transmission channel combinations between 2 nodes. Creates more channels to be compromised which increase cost for adversary
Attack-3 (C)	Equation 5: 1 authority capacity	Equation 11: Validators = Authority Capacity	Equation 17: All = authority capacity

A simulation has been done over the Equations 6, 12, and 18. For factors α, θ, ϕ , and Φ , values in the (0.9-1) range are assumed and will be assigned for each based on the difficulty of an attack [16]. For ω , it is assumed a value of (0-0.1) will be assigned [16]. The number of nodes are chosen to be 4 to 64.

It is seen from Equations 6, 12 and 18 that FlexiChain has more security layers, which would make any malicious attack very expensive. Also, another factor is the number of nodes that play a major role in the feasibility of an attack. The more the nodes required, the less vulnerable is the network (Table 7).

In Figure 13, in the early stages, all scenarios are at high risk. However, the more nodes join the network the more stable it becomes. The traditional central scenario needs a huge

Table 7. Comparative Analysis Between Central Versus Blockchain Versus FlexiChain: This table shows the probabilities acquired from our the security analysis for 3 categories attacks for three scenarios.

Number of Nodes	Central (%)	Blockchain (%)	FlexiChain (%)
4	84%	87%	76%
24	65%	26%	11%
44	52%	18%	4%
64	43%	14%	2%

Table 8. Quality of Regression of Attack Success Probability to $P = a \exp bx$.

Figure	a	b	R^2
Figure 10	0.84	0.011	0.99
Figure 11	0.62	0.027	0.837
Figure 12	0.51	0.055	0.872

number of nodes to reach a stable security and for our simulation for the highest number of nodes used, it reaches 43% security vulnerability to attacks. For Blockchain Based V2V, the same factors play role. However, the decentralization and distributed authority have reduced the risk to less than 14% at a secure stage. In FlexiChain, based on the multiple factors as shown in Table 6, the security risk level has been further reduced from an earlier stage due to fairness of authority distribution, complete decentralization, and the extra security layers.

However, up to some stages the curve will run close to zero in blockchain and FlexiChain, as shown in Figures 10, 11, and 12. All curves follow an exponential decay that declines toward zero. However, in blockchain and FlexChain it is obvious that the dependency is lower since the network has more security factors, as shown in Table 6. Also, the threat level decreases faster in FlexiChain than the blockchain due to more security levels. A comparative perspective with previous works is given in table 9.

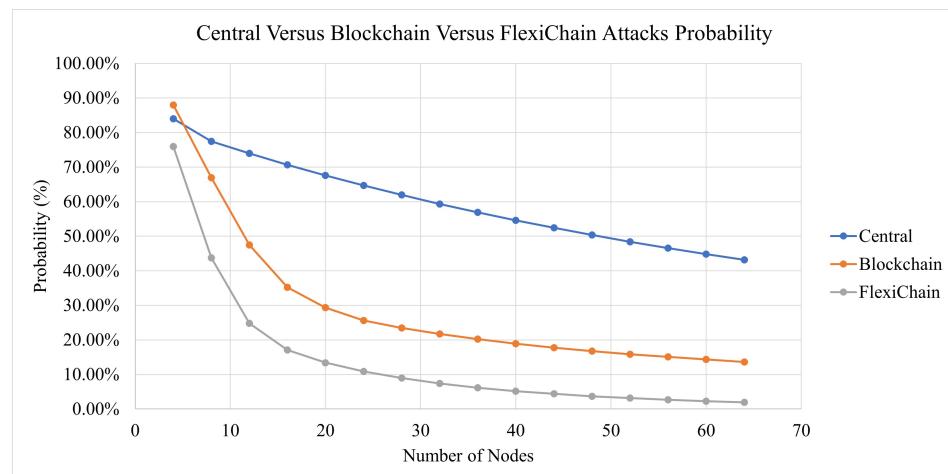


Figure 13. Chart Comparison Between Central, Blockchain and FlexiChain

Table 9. A Perspective Comparative of the Proposed Consensus Algorithm with Related Works

Consensus Algorithm	Ledger	Tolerance	DLT Type	Trust Type
Proof of Work (PoW) [67]	Full	<25%	Public/Permissionless	No Trust
Proof of Stake (PoS) [67]	Full	<51%	Public/Permissionless	No Trust
Byzantine Fault Tolerance (BFT) [68]	Full	<33.3%	Private/Permissioned	Trust
Federated BFT (FBFT) [69]	Full	<33.3%	Private/Permissioned	Trust
Practical BFT (PBFT) [69]	Full	<33.3%	Private/Permissioned	Trust
Proof of Authority (PoA) [70] [71]	Full	<51%	Public/Permissioned	Trust
NPoRa figure 7 (Current)	Portion/Full	<100%	Public/Permissioned	Manufacturing Trust

Table 10. Comparative Analysis Between Current Consensus Algorithm with Related Works

Attributes	PoW	PoS	DPoS	LPoS	PoI	PoA	PoET	PoB	PoC	BFT	PBFT	Tangle	NPoRa
Hardware Requirements	H	M	M	M	M	M	M	M-H	M	M	M	L-M	L-M
Pre-Trust Level	L	M	M	M	M	H	M	M	M	H	H	M	L-M
Tolerance Level	M	M	M	M	M	H	M	M	M	H	H	L-M	H
Overhead Computation	H	M	L	M	M	L	L	M	M	M	M	L	L
Centralization Level	M	M	M	M	M	H	M	M	M	H	H	M-H	L
Scalability Level	M	M	M	M	M	H	M	M	M	H	H	H	H
Latency Level	M	M	M	M	M	H	M	M	M	H	H	L	L-M
Cost Level	M	M	M	M	M	H	M	M	M	H	H	M	L
Security Level	M	M	M	M	M	H	M	M	M	H	H	M	H
ITS Compatibility	L	L	L	L	L	L-M	L	L	L	L-M	M-H	H	H

Definitions: H: High M: Moderate L: Low. Definitions: Pre-hardware requirements: The necessary computing resources, components, and infrastructure that a node must possess to participate effectively in the network. Pre-trust level: The inherent trust assumptions or level of trust required for each consensus mechanism to function properly. Tolerance level: The resilience and adaptability of a consensus mechanism under various adversarial conditions or system failures. Overhead computation: The additional processing effort or resources required by nodes to participate in the consensus process and maintain the network. Centralization level: The degree to which control, decision-making power, and resources are concentrated within a network. Scalability level: The ability of a network to handle an increasing number of transactions and participants while maintaining acceptable performance levels. Latency level: The amount of time it takes for a transaction to be processed, confirmed, and added to the ledger. Cost level: The various expenses associated with operating, maintaining, and participating in a network. Security level: The ability of a network to protect itself from various threats, such as cyber-attacks, fraud, and manipulation.

6. Conclusions and Future Directions

ITS, the IoV, and VANETs can be transformed by DLT. A DLT's decentralization, transparency, security, and immutability can help stakeholders address data sharing, trust management, and privacy issues in these networked systems.

DLT can create secure data sharing platforms, efficient payment systems, and decentralized marketplaces for vehicle digital assets and services in ITS, IoV, and VANETs. Smart contracts automate processes, improving stakeholder transactions.

Despite its promise, DLT implementation in ITS, IoV, and VANETs must address scalability, latency, energy efficiency, and privacy issues. DLT's full potential in establishing intelligent, safe, and sustainable transportation systems in smart cities depends on further research and development in these areas and the deployment of proper consensus algorithms and blockchain platforms.

FlexiChain Technology 3.0 has been proposed as an ITS platform that could provide safe and secure operation, and a scalable architecture that could match the expected operation volumes in the IoV. FlexiChain 3.0 achieved 2.3 trx/s which is not an optimal target but adequate to serve IoV. However, these results provide motivation to optimize the implementation and reduce latency by using better mechanisms to elect a block location. Security analysis has been introduced to show that the security measures used in FlexiChain were a match to the ones used in the blockchain. The difference is that FlexiChain is BlockDAG and its highest security is achieved early stages.

The integration between DLTs and AI will complete the missing pieces of both technologies. AI is a future target to integrate FlexiChain with Deep Reinforcement Learning models for better authority distribution and autonomous authentication.

The next mode of transportation, the Decentralized Intelligent Transportation System (DITS), is still in its infancy. Research into self-driving cars has begun at several universities and businesses, indicating that the suggested work will be needed in the not too distant future. Vehicle-to-vehicle communication is expected to speed up the development of autonomous vehicles.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

References

1. Mallikarjuna, G.C.P.; Hajare, R.; Mala, C.S.; Rakshith, K.R.; Nadig, A.R.; Prtathana, P. Design and implementation of real time wireless system for vehicle safety and vehicle to vehicle communication. In Proceedings of the 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT), 2017, pp. 354–358. <https://doi.org/10.1109/ICEECCOT.2017.8284527>.
2. Jabbar, R.; Dhib, E.; Said, A.B.; Krichen, M.; Fetais, N.; Zaidan, E.; Barkaoui, K. Blockchain Technology for Intelligent Transportation Systems: A Systematic Literature Review. *IEEE Access* **2022**, *10*, 20995–21031. <https://doi.org/10.1109/ACCESS.2022.3149958>.
3. Tanwar, S.; Tyagi, S.; Budhiraja, I.; Kumar, N. Tactile Internet for Autonomous Vehicles: Latency and Reliability Analysis. *IEEE Wireless Communications* **2019**, *26*, 66–72. <https://doi.org/10.1109/MWC.2019.1800553>.
4. Dai, Y.; Xu, D.; Maharjan, S.; Qiao, G.; Zhang, Y. Artificial Intelligence Empowered Edge Computing and Caching for Internet of Vehicles. *IEEE Wireless Communications* **2019**, *26*, 12–18. <https://doi.org/10.1109/MWC.2019.1800411>.
5. Lamssaggad, A.; Benamar, N.; Hafid, A.S.; Msahli, M. A Survey on the Current Security Landscape of Intelligent Transportation Systems. *IEEE Access* **2021**, *9*, 9180–9208. <https://doi.org/10.1109/ACCESS.2021.3050038>.
6. Chen, J.; Mao, G. Secure Message Dissemination in Vehicular Networks: A Topological Approach. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), 2018, pp. 1–7. <https://doi.org/10.1109/GLOCOM.2018.8647910>.
7. Zheng, K.; Zheng, Q.; Chatzimisios, P.; Xiang, W.; Zhou, Y. Heterogeneous Vehicular Networking: A Survey on Architecture, Challenges, and Solutions. *IEEE Communications Surveys & Tutorials* **2015**, *17*, 2377–2396. <https://doi.org/10.1109/COMST.2015.2440103>.
8. Karagiannis, G.; Altintas, O.; Ekici, E.; Heijenk, G.; Jarupan, B.; Lin, K.; Weil, T. Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions. *IEEE Communications Surveys & Tutorials* **2011**, *13*, 584–616. <https://doi.org/10.1109/SURV.2011.061411.00019>.
9. Queiroz, A.; Oliveira, E.; Barbosa, M.; Dias, K. A Survey on Blockchain and Edge Computing applied to the Internet of Vehicles. In Proceedings of the 2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2020, pp. 1–6. <https://doi.org/10.1109/ANTS50601.2020.9342818>.
10. Limbasiya, T.; Das, D. Secure message transmission algorithm for Vehicle to Vehicle (V2V) communication. In Proceedings of the 2016 IEEE Region 10 Conference (TENCON), 2016, pp. 2507–2512. <https://doi.org/10.1109/TENCON.2016.7848485>.
11. Yu, S.; Lee, J.; Park, K.; Das, A.K.; Park, Y. IoV-SMAP: Secure and Efficient Message Authentication Protocol for IoV in Smart City Environment. *IEEE Access* **2020**, *8*, 167875–167886. <https://doi.org/10.1109/ACCESS.2020.3022778>.
12. Dutta, S. An overview on the evolution and adoption of deep learning applications used in the industry. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* **2017**, *8*. <https://doi.org/10.1002/widm.1257>.
13. Xie, J.; Tang, H.; Huang, T.; Yu, F.R.; Xie, R.; Liu, J.; Liu, Y. A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. *IEEE Communications Surveys and Tutorials* **2019**, *21*, 2794–2830. <https://doi.org/10.1109/COMST.2019.2899617>.
14. Barron, L. The Road to a Smarter Future: The Smart City, Connected Cars and Autonomous Mobility. In Proceedings of the 2021 26th International Conference on Automation and Computing (ICAC), 2021, pp. 1–6. <https://doi.org/10.23919/ICAC50006.2021.9594125>.

15. Zhang, S.; Wu, Y.; Wang, Y. An embedded Node Operating System for real-time information interaction in Vehicle-to-Vehicle communication. 2016, pp. 887–892. <https://doi.org/10.1109/ITSC.2016.7795660>. 736
737
16. Rathore, S.; Park, J.H. A Blockchain-Based Deep Learning Approach for Cyber Security in Next Generation Industrial Cyber-Physical Systems. *IEEE Transactions on Industrial Informatics* **2021**, *17*, 5522–5532. <https://doi.org/10.1109/TII.2020.3040968>. 738
739
17. Alkhodair, A.; Mohanty, S.; Kougianos, E.; Puthal, D. McPoRA: A Multi-chain Proof of Rapid Authentication for Post-Blockchain Based Security in Large Scale Complex Cyber-Physical Systems. In Proceedings of the 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2020, pp. 446–451. <https://doi.org/10.1109/ISVLSI49217.2020.00-16>. 740
741
742
18. Mollah, M.B.; Zhao, J.; Niyato, D.; Guan, Y.; Sun, S.; Lam, K.Y.; Koh, L. Blockchain for the Internet of Vehicles Towards Intelligent Transportation Systems: A Survey. *IEEE Internet of Things Journal* **2020**, *PP*, 1–28. <https://doi.org/10.1109/JIOT.2020.3028368>. 743
744
19. Alladi, T.; Chamola, V.; Sahu, N.; Venkatesh, V.; Goyal, A.; Guizani, M. A Comprehensive Survey on the Applications of Blockchain for Securing Vehicular Networks. *IEEE Communications Surveys & Tutorials* **2022**, *24*, 1212–1239. <https://doi.org/10.1109/COMST.2022.3160925>. 745
746
747
20. Alkhodair, A.J.; Mohanty, S.P.; Kougianos, E. ASID: Accessible Secure Unique Identification File Based Device Security in Next Generation Blockchains. In Proceedings of the 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2021, pp. 1–2. <https://doi.org/10.1109/ICBC51069.2021.9461120>. 748
749
750
21. D.Puthal.; N.Malik.; S.P.Mohanty.; E.Kougianos.; G.Das. Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems. *IEEE Consumer Electronics Magazine* **2018**, *7*, 6–14. 751
752
22. Wang, S.; Sun, S.; Wang, X.; Ning, Z.; Rodrigues, J.J.P.C. Secure Crowdsensing in 5G Internet of Vehicles: When Deep Reinforcement Learning Meets Blockchain. *IEEE Consumer Electronics Magazine* **2021**, *10*, 72–81. <https://doi.org/10.1109/MCE.2020.3048238>. 753
754
755
23. Liu, J.; Zhang, L.; Li, C.; Bai, J.; Lv, H.; Lv, Z. Blockchain-Based Secure Communication of Intelligent Transportation Digital Twins System. *IEEE Transactions on Intelligent Transportation Systems* **2022**, *23*, 22630–22640. <https://doi.org/10.1109/TITS.2022.3183379>. 756
757
24. Mukathe, K.D.; Wu, D.; Ahmed, W. Secure and Efficient Blockchain-Based Certificateless Authentication Scheme for Vehicular Ad-Hoc Networks (VANETs). In Proceedings of the 2022 4th International Conference on Applied Machine Learning (ICAML), 2022, pp. 302–307. <https://doi.org/10.1109/ICAML57167.2022.00065>. 758
759
760
25. Lin, C.; He, D.; Huang, X.; Kumar, N.; Choo, K.K.R. BCPPA: A Blockchain-Based Conditional Privacy-Preserving Authentication Protocol for Vehicular Ad Hoc Networks. *IEEE Transactions on Intelligent Transportation Systems* **2021**, *22*, 7408–7420. <https://doi.org/10.1109/TITS.2020.3002096>. 761
762
763
26. Wang, X.; Garg, S.; Lin, H.; Kaddoum, G.; Hu, J.; Hassan, M.M. Heterogeneous Blockchain and AI-Driven Hierarchical Trust Evaluation for 5G-Enabled Intelligent Transportation Systems. *IEEE Transactions on Intelligent Transportation Systems* **2023**, *24*, 2074–2083. <https://doi.org/10.1109/TITS.2021.3129417>. 764
765
766
27. Singh, M. Tri-Blockchain Based Intelligent Vehicular Networks. In Proceedings of the IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2020, pp. 860–864. <https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162692>. 767
768
769
28. Li, X.J.; Ma, M.; Yong, Y.X. A Blockchain-Based Security Scheme for Vehicular Ad Hoc Networks in Smart Cities. In Proceedings of the TENCON 2021 - 2021 IEEE Region 10 Conference (TENCON), 2021, pp. 266–271. <https://doi.org/10.1109/TENCON54134.2021.9707356>. 770
771
772
29. Diarra, N. Choosing a Consensus Protocol for Uses Cases in Distributed Ledger Technologies. In Proceedings of the 2019 Sixth International Conference on Software Defined Systems (SDS), 2019, pp. 306–309. <https://doi.org/10.1109/SDS.2019.8768631>. 773
774
30. Alkhodair, A.J.; Mohanty, S.P.; Kougianos, E. FlexiChain: A Minerless Scalable Next Generation Blockchain for Rapid Data and Device Security in Large Scale Complex Cyber-Physical Systems. *SN Computer Science* **2022**, *3*. <https://doi.org/10.1007/s42979-022-01139-4>. 775
776
777
31. Alkhodair, A.J.; Mohanty, S.P.; Kougianos, E. FlexiChain 2.0: NodeChain Assisting Independent Decentralized Vault for Rapid Data Authentication and Device Security in Large Scale Complex Cyber-Physical Systems. *OAE Journal of Surveillance, Security and Safety (JSSS)* **2023**, Under Review. 778
779
780
32. Mohanty, S.P.; Choppali, U.; Kougianos, E. Everything you wanted to know about smart cities: The Internet of things is the backbone. *IEEE Consumer Electronics Magazine* **2016**, *5*, 60–70. <https://doi.org/10.1109/MCE.2016.2556879>. 781
782
33. Fernández Áñez, V. Stakeholders Approach to Smart Cities: A Survey on Smart City Definitions. 2016, pp. 157–167. https://doi.org/10.1007/978-3-319-39595-1_16. 783
784
34. Kirimtak, A.; Krejcar, O.; Kertész, A.; Tasgetiren, M. Future Trends and Current State of Smart City Concepts: A Survey. *IEEE Access* **2020**, *PP*, 1–1. <https://doi.org/10.1109/ACCESS.2020.2992441>. 785
786
35. Yin, C.; Xiong, Z.; Chen, H.; Wang, J.; Cooper, D.; David, B. A literature survey on smart cities. *Science China Information Sciences* **2015**, *58*. <https://doi.org/10.1007/s11432-015-5397-4>. 787
788
36. Kakarontzas, G.; Anthopoulos, L.; Chatzakou, D.; Vakali, A. A conceptual enterprise architecture framework for smart cities: A survey based approach. In Proceedings of the 2014 11th International Conference on e-Business (ICE-B), 2014, pp. 47–54. 789
790
37. Yeh, H. The effects of successful ICT-based smart city services: From citizens' perspectives. *Government Information Quarterly* **2017**, *34*, 556–565. <https://doi.org/https://doi.org/10.1016/j.giq.2017.05.001>. 791
792
38. An, J.; Le Gall, F.; Kim, J.; Yun, J.; Hwang, J.; Bauer, M.; Zhao, M.; Song, J. Toward Global IoT-Enabled Smart Cities Interworking Using Adaptive Semantic Adapter. *IEEE Internet of Things Journal* **2019**, *6*, 5753–5765. <https://doi.org/10.1109/JIOT.2019.2905275>. 793
794

39. Cledou, G.; Estevez, E.; Soares Barbosa, L. A taxonomy for planning and designing smart mobility services. *Government Information Quarterly* **2018**, *35*, 61–76. Internet Plus Government: Advancement of Networking Technology and Evolution of the Public Sector, <https://doi.org/https://doi.org/10.1016/j.giq.2017.11.008>. 795
796
797
40. Kumar, H.; Singh, M.; Gupta, M. Evaluating the competitiveness of Indian metro cities: in smart city context. *International Journal of Information Technology and Management* **2017**, *16*, 333. <https://doi.org/10.1504/IJITM.2017.086866>. 798
799
41. Miles, A.; Zaslavsky, A.; Browne, C. IoT-based decision support system for monitoring and mitigating atmospheric pollution in smart cities. *Journal of Decision Systems* **2018**, *27*, 1–12. <https://doi.org/10.1080/12460125.2018.1468696>. 800
801
42. Polenghi-Gross, I.; Sabol, S.; Ritchie, S.; Norton, M. Water storage and gravity for urban sustainability and climate readiness. *Journal - American Water Works Association* **2014**, *106*, E539–E549. <https://doi.org/10.5942/jawwa.2014.106.0151>. 802
803
43. Ul Hassan, M.; Rehmani, M.H.; Chen, J. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Generation Computer Systems* **2019**, *97*. <https://doi.org/10.1016/j.future.2019.02.060>. 804
805
806
44. Hamad, A.A.; Alkadi, I.; Aloufi, F. Renewable Energy Mix of Futuristic NEOM City. In Proceedings of the 2021 IEEE Green Technologies Conference (GreenTech), 2021, pp. 125–132. <https://doi.org/10.1109/GreenTech48523.2021.00030>. 807
808
45. Albalawi, H.; Eisa, A.; Aggoune, e.H.M. Energy Warehouse - A New Concept for NEOM Mega Project. In Proceedings of the 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), 2019, pp. 215–221. <https://doi.org/10.1109/JEEIT.2019.8717480>. 809
810
811
46. Wang, J.; Wang, W.; Wu, D.; Lei, T.; Liu, D.; Li, P.; Su, S. Research on Business Model of Internet of Vehicles Platform Based on Token Economy. In Proceedings of the 2021 2nd International Conference on Big Data Economy and Information Management (BDEIM), 2021, pp. 120–124. <https://doi.org/10.1109/BDEIM55082.2021.00033>. 812
813
47. Sharma, S.; Agarwal, P.; Mohan, S. Security Challenges and Future Aspects of Fifth Generation Vehicular Adhoc Networking (5G-VANET) in Connected Vehicles. In Proceedings of the 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), 2020, pp. 1376–1380. <https://doi.org/10.1109/ICISS49785.2020.9315987>. 814
815
816
817
48. Ahi, A.; Singh, A.V. Role of Distributed Ledger Technology (DLT) to Enhance Resiliency in Internet of Things (IoT) Ecosystem. In Proceedings of the Proc. Amity International Conference on Artificial Intelligence (AICAI), 2019, pp. 782–786. 818
819
49. Talukder, S.; Vaughn, R. A Template for Alternative Proof of Work for Cryptocurrencies. In Proceedings of the 2021 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), 2021, pp. 1–6. <https://doi.org/10.1109/SMARTGENCON51891.2021.9645773>. 820
821
822
50. Nair, P.R.; Dorai, D.R. Evaluation of Performance and Security of Proof of Work and Proof of Stake using Blockchain. In Proceedings of the 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 2021, pp. 279–283. <https://doi.org/10.1109/ICICV50876.2021.9388487>. 823
824
825
51. Saad, S.M.S.; Radzi, R.Z.R.M.; Othman, S.H. Comparative Analysis of the Blockchain Consensus Algorithm Between Proof of Stake and Delegated Proof of Stake. In Proceedings of the 2021 International Conference on Data Science and Its Applications (ICoDSA), 2021, pp. 175–180. <https://doi.org/10.1109/ICoDSA53588.2021.9617549>. 826
827
828
52. Gan, B.; Wu, Q.; Li, X.; Zhou, Y. Classification of Blockchain Consensus Mechanisms Based on PBFT Algorithm. In Proceedings of the 2021 International Conference on Computer Engineering and Application (ICCEA), 2021, pp. 26–29. <https://doi.org/10.1109/ICCEA53728.2021.00012>. 829
830
831
53. Boreiri, Z.; Azad, A.N. A Novel Consensus Protocol in Blockchain Network based on Proof of Activity Protocol and Game Theory. In Proceedings of the 2022 8th International Conference on Web Research (ICWR), 2022, pp. 82–87. <https://doi.org/10.1109/ICWR54782.2022.9786224>. 832
833
834
54. Živi, N.; Kadušić, E.; Kadušić, K. Directed Acyclic Graph as Tangle: an IoT Alternative to Blockchains. In Proceedings of the 2019 27th Telecommunications Forum (TELFOR), 2019, pp. 1–3. <https://doi.org/10.1109/TELFOR48224.2019.8971190>. 835
836
55. Baird, L.; Luykx, A. The Hashgraph Protocol: Efficient Asynchronous BFT for High-Throughput Distributed Ledgers. In Proceedings of the 2020 International Conference on Omni-layer Intelligent Systems (COINS), 2020, pp. 1–7. <https://doi.org/10.1109/COINS49042.2020.9191430>. 837
838
839
56. Li, F.; Lam, K.Y.; Liu, X.; Wang, J.; Zhao, K.; Wang, L. Joint Pricing and Power Allocation for Multibeam Satellite Systems With Dynamic Game Model. *IEEE Transactions on Vehicular Technology* **2018**, *67*, 2398–2408. <https://doi.org/10.1109/TVT.2017.2771770>. 840
841
57. Li, F.; Lam, K.Y.; Chen, H.H.; Zhao, N. Spectral Efficiency Enhancement in Satellite Mobile Communications: A Game-Theoretical Approach. *IEEE Wireless Communications* **2020**, *27*, 200–205. <https://doi.org/10.1109/MWC.001.1900160>. 842
843
58. Kang, J.; Yu, R.; Huang, X.; Wu, M.; Maharjan, S.; Xie, S.; Zhang, Y. Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks. *IEEE Internet of Things Journal* **2019**, *6*, 4660–4670. <https://doi.org/10.1109/JIOT.2018.2875542>. 844
845
59. Javaid, U.; Aman, M.N.; Sikdar, B. DrivMan: Driving Trust Management and Data Sharing in VANETs with Blockchain and Smart Contracts. In Proceedings of the 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), 2019, pp. 1–5. <https://doi.org/10.1109/VTCSpring.2019.8746499>. 846
847
848
60. Chen, Y.; Hao, X.; Ren, W.; Ren, Y. Traceable and Authenticated Key Negotiations via Blockchain for Vehicular Communications. *Mobile Information Systems* **2019**, 2019, 1–10. <https://doi.org/10.1155/2019/5627497>. 849
850
61. Chen, C.; Wu, J.; Lin, H.; Chen, W.; Zheng, Z. A Secure and Efficient Blockchain-Based Data Trading Approach for Internet of Vehicles. *IEEE Transactions on Vehicular Technology* **2019**, *68*, 9110–9121. <https://doi.org/10.1109/TVT.2019.2927533>. 851
852

62. Li, Z.; Yang, Z.; Xie, S. Computing Resource Trading for Edge-Cloud-Assisted Internet of Things. *IEEE Transactions on Industrial Informatics* **2019**, PP, 1–1. <https://doi.org/10.1109/TII.2019.2897364>. 853
854
63. Qiao, G.; Leng, S.; Chai, H.; Asadi, A.; Zhang, Y. Blockchain Empowered Resource Trading in Mobile Edge Computing and Networks. In Proceedings of the ICC 2019 - 2019 IEEE International Conference on Communications (ICC), 2019, pp. 1–6. <https://doi.org/10.1109/ICC.2019.8761664>. 855
856
857
64. Amiri, W.A.; Baza, M.; Banawan, K.; Mahmoud, M.; Alasmary, W.; Akkaya, K. Privacy-Preserving Smart Parking System Using Blockchain and Private Information Retrieval. In Proceedings of the 2019 International Conference on Smart Applications, Communications and Networking (SmartNets), 2019, pp. 1–6. <https://doi.org/10.1109/SmartNets48225.2019.9069783>. 858
859
860
65. Zichichi, M.; Ferretti, S.; D’angelo, G. A Framework Based on Distributed Ledger Technologies for Data Management and Services in Intelligent Transportation Systems. *IEEE Access* **2020**, 8, 100384–100402. <https://doi.org/10.1109/ACCESS.2020.2998012>. 861
862
66. Maffioli, D.; Longari, S.; Carminati, M.; Tanelli, M.; Zanero, S. GOLIATH: A Decentralized Framework for Data Collection in Intelligent Transportation Systems. *IEEE Transactions on Intelligent Transportation Systems* **2022**, 23, 13372–13385. <https://doi.org/10.1109/TITS.2021.3123824>. 863
864
865
67. Morganti, G.; Schiavone, E.; Bondavalli, A. Risk Assessment of Blockchain Technology. In Proceedings of the 2018 Eighth Latin-American Symposium on Dependable Computing (LADC), 2018, pp. 87–96. <https://doi.org/10.1109/LADC.2018.00019>. 866
867
68. Guo, H.; Yu, X. A survey on blockchain technology and its security. *Blockchain: Research and Applications* **2022**, 3, 100067. <https://doi.org/https://doi.org/10.1016/j.bcra.2022.100067>. 868
869
69. Zhang, S.; Lee, J.H. Analysis of the main consensus protocols of blockchain. *ICT Express* **2020**, 6, 93–97. <https://doi.org/https://doi.org/10.1016/j.icte.2019.08.001>. 870
871
70. Parity: Fast, light, robust Ethereum implementation, Parity Technologies, 2017-12-12, retrieved 2017-12-12.
71. Gavin, Wood (November 2015). "PoA Private Chains". Github. <https://github.com/poanetwork/wiki/wiki/POA-Network-Whitepaper>. 872
873
874