

Article

A Trustable and Secure Usage-Based Insurance Policy Auction Mechanism and Platform Using Blockchain and Smart Contract Technologies

Wen-Yao Lin, Kuang-Yen Tai *  and Frank Yeong-Sung Lin

Department of Information Management, National Taiwan University, Taipei 10617, Taiwan; linwy1399@gmail.com (W.-Y.L.); yeongsunglin@gmail.com (F.Y.-S.L.)

* Correspondence: davidking53211@gmail.com

Abstract: This study presents an architectural framework for the blockchain-based usage-based insurance (UBI) policy auction mechanism in the internet of vehicles (IoV) applications. The main objective of this study is to analyze and design the specific blockchain architecture and management considerations for the UBI environment. An auction mechanism is developed for the UBI blockchain platform to enhance consumer trust. The study identifies correlations between driving behaviors and associated risks to determine a driver's score. A decentralized bidding algorithm is proposed and implemented on a blockchain platform using elliptic curve cryptography and first-price sealed-bid auctions. Additionally, the model incorporates intelligent contract functionality to prevent unauthorized modifications and ensure that insurance prices align with the prevailing market value. An experimental study evaluates the system's efficacy by expanding the participant pool in the bidding process to identify the winning bidder and is investigated under scenarios where varying numbers of insurance companies submit bids. The experimental results demonstrate that as the number of insurance companies increases exponentially, the temporal overhead incurred by the system exhibits only marginal growth. Moreover, the allocation of bids is accomplished within a significantly abbreviated timeframe. These findings provide evidence that supports the efficiency of the proposed algorithm.



Citation: Lin, W.-Y.; Tai, K.-Y.; Lin, F.Y.-S. A Trustable and Secure Usage-Based Insurance Policy Auction Mechanism and Platform Using Blockchain and Smart Contract Technologies. *Sensors* **2023**, *23*, 6482. <https://doi.org/10.3390/s23146482>

Academic Editor: Omprakash Kaiwartya

Received: 27 June 2023

Revised: 13 July 2023

Accepted: 17 July 2023

Published: 18 July 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: usage-based insurance; blockchain; auction mechanism; internet of vehicles; security

1. Introduction

The internet of vehicles (IoV) is a cloud-based vehicle operation information platform that provides big data and information services from multiple sources. Comprehensive protection measures are required to ensure the security of IoV information [1]. To promote the technological development of self-driving smart vehicles, IoV communication technology and the IoV policies of various countries are both primarily focused on increasing demand for IoV [2,3]. Car dealers and chip manufacturers have adopted strategic alliances and optimized their technical capabilities to capture a larger market territory [4].

Usage-based insurance (UBI) is a type of automobile insurance that leverages driving technology to determine a car's status by analyzing driving data to calculate insurance premiums on the basis of driving behavior [5] instead of the owner's age, gender, or accident record. However, conventional UBI car insurance has some disadvantages. The vehicle must be equipped with an onboard diagnostic device (OBD) that monitors and collects driving data. Nonetheless, a potential concern arises in relation to the susceptibility of the device employed in this context, the OBD system, to tampering by the vehicle owner through software modifications. Consequently, the data collected from OBDs may encounter skepticism from authorities [6]. In an effort to address this issue, the present study has developed a blockchain-based UBI platform. By leveraging blockchain technology, the platform facilitates the publication of digitized driving data on the chain in an encrypted or

otherwise verified manner, while simultaneously safeguarding personal privacy. Moreover, this approach ensures the credibility of the data and generates value by creating readable and trustworthy intangible assets. As the rightful possessor of these assets, the car owner can exercise unrestricted control over them, such as by providing the corresponding data to insurance or financial organizations in order to obtain individually tailored insurance rates.

After receiving owner authorization, the IoV blockchain platform encrypts vehicle data—such as driving time, period, speed, mileage, and braking—and uploads them to the chain. After the owner's consent is obtained, other operators on the chain can create customized financial services on the basis of these data [7,8]. For example, car owners with safer driving habits could obtain more favorable car insurance premiums.

However, it is important to note that the IoV blockchain financial platform is currently in the proof-of-concept stage [9,10]. The advent of the blockchain ecosystem is anticipated to drive a new wave of car owners who recognize the fundamental principles of “data belonging to users” and “data as an asset” [11]. This paradigm shift implies that consumers, particularly car owners operating within the blockchain framework, will reevaluate their perspectives on personal information and privacy. For enterprises, the expanded participation within the ecosystem will enable the provision of a wide range of supplementary services for car owners [12]. The utilization of blockchain technology ensures the protection of driver privacy, while the integration of automated UBI technology enhances profitability for insurers. Moreover, the platform proposed in this study has the potential to facilitate reliable and transparent pricing mechanisms for insurers, resulting in benefits for customers. Additionally, the platform could aid automobile manufacturers in refining their products by granting them access to extensive datasets derived from driving activities.

To overcome the difficulties of IoV blockchain development [13,14], the proposed platform connects insurance and financial services on the basis of the driving data of the car owners on the chain. Furthermore, the driving behavior model [15] was used to develop the following application scenarios and address the research goals:

- (1) Develop a blockchain-based UBI maintenance system: Driving data and insurance claims cases could be compared to identify correlations between various driving behaviors and risks such that insurance plans corresponding to a driver's typical driving habits can be recommended.
- (2) Auction mechanism: The implementation of an auction mechanism that is appropriate for the blockchain-based UBI platform has the potential to reduce information asymmetry between the insurance company and consumers, which could result in an increase in the level of trust that consumers have in the platform.
- (3) Safety reminders: Drivers could be informed of the risk for various road sections while driving; during GPS navigation, safer road sections could be preemptively recommended to the driver. Various application scenarios could be developed from the driving behavior model based on the driving data of the car owners on the chain. Because the IoV enables all machines to communicate with each other, many novel forms of assistance could also be achieved. For example, the car could signal a garage if it notices an abnormal tire pressure sensor reading and remind the driver to check and repair the tire to prevent an accident. The car owner could also directly connect to the system of a financial institution through an application programming interface (API) to have the cost of the repair reimbursed.

2. Literature Review

2.1. IoV Infrastructure with Blockchain

In recent years, the financial industry has poured resources into blockchain technology. However, achieving its goals regarding this technology, implementing it in business, and creating fundamental scientific or technological financial services have been challenging [16]. A blockchain financial platform for vehicle networking could collect driving behavior, cryptographically store these data, and transmit the data to the blockchain in real time [17,18]. Because the blockchain is incorruptible, companies can link insurance and financial services

to authentic and reliable driving information on the chain. Providing car owners with faster and more convenient financing applications, insurance claims, and personalized product recommendations could significantly improve internal enterprise operations and the customer experience [19]. For example, the Data Hub platform built by the electric car manufacturer Tesla regularly collects data from the driving computer of each Tesla car and also has an official open API [20]. Tesla's blockchain team wrote its own decentralized application (DApp) and smart contracts to establish nodes through charging stations. After the owner is authorized, the DApp directly connects to the official API, and the electric vehicle is designated. The trip computer data are then input to the DApp, and the DApp uploads the data from the node to the chain on the basis of the smart contract [21].

To create financial insurance products that meet individual needs, information from various sources is required, such as driving habits, vehicle information, and consumption habits [22]. Auditing the authenticity of these data is expensive and limits their usage in the business process. For example, to confirm the authenticity of accounts receivable, a bank must also ensure that the statements of both parties and stakeholders are genuine [23]. High audit costs have led to numerous incidents of fraud; however, companies that require financing turnover have enormous operating pressures during information review periods.

Many blockchain developers have shifted their focus to the decentralized finance field by using the incorruptibility of the blockchain to achieve code enforcement (known as Code is Law). This method can greatly reduce the cost of some financial institution activities, such as deposits and lending [24].

2.2. Development of UBI System

In UBI, driving data, such as vehicle usage and driving behavior, are analyzed in a cloud system [25]. UBI systems can determine driving risk more accurately than can conventional car insurance systems, which base risk on gender, age, and accident frequency [26]. One advantages of UBI is its high pricing flexibility [27]. For example, drivers who rarely use the accelerator and brake, have safe driving habits, obey traffic rules, and rarely drive during peak hours could have greater flexibility and discounts on insurance costs in a UBI scheme than for conventional auto insurance.

UBI typically requires an OBD to be installed in the car or a mobile app to record driving behavior [28]. Moreover, UBI could also use car maintenance records in addition to owner driving habits to more objectively price car insurance [29]. However, an urgent problem that is encountered when implementing UBI is determining how the owner's vehicle information and personal data can be obtained. An owner who values their privacy may be concerned about whether personal driving data will be adequately and safely stored; these doubts regarding privacy are a key barrier to the universal implementation of UBI [30,31].

2.3. Blockchain-Based Security Auction Algorithm

E-auctions are widely practiced in e-commerce, enabling bidders to participate directly in online product bidding processes [32]. However, in the case of sealed bids, an intermediary must be involved. They were incurring additional transaction costs to facilitate trade between buyers and sellers during the auction. Regrettably, there exists a need for more assurance regarding the trustworthiness of this third-party entity. Blockchain technology can be leveraged to tackle this predicament, offering the advantages of low transaction costs and the ability to establish smart contracts for both public and sealed bids. A blockchain is an immutable and distributed database that maintains transactional data within a peer-to-peer network [33]. The database operates decentralized to allow any member node in the overlay blockchain network to participate in its maintenance anonymously. Transactions between member nodes are recorded in cryptographic hash-linked data structures called blocks. Smart contracts are crucial in ensuring transactions' security, privacy, irrefutability, and immutability. All transactions are recorded in identical but decentralized ledgers. A smart contract encompasses essential details, such as the

auctioneer's address, auction start time, deadline, the current winner's address, and the highest bid at the present moment [34].

Blockchain has garnered considerable popularity as an emerging decentralized and secure data management platform [35]. In proof-of-work-based consensus protocols, network nodes, referred to as miners, are motivated to verify new transaction blocks by solving a cryptographic puzzle through a process known as "block mining". This study primarily focuses on utilizing a blockchain network as an infrastructure for decentralized data management applications, considering the constraints imposed by computing resources. Allocative externalities take precedence when devising auction mechanisms for such a network.

The permissionless blockchain represents an exemplary decentralized and autonomous platform for data management in numerous applications, as it operates without requiring prior authorization [36]. Permissionless blockchains offer the advantage of rapidly establishing a self-organized data management platform capable of supporting a broad array of decentralized applications. Without the need for assistance or permission from trusted intermediaries, individuals can independently design smart contracts and freely develop decentralized applications.

2.4. UBI Maintenance System Using IoV and Blockchain

The growing interest in leveraging the decentralized nature of blockchain technology has sparked recent research efforts to develop authentication and authorization mechanisms for the IoV [30,37]. These mechanisms seek to eliminate the reliance on centralized third-party intermediaries. This study presents a comprehensive framework that facilitates decentralized and a privacy-centric data exchange in the IoV, explicitly focusing on monetized services. The framework is built upon a tiered blockchain architecture and employs the InterPlanetary file system for secure data storage and transfer [38]. Its main objective is to empower IoV data users to have fine-grained control over data sharing with entities authenticated by the blockchain. Two use cases are provided to demonstrate the practical application of the framework: an IoV data marketplace and decentralized connected vehicle insurance. These examples showcase the framework's versatility in enabling smart contract-based applications involving exchanging IoV data and cryptocurrencies. Furthermore, the paper conducts a thorough security analysis, evaluating the proposed framework against various attack scenarios, and presents comprehensive performance metrics from real-world implementation [39].

Existing data management solutions for IoV data encounter challenges in verifying data source credibility and maintaining data security [40]. However, the decentralized nature of blockchain technology offers promising solutions to address these challenges. Nonetheless, obstacles remain to overcome, such as computing resource consumption and data segmentation between on-chain and off-chain components. To solve these issues mentioned above, the paper presents a recent study proposing a blockchain-based information management system designed to handle vehicle-related data reliably [41]. The system adopts a sharding blockchain structure, where IoV nodes within a particular geographical area form sub-chains to enhance computational speed and reduce the workload on the main chain. Additionally, an on-chain and off-chain computing scheme based on trusted execution environments is proposed to ensure data source credibility and optimize the computational resource consumption of smart contracts [42].

In vehicle insurance, UBI has emerged as a contemporary and practical approach. Unlike traditional methodologies, UBI determines insurance premiums based on real-time driver behavior. However, challenges arise due to the need for more transparency in claims processing, resulting in delays and increased fraudulent activities. In response, decentralized technologies, particularly blockchain, have gained attention as a promising solution. Consequently, this study proposes a blockchain-based framework for implementing vehicular UBI and incentives within the IoV context.

3. Research Method

3.1. Design of Blockchain IoV System Infrastructure

The blockchain consensus mechanism aims to achieve decentralization, security, and scalability simultaneously [37]. However, increasing transmission speeds may entail compromising decentralization, while prioritizing decentralization may result in reduced scalability. Existing blockchain platforms face challenges in meeting all three objectives concurrently. For instance, delegated proof of stake (DPoS) sacrifices decentralization to achieve high transmission speeds [43]. By contrast, proof of work (PoW) maintains decentralization but struggles to attain high transaction speeds [44]. Tendermint, a consensus blockchain mechanism, addresses these challenges by introducing asynchronicity to the Ethereum blockchain [45]. Tendermint primarily focuses on enhancing fault tolerance and efficiency. To overcome these challenges, the whole Ethereum blockchain incorporates the essential functions of Ethereum by integrating the Tendermint consensus algorithm. Nodes within this system are categorized into externally owned accounts (EOAs) and smart contracts. The platform determines the voting rights of EOAs for financing purposes based on the stakeholders' influence. Moreover, within the Tendermint system, every node assumes the role of a verifier, possessing the necessary privileges to access, transmit, and authenticate transactions. This characteristic aligns with the blockchain DNS solutions [46], which similarly adopts a decentralized gateway architecture to connect private blockchains with end-users. This is accomplished by harnessing the distinctive features of both public and private blockchain platforms through its underlying Ethereum structure [47].

This research platform is developed based on the architecture of Tendermint, which integrates a security auction mechanism to address apprehensions regarding potential data leaks arising from operational negligence. To ensure authentication for all auction nodes and participants and minimize data loss risk, a public–private key pair is assigned to each bidder. This research presents an architectural framework for the UBI blockchain policy auction mechanism in IoV applications. It includes a customized auction mechanism, a decentralized bidding algorithm, and intelligent contract functionality to enhance the security, fairness, and trustworthiness of the system. The experimental evaluation validates the efficiency of the proposed algorithm, highlighting its potential for real-world implementation in the UBI domain.

In an IoV system, driving data are standardized and preprocessed before being uploaded to the blockchain platform (Figure 1). The IoV sensor on vehicles collects driving habits and transmits them to the blockchain platform. The platform identifies the vehicle, assesses the driver's risk and driving habits, generates a risk judgment model, and adjusts the premium accordingly. The driving data collected are used to establish a risk evaluation model that results in a higher dividend, increasing the insurance company's profitability. Onboard sensors record the behavior of a driver whenever they operate a vehicle, and this behavior is integrated, analyzed, encrypted, and subsequently uploaded to the UBI platform based on blockchain technology. Following this, the data undergo several validation and confirmation processes performed by dealers, manufacturers, and maintenance depots. After verification, insurance agencies can access this data to evaluate the driver's behavior, modify the premium, and create a new tailored contract that includes different insurance products for the driver's selection and also provide driving advice. This approach enables insurance pricing to be based on two risk factors: driver-related and vehicle-related. Consequently, there are three types of insurance plans: (1) billing the driver and vehicle owner separately based on their risks; (2) billing only the vehicle owner based on both driver-related and vehicle-related risks; and (3) billing only the driver based on driver-related risk.

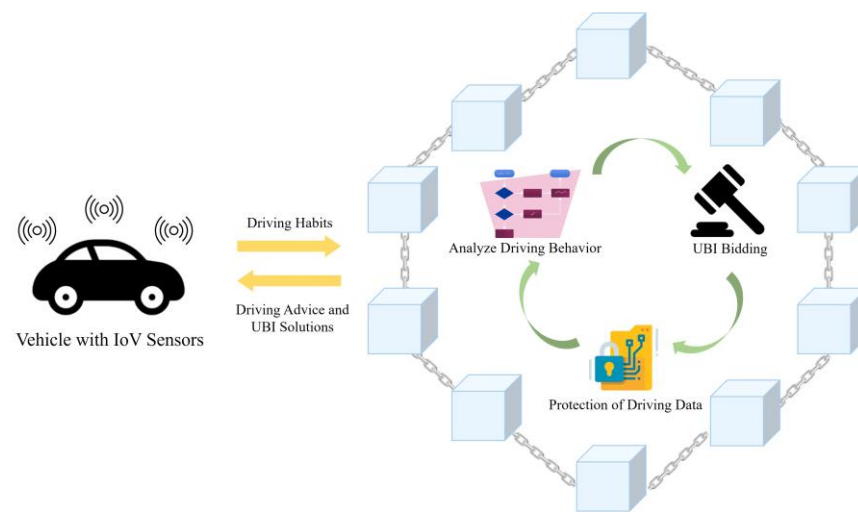


Figure 1. Blockchain-based UBI system model.

3.2. Auction Mechanism

This study constructs a driver blockchain that is based on the driver and vehicle information collected by an IoV-capable vehicle system that meets the insurance requirements of the vehicle owner. After the driver blockchain is completed, the blockchain-based UBI platform generates an auction agent and connects to an insurance company's auction platform. The driver's insurance requirements are stored on the auction platform. After auction on the auction platform, the auction agent automatically matches the bid with the most appropriate insurance portfolio. The detailed process is illustrated in Figure 2. The primary participants in the designed blockchain-based UBI platform are as follows:

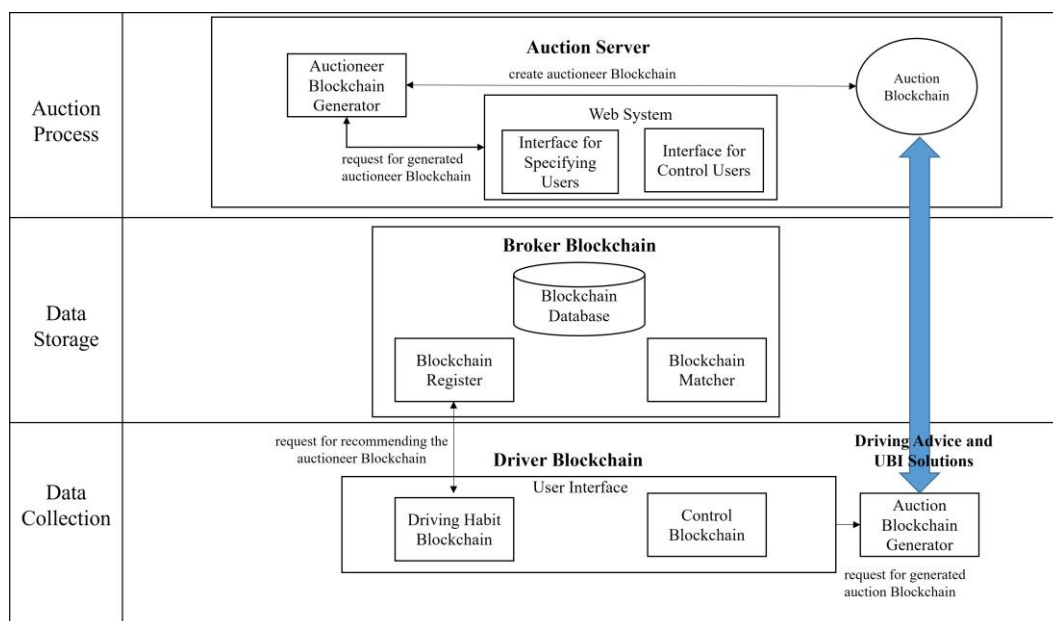


Figure 2. System structure of the blockchain-based UBI platform with auction algorithm.

- (1) Broker blockchain pairs bidders and auctioneers, generates auction lists, and gives bid price information to users.
- (2) Auctioneer blockchain generator is used by individuals to participate in auctions and place bids.
- (3) Driver blockchain collects driving habits and UBI requests.

- (4) Broker blockchain pairs auctioneers, generates auction lists, and gives bid price information to users.
- (5) Auction server operation is a Web interface offered by the auction house server that enables auctioneers to execute the set of instructions and has two parts: First, to specify the auctioneer agent, the auctioneer sends a request and auction information to the auctioneer agent generator, which creates an agent from a pre-existing template. The newly created agent and auction information are then registered with the broker agent. Second, the auctioneer can control the auctioneer agent's behavior by communicating with it directly.

4. System Implementation

4.1. Blockchain-Based Auction Algorithm for UBI

Elliptic curve cryptography and a first-price sealed-bid auction was implemented to develop a suitable auction mechanism for the UBI blockchain platform [48–50]. The proposed blockchain auction mechanism has four phases: auction initialization, bidder registration, auction process, and winner announcement. This process has four main participants: bidder registration manager, bidder agent house, blockchain auction house, and bidder.

- (1) Bidder registration manager oversees the mandatory bidder registration process prior to the commencement of an auction, allowing bidders to participate in multiple auctions following registration. Additionally, the manager stores and verifies the corresponding secret parameters of registered bidders. They also manage and maintain a virtual bulletin board containing two types of information: a bidder's registration key and identity information, as well as their pseudonym utilized in a single auction round. Access to the board is exclusive to the bidder registration manager, who has the ability to write and update it, while all users may refer to the posted information for identity verification purposes.
- (2) Bidder agent house is an entity that is responsible for establishing communication with the broker blockchain and creating bid agents. Its primary function is to manage and maintain a bulletin board that stores the public keys of bidders' transactions, which can be used for verification purposes.
- (3) Blockchain auction house provides the auction location, hosts auctions, and manages auction operations. It also maintains a virtual bulletin board that contains the auction information of all bidders and the winning bidder for verifying bidder identities.
- (4) Bidder is an insurance company that participate and places bids in the auction.

4.2. Auction Algorithm Initialization

The parameters for the auction algorithm are listed in Table 1.

Table 1. Parameters for the Auction Algorithm.

Parameter	Description
B	Set of all bidders in the auction $\{1, 2, 3, \dots, i\}$
P	Set of large prime number includes $\{1, 2, 3, \dots, p\}$
Q	Set of large prime number includes $\{1, 2, 3, \dots, q\}$ as the order of a generative point on the elliptic curve with value within $p + 1 \pm \sqrt[3]{p}$
E	The elliptic curve equation $y^2 = x^3 + ax + b \pmod{p}$ where a and b satisfy $4a^3 + 27b^2 \pmod{p} \neq 0$
G	A point on the elliptic curve
F	A point on the elliptic curve
x_F	The x-coordinate value of F
y_F	The y-coordinate value of F
$H(x)$	A hash function that satisfies $H_i(x) = H(x, H_{i-1}(x))$ and $H_0(x) = x$

Table 1. Cont.

Parameter	Description
S_{AH}	The private key of the bidder agent house
P_{AH}	The public key of the bidder agent house
S_{Bi}	The private key of B_i
R_{Bi}	The registration key of B_i
B_{ij}	The price of B_i in the j^{th} auction round
$S_i, B_{1,i}, B_{2,i}$	Three secret parameters chosen by B_i
N_{ij}	A pseudonym created by the bidder registration manager for B_{ij}
R_j	Random number chosen by the bidder agent house in the j^{th} auction round
P_{Ij}	The public information provided by the bidder agent house in the j^{th} auction round
PK_{ij}	The transaction public key generated for B_{ij}

The bidder registration manager and bidder agent house establish system parameters through the following steps:

(1) Bidder Registration Manager

Step 1: Set up a read-only virtual bulletin board and post all bidders' registration keys, identity information, and pseudonyms used by the bidders in the j^{th} auction round. Only the bidder registration manager can write to and update the bulletin board.

Step 2: Select a prime number greater than one million as p .

Step 3: Develop an elliptic curve equation where a and b satisfy $4a^3 + 27b^2 \bmod p \neq 0$

Step 4: Declare G and Q .

(2) Bidder Agent House

Step 1: Set up a read-only virtual bulletin board and post the information of all bidders and the transaction public key on the board. Only the bidder agent house can write to and update the bulletin board.

Step 2: Select S_{AH} randomly to calculate a P_{AH} that satisfies:

$$P_{AH} = G * S_{AH} \quad (1)$$

Step 3: Post P_{AH} on the read-only virtual bulletin board.

(3) Registration

The bidder registration manager generates a pseudonym for a bidder before it joins a new auction and also encrypts the information into the hash function. The pseudonym can only be used while the auction is in progress, and the bidders will obtain their private key. The registration process is described as follows:

Step 1: Select S_{Bi} as the private key of bidder i and calculate the corresponding registration key R_{Bi} as follows:

$$R_{Bi} = G * S_{Bi} \quad (2)$$

Step 2: Each bidder selects a secret parameter S_i .

Step 3: Each bidder select a random integer $B_{1,i}$ and calculates the verification information (Ψ_i, δ_i) as follows:

$$S_i = G * B_{1,i} = (x_{F_{1,i}}, y_{F_{1,i}}) \quad (3)$$

$$\Psi_i = H(x_{F_{1,i}} || y_{F_{1,i}}) \quad (4)$$

$$\delta_i = B_{1,i} + (\Psi_i * S_{Bi}) \bmod q \quad (5)$$

Step 4: Each bidder transmits R_{Bi} , S_i , Ψ_i , and δ_i to the bidder registration manager.

Step 5: The bidder registration manager begins the registration progress and verifies the information by using the following equations:

$$S_i' = G * \Psi_i - R_{Bi} * \delta_i = (xF_{1,i}', yF_{1,i}') \quad (6)$$

$$\Psi_i' = H(xF_{1,i}' || yF_{1,i}') \quad (7)$$

$$\Psi_i' \stackrel{?}{=} \Psi_i \quad (8)$$

Step 6: The bidder registration manager posts the registration information R_{Bi} of bidder i on the virtual bulletin board.

Step 7: The bidder registration manager generates a pseudonym for each bidder before the j^{th} auction begins in a random order.

$$N_{ij} = H(S_i) * R_{Bi} \quad (9)$$

Step 8: By using Equation (9), each bidder can obtain and verify its own pseudonym.

(4) Auction Progress

Step 1: The auction information for a bidder (PK_{ij}, B_{ij}) is sent to the bidder agent house to request a bid agent.

Step 2: The bidder agent house sends the auction information to the blockchain auction house, and PK_{ij} is verified using the virtual bulletin board.

Step 3: The blockchain auction house announces the auction information of B on the virtual bulletin board.

(5) Winner Announcement

The bidder who places the highest bid is the winner after the j^{th} auction round, and the blockchain auction house verifies the authenticity of B before announcing the winner on the virtual bulletin board as follows:

Step 1: The blockchain auction house asks for the winner's PK_{ij} , R_{Bi} , and N_{ij} from the bidder agent house.

Step 2: The blockchain auction house checks the consistency of the PK_{ij} , R_{Bi} , and N_{ij} by using Equation (9).

Step 3: After announcing the winner, anyone can verify the auction process by using the virtual bulletin board.

4.3. Security and Practicality Analysis

4.3.1. Security Analysis

The following common security issues are discussed to analyze the security of the elliptic curve cryptosystem-based bidding mechanism applied to the IoV blockchain platform proposed in this study:

- (1) Anonymity: The bidder's identity in the auction process is known only to the broker blockchain and auction server. It is not accessible to external entities.
- (2) Fairness: All participants in the auction use pseudonyms. The bidder agent house is responsible for sharing valid auction information on a virtual bulletin board. If a bidder cannot find their auction information, they can appeal to the bidder agent house. This ensures impartial administration of bidder information.
- (3) Efficiency and easy revocation of auction: The use of the elliptic curve cryptosystem reduces the computational burden of online auction operations. The broker blockchain can quickly remove a bidder's identification and confidential parameters from the database. Once this information is removed, the bidder loses their eligibility for future auctions.

4.3.2. Practicality Analysis

A comparative analysis of the merits of utilizing blockchain technology in the proposed insurance policy auction mechanism reveals significant advantages compared to a system without blockchain were discussed as follows:

In a traditional system lacking blockchain integration, the insurance policy auction mechanism operates under centralized control, typically governed by a central authority or intermediary. Such centralization introduces potential bottlenecks, delays, and increased costs due to the reliance on intermediaries [51]. Additionally, storing sensitive customer data on centralized servers exposes it to vulnerabilities, including security breaches and unauthorized access, thus jeopardizing drivers' information and privacy. Consequently, the policy issuance and settlement processes must be more active and effective [49].

The adoption of blockchain technology in the proposed insurance policy auction mechanism offers notable advantages. Blockchain's inherent decentralization ensures a distributed auction mechanism, rendering intermediaries unnecessary. Participants gain equal access to an immutable and transparent ledger, establishing transparency and fairness within the auction process. This decentralized nature also fosters trust and verifiability among participants, as reliance on intermediaries is replaced by trust in blockchain technology's protocol and consensus mechanism [50]. Blockchain's implementation guarantees enhanced security through cryptographic algorithms and a distributed ledger system. Encrypted and distributed data storage across multiple nodes diminishes the risk of data breaches and unauthorized access, thus safeguarding drivers' sensitive information. By eliminating the need for manual interventions, smart contracts streamline operations, reducing administrative costs and processing times. Furthermore, blockchain technology facilitates efficient settlements, significantly reducing settlement times [51]. It becomes evident that incorporating blockchain technology in the proposed insurance policy auction mechanism provides substantial merits. These include decentralization, transparency, enhanced security, automation, efficient settlements, improved data management, and global accessibility. Collectively, these advantages contribute to establishing trust, fairness, efficiency, and cost reduction, thereby benefiting insurers and drivers.

4.4. System Simulation Experiment

In this section, system simulation experiment for a blockchain-based UBI policy auction mechanism in the IoV is developed to evaluate the feasibility and performance. By utilizing a simulation model that incorporates the essential components of blockchain technology and the IoV environment, this experiment seeks to assess the effectiveness of the UBI policy auction mechanism. Through the design of various scenarios, parameters, and performance metrics, the simulation experiments can provide valuable insights into the efficiency of the blockchain-based UBI policy auction mechanism.

4.4.1. Generate Time of the Auction When Driving Behavior Changed

This experiment aims to assess the efficiency of a blockchain-based UBI auction mechanism in determining insurance premiums by leveraging real-time driving behavior data obtained from connected vehicles. Additionally, the study aims to evaluate the influence of vehicle-to-platform communication on a policyholder's behavior and analyze the system's scalability. This experiment was explicitly designed to examine the system's operational speed under varying conditions of sensor activation, representing shifts in driving behavior. By investigating the relationship between sensor triggers and the resulting system performance, this research seeks to verify the observed trends and draw conclusions regarding the system's responsiveness to changes in driving patterns. The results were shown in Figure 3.

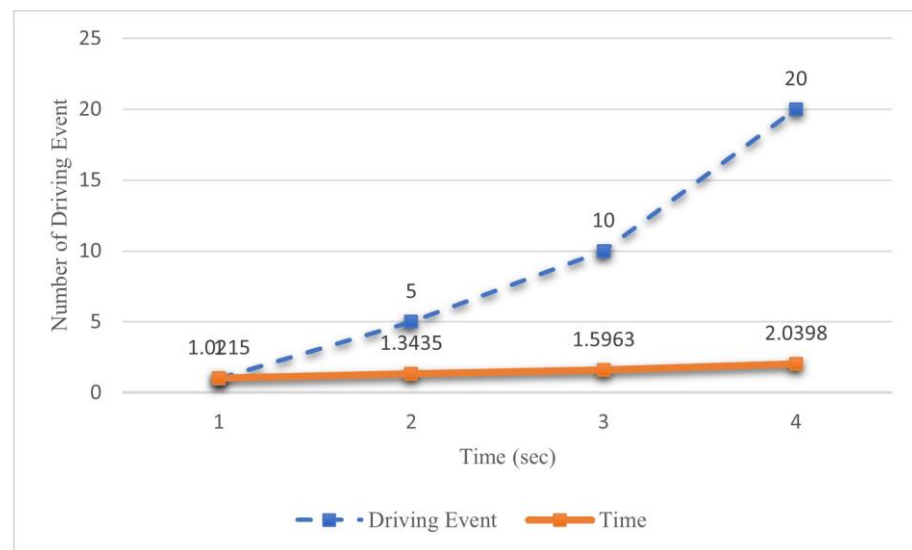


Figure 3. Experiment results when a different number of driving events happens.

In light of each driving event, the system must modify the insurance record per the particular event. Based on the empirical findings, it becomes evident that when the occurrence of driving events exhibits a significant rise, albeit with a slight increase in the system's processing time for generating an insurance plan, it can be observed that the incremental increments are minute in nature. This observation underscores the system's ability to effectively and promptly update the driver's status information in real time.

4.4.2. Different Number of Insurance Company

The number of bidders participating in an auction process significantly influences the operational speed of the overall system. The presence of a larger pool of bidders leads to an increased number of bidding rounds, complexity of the hash function, and a subsequent expansion of the auction's scale. In the scope of this experimental investigation, as shown in Figure 4, we aim to empirically validate the operational efficiency of the proposed elliptic curve cryptography-based first-price sealed-bid auction algorithm on a blockchain platform, particularly when confronted with a scenario involving multiple insurance companies and an augmented number of stakeholders in the system.

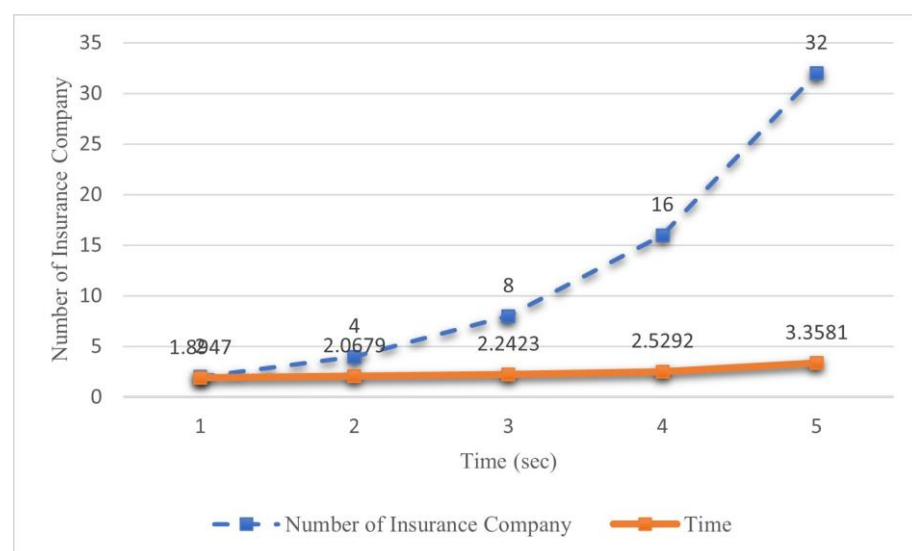


Figure 4. Experiment results in different number of insurance company.

The objective of this experimental study is to evaluate the efficacy of the system by augmenting the participant pool in the bidding process. Specifically, we investigate the duration required for the system to identify the winning bidder in scenarios where varying numbers of insurance companies submit bids. The experimental results reveal that as the number of insurance companies increases exponentially, the temporal overhead incurred by the system exhibits only marginal growth. Moreover, the allocation of bids is accomplished within a significantly abbreviated timeframe. Consequently, these findings substantiate the efficiency of the proposed algorithm.

5. Conclusions

5.1. Lessons Learned

Individual driving behavior complicates the relationship between responsibility and obligation in traffic behavior. This study investigated driving insurance. In practice, the two key aspects of insurance plans are how insurance companies can learn about driving habits to evaluate insurance premiums and how consumers can protect their rights. These processes have various limitations and incur informational asymmetry. Previously, only gender and age were used to evaluate driving risk; this method is unsuitable in practice.

In conclusion, this research presents a robust framework for implementing a fair auction mechanism on a practical blockchain platform in the UBI and the IoV domains. Incorporating driving behavior recordings, auction mechanisms, and safety reminders contribute significantly to advancing these fields. Leveraging the capabilities of blockchain technology and IoV advancements enhances the platform's overall efficiency, fairness, and trustworthiness, thereby establishing a mutually beneficial environment for drivers and insurance companies. The key contributions of this study can be summarized as follows:

Firstly, constructing the UBI system on the blockchain platform, combined with utilizing IoV technology, facilitates detailed recordings of driving behavior. By incentivizing drivers to adopt safe habits through reduced insurance premiums, this system promotes the cultivation of safer driving practices. Integrating IoV technology enables the comprehensive collection and analysis of driving data, providing valuable insights into driver behavior. Secondly, an auction mechanism has been designed for implementation on a blockchain platform utilizing elliptic curve cryptography and first-price sealed-bid auctions. These sophisticated technologies ensure both information security and auction fairness. By simplifying the process for drivers, who are only required to provide their insurance requirements, and enabling insurance companies to bid based on the drivers' recorded behavior on the blockchain, this auction mechanism prevents drivers from being subjected to excessive charges. Simultaneously, it facilitates insurance companies' understanding of drivers' behavior, fostering a mutually beneficial environment. Thirdly, the development of a blockchain-based UBI maintenance system allows for the comparison of driving data and insurance claims, enabling the identification of correlations between various driving behaviors and associated risks. This knowledge facilitates the recommendation of insurance plans that align with a driver's typical driving habits, ultimately enhancing the overall efficiency and effectiveness of the UBI system.

Additionally, implementing an auction mechanism appropriate for the blockchain-based UBI platform can address the issue of information asymmetry between insurance companies and consumers. By increasing transparency and fairness in the auction process, consumer trust and confidence in the platform can be enhanced, resulting in a more reliable and trustworthy UBI system. Integrating safety reminders into the system provides real-time notifications to drivers about the risks associated with different road sections during their journeys. Moreover, the system proactively recommends safer road sections through GPS navigation, thereby contributing to improved driver safety. The driving behavior model, based on the recorded data of vehicle owners on the blockchain, serves as a foundation for developing various application scenarios. Leveraging the communication capabilities of the IoV, novel forms of assistance can be achieved. For example, the system

can promptly notify a nearby garage in case of an abnormal tire pressure sensor reading, prompting the driver to inspect and repair the tire to prevent potential accidents.

5.2. Future Work

This research showcases a comprehensive framework for implementing a fair auction mechanism on a practical blockchain platform within the UBI and IoV domains, integrating driving behavior recordings, auction mechanisms, and safety reminders. By harnessing the potential of blockchain technology and IoV advancements, the platform achieves improved efficiency, fairness, and trustworthiness, fostering a mutually beneficial environment for drivers and insurance companies.

Future work in this area should address the complexities of individual driving behavior and its implications for the relationship between responsibility and obligation in traffic behavior. While this study has specifically investigated driving insurance, two key aspects require further attention: how insurance companies can effectively learn about driving habits to accurately evaluate insurance premiums and how consumers can protect their rights. Current approaches have limitations and often result in informational asymmetry. Previous methods that relied solely on factors, such as gender and age to assess driving risk are inadequate in practice. Future research can explore innovative approaches to gathering and analyzing driving behavior data to advance this field, which could involve developing more sophisticated technologies and methodologies for evaluating driving habits and determining insurance premiums. Insurance companies can gain deeper insights into individual driving behavior and accurately assess risk levels by leveraging emerging technologies and techniques, such as advanced data analytics, machine learning algorithms, and artificial intelligence. This would contribute to fairer and more personalized insurance plans.

Author Contributions: Methodology, W.-Y.L., K.-Y.T. and F.Y.-S.L.; Validation, W.-Y.L.; Writing—original draft, W.-Y.L. and K.-Y.T.; Supervision, F.Y.-S.L.; Project administration, W.-Y.L. and K.-Y.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This work was supported by National Science and Technology Council of Taiwan, R.O.C through its grants 112-2622-E-002-024.

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

References

1. Ji, B.; Zhang, X.; Mumtaz, S.; Han, C.; Li, C.; Wen, H.; Wang, D. Survey on the internet of vehicles: Network architectures and applications. *IEEE Commun. Stand. Mag.* **2020**, *4*, 34–41. [\[CrossRef\]](#)
2. Abu Talib, M.; Abbas, S.; Nasir, Q.; Mowakeh, M.F. Systematic literature review on Internet-of-Vehicles communication security. *Int. J. Distrib. Sens. Netw.* **2018**, *14*, 1550147718815054. [\[CrossRef\]](#)
3. Lin, W.Y.; Lin, F.Y.; Wu, T.H.; Tai, K.Y. An on-board equipment and blockchain-based automobile insurance and maintenance platform. In *Advances on Broad-Band Wireless Computing, Communication and Applications. Proceedings of the 15th International Conference on Broad-Band and Wireless Computing, Communication and Applications (BWCCA-2020), Yonago, Japan, 28–30 October 2020*; Springer International Publishing: Cham, Switzerland, 2021; pp. 223–232.
4. O'Dwyer, M.; Gilmore, A. Value and alliance capability and the formation of strategic alliances in SMEs: The impact of customer orientation and resource optimisation. *J. Bus. Res.* **2018**, *87*, 58–68. [\[CrossRef\]](#)
5. Arumugam, S.; Bhargavi, R. A survey on driving behavior analysis in usage based insurance using big data. *J. Big Data* **2019**, *6*, 86. [\[CrossRef\]](#)
6. Patsakis, C.; Dellios, K.; Bouroche, M. Towards a distributed secure in-vehicle communication architecture for modern vehicles. *Comput. Secur.* **2014**, *40*, 60–74. [\[CrossRef\]](#)
7. Biswas, A.; Wang, H.C. Autonomous vehicles enabled by the integration of IoT, edge intelligence, 5G, and blockchain. *Sensors* **2023**, *23*, 1963. [\[CrossRef\]](#)
8. Cui, J.; Ouyang, F.; Ying, Z.; Wei, L.; Zhong, H. Secure and efficient data sharing among vehicles based on consortium blockchain. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 8857–8867. [\[CrossRef\]](#)

9. Fernando, Y.; Rozuar NH, M.; Mergeresa, F. The blockchain-enabled technology and carbon performance: Insights from early adopters. *Technol. Soc.* **2021**, *64*, 101507. [\[CrossRef\]](#)
10. Jabbar, R.; Dhib, E.; Ben Said, A.; Krichen, M.; Fetais, N.; Zaida, E. Blockchain technology for intelligent transportation systems: A systematic literature review. *IEEE Access* **2022**, *10*, 20995–21031. [\[CrossRef\]](#)
11. Sharma, P.K.; Kumar, N.; Park, J.H. Blockchain-based distributed framework for automotive industry in a smart city. *IEEE Trans. Ind. Inform.* **2018**, *15*, 4197–4205. [\[CrossRef\]](#)
12. Martins, J.; Parente, M.; Amorim-Lopes, M.; Amaral, L.; Figueira, G.; Rocha, P.; Amorim, P. Fostering customer bargaining and E-procurement through a decentralised marketplace on the blockchain. *IEEE Trans. Eng. Manag.* **2020**, *69*, 810–824. [\[CrossRef\]](#)
13. Hammoud, A.; Sami, H.; Mourad, A.; Otrók, H.; Mizouni, R.; Bentahar, J. AI, blockchain, and vehicular edge computing for smart and secure IoV: Challenges and directions. *IEEE Internet Things Mag.* **2020**, *3*, 68–73. [\[CrossRef\]](#)
14. Kumar, R.; Kumar, P.; Tripathi, R.; Gupta, G.P.; Kumar, N. P2SF-IoV: A privacy-preservation-based secured framework for Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 22571–22582. [\[CrossRef\]](#)
15. Zaremozhzabieh, Z.; Abu Samah, B.; Muhammad, M.; Omar, S.Z.; Bolong, J.; Hassan, M.S.; Mohamed Shaffril, H.A. A test of the technology acceptance model for understanding the ICT adoption behavior of rural young entrepreneurs. *Int. J. Bus. Manag.* **2015**, *10*, 158–169. [\[CrossRef\]](#)
16. Rocha, C.; Quandt, C.; Deschamps, F.; Philbin, S.; Cruzara, G. Collaborations for digital transformation: Case studies of industry 4.0 in Brazil. *IEEE Trans. Eng. Manag.* **2021**, *70*, 2404–2418. [\[CrossRef\]](#)
17. Jiang, T.; Fang, H.; Wang, H. Blockchain-based internet of vehicles: Distributed network architecture and performance analysis. *IEEE Internet Things J.* **2018**, *6*, 4640–4649. [\[CrossRef\]](#)
18. Jabbar, R.; Kharbeche, M.; Al-Khalifa, K.; Krichen, M.; Barkaoui, K. Blockchain for the internet of vehicles: A decentralized IoT solution for vehicles communication using ethereum. *Sensors* **2020**, *20*, 3928. [\[CrossRef\]](#)
19. Parise, S.; Guinan, P.J.; Kafka, R. Solving the crisis of immediacy: How digital technology can transform the customer experience. *Bus. Horiz.* **2016**, *59*, 411–420. [\[CrossRef\]](#)
20. Rayes, A.; Salam, S.; Rayes, A.; Salam, S. Internet of things (IoT) overview. In *Internet of Things from Hype to Reality: The Road to Digitization*; Springer: Cham, Switzerland, 2017; pp. 1–34.
21. Hamledari, H.; Fischer, M. The application of blockchain-based crypto assets for integrating the physical and financial supply chains in the construction & engineering industry. *Autom. Constr.* **2021**, *127*, 103711.
22. Zehir, C.; Zehir, M. Emerging blockchain solutions in the mobility ecosystem: Associated risks and areas for applications. *Bussecon Rev. Soc. Sci.* **2022**, *4*, 1–14.
23. Postorino, M.N.; Sarnè, G.M. Using Reputation Scores to Foster Car-Sharing Activities. *Sustainability* **2023**, *15*, 3295. [\[CrossRef\]](#)
24. Guo, M.; Jin, J.; Liu, Y.; Nainar, S.K. Non-traditional Banking Activities and Bank Financial Reporting Quality. *Asia-Pac. J. Financ. Stud.* **2021**, *50*, 238–264. [\[CrossRef\]](#)
25. Azadani, M.N.; Boukerche, A. Driving behavior analysis guidelines for intelligent transportation systems. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 6027–6045. [\[CrossRef\]](#)
26. Soleymanian, M.; Weinberg, C.B.; Zhu, T. Sensor data and behavioral tracking: Does usage-based auto insurance benefit drivers? *Mark. Sci.* **2019**, *38*, 21–43. [\[CrossRef\]](#)
27. Liu, Z.; Shen, Q.; Ma, J. A driving behavior model evaluation for UBI. *Int. J. Crowd Sci.* **2017**, *1*, 223–236. [\[CrossRef\]](#)
28. Händel, P.; Ohlsson, J.; Ohlsson, M.; Skog, I.; Nygren, E. Smartphone-based measurement systems for road vehicle traffic monitoring and usage-based insurance. *IEEE Syst. J.* **2013**, *8*, 1238–1248. [\[CrossRef\]](#)
29. Neyestani, N.; Damavandi, M.Y.; Shafie-Khah, M.; Contreras, J.; Catalão, J.P. Allocation of plug-in vehicles' parking lots in distribution systems considering network-constrained objectives. *IEEE Trans. Power Syst.* **2014**, *30*, 2643–2656. [\[CrossRef\]](#)
30. Ali, M.S.; Vecchio, M.; Pincheira, M.; Dolui, K.; Antonelli, F.; Rehmani, M.H. Applications of blockchains in the Internet of Things: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 1676–1717. [\[CrossRef\]](#)
31. den Hartog, J.; Zannone, N. Security and privacy for innovative automotive applications: A survey. *Comput. Commun.* **2018**, *132*, 17–41.
32. Wu, S.; Chen, Y.; Wang, Q.; Li, M.; Wang, C.; Luo, X. CReam: A smart contract enabled collusion-resistant e-auction. *IEEE Trans. Inf. Forensics Secur.* **2018**, *14*, 1687–1701. [\[CrossRef\]](#)
33. Muzumdar, A.; Modi, C.; Madhu, G.M.; Vyjayanthi, C. A trustworthy and incentivized smart grid energy trading framework using distributed ledger and smart contracts. *J. Netw. Comput. Appl.* **2021**, *183*, 103074. [\[CrossRef\]](#)
34. Tolmach, P.; Li, Y.; Lin, S.W.; Liu, Y.; Li, Z. A survey of smart contract formal specification and verification. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 1–38. [\[CrossRef\]](#)
35. Jiao, Y.; Wang, P.; Niyato, D.; Suankaewmanee, K. Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks. *IEEE Trans. Parallel Distrib. Syst.* **2019**, *30*, 1975–1989. [\[CrossRef\]](#)
36. Guo, F.; Yu, F.R.; Zhang, H.; Li, X.; Ji, H.; Leung, V.C. Enabling massive IoT toward 6G: A comprehensive survey. *IEEE Internet Things J.* **2021**, *8*, 11891–11915. [\[CrossRef\]](#)
37. Lin FY, S.; Lin, W.Y.; Tai, K.Y.; Hsiao, C.H.; Yang, H.J. A Usage-Based Insurance Policy Bidding and Support Platform Using Internet of Vehicles Infrastructure and Blockchain Technology. In *Advanced Information Networking and Applications. Proceedings of the 35th International Conference on Advanced Information Networking and Applications (AINA-2021)*; Springer International Publishing: Cham, Switzerland, 2021; Volume 2, pp. 240–249.

38. Naz, M.; Al-zahrani, F.A.; Khalid, R.; Javaid, N.; Qamar, A.M.; Afzal, M.K.; Shafiq, M. A secure data sharing platform using blockchain and interplanetary file system. *Sustainability* **2019**, *11*, 7054. [\[CrossRef\]](#)
39. He, Q.; Xie, X.; Wang, Y.; Ye, D.; Chen, F.; Jin, H.; Yang, Y. Localizing runtime anomalies in service-oriented systems. *IEEE Trans. Serv. Comput.* **2016**, *10*, 94–106. [\[CrossRef\]](#)
40. Saggi, M.K.; Jain, S. A survey towards an integration of big data analytics to big insights for value-creation. *Inf. Process. Manag.* **2018**, *54*, 758–790. [\[CrossRef\]](#)
41. Campanile, L.; Iacono, M.; Marulli, F.; Mastroianni, M. Designing a GDPR compliant blockchain-based IoV distributed information tracking system. *Inf. Process. Manag.* **2021**, *58*, 102511. [\[CrossRef\]](#)
42. Asante, M.; Epiphaniou, G.; Maple, C.; Al-Khateeb, H.; Bottarelli, M.; Ghafoor, K.Z. Distributed ledger technologies in supply chain security management: A comprehensive survey. *IEEE Trans. Eng. Manag.* **2021**, *70*, 713–739. [\[CrossRef\]](#)
43. Kaur, S.; Chaturvedi, S.; Sharma, A.; Kar, J. A research survey on applications of consensus protocols in blockchain. *Secur. Commun. Netw.* **2021**, *2021*, 6693731. [\[CrossRef\]](#)
44. Akbar, N.A.; Muneer, A.; ElHakim, N.; Fati, S.M. Distributed Hybrid Double-Spending Attack Prevention Mechanism for Proof-of-Work and Proof-of-Stake Blockchain Consensuses. *Future Internet* **2021**, *13*, 285. [\[CrossRef\]](#)
45. Feng, J.; Zhao, X.; Chen, K.; Zhao, F.; Zhang, G. Towards random-honest miners selection and multi-blocks creation: Proof-of-negotiation consensus mechanism in blockchain networks. *Future Gener. Comput. Syst.* **2020**, *105*, 248–258. [\[CrossRef\]](#)
46. Ghosh, B.C.; Bhartia, T.; Addya, S.K.; Chakraborty, S. Leveraging public-private blockchain interoperability for closed consortium interfacing. In *IEEE Infocom 2021-IEEE Conference on Computer Communications, Virtual, 10–13 May 2021*; IEEE: Piscataway, NJ, USA, 2021; pp. 1–10.
47. Casino, F.; Lykousas, N.; Katos, V.; Patsakis, C. Unearthing malicious campaigns and actors from the blockchain DNS ecosystem. *Comput. Commun.* **2021**, *179*, 217–230. [\[CrossRef\]](#)
48. Omolara, A.E.; Alabdulatif, A.; Abiodun, O.I.; Alawida, M.; Alabdulatif, A.; Arshad, H. The internet of things security: A survey encompassing unexplored areas and new insights. *Comput. Secur.* **2022**, *112*, 102494. [\[CrossRef\]](#)
49. Alharbi, F.; Zakariah, M.; Alshahrani, R.; Albakri, A.; Viriyasitavat, W.; Alghamdi, A.A. Intelligent Transportation Using Wireless Sensor Networks Blockchain and License Plate Recognition. *Sensors* **2023**, *23*, 2670. [\[CrossRef\]](#)
50. Chen, S.; Mi, H.; Ping, J.; Yan, Z.; Shen, Z.; Liu, X.; Zhang, N.; Xia, Q.; Kang, C. A blockchain consensus mechanism that uses Proof of Solution to optimize energy dispatch and trading. *Nat. Energy* **2022**, *7*, 495–502. [\[CrossRef\]](#)
51. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. A survey on the adoption of blockchain in iot: Challenges and solutions. *Blockchain Res. Appl.* **2021**, *2*, 100006. [\[CrossRef\]](#)

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.