applied sciences

MDPI

Article

Authenticity, and Approval Framework for Bus Transportation Based on Blockchain 2.0 Technology

Tariq J. S. Khanzada [1,2,*], Muhammad Farrukh Shahid [3,*], Ahmad Mutahhar [1,4], Muhammad Ahtisham Aslam [1,5], Rehab Bahaaddin Ashari [1], Sarmad Jamal [3], Mustafa Nooruddin [6] and Shahbaz Siddiqui [3]

1 Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia; ahmed.mutaher@gmail.com (A.M.); muhammad.ahtisham.aslam@fokus.fraunhofer.de (M.A.A.); rashary@kau.edu.sa (R.B.A.)
2 Computer Systems Engineering Department, Mehran University of Engineering and Technology (UET), Jamshoro 76062, Pakistan
3 FAST School of Computing, National University of Computer & Emerging Sciences (FAST-NUCES), Karachi 75030, Pakistan; sarmadjamal2002@gmail.com (S.J.); shahbaz.siddiqui@nu.edu.pk (S.S.)
4 Higher Committee for Monitoring of Pilgrims Transportation, Makkah 24242, Saudi Arabia
5 Fraunhofer FOKUS, 10589 Berlin, Germany
6 College of Engineering, Karachi Institute of Economics and Technology, Karachi 75190, Pakistan; mustafanooruddin37@gmail.com
* Correspondence: tkhanzada@kau.edu.sa (T.J.S.K.); mfarrukh.shahid@nu.edu.pk (M.F.S.)

Abstract: The intelligent transport system (ITS) has transformed urban transportation, enhancing daily commutes with services like congestion management, vehicle crash prevention, traffic control, roadside safety, breakdown assistance, ticket booking, vehicle registration, and insurance. However, in urban bus transportation, the ITS faces security threats, such as data forgery and manipulation. To counter these challenges, a blockchain-based framework for bus transportation approval is proposed, ensuring data integrity and security. The framework's performance is evaluated based on processing time, central processing unit (CPU), graphical processing unit (GPU), cloud usage, and memory consumption, and compared to Ethereum and Aurora testnet, in terms of gas cost, security, and performance. Stochastic algorithms, including the genetic algorithm and Tabu search, are used for time complexity analysis, to obtain an optimized solution. The decision-making trial and evaluation laboratory (DEMATEL) analysis is also performed to assess factors like transaction costs, execution time, memory consumption, and security. The results show that execution time, memory consumption, and processing time are crucial, while transaction cost, reliability, and transparency positively impact the system's effectiveness. By reducing the risk of false data presentation and ensuring accurate records, the proposed framework contributes to a more efficient and reliable transportation system.

Keywords: blockchain; ledger; ITS; cryptography; Ethereum; IoV; V2X; DEMATEL; Tabu search; genetic algorithm

Citation: Khanzada, T.J.S.; Shahid, M.F.; Mutahhar, A.; Aslam, M.A.; Ashari, R.B.; Jamal, S.; Nooruddin, M.; Siddiqui, S. Authenticity, and Approval Framework for Bus Transportation Based on Blockchain 2.0 Technology. *Appl. Sci.* **2023**, *13*, 11323. https://doi.org/10.3390/app132011323

Academic Editors: Roland Jachimowski and Michał Kłodawski

Received: 11 September 2023
Revised: 7 October 2023
Accepted: 9 October 2023
Published: 15 October 2023

1. Introduction

The expansion of city structures, due to increasing populations, has resulted in a huge amount of traffic on roads and highways. This escalation has brought a variety of challenges to the urban transportation system, which demands State-of-the-Art solutions equipped with the latest technologies. These challenges include road congestion, traffic jams, accidents, roadside safety, the availability of transport, vehicle maintenance, and many more. Such problems directly influence people's lives and affect a nation's economy. For instance, it is cumbersome to be stuck in traffic while going to the office for an important business meeting, to be unable to find a proper seat booking system from the local transportation service, or not to get an intimation about road blocking due to an ongoing

protest. Therefore, it is imperative to incorporate the latest technologies into facilitating urban transportation systems. Introducing information and communication techniques into the transport system gives rise to the concept of an intelligent transport system (ITS). It helps to address challenges, such as traffic congestion, transport availability, road safety, blockages on the routes, alternate route information, vehicle breakdown recovery, and many more [1]. Moreover, it also facilitates reducing commute times during travel and waiting times at bus or train stops, while adding comfort to the lives of people. An ITS is the backbone of a smart city: it reshapes the whole transportation mechanism of the city, with the latest technologies, and it greatly enhances the commuting experience of the people [2]. Communication among different vehicles, pedestrians, cyclists, and roadside objects is essential in an ITS, to get updates about road conditions, traffic situations, and many more things, and, therefore, the internet of vehicles (IoV) and vehicle-to-everything (V2X) are the backbone of an ITS system [3,4]. According to the US Department of Transportation, the internet of vehicles (IOV) can reduce the chances of car crashes significantly, by communicating effectively among vehicles [5]. It also facilitates avoiding traffic jams, blocked or congested roads, etc. [6,7]. Nowadays, blockchain has been considered in ITSs, to further enhance the system and improve network security. Introduced initially for the financial sector, blockchain has later been considered and implemented in many other sectors, such as healthcare, supply chain management, banking, transportation, and others. Blockchain has significantly altered digital currencies [1]. Blockchain is a decentralized database with no single point of failure. Before addressing the specifics of blockchain, it is important to note that we are talking about an alternative to traditional databases, not a replacement. Conventional databases outperform blockchain in a variety of real-time scenarios, and use cases and are also more versatile, easier to build, and easier to manage. As a result, traditional databases will survive and be widely used for the foreseeable future. Blockchain was initially adopted as a financial technology (fintech), which was a pioneering step, and it then followed the supply chain technology [8], which has expanded to public administration, transport, and logistics. It is based on a decentralized, transparent, and tamper-proof framework that can maintain transaction logs within the network. Blockchain maintains real-time information, transaction transparency, and the changing of records and data, making it a more secure, versatile, and trustworthy technology. The adaptation of blockchain to the IoV can greatly enhance network security, reliability, and efficiency. The authors in [9] studied the usage of blockchain technology in the used car market, with the goal of eradicating fraud by building a secure ledger to document the events that occur over a vehicle's life cycle. Moreover, the paper suggests that developing a blockchain-based system to perform logging and tracking of vehicle data is vital, as the market for used automobiles is a crucial economic sector that is defined by multiple players and has significant potential for fraud (for example, odometer fraud). Mendiboure et al. [10] studied and compared the current deployments of blockchain technology, to improve security, increase privacy, and trust in vehicular networks. But, more crucially, they looked into the main obstacles to merging vehicular networks and blockchain technology (such as performance evaluation and limits on vehicular networks).

Motivation

Intelligent transportation is a crucial component of smart cities, as it plays a vital role in enhancing the quality of life. Smart transport systems employ advanced technologies and data, to provide safe, reliable, and convenient transportation solutions. Intelligent transport systems can optimize traffic flow, traffic delays, passenger queries, vehicle registration, maintenance checks, and transportation approvals from the concerned authorities (the bus approval process involves an administrator, a coordinator, and bus companies). To provide citizens with efficient and convenient transport services, intelligent transport systems must automate processes, such as registration, seat reservations, and vehicle-related approvals, which fall under intelligent transport's inter-process communication. Automation can help expedite processes like bus route registration and seat reservations, thereby improving

the overall passenger experience. However, during inter-process communication in the transport system, it is essential to keep in mind that security is a top priority. Regarding vehicle approvals in a conventional transportation system around the world, three entities are usually involved: the authorized organization, the coordinator, and the bus operators providing transportation facilities. Bus companies acquire approval from the authorized organization through the coordinator, by going through the documentation process. The coordinator acts as an agent who deals with the bus companies and the authorized organization. The bus approval process may undergo data breaches at different levels during its execution. For example, data may be altered by the coordinator and sent to the authorized entity, bus companies may wrongly register a bus that does not exist or data from the coordinator may be misplaced. Therefore, it is essential to make the entire process secure, smooth, and immutable. The solution is to develop a blockchain-based framework for the bus approval system, as represented in this research work. With blockchain at its core, the system becomes virtually impervious to tampering or unauthorized access. Each piece of data, from bus certifications to maintenance records, is securely stored in a decentralized and immutable ledger (record of entries). This means that once information has been recorded, it cannot be altered or manipulated by any malicious entity. The integrity of the data remains intact, assuring passengers and authorities that they can trust the information provided by the system. This level of data security not only protects against fraudulent certifications or attempts to compromise safety standards but also ensures that every aspect of the bus transportation system operates with transparency and accountability. It guarantees that the bus transportation approval system is not just a technological advancement but a safeguard for the well-being and convenience of our citizens, providing them with a public transportation system they can trust and rely on without hesitation. The overall problems faced by the transport sector are highlighted in Figure 1. The contributions of this paper are multifold:

1. Understanding the bus approval system of a transportation system.
2. Developing a blockchain-based bus approval system (BC-BAS), using blockchain 2.0 technology.
3. Evaluating the BC-BAS performance, by considering various metrics, such as processing time, transaction fees, and registration time.
4. Analyzing the proposed solution, by comparing its performance with and without the use of stochastic algorithms, in terms of processing time.
5. Performing DEMATEL analysis, to identify critical factors of the proposed approach, their effect, and their influence on one other.
6. Deployment of the BC-BAS, and testing of the deployed system.

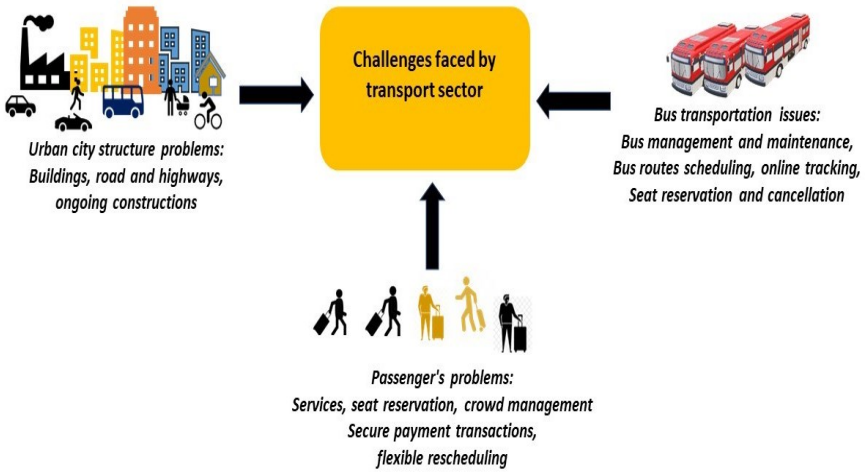

Figure 1. Problems faced by the Transport sector.

The rest of the article is organized as follows: Section 2 presents a blockchain-based deployed system. The problem statement is presented in Section 3, and a review of the literature is provided in Section 4. Our explanation and analysis of the use case and the scenario considered are in Section 5. Section 6 overhauls the methodologies, the proposed solution, the implementation, and the architectural model. The evaluation and exploration of the proposed strategy in relation to current research and industrial practices are discussed in Section 7. In Section 8, the system and the application developed are thoroughly tested. Finally, in Section 9, we conclude the paper, by forecasting the prospects and expanding the functionalities of the implemented approach.

2. Blockchain: Main Applications

2.1. Banking Sector

Blockchain is one of the most eminent technologies, with a pervasive influence on all major industries— particularly, banking, supply chain, and financial services. The technology is being commercialized, and numerous industry groups are releasing use cases exploiting a variety of industrial verticals. Forthcoming applications in digital identity, fundraising, and transactions exhibit tremendous exploitation of blockchain technology in perpetual business applications. A new school of thinking has recently emerged, to foster blockchain in cultivating global efforts to enrich environmental sustainability. According to [11], 44% of organizations worldwide have been involved in using blockchain up to May 2019. In this section, the benefits of recurrent blockchain industrial applications are manifested. These applications are classified according to their domains.

2.2. Healthcare Sector

Patients' data comprise one of healthcare's most sensitive and crucial components. Different providers retain records on their patients in today's healthcare system, yet they frequently cannot or do not share their data with other doctors. The digital transformation has enabled the digitalization of patient information into what is commonly known as an electronic medical record (EMR). The blockchain revelation in the healthcare system is to save administrative time for doctors and equip them to devote more time to their patients and exchange data. MIT researchers have suggested MedRec [12], a health record system based on blockchain that reinstates patients' sovereignty over their medical-related data. It combines a patient's medical data from multiple doctors' databases and concedes them to numerous janitors. Gem [13], which is a startup company, has developed a network based on blockchain technology, to facilitate the development of healthcare applications and to establish an infrastructure for universal healthcare data sharing. Another study introduced the health data gateway (HDG) [14] as an application framework built upon blockchain technology. The HDG enables patients to have authority over their health data, to securely exchange it, and to maintain their privacy. While patients possess ownership of their medical records, they cannot modify, erase, or append any information within these records. Within this architecture, software services are used to define access policies, allowing other entities to access electronic medical records (EMRs) through supplementary services.

2.3. Supply Chain Sector

Logistics management is one of the most promising blockchain applications in supply chain management (SCM). Blockchain technology may be used to track the movement of commodities from the point of origin to the point of consumption. This can aid in ensuring that commodities are delivered on time and in good condition. Overall, blockchain can transform supply chain management. Blockchain can help organizations enhance their supply chains and better serve their customers, by boosting efficiency, traceability, and security. Various logistics activities are connected by traceability systems, such as Provenance [15], which link consumers and suppliers. Another example is Hijro [16], an application that aids in supply chain management globally. In the realm of tracking the origin of goods and

ensuring the complete traceability of items on shelves, Walmart [17] utilizes International Business Machines (IBM) Hyperledger (blockchain) technology. Everledger has employed blockchain technology in the diamond industry. A hybrid of public and private blends of blockchains is used to give permission control while also providing a clear audit trail for the stakeholders [18].

2.4. Energy-Related Sector

The implementation of microgrids showcases one of the prominent applications of blockchain in the energy sector. Microgrids refer to localized networks of integrated and controlled electric power sources designed to enhance energy production, improve consumption efficiencies, and ensure reliable power supply [19]. Multiple energy suppliers and electric power sources establish and possess facilities that integrate distributed power generators, energy storage components, and renewable energy stations. A demonstration of blockchain application is evident in a microgrid that links 130 structures in Brooklyn, New York. This utilization eliminates the middleman's need to facilitate energy transactions among these buildings [20].

3. Problem Statement

The existing transportation system is mostly characterized by automation, whereby the majority of its operations are executed via automated means. The vehicle approval process (bus approval in our case)—which involves the administrator, coordinator, and bus companies—is subject to the risk of data breaches. There are security apprehensions about the transmission of data during inter-process communication within the transport application that may result in the possibility of message falsification. Some of the highlighted security challenges are given below:

1. **Unauthorized Access:** There are concerns over unauthorized access to crucial data, which can jeopardize the integrity of the system.
2. **Data Manipulation:** The potential for data to be subjected to unauthorized tampering or alteration, resulting in the generation of inaccurate instructions or the execution of erroneous operations within the transportation system. Some of those that are related to the bus approval system are as follows: Bus companies may supply the wrong data (wrong bus number, incorrect bus model) while filling out the registration form. The coordinator can manipulate the information and amend the data. For example, it can alter bus road fitness certification expiration dates, modify seat information, and other forgeries can be inscribed. The administrator may approve a bus that was not fully registered, was in a faulty condition, or did not have a road fitness certificate.
3. **Cybersecurity Risks:** The realm of automated transportation systems encompasses a spectrum of possible attacks and vulnerabilities.

In this work, we have considered the data manipulation challenge, and we have developed a framework bus approval system based on blockchain (the BC-BAS).

4. Review of the Literature

Blockchain is an intriguing new technology that provides an alternative to traditional database systems. Traditional database systems store data on a centralized server. User computers can then request this data and send it to the server as necessary, using a set of standard protocols. These computers are known as client machines, or simply clients. In a client-server architecture, all data are saved on a single server or several servers, which are either stored in a single place or distributed globally, for improved data redundancy and fault tolerance. The security of the data in this system is dependent on the security of the servers (or servers) on which it is stored. If one of the servers is hacked or stops performing for any reason, the data on that server are compromised. As a result, significant care is taken to ensure that the servers are secure and fault-resilient, as they constitute a single point of failure [21]. Bitcoin [22], first released in 2008, has been known as the world's most commonly used digital currency, with a broad range of applications. Surprisingly, it is

supported by a revolutionary mechanism known as distributed ledger technology (DLT), which provides its robust technical base. Blockchain, as described in [23], is fundamentally a distributed database system designed to secure transactional data and other information through a consensus process. It operates by combining data records, known as blocks, into a chain format. The concept of blockchain was introduced in 2008 by Satoshi Nakamoto, an anonymous individual or group responsible for the bitcoin white paper. Blockchain is also an immutable ledger, which makes it difficult to change or tamper with data [24]. It provides a high-quality and secure data exchange channel with a bounty of efficient decentralized cryptography algorithms. By leveraging blockchain technology, the network is able to securely record transactions and monitor assets. Assets, which can include both tangible and intangible objects of value, are meticulously tracked, through a list of records known as blocks. These blocks undergo encryption, using sophisticated cryptographic functions, ensuring their integrity and protection against any unauthorized changes. In addition, blockchain facilitates faster and more cost-effective data exchange operations and transactions, compared to traditional systems. Described as a trustless system, blockchain operates on the principle that participants in a transaction do not need to place trust in specific individuals [25]. Instead, transactions are facilitated through a predefined set of rules and algorithms embedded within the blockchain protocol. The trustless nature of blockchain decentralizes transaction approval across multiple network participants, resulting in the need for trust being irrelevant. However, trust remains a fundamental and widely acknowledged characteristic of blockchain, which extends beyond its trustless paradigm. In the context of blockchain-supported supply chains, transportation, and logistics, there are various other characteristics that contribute to building trust in the system.

Currently, asset ownership verification and transaction processing predominantly rely on intermediation. Intermediaries play a crucial role in scrutinizing each participating party within a chain of intermediaries. As highlighted in [26], the prevailing practice of third parties collecting personal data introduces the inherent risk of security breaches. Nevertheless, this approach not only incurs significant time and financial costs but also entails credit risk in the event of intermediary failure. However, blockchain technology—often referred to as a shift from relying on human trust to relying on mathematical algorithms—offers a solution to address these critical aspects [27]. The need for human intervention is eliminated in blockchain, promising a more efficient and secure system. Tengfei et al. [28] developed a blockchain-based traffic service management system. It resolves the cross-organization cooperation and settlement process, streamlining intelligent traffic planning and route scheduling. An enhanced authentication mechanism known as decentralized authentication or Web 3.0 authentication is proposed, which provides a solution to existing third-party security providers dependent on authentication schemes [29]. Jabbar et al. [1] and Guo et al. [30] compared and identified the strengths and limitations of the blockchain-based system's implementation, and they summarized future directions. A solution was modeled in work [31] to overcome the limitations of existing data management practices using a centralized approach. The work presented in [32] proposed an efficient and lightweight system that utilizes the characteristics of authorization encryption schemes and hash functions. It establishes a secure channel by encrypting a session key and verifying the authenticity of the user.

Yang et al. [33] proposed a trustworthy and reliable distributed blockchain network, in which vehicle users can validate incoming messages from nearby vehicles. The work in [34] explored distributed ledger technologies and compared data on different consensus algorithms; it also introduced an intelligent transport system, FlexiChain 3.0, which has higher transaction speed. A deep reinforcement learning blockchain system [35] to accelerate the block verification process, achieving better security and privacy, was proposed. Xiaohong et al. [36] proposed a data sharing and storage system, for more secure and reliable system evaluation than existing systems. The authors in [37] proposed a context-aware offloading approach in mobile edge computing (MEC), utilizing Bayesian learning automata (BLA) to enhance the offloading algorithm's performance. It analyzes the states and

actions of the system, to determine the offloading algorithm, and it diverts the processes to edge computing. Table 1 provides a comparative analysis between existing solutions and a proposed solution, in the context of authentication, authorization, confidentiality, and DEMATEL analysis. Among the existing solutions, there is variability in their strengths and weaknesses.

Table 1. Comparative analysis of existing solutions and the proposed solution.

S-No	Studies	Authentication	Authorization	Confidentiality	DEMATEL Analysis
1	[38]	✓	✓	x	x
2	[39]	✓	x	✓	x
3	[40]	✓	x	✓	x
4	[41]	x	x	✓	x
5	[42]	✓	✓	✓	x
6	[43]	✓	✓	✓	x
7	[44]	x	✓	x	x
8	[45]	✓	✓	x	x
9	[46]	✓	x	x	x
10	[47]	✓	✓	✓	x
11	[48]	x	✓	x	x
12	**Proposed**	✓	✓	✓	✓

Blockchain implementation is built on four key concepts: distributed ledger, cryptography, consensus protocol, and smart contracts [49].

A. Distributed Ledger

Distributed ledgers, Ref. [22], are databases that are shared among all nodes in a peer-to-peer (P2P) network. Each network node maintains a backup copy of the database. Whenever any node modifies its copy version of the database, the other nodes in the network coordinate and integrate with the updated version. Distributed ledgers serve as repositories for various types of data, including land records, cryptocurrency transactions, degree verification, patient health records, and related datasets.

B. Cryptographic Functions

User trust in the blockchain network is ensured through the use of cryptographic functions, which encrypt transactions within the network [50]. These functions use mathematical calculations to protect network transactions from fraudulent users. To complete the transactions, the end user employs a public and private key pair. Public keys are used to identify end users, whereas private keys are used to validate transactions.

C. Consensus Mechanism

It is the process in which all or majority of network validators approve and agree on the ledger's state. It encompasses a set of predefined rules, protocols, and procedures that enable multiple active nodes to maintain a coherent set of states. Consequently, transactions are not immediately recorded in the ledger but rather undergo a consensus mechanism where they are included in a block for a specific duration [23]. When selecting a consensus algorithm, developers consider the requirements of the application. For instance, bitcoin [22] employs proof of work (PoW), to safeguard against double-spending attacks. By contrast, Ethereum, founded by Vitalik Buterin, utilizes proof of stake (PoS), to prevent the centralization of mining centers. Private blockchains often employ hybrid protocols, such as proof of authority (PoA) [51], which enhance practical byzantine fault tolerance (PBFT) by achieving consensus across smaller networks, known as federates.

D. Smart Contracts

Szabo was the first to introduce and coin the phrase smart contract [52]. Smart contracts function in the same way as formal contracts or agreements signed by two parties. Smart contracts are computer language scripts that are designed to execute when specific events occur within the system. In the case of bitcoin, preference is given to simpler and less expressive programming languages. However, platforms like Ethereum (using Solidity) and Hyperledger (using Golang) utilize Turing complete programming languages, to enable the creation of more complex smart contracts. These smart contracts can regulate ownership rights over a wide range of assets, both tangible (such as houses and automobiles) and intangible (including shares and access rights). Ethereum stands out as a prominent example of blockchain technology that considers smart contracts as first-class citizens in its ecosystem.

4.1. Blockchain Types

Blockchain has been further classified into multiple types, depending on the features it has and the functions it carries out. Each type has its own specific use case.

4.1.1. Permission-Less Blockchain

Permission-less blockchain is, at its core, a public blockchain platform. It is a shared network with no restrictions on participation [53]. In such blockchain networks, anyone from anywhere in the world can join and become a validator. These networks are fully decentralized and feature the highest levels of security and openness. Major blockchains in use today, including Bitcoin, Ethereum, and Litecoin, are characterized as permission-less or public blockchains. These chains involve the replication and storage of complete copies of the ledger across multiple locations worldwide, providing great resistance to and security from hackers and tampering. Participants can stay anonymous because no identity is required to gain access to the system [54].

4.1.2. Permissioned Blockchain

In contrast to permission-less blockchains, a permissioned blockchain requires explicit network clearance to access the chain and ledger. These are private networks that function as closed ecosystems, allowing only those authorized by the central authority to access or validate transactions [54]. They are substantially less transparent than permission-less chains and, thus, appropriate for situations involving sensitive data. They are useful for organizations such as banks and private corporations that desire complete control over their data. Ripple and Hyperledger are two examples of permissioned blockchains [55].

4.2. Approval Processes

Approval processes are a critical component of every organization's administration [56], as they sanction business activities through the different checks and balances required to attain an organizational goal. Traditionally, approval processes are carried out using a variety of techniques. Examples of approaches to managing business processes include business process management (BPM) [57], rule-based approaches [58], and workflow management [59]. BPM systems have conventionally focused on document-centric workflows, human-centric, and system-centric [60]. Research conducted by [61] indicates that document-centric workflows are heavily reliant on paperwork. Various proprietary workflow management systems, such as FlowLogic, FlowMan [62], FloWare, and FlowMark (IBM) [63], are commercially available. These technologies typically adopt a centralized client–server architecture and incorporate a archive for centralized content storage. The workflow management systems built on these platforms adhere to predefined rules.

5. Use Case Implementation

To illustrate a potential misuse of intelligent transport in a smart city scenario, consider the following use case: A bus company seeks approval from administrative authorities to

operate within the city. Unfortunately, a security or data breach in the system managing these approvals leads to incorrect approvals being granted. This vulnerability has also been exploited by malicious entities for their own gain. Smart cities with connected administrative systems for transportation introduce new concerns regarding the security and integrity of approval processes. To address this security issue, we propose a design that utilizes a decentralized approach, leveraging smart contracts to tackle the security challenges associated with the approval process. In our proposed design, the verification of a bus company seeking approval is conducted through blockchain technology, ensuring a more secure and tamper-resistant process. After successful verification, the message is forwarded to the next process by interacting with the smart contract for security verification of previous inter-process communication, as shown in Figure 2. To model the approval of buses in the ITS, we first represent each bus as a_i at any given time, and each node of buses executes the inter-process communication system of the ITS, represented by c. Initially, transportation companies send their bus data to the client nodes, which then send a request to the administrator. The ITS system processes the request by passing the message to different inter-processes within their system. All the passed messages first interact with the smart contract, to ensure the security verification of the process to communicate with other connected processes. Equation (1) represents the mathematical model of the proposed intelligent ITS system:

$$Bus_{nodes} = [a_1^C, a_2^C, a_3^C, ...a_{10}^C] \tag{1}$$

$$\begin{cases} a_1 = \text{Number of Bus Nodes} \\ C = \text{Process of ITS System} \end{cases}$$

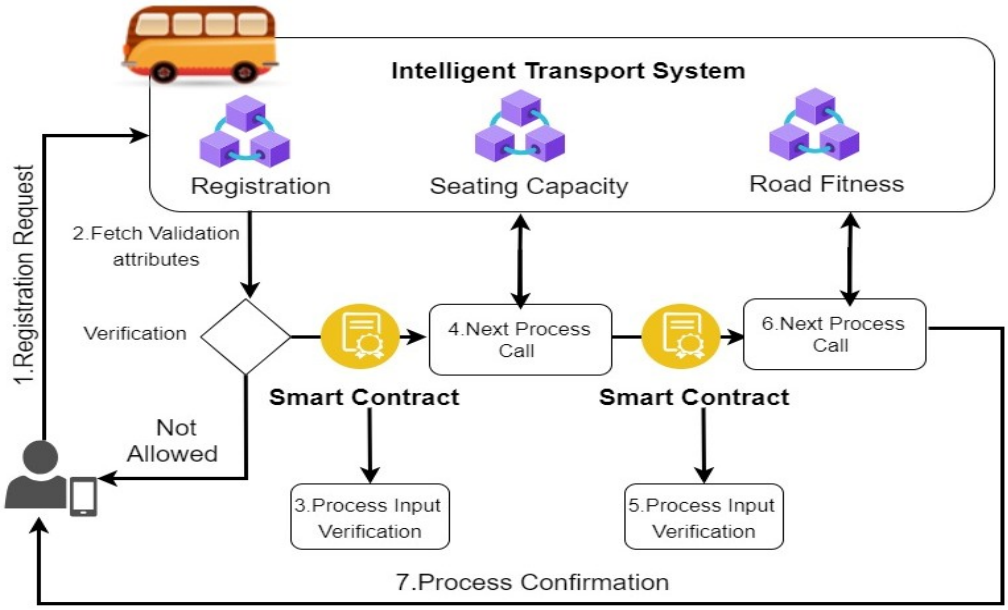

Figure 2. Proposed usecase scenario.

6. Methodology

This study employs a structured approach to constructing a blockchain system for bus approval. Specifically, we employ a framework based on the Ethereum blockchain. The reason behind selecting Ethereum as the underlying blockchain technology will be elucidated in the subsequent sections.

Developing Blockchain Framework

The complete application process from the bus company registering itself for approval is fostered. The process includes all the stakeholders, i.e., the bus company, the coordinator, and the administration, as shown in Figure 3. The bus company requests the coordinator

for portal access. After successful registration, the company then applies for approval. The coordinator and the administrator can also access and view the pending application as well as the approved application on their respective dashboards. It also shows the data transfer process to the interplanetary file system (IPFS), which is then logged onto the blockchain. The IPFS is a distributed file system that allows data sharing and storage in peer-to-peer mode. It solves several problems associated with traditional client–server file systems, assures data security, preserves users' privacy, and enables scaled communications. Unlike the location-addressing approach used by HTTP and other protocols, the IPFS searches for data by using content addressing. Using the interplanetary linked data (IPLD) protocol, the IPFS may share information with blockchain and smart contracts. The IPFS's major components are distributed hash tables for routing(DHT), Merkle trees for encryption, and directed acyclic graphs for representations (DAG). The IPFS decentralization delivers low latency and high throughput while also making the system safe and tamper-proof. For all these transactions and processes to be completed, fees are charged, which are deducted from the user wallet, i.e., "Metamask" in our implemented approach.

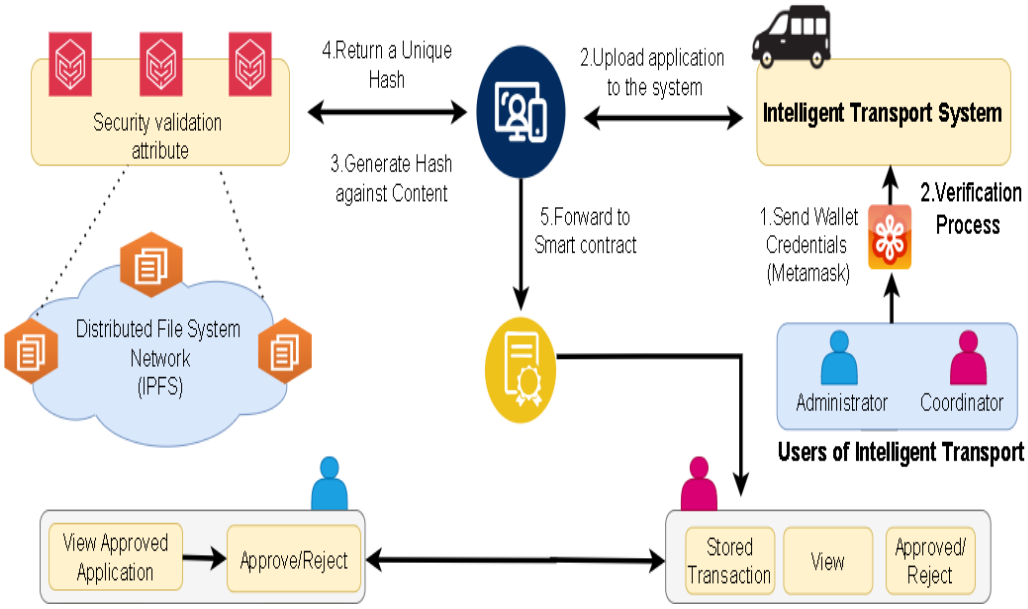

Figure 3. Application approval process.

In Figure 4, we present the sequence diagram depicting the registration and authentication procedures. Within this context, the user, representing the bus company, initiates the process of gaining access to the bus company portal by means of registration through an online form. The form requests key credentials from the user. Upon the successful submission of the credentials, which also include the Metamask key of the user, used for transactions in the blockchain, access is granted to the user. Metamask is a software cryptocurrency wallet that serves as a gateway to the Ethereum blockchain. It facilitates users to access their Ethereum wallet, using either a mobile application or a web browser extension. This accessibility enables users to seamlessly interact with decentralized applications. Metamask, as one of the meta-transaction implementations, is useful to both users and developers. Metamask simplifies the use of the Ethereum network, particularly for users who may not be acquainted with its operations. It handles complex tasks, such as creating and managing Ethereum accounts, handling keys and wallets, and related procedures. Similarly, developers can easily interface with the Ethereum application programming interface (API) on a global scale, streamlining their development process. Furthermore, a decentralized application (DApp) is used to connect to the network without synchronizing a complete node, because it routes the connection over an Ethereum node provider [64]. The credentials are then transferred to the smart contracts and, if the conditions are met, the mentioned user can access the portal using his Metamask key.

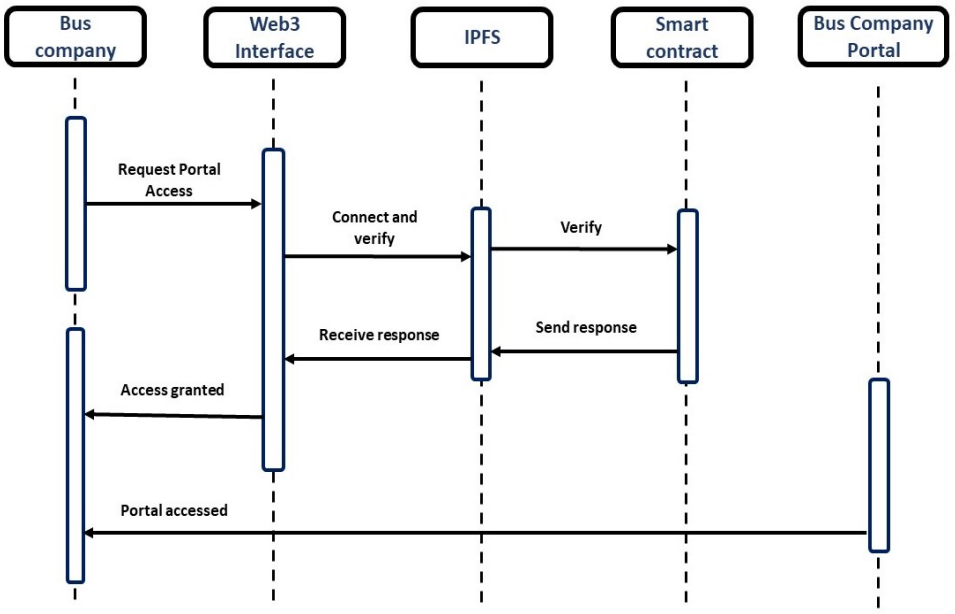

Figure 4. Sequence diagram for registration and authentication.

At this stage, the user has obtained access to the portal, which serves as the platform for submitting applications and seeking approval for bus-related activities. This particular process is illustrated in Figure 5. The bus company uploads an application to the portal; a sample file is also provided to instruct the user about the template of the file to be uploaded. As the ledger only supports textual information, heavier data, such as photos and documents, must be saved to the IPFS. The Web3 user interface (UI) sends the file content to the IPFS, which provides the CID (hash) for the file sent, which is then consequently endorsed on the blockchain. Figure 6 refers to the access control and the relationship between the coordinator and administrator in our implemented system. The coordinator can first view, examine, and inspect the application submitted by the bus company. Upon completion of the prerequisites, the coordinator approves the application, which is then forwarded to the administrator, who can, after a final check, approve or reject the application. The coordinator can also find all the pending applications and approved applications on the dashboard, which is cryptographically secured using the private key. The application can only be forwarded to the administrator when the coordinator has approved it.

The generic software architecture is shown in Figure 7, which facilitates a seamless flow of operations from the HTTP browser layer, where users interact with the system, to the user interface layer that provides an intuitive interface. The smart contracts layer handles the core business logic and enforces predefined rules, while the data access layer based on the IPFS ensures the secure and decentralized storage of data objects. This layered approach enhances the scalability, modularity, and maintainability of the system, allowing for easier updates and modifications to specific layers without impacting the overall architecture.

Algorithm 1 presents the bus user registration process, where the user inputs the required credentials and requests access to the bus portal. Algorithm 2, the second inter-process procedure of the intelligent transport system, is invoked. This procedure is responsible for bus approval application retrieval. The process begins by retrieving the validation attribute from the blockchain, to perform security verification, ensuring that the user is a legitimate participant in the blockchain network. Upon successful security verification, the process is executed, and the application is uploaded to the portal. This involves creating a process object and assigning a digital identity to it. Subsequently, a blockchain transaction is initiated, to record the validation attribute of this process on the blockchain. These data are then sent to the smart contract, triggering the execution of the next inter-process procedure within the system. Finally, in Algorithm 3, the third inter-process procedure of the intelligent transport system is invoked. This procedure is responsible for the approval

of applications uploaded to the portal. First, the validation attribute is retrieved from the blockchain, to verify the user's legitimacy in the network. Upon successful security verification, the execution of the procedure proceeds, approving or rejecting the approval as per the terms and conditions. The time complexity of each interconnected process and the smart contract in the BC-BAS system is $O(N)$. The overall complexity of inter-process communication, along with the smart contract, is $O(N^2)$, which indicates that the system's performance is heavily dependent on the interaction between inter-process communication and the smart contract. The flow chart of the overall process execution is shown in Figure 8.

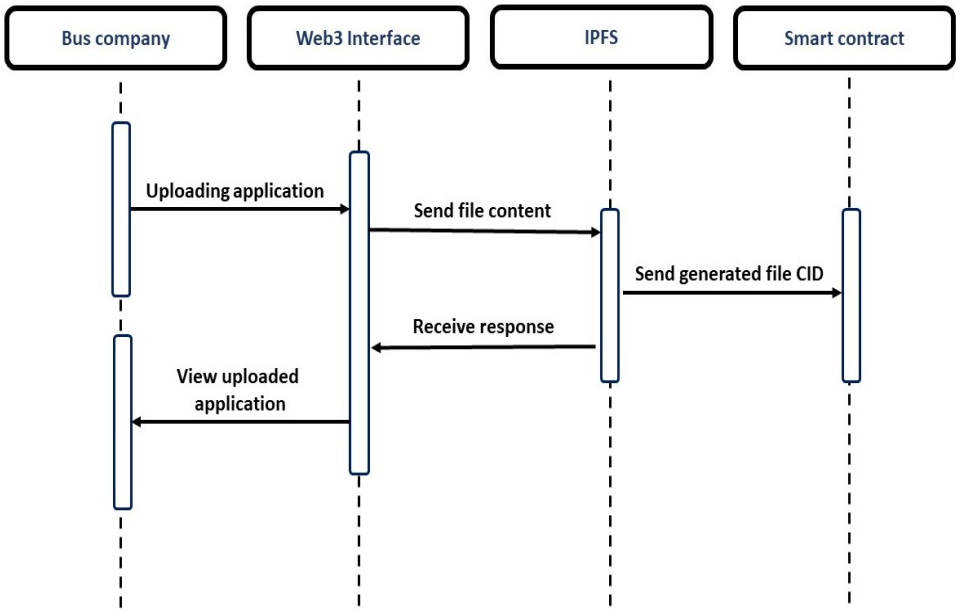

Figure 5. Sequence diagram for uploading application.

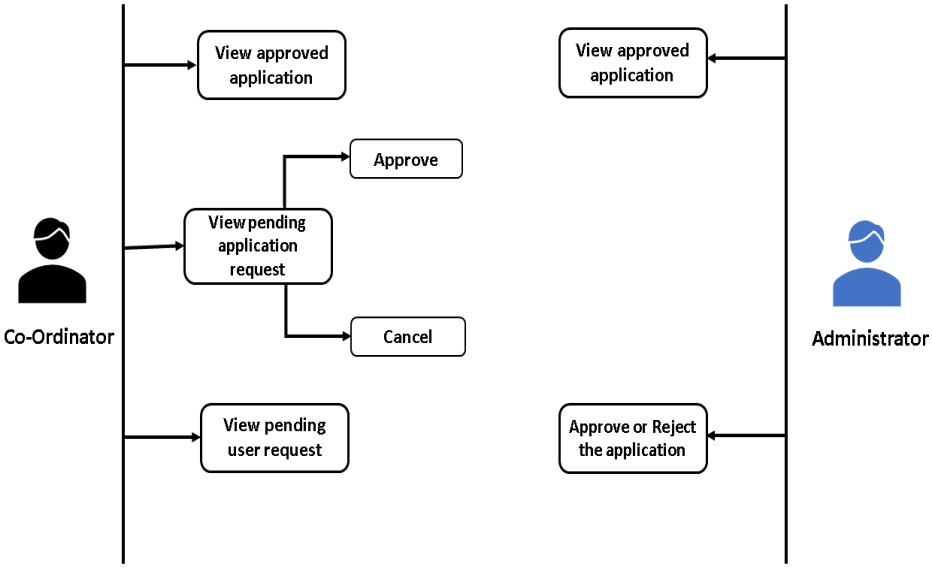

Figure 6. Interaction and relationship between the coordinator and the administration.

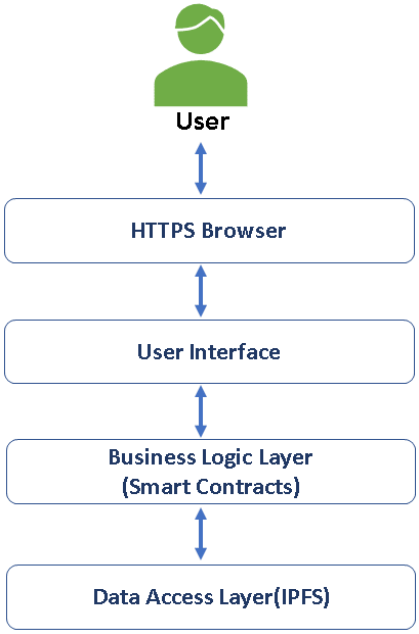

Figure 7. Software Architecture.

Algorithm 1: Bus User Registration

Input: firstName (*str*), email (*str*), publickeyAddress (*str*), organization Address (*str*)
Output: call *registerUser* () that validates the address of the contract deployer and creates a new User

```
if Yes then
    Create a User object Add it to the registeredUsers[] list
else
    Reject Transaction
```

Algorithm 2: Uploading Application

Input: applicationHash (*str*), publickeyAddress (*str*)
Output: call uploadApplication () to store application Data

```
if applicationUploaded then
    Create an application object
    Assign randomId to the application object
    Add it to the applicationList[]
else
    Transaction rejected
```

Algorithm 3: Application Approval

Input: applicationId (*int*), selection (*int*)
Output: call approvalfunction () with the parameters of applicationId and selection

```
if digitalSignatureApproved then
    Filter through the applicationList
    Assign applicationList[index]=selection
    Return result
else
    DigitalSignature not authenticated
    Return
```

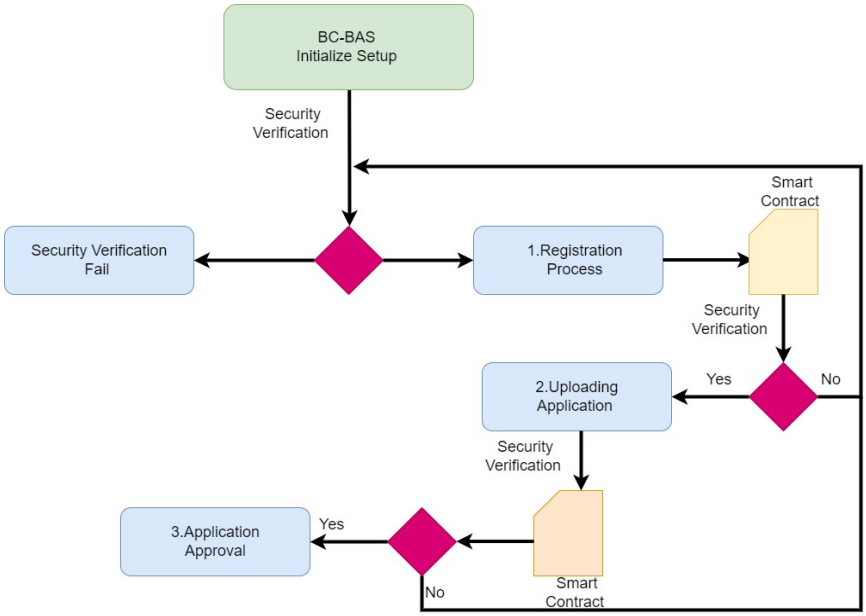

Figure 8. Flow Chart of the Overall Process Execution.

7. Evaluation and Results

In this section, we evaluate the developed blockchain-based bus approval system, in terms of its performance, including gas cost, processing time, memory consumption, and user scalability. The transaction fee, also known as the gas cost, is required, to record the transaction on the blockchain. As the decentralized application is developed on a public blockchain, one has to pay the gas costs to miners, to maintain the Merkle tree-like structure. Merkle trees are a type of data structure used in blockchain, to maintain the transactional record of the network nodes [65]. Figure 9a and Table 2 present an overview of the transaction costs associated with the execution of smart contracts in the use case implemented within the deployed decentralized application (DApp). A decentralized application (DApp) refers to an application that is constructed using blockchain technology. The customary approach involves the use of intelligent contracts to automate procedures, and it depends on a blockchain network for data storage and validation. Decentralized applications (DApps) strive to enhance transparency, security, and trust by integrating blockchain technology. The ITS solution we offer is a technologically sophisticated system that leverages blockchain technology, to enhance transportation management, efficiency, and security. The integration of blockchain into this service is intended to capitalize on the advantages offered by blockchain technology, including decentralization, immutability, and enhanced security. The integration of blockchain technology into ITS services is being pursued, to augment many facets, including security, data integrity, and the possible automation of certain procedures. The process of integration offers many advantages, including the provision of safe data storage, the establishment of tamper-resistant records, and the fostering of trust among participants. The transaction fees for the registration process and application submission are very high compared to other inter-process communications from the BC-BAS. This is due to the first-time connection to the main network and the verification of security validation attributes from the network. The application submission is associated directly with the registration process, which is why the transaction fees for both processes are directly proportional. For application approval and rejection actions, Boolean qualities are employed, to store the after-effect of the application being supported or objected to, bringing about lower gas costs. There are no transaction fees for retrieving any state variable from the blockchain because it takes minimal gas. Figure 9b and Table 3 show a comparison of the processing time of the deployed system. As the number of clients increased, the processing time of each ITS inter-process and smart contract also increased,

indicating the processing strength of the ITS system. The results demonstrate that an increase in the number of users plays a vital role in the performance of the ITS system.

The BC-BAS was tested on various machines. The results are shown in Figure 9c, and the corresponding values are listed in Table 4. We observed substantial differences in performance when implementing the solution on the CPU, GPU, and in the cloud. Therefore, it can be concluded that deploying the solution in the cloud is a better option, as the number of applications increases. The amount of memory consumed by the BC-BAS is depicted in Figure 9d and Table 5. The memory constraints of the BC-BAS were tested using developer tools, and it was found that the event listeners were using a lot of memory, because it is built on JavaScript (JS), which is an event-driven programming language. The heap (a different space for storing data where JS stores objects and functions), which takes up a small amount of memory in the BC-BAS, is followed by nodes that are attempting to construct a tree-like structure, to establish a child–parent relationship.

The relationship between gas cost and processing time is illustrated in Table 6 and Figure 10a, revealing that higher utilization of gas cost leads to faster processing times. The performance of Aurora testnet and Ethereum, in terms of security, concerning the number of users is plotted in Figure 10b, and the corresponding values are listed in Table 7. It demonstrates that the Ethereum main network became more secure as the number of users increased. Similarly, the performance of the mentioned testnet with Ethereum, in terms of increasing number of users, is depicted in Figure 10c, and the corresponding values are listed in Table 8. We can observe that the Ethereum network outperformed the Aurora test network as the number of users increased. Furthermore, both networks are compared in terms of gas cost, as shown in Figure 10d, and the values are listed in Table 9.

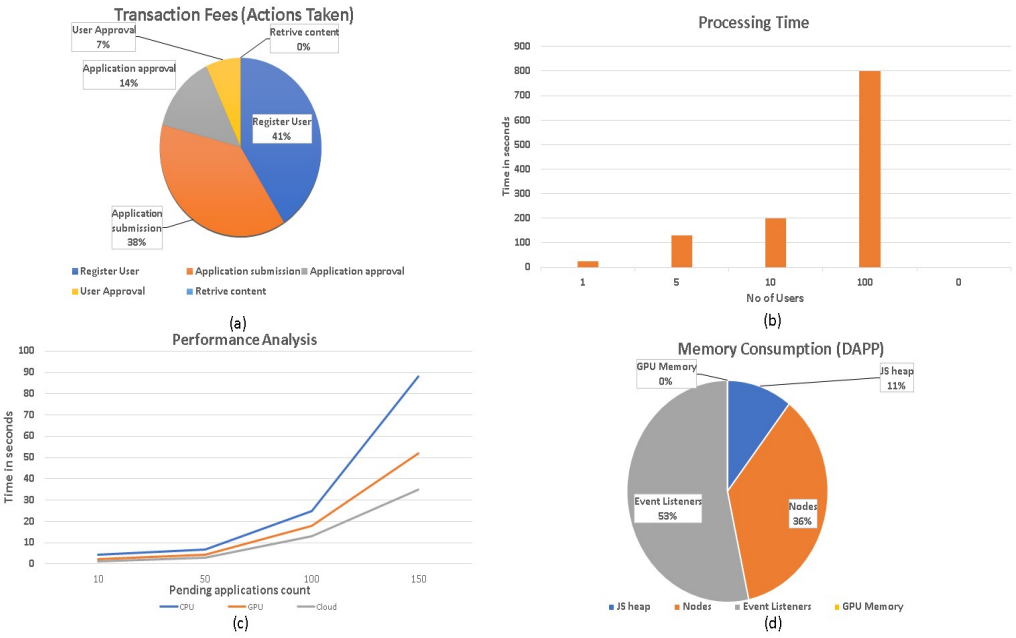

Figure 9. (**a**) transaction fee distribution between different processes, (**b**) processing time, (**c**) execution time, (**d**) memory utilization.

Table 2. Figure 9a. Process vs. transaction fees.

Actions	Transaction Fees (Percentage)
Register user	41.00%
Application submission	38%
Application approval	14%
User approval	7%
Retrieve content	0

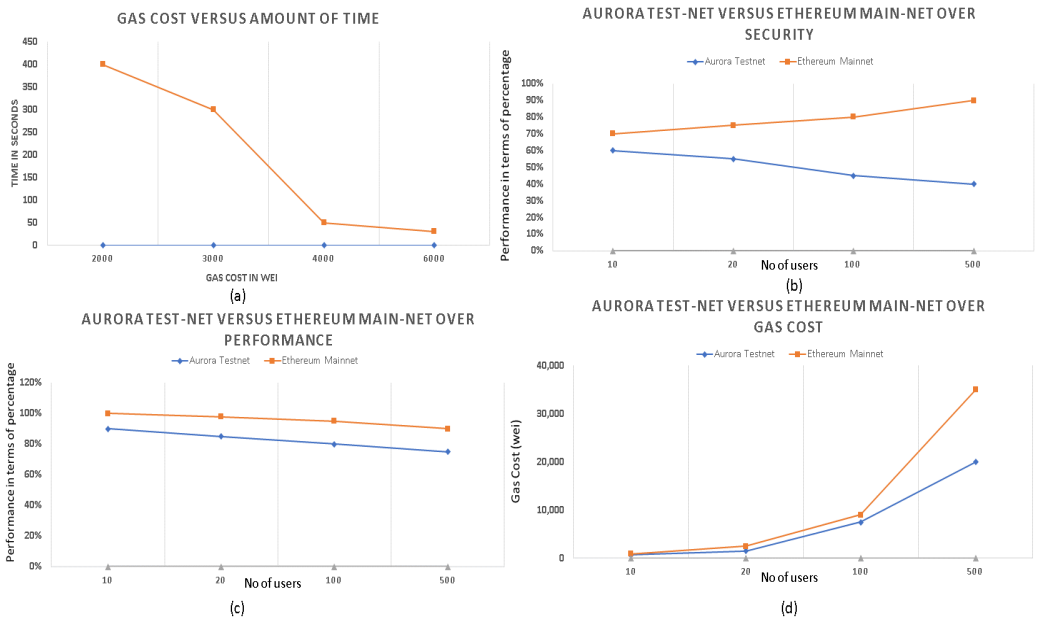

Figure 10. (**a**) Gas cost vs Processing time, (**b**) Security comparison with increasing users (Aurora testnet and Ethereum), (**c**) Performance comparison with increasing users (Aurora testnet and Ethereum), (**d**) Gas cost comparison with increasing users (Aurora testnet and Ethereum).

Table 3. Figure 9b. Number of users vs. processing time.

Index	No. of Users	Processing Time (seconds)
1	1	25
2	5	130
3	10	200
4	100	800

Table 4. Figure 9c. Execution time comparison.

Index	Number of Applications	CPU	GPU	Cloud
1	10	4.3	2.4	1.2
2	50	6.7	4.4	3.1
3	100	25	18	13
4	150	88	52	35

Table 5. Figure 9d. Memory consumption.

Memory Data Structure	Memory (Browser Data)
JS heap	31
Nodes	106
Event listeners	157
GPU memory	0
Web3 injector	3

Table 6. Figure 10a. Gas cost vs. time.

Index	Gas Cost (Wei)	Time
1	2000	400
2	3000	300
3	4000	50
4	6000	30

Table 7. Figure 10b. Comparison between Aurora testnet and Ethereum mainnet regarding security.

Index	Number of Users	Aurora Testnet	Ethereum Mainnet
1	10	60%	70%
2	20	55%	75%
3	100	45%	80%
4	500	40%	90%

Table 8. Figure 10c. Comparison between Aurora testnet and Ethereum mainnet regarding performance.

Index	Number of Users	Aurora Testnet	Ethereum Mainnet
1	10	90%	100%
2	20	85%	98%
3	100	80%	95%
4	500	75%	90%

Table 9. Figure 10d. Comparison between Aurora testnet and Ethereum mainnet regarding gas cost.

Index	Number of Users	Aurora Testnet	Ethereum Mainnet
1	10	700	900
2	20	1500	2500
3	100	7500	9000
4	500	20,000	35,000

7.1. Time Complexity of the Proposed System

To assess the feasibility of the proposed solution, we conducted a series of experiments, by varying the number of users of the BC-BAS system and the selection of administrative nodes to process user requests. Two different approaches were employed: the default proof of stake (PoS) and proof of stake with two distinct stochastic algorithms: the genetic algorithm [66] and Tabu search [67]. Proof of stake is often praised for its energy efficiency compared to proof of work (PoW), as it does not require miners to solve complex mathematical problems. In both stochastic algorithms, computational nodes were determined, based on the least number of pending unspent transactions, thereby enhancing transaction processing efficiency.

Tabu search is a well-established metaheuristic optimization approach specifically tailored to addressing combinatorial optimization issues [67]. Fred W. Glover introduced this concept in the late 1980s. Tabu search is a computational optimization algorithm designed to effectively navigate solution spaces, particularly in scenarios characterized by numerous potential solutions and intricate search landscapes. The genetic algorithm (GA) is an optimization technique inspired by natural selection and genetics [66]. It is commonly employed to obtain approximate solutions for optimization and search issues. Genetic algorithms demonstrate significant efficacy in addressing problems with extensive solution spaces and various feasible solutions. Table 10 presents the processing time performance. Figure 11 illustrates that as we increased the number of users by a constant number of application requests per user the default approach resulted in application access delays, due to the number of pending transactions in processing nodes. Conversely, the processing time decreased with the stochastic algorithm GA approach, leading to fewer pending processing transactions at the nodes. Furthermore, this processing time decreased even more with the stochastic algorithm, the Tabu search approach.

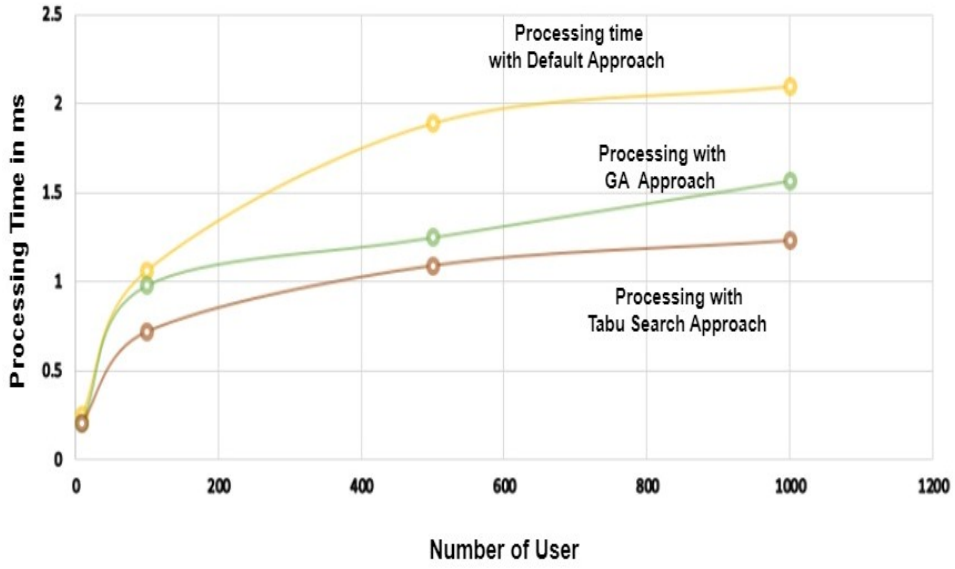

Figure 11. Performance analysis of the proposed solution with and without the stochastic algorithms.

Table 10. Time complexity of system's performance with and without stochastic algorithms.

Number of Users	Processing Time		
	Proof of Stake	Proof of Stake with GA Algorithms	Proof of Stake with Tabu Algorithms
10	0.25	0.21	0.21
100	1.06	0.98	0.72
500	1.89	1.25	1.09
1000	2.098	1.568	1.23

7.2. DEMATEL Analysis

A DEMATEL analysis was further performed for the BC-BAS. The Geneva Research Centre of the Battelle Memorial Institute (GRCBMI) invented the DEMATEL technique, in order to illustrate the structure of complex causal interactions using matrices or digraphs [68]. It is particularly helpful in examining the cause-and-effect interactions between system components, as a type of structural modeling methodology. The DEMATEL is used to investigate and resolve complex, interconnected situations because it proves the interdependence of elements and helps create a map that reflects the relative relationships between them. In pursuit of this analysis, we identified nine critical factors: transaction cost F_1, execution time F_2, memory consumption F_3, processing time F_4, security F_5, portability F_6, scalability F_7, transparency F_8, and reliability F_9. The segments of the DEMATEL analysis are as follows, as shown in Table 11:

- We took the expert's opinion on the BC-BAS in the form of a survey, based on the factors identified in Table 11, and we formed a direct influence matrix, X, shown in Table 12, accounting for the expert score criteria mentioned. The triangular fuzzy number (TFN) method was used to transform human linguistics into a commutable form. The transformation table had the following information: N (no influence) had TFN (0, 0, 0.2), very low influence (VL) had TFN (0, 0.2, 0.4), low influence (L) with TFN (0.2, 0.4, 0.6), high influence with TFN (0.4, 0.6, 0.8), and very high influence (VH) with TFN (0.8, 1, 1) [2].
- After obtaining the direct influence matrix, X, normalization was performed according to Equation (2), where n is the total number of elements in X. The standardized direct influence matrix, $\widetilde{X}$, shown in Table 13, is obtained as the result:

$$\widetilde{X} = \frac{1}{max_{1 \leqslant i \leq n} \sum_{j=1}^{n} x_{ij}}. \quad (2)$$

- The comprehensive influence matrix T, shown in Table 14, is obtained as the next step, according to Equation (3) [2], where I is the identity matrix of size (9 × 9):

$$T = \widetilde{X}(I - \widetilde{X})^{-1}. \tag{3}$$

- Next, we calculated two important factors from the T matrix, which were influence degree D and affected degree R, as shown by Equations (4) and (5) [2]:

$$D_i = \sum_{j=1}^{n} t_{i,j} \tag{4}$$

$$R_i = \sum_{i=1}^{n} t_{i,j}. \tag{5}$$

  Furthermore, centrality and causality were calculated. Centrality was defined as the sum of D and R, and causality was the difference between D and R. The resultant comprehensive impact matrix is shown in Table 15, which contains centrality, causality, affected degree, and influence degree information.
- The overall influence matrix is required, to determine how the overall influence relationship imitates factors in the system, because the comprehensive influence matrix T only shows mutual influence between different factors. Equation (6) [2] calculated the influence matrix H, and its values are shown in Table 16:

$$H = T + I. \tag{6}$$

- The reachable matrix M, as shown in Table 17, was calculated after applying threshold value γ, which was calculated after taking the average of the T matrix. Consequently, M was obtained after some redundant factors were removed, according to Equation (7):

$$\gamma = \sum_{i-1}^{n} \sum_{j=1}^{n} \frac{[t_{i,j}]}{N} \tag{7}$$

$$M = [m_{ij}]_{n*m} \tag{8}$$

$$m_{ij} = \begin{cases} 1, & \text{if } \gamma \geq h \\ 0, & \text{if } \gamma \leq h. \end{cases} \tag{9}$$

From Table 15, it can be analyzed that factors F_1 (transaction cost), F_7 (scalability), and F_8 (transparency) created an effect on other factors, as their causality value was greater than zero. Similarly, it can also be deduced that factors F_2 (execution time), F_3 (memory consumption), F_4 (processing time), F_5 (security), and F_6 (portability) were greatly affected by other factors, as their causality value was less than zero. F_2 (execution time) was affected by F_1 (transaction cost) in the proposed BC-BAS system. Similarly, it can be observed that F_5 (security) was greatly affected by F_8 (transparency). Moreover, F_7 (scalability) had a significant effect on the system's F_6 (portability). Centrality identifies the most important factors in our proposed BC-BAS system. Subsequently, it can be observed that when sorted in descending order, F_2 (execution time), F_7 (scalability), F_9 (reliability), F_3 (memory consumption), and F_5 (security), this order reflects the importance of these factors in our system. It can also be observed that memory consumption is very critical for our system, as shown in Figure 9d. Moreover, the F_2 (execution time), F_4 (processing time), F_7 (scalability), F_8 (transparency), and F_9 (reliability) values reflect that these factors are the most influential elements of the system. For example, F_2 greatly influences the overall system performance. Therefore, the proposed framework must consider the execution time of the system. Hence, Figure 9c depicts the execution time of the application on the CPU, GPU, and cloud.

Table 11. Matrix Key.

F1	Transaction cost
F2	Execution time
F3	Memory consumption
F4	Processing time
F5	Security
F6	Portability
F7	Scalability
F8	Transparency
F9	Reliability

Table 12. Direct Influence Matrix.

	F1	**F2**	**F3**	**F4**	**F5**	**F6**	**F7**	**F8**	**F9**
F1	0	0.85	0.55	0.8	0.3	0.175	0.4	0.35	0.25
F2	0.4	0	0.8	0.7	0.3	0.466	0.83	0.5	0.5
F3	0.54	0.7	0	0.8	0.26	0.1875	0.46	0.35	0.194
F4	0.7	0.8	0.7	0	0.3	0.4	0.556	0.3	0.4
F5	0.2	0.26	0.4	0.183	0	0.55	0.53	0.2075	0.606
F6	0.05	0.46	0.187	0.29	0.556	0	0.6	0.32	0.116
F7	0.3	0.8	0.7	0.7	0.5	0.7	0	0.45	0.8
F8	0.175	0.4	0.54	0.4	0.7	0.55	0.4	0	0.7
F9	0.3	0.7	0.33	0.54	0.7	0.4	0.7	0.7	0

Table 13. Standardized Direct Influence Matrix.

	F1	**F2**	**F3**	**F4**	**F5**	**F6**	**F7**	**F8**	**F9**
F1	0	0.171717	0.111111	0.161616	0.060606	0.035354	0.080808	0.070707	0.050505
F2	0.080808	0	0.161616	0.141414	0.060606	0.094141	0.167677	0.10101	0.10101
F3	0.109091	0.141414	0	0.161616	0.052525	0.037879	0.092929	0.070707	0.039192
F4	0.141414	0.161616	0.141414	0	0.060606	0.080808	0.112323	0.060606	0.080808
F5	0.040404	0.052525	0.080808	0.03697	0	0.111111	0.107071	0.041919	0.122424
F6	0.010101	0.092929	0.037778	0.058586	0.112323	0	0.121212	0.064646	0.023434
F7	0.060606	0.161616	0.141414	0.141414	0.10101	0.141414	0	0.090909	0.161616
F8	0.035354	0.080808	0.109091	0.080808	0.141414	0.111111	0.080808	0	0.141414
F9	0.060606	0.141414	0.066667	0.109091	0.141414	0.080808	0.141414	0.141414	0

Table 14. Comprehensive Influence Matrix.

	F1	**F2**	**F3**	**F4**	**F5**	**F6**	**F7**	**F8**	**F9**
F1	0.245993	0.559616	0.464675	0.515511	0.343057	0.322686	0.447715	0.333951	0.348467
F2	0.359845	0.486019	0.566796	0.565213	0.405065	0.429697	0.586576	0.411435	0.448805
F3	0.333329	0.517451	0.347988	0.498739	0.323464	0.311923	0.439416	0.32109	0.325567
F4	0.391785	0.593622	0.522173	0.413208	0.375243	0.389622	0.511397	0.354533	0.402267
F5	0.219597	0.3664	0.346983	0.321506	0.234258	0.329625	0.38898	0.253794	0.345262
F6	0.17472	0.363061	0.287657	0.307138	0.308836	0.209787	0.370196	0.247088	0.24252
F7	0.359894	0.65688	0.576791	0.591209	0.467168	0.49494	0.477831	0.428321	0.523109
F8	0.266682	0.472126	0.445878	0.432509	0.422971	0.391119	0.446134	0.268098	0.425958
F9	0.325143	0.584128	0.47208	0.513643	0.465951	0.413296	0.552167	0.434261	0.352809

Table 15. Comprehensive Impact Matrix.

	Influence Degree (D)	Affected Degree (R)	Causality (D-R)	Centrality (D + R)
F1	3.58167	2.676988	0.904683	6.258658
F2	4.259452	4.599302	−0.33985	8.858754
F3	3.418967	4.031022	−0.61205	7.449989
F4	3.953851	4.158675	−0.20482	8.112526
F5	2.806404	3.346012	−0.53961	6.152416
F6	2.511004	3.292696	−0.78169	5.803699
F7	4.576141	4.220411	0.35573	8.796552
F8	3.571475	3.052571	0.518904	6.624046
F9	4.113478	3.414765	0.698713	7.528243

Table 16. Overall Influence Matrix.

	F1	F2	F3	F4	F5	F6	F7	F8	F9
F1	1.245993	0.559616	0.464675	0.515511	0.343057	0.322686	0.447715	0.333951	0.348467
F2	0.359845	1.486019	0.566796	0.565213	0.405065	0.429697	0.586576	0.411435	0.448805
F3	0.333329	0.517451	1.347988	0.498739	0.323464	0.311923	0.439416	0.32109	0.325567
F4	0.391785	0.593622	0.522173	1.413208	0.375243	0.389622	0.511397	0.354533	0.402267
F5	0.219597	0.3664	0.346983	0.321506	1.234258	0.329625	0.38898	0.253794	0.345262
F6	0.17472	0.363061	0.287657	0.307138	0.308836	1.209787	0.370196	0.247088	0.24252
F7	0.359894	0.65688	0.576791	0.591209	0.467168	0.49494	1.477831	0.428321	0.523109
F8	0.266682	0.472126	0.445878	0.432509	0.422971	0.391119	0.446134	1.268098	0.425958
F9	0.325143	0.584128	0.47208	0.513643	0.465951	0.413296	0.552167	0.434261	1.352809

Table 17. Reachable Matrix.

	F1	F2	F3	F4	F5	F6	F7	F8	F9
F1	1	1	0	0	0	0	0	0	0
F2	0	1	1	1	0	0	1	0	0
F3	0	1	1	0	0	0	0	0	0
F4	0	1	1	1	0	0	0	0	0
F5	0	0	0	0	1	0	0	0	0
F6	0	0	0	0	0	1	0	0	0
F7	0	1	1	1	0	0	1	0	1
F8	0	0	0	0	0	0	0	1	0
F9	0	1	0	0	0	0	1	0	1

8. Test Bed BC-BAS Application Testing

The designed decentralized application features several user interfaces (UIs), as illustrated in Figure 12. These UIs encompass various components, including the front page layout of the bus company portal, the application access page for administration and coordinators, and the approved application page. Additionally, a sample smart contract metadata is included, which contains comprehensive information about the deployed and activated smart contract.

Our decentralized application (DApp) aims to streamline the process of obtaining approvals for transportation-related activities, by leveraging the benefits of blockchain technology. The three main actors in the system are described as follows:

1. Users:
    - They refer to individuals or bus organizations seeking transport-related approvals.
    - They can submit their requests for approval through the system.
    - They can view the status of their requests and any notifications received.
2. Administrative Entities:
    - These entities are responsible for reviewing and approving transport requests.
    - They have access to the submitted requests and can provide approvals or rejections.

- They can also communicate with the users and coordinator entities through the system.

3. Coordinator Entities:
   - They act as intermediaries between the users and administrative entities.
   - They facilitate the submission and processing of transport requests.
   - They maintain the integrity and transparency of the BC-BAS.

Testing Objectives: The primary objectives for testing the BC-BAS application are as follows:

1. Functionality:
   - Validate that users can successfully submit transport approval requests.
   - Verify that administrative entities can review and approve/reject transport requests.
   - Ensure coordinator entities can effectively manage the communication between users and administrative entities.
   - Confirm that the system accurately reflects the status of requests and provides appropriate notifications.
2. Security:
   - Assess the system's resilience against potential security threats, such as unauthorized access and data tampering.
   - Validate the encryption mechanisms used to protect sensitive data.
   - Verify that access controls are properly implemented and enforced for each actor.
3. Reliability:
   - Evaluate the system's ability to handle a high volume of transport approval requests simultaneously.
   - Verify that the system remains responsive and available during peak usage times.
   - Perform stress testing to identify any performance bottlenecks and ensure the system can scale effectively.

Testing Approach: To achieve the testing objectives, the following testing approach is proposed:

1. Test Case Development:
   - Develop comprehensive test cases covering all functional requirements.
   - Include test cases for both positive and negative scenarios, to ensure robustness.
   - Design test cases, to validate security controls and access restrictions.
2. Functional Testing:
   - Conduct end-to-end testing, to validate the entire transport approval process.
   - Test user registration, request submission, approval/rejection processes, and notifications.
   - Perform boundary testing, input validation, and error handling verification.
3. Security Testing:
   - Perform vulnerability assessment and penetration testing, to identify any security weaknesses.
   - Test data encryption, access controls, and authentication mechanisms.
   - Validate the system against common security threats, including SQL injection, cross-site scripting, and session hijacking.
4. Performance Testing:
   - Conduct load testing, to assess the system's performance under normal and peak load conditions.
   - Identify and address any performance bottlenecks or scalability issues.
   - Measure the response time and throughput of the system.

Table 18 outlines various scenarios for approving or rejecting transport data applications, considering both physical condition and documentation.

1. Defective bus data are rejected but can be updated and re-sent if rejected by the coordinator.

2. Physically repairable but unreceived bus data are placed on hold, pending coordinator approval.
3. Buses with missing or invalid certificates are conditionally approved, but applicants must complete and re-send the required certificates. The administration does not provide final approval in these cases.
4. Buses with valid certificates are approved and require clearance from both the coordinator and the administrator.
5. Buses without completed physical tests are initially approved but put on hold until the necessary tests are conducted.
6. Buses with sound physical condition and valid certificates are approved, but company clearance is needed within a specified time frame.
7. Older model buses with valid certificates are rejected, requiring replacement with newer ones. The administration does not grant approval in such cases.
8. Bus data with lost approval documents are rejected but can be resubmitted, with no further processing if rejected by the coordinator.
9. Buses with some unregistered units are approved, with a requirement to register those units.
10. Bus data with a history of accidents are placed on hold for inspection, with updates from the administration.
11. Buses with sound physical condition but insufficient seating are placed on hold for inspection by the administration.

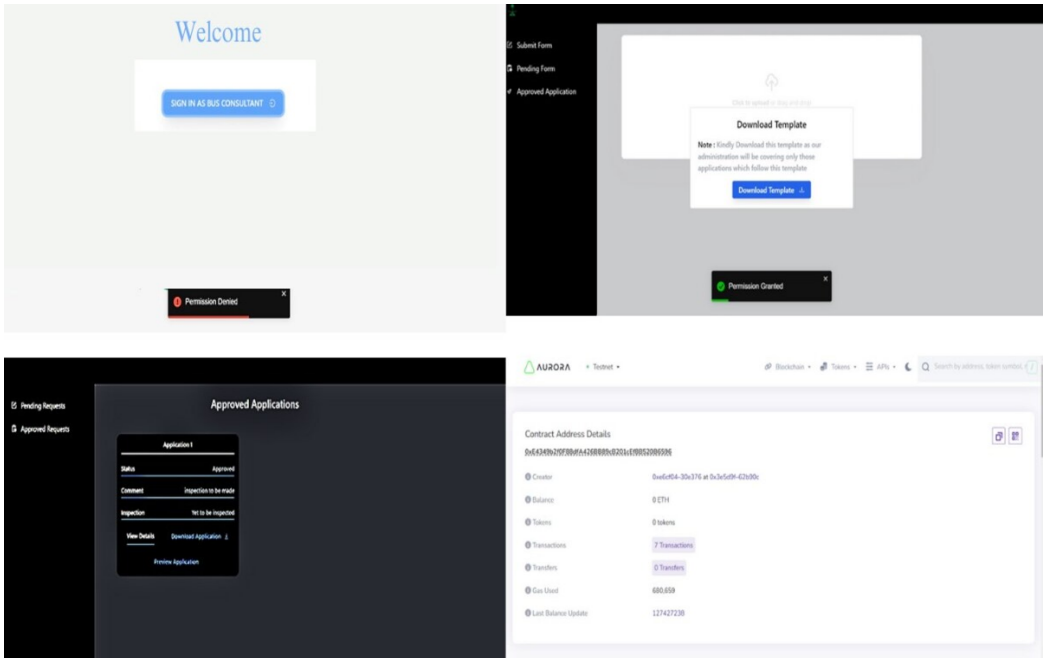

Figure 12. Front interface of the application; access to the application; approved application page; sample smart contract metadata.

Also, the BC-BAS reduces the processing time of applications, by only allowing those applications to be sent to the administration that have been approved by the coordinator. If the application is initially rejected by the coordinator, it will not be processed further, and only the approved applications will be asked for inspection. The overall limitations of the proposed solution depend on the design structure of the use case for the proposed ITS inter-process communication and the integration of the blockchain, considering factors such as the nature of the blockchain (public or private). Private blockchains generally offer faster transaction processing times when compared to public blockchains.

Table 18. Application Approval and Rejection Scenarios by the Administration and Coordinator.

Test-Case	Company	Coordinator	Administration	Status	Message	Action	Improvement by Our System
1-1	Unhealthy (physically defected) transport data.	Reject	Not arrived	Rejected	Update physically. Re-send.	Not approved (coordinator).	Application will not be processed further once rejected by co-ordinator.
1-2	Unhealthy (physically repairable) transport data.	On hold	Not arrived	On hold	Repair physically. Re-send.	Pending approval (coordinator).	Application remains in pending section.
1-3	Healthy transport data– approval certificate not valid.	Approve	Reject	Rejected	Complete certificates. Re-send.	Not approved (administration).	Administrative entity rejects the application and discards it.
1-4	Healthy transport data– with certificates.	Approve	Approve	Approved	Get approval clearance.	Approved by both (co and gov).	Approved by both and added to approved applications.
2-1	Healthy (physically OK) but physical test not done.	Approve	On hold	Pending	Get physical tests and send reports.	Pending (administration).	Inspection details would be sent as an email to bus entity.
2-2	Healthy (physically OK)– certificates OK.	Approve	Approve	Approved	Get approval clearance (clearance not taken by company).	Approved but not utilized in due time.	Approved by both and added to approved applications.
2-3	Healthy (older model of buses)– certificates OK.	Approve	Reject	Rejected	Replace the old buses with the newer ones.	Not approved (administration).	Administrative entity can search through the data and finds the buses according to the model number.
2-4	Healthy (physically OK) but lots of approval documents.	Reject	Not arrived	Rejected	Submit application again.	Not approved (coordinator).	Application will not be processed further once rejected by co ordinator.
2-5	Healthy (physically OK) but some buses seem to be not registered.	Approve	Reject	Rejected	Register the buses.	Not approved (administration).	Administrative entity rejects the application and discards it.
2-6	Healthy (physically OK) but history of accidental issues.	Approve	On hold	Pending	Inspection should be done.	Pending (administration).	Application remains in pending section.
3-1	Healthy (physically OK) but seats of most buses are less.	Approve	On hold	Pending	Inspection should be done.	Pending (administration).	Application remains in pending section.

9. Conclusions, Discussion, and Future Directions

The identification of security weaknesses in current intelligent transport system (ITS) technologies was accomplished through a comprehensive literature analysis. This article presents a proposal for a bus approval system that utilizes Blockchain 2.0 technology to enhance security and privacy measures. To effectively address security concerns, a DEMATEL analysis was performed on the intended intelligent transportation system (ITS) application. The DEMATEL technique is widely acknowledged as a highly effective approach to discerning the components of a cause-and-effect chain within a complicated system. It facilitates the evaluation of interdependent interactions among elements and the identification of essential factors through the use of a visual structural model.

The permission-based system in place involved coordinators and administrative entities responsible for providing approval. This ensured that only applications approved by the coordinator were subsequently passed to the administrative entity. The distributed file system used the IPFS to acquire content hashes, also known as CIDs, which were then placed on the blockchain via smart contracts. The use of DEMATEL analysis facilitated the identification of pivotal aspects that needed consideration in the process of application development. Additionally, a stochastic proof of stake (POS) methodology was used, to expedite transaction processing. The efficiency of transaction processing within the system is improved by using this strategy, as discovered by the study. The anticipated architectural design aims to facilitate increased transaction throughput, minimize latency, and optimize overall system efficiency. The use of robust encryption and authentication protocols will effectively safeguard the integrity and confidentiality of data. Well-defined rules and regulations are essential for effectively managing participant roles, permissions, and consensus procedures. These measures aim to strike a balance between decentralization, efficient decision making, and accountability. The use of a private blockchain has the potential to significantly enhance the efficiency, security, and privacy of the approval system. The successful completion of this forthcoming task will result in the optimization of transportation vehicle approval procedures. For future advancements, it is recommended to use diverse stochastic algorithm methodologies to enhance the processing capabilities of intelligent transportation systems (ITS) applications. The transition process would include meticulous evaluation and customization of the private blockchain platform, taking into account factors such as scalability, security, and compatibility.

Author Contributions: Conceptualization, T.J.S.K., S.J. and M.N.; formal analysis, T.J.S.K. and M.F.S.; investigation, M.F.S. and S.J.; methodology, M.F.S. and M.N.; software, M.N.; supervision, T.J.S.K., A.M., M.A.A. and R.B.A.; validation, T.J.S.K., M.F.S. and S.S.; visualization, M.A.A., R.B.A. and S.S.; writing—original draft, M.F.S.; writing—review and editing, T.J.S.K., A.M., M.A.A. and S.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research work was funded by the Institutional Fund Project under grant no. (IFPIP-620-611-1443), the Ministry of Education and King Abdulaziz University (KAU), and 28 The Deanship of Scientific Research (DSR) of KAU, Jeddah, Saudi Arabia.

Institutional Review Board Statement: Not applicable

Informed Consent Statement: Not applicable

Data Availability Statement: The data is provided by the concerned transportation department. It can be provided on demand.

Acknowledgments: The authors gratefully acknowledge technical and financial support from the Ministry of Education and King Abdulaziz University (KAU), and 28 The Deanship of Scientific Research (DSR) of KAU, Jeddah, Saudi Arabia.

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

References

1. 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. [CrossRef]
2. Du, X.; Gao, Y.; Wu, C.H.; Wang, R.; Bi, D. Blockchain-based intelligent transportation: A sustainable GCU application system. *J. Adv. Transp.* **2020**, *2020*, 5036792. [CrossRef]
3. Tanwar, S.; Tyagi, S.; Budhiraja, I.; Kumar, N. Tactile Internet for Autonomous Vehicles: Latency and Reliability Analysis. *IEEE Wirel. Commun.* **2019**, *26*, 66–72. [CrossRef]
4. Sharma, S.; Kaushik, B. A survey on internet of vehicles: Applications, security issues & solutions. *Veh. Commun.* **2019**, *20*, 100182. [CrossRef]
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. [CrossRef]
6. Zheng, K.; Zheng, Q.; Chatzimisios, P.; Xiang, W.; Zhou, Y. Heterogeneous Vehicular Networking: A Survey on Architecture, Challenges, and Solutions. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2377–2396. [CrossRef]
7. 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 Commun. Surv. Tutor.* **2011**, *13*, 584–616. [CrossRef]
8. Underwood, S. Blockchain beyond Bitcoin. *Commun. ACM* **2016**, *59*, 15–17. [CrossRef]
9. El-Switi, S.; Qatawneh, M. Application of Blockchain Technology in Used Vehicle Market: A Review. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 49–54. [CrossRef]
10. Mendiboure, L.; Chalouf, M.A.; Krief, F. Survey on blockchain-based applications in Internet of Vehicles. *Comput. Electr. Eng.* **2020**, *84*, 106646. [CrossRef]
11. Laroiya, C.; Saxena, D.; Komalavalli, C. Chapter 9—Applications of Blockchain Technology. In *Handbook of Research on Blockchain Technology*; Krishnan, S., Balas, V.E., Julie, E.G., Robinson, Y.H., Balaji, S., Kumar, R., Eds.; Academic Press: Cambridge, MA, USA, 2020; pp. 213–243. [CrossRef]
12. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. MedRec: Using Blockchain for Medical Data Access and Permission Management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30. [CrossRef]
13. Prisco, G. The Blockchain for Healthcare: Gem Launches Gem Health Network with Philips Blockchain Lab. *Bitcoin Magazine*, 26 April 2016; p. 26. Available online: https://bitcoinmagazine.com/business/the-blockchain-for-heathcare-gem-launches-gem-health-network-with-philips-blockchain-lab-1461674938 (accessed on 2 June 2023).
14. Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. *J. Med. Syst.* **2016**, *40*, 218. [CrossRef]
15. Blockchain: The Solution for Transparency in Product Supply Chains. 2015. Available online: https://www.provenance.org/whitepaper (accessed on 15 April 2023).
16. Hijro. 2018. Available online: https://hijro.com/ (accessed on 15 April 2023).
17. Walton Food Safety. 2018. Available online: https://tinyurl.com/ybu9xff7 (accessed on 2 June 2023).
18. Everledger. 2020. Available online: https://www.everledger.io/ (accessed on 2 June 2023).
19. Lasseter, R.; Paigi, P. Microgrid: A Conceptual Solution. In Proceedings of the 2004 IEEE 35th Annual Power Electronics Specialists Conference, Aachen, Germany, 20–25 June 2004; Volume 6, pp. 4285–4290. [CrossRef]
20. Cohn, A.D.; West, T.; Parker, C. Smart after all: Blockchain, smart contracts, parametric insurance, and smart energy grids. *Georget. Law Technol. Rev.* **2017**, *1*, 273.
21. Sarangam, A. What Is Client Server Architecture? An Overview. Available online: https://u-next.com/blogs/cyber-security/what-is-client-server-architecture (accessed on 2 April 2023).
22. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. Available online: https://metzdowd.com (accessed on 9 May 2023).
23. Swan, M. *Blockchain*; O'Reilly: Springfield, IL, USA, 2015.
24. Crosby, M. BlockChain Technology Beyond Bitcoin. *Appl. Innov.* **2016**, *2*, 71.
25. Cole, R.; Stevenson, M.; Aitken, J. Blockchain technology: Implications for operations and supply chain management. *Supply Chain. Manag. Int. J.* **2019**, *24*, 469–483. [CrossRef]
26. Zyskind, G.; Zekrifa, D.; Alex, P.; Nathan, O. Decentralizing Privacy: Using Blockchain to Protect Personal Data. In Proceedings of the 2015 IEEE Security and Privacy Workshops, San Jose, CA, USA, 21–22 May 2015; pp. 180–184. [CrossRef]
27. Antonopoulos, A. Bitcoin security model: Trust by computation. *Forbes. Com, Febr.* **2014**, *20*, 42.
28. Li, T.; Xiong, X.; Zheng, G.; Li, Y.; Tolba, A. A Blockchain-Based Shared Bus Service Scheduling and Management System. *Sustainability* **2023**, *15*, 12516. [CrossRef]
29. Petcu, A.; Pahontu, B.; Frunzete, M.; Stoichescu, D.A. A Secure and Decentralized Authentication Mechanism Based on Web 3.0 and Ethereum Blockchain Technology. *Appl. Sci.* **2023**, *13*, 2231. [CrossRef]
30. Guo, X.; Guo, X. A Research on Blockchain Technology: Urban Intelligent Transportation Systems in Developing Countries. *IEEE Access* **2023**, *11*, 40724–40740. [CrossRef]

31. Sharma, S.; Ghanshala, K.K.; Mohan, S. Blockchain-Based Internet of Vehicles (IoV): An Efficient Secure Ad Hoc Vehicular Networking Architecture. In Proceedings of the 2019 IEEE 2nd 5G World Forum (5GWF), Dresden, Germany, 30 September–2 October 2019; pp. 452–457. [CrossRef]
32. Alasmary, H.; Tanveer, M. ESCI-AKA: Enabling Secure Communication in the IoT-enable Smart Home Environment Using Authenticated Key Agreement Framework. *Mathematics* **2023**, *11*, 3450. [CrossRef]
33. Yang, Z.; Yang, K.; Lei, L.; Zheng, K. Blockchain-Based Decentralized Trust Management in Vehicular Networks. *IEEE Internet Things J.* **2018**, *6*, 1495–1505. [CrossRef]
34. Alkhodair, A.; Mohanty, S.P.; Kougianos, E. FlexiChain 3.0: Distributed Ledger Technology-Based Intelligent Transportation for Vehicular Digital Asset Exchange in Smart Cities. *Sensors* **2023**, *23*, 4114. [CrossRef]
35. Zhang, Y.; Dai, Y.; Xu, D.; Zhang, K.; Maharjan, S. Deep Reinforcement Learning and Permissioned Blockchain for Content Caching in Vehicular Edge Computing and Networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 4312–4324. [CrossRef]
36. Zhang, X.; Chen, X. Data Security Sharing and Storage Based on a Consortium Blockchain in a Vehicular Ad-hoc Network. *IEEE Access* **2019**, *7*, 58241–58254. [CrossRef]
37. Farahbakhsh, F.; Shahidinejad, A.; Ghobaei-Arani, M. Multi-user context-aware computation offloading in mobile edge computing based on Bayesian learning automata. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4127. [CrossRef]
38. Meijer, A.; Bolívar, M.P.R. Governing the smart city: A review of the literature on smart urban governance. *Int. Rev. Adm. Sci.* **2016**, *82*, 392–408. [CrossRef]
39. Rathee, G.; Kumar, A.; Kerrache, C.A.; Iqbal, R. A trust-based mechanism for drones in smart cities. *IET Smart Cities* **2022**, *4*, 255–264. [CrossRef]
40. Msahli, M.; Labiod, H.; Ampt, G. Security Interoperability for Cooperative ITS: Architecture and Validation. In Proceedings of the 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Canary Islands, Spain, 24–26 June 2019; pp. 1–6.
41. Rahman, M.S.; Chamikara, M.; Khalil, I.; Bouras, A. Blockchain-of-blockchains: An interoperable blockchain platform for ensuring IoT data integrity in smart city. *J. Ind. Inf. Integr.* **2022**, *30*, 100408. [CrossRef]
42. Karumba, S.; Jurdak, R.; Kanhere, S.; Sethuvenkatraman, S. BAILIF: A Blockchain Agnostic Interoperability Framework. In Proceedings of the 5th IEEE International Conference on Blockchain and Cryptocurrency, Dubai, United Arab Emirates, 1–5 May 2023; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2023.
43. Guvenc, I.; Koohifar, F.; Singh, S.; Sichitiu, M.L.; Matolak, D. Detection, tracking, and interdiction for amateur drones. *IEEE Commun. Mag.* **2018**, *56*, 75–81. [CrossRef]
44. Al Batayneh, R.M.; Taleb, N.; Said, R.A.; Alshurideh, M.T.; Ghazal, T.M.; Alzoubi, H.M. IT governance framework and smart services integration for future development of Dubai infrastructure utilizing AI and big data, its reflection on the citizens standard of living. In Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2021), Hassan, Morocco, 28–30 June 2021; Springer: Berlin/Heidelberg, Germany, 2021; pp. 235–247.
45. Dua, A.; Kumar, N.; Das, A.K.; Susilo, W. Secure message communication protocol among vehicles in smart city. *IEEE Trans. Veh. Technol.* **2017**, *67*, 4359–4373. [CrossRef]
46. Knowles Flanagan, S.A. Cooperative Connected Intelligent Vehicles and Infrastructure for Road Safety Applications. Ph.D. Thesis, Aston University, Birmingham, UK, 2022.
47. Xu, R.; Chen, Y.; Blasch, E.; Chen, G. Blendcac: A blockchain-enabled decentralized capability-based access control for iots. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1027–1034.
48. Gilani, S.M.M.; Usman, M.; Daud, S.; Kabir, A.; Nawaz, Q.; Judit, O. SDN-based multi-level framework for smart home services. In *Multimedia Tools and Applications*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 1–21.
49. Dinh, T.; Liu, R.; Zhang, M.; Chen, G.; Ooi, B.; Wang, J. Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Trans. Knowl. Data Eng.* **2017**, *30*, 1366–1385. [CrossRef]
50. Storublevtcev, N. Cryptography in Blockchain. In *Computational Science and Its Applications—ICCSA 2019*; Misra, S., Gervasi, O., Murgante, B., Stankova, E., Korkhov, V., Torre, C., Rocha, A.M.A., Taniar, D., Apduhan, B.O., Tarantino, E., Eds.; Springer International Publishing: Berlin/Heidelberg, Germany, 2019; pp. 495–508.
51. Proof of Authority Chains. Available online: https://github.com/paritytech/parity/wiki/Proof-of-Authority-Chains (accessed on 10 March 2023).
52. Molina-Jiménez, C.; Solaiman, E.; Sfyrakis, I.; Ng, I.; Crowcroft, J. On and Off-Blockchain Enforcement of Smart Contracts. In Proceedings of the Euro-Par 2018 International Workshops, Turin, Italy, 27–28 August 2018. [CrossRef]
53. Stifter, N.; Judmayer, A.; Schindler, P.; Kern, A.; Fdhila, W. What Is Meant by Permissionless Blockchains? Cryptology ePrint Archive, Paper 2021/023. 2021. Available online: https://eprint.iacr.org/2021/023 (accessed on 13 March 2023).
54. Sharma, T.K. Permissioned And Permissionless Blockchains. 2022. Available online: https://www.blockchain-council.org/blockchain/permissioned-and-permissionless-blockchains-a-comprehensive-guide/ (accessed on 22 March 2023).
55. Ripple. 2018. Available online: https://arxiv.org/pdf/1802.07242.pdf (accessed on 15 April 2023).
56. Markus, M.; Jacobson, D. The Governance of Business Processes. In *Handbook on Business Process Management 2: Strategic Alignment, Governance, People and Culture*, 2nd ed.; Springer: Berlin, Germany, 2015; pp. 311–332. [CrossRef]

57. Seidel, S.; Rosemann, M. Creativity Management—The New Challenge for BPM. 2012. Available online: https://eprints.qut.edu.au/71378/ (accessed on 9 June 2023).
58. Governatori, G.; Shek, S. Rule Based Business Process Compliance. In *International Web Rule Symposium*; Springer: Berlin/Heidelberg, Germany, 2012. Available online: https://api.semanticscholar.org/CorpusID:6159818 (accessed on 9 June 2023).
59. Agarwal, R.; Bruno, G.; Torchiano, M. An operational approach to the design of workflow systems. *Inf. Softw. Technol.* **2000**, *42*, 547–555. . [CrossRef]
60. Van der Aalst, W.M.P. Business process management: A comprehensive survey. *ISRN Softw. Eng.* **2013**, *2013*, 507984. [CrossRef]
61. Carbon, R.; Johann, G.; Keuler, T.; Muthig, D.; Naab, M.; Zilch, S. Mobility in the virtual office: A document-centric workflow approach. In Proceedings of the 1st International Workshop on Software Architectures and Mobility, Leipzig, Germany, 19 May 2008; pp. 21–26. [CrossRef]
62. Mondal, A.; Misra, S. FlowMan: QoS-Aware Dynamic Data Flow Management in Software-Defined Networks. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 1366–1373. [CrossRef]
63. Grefen, P.; de Vries, R.R. A reference architecture for workflow management systems. *Data Knowl. Eng.* **1998**, *27*, 31–57. . [CrossRef]
64. Pramulia, D.; Anggorojati, B. Implementation and evaluation of blockchain based e-voting system with Ethereum and Metamask. In Proceedings of the 2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), Jakarta, Indonesia, 19–20 November 2020; pp. 18–23. [CrossRef]
65. Yuan, Y. Towards Blockchain-based Intelligent Transportation Systems. In Proceedings of the 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Rio de Janeiro, Brazil, 1–4 November 2016. [CrossRef]
66. Sastry, K.; Goldberg, D.; Kendall, G. Genetic Algorithms. In *Search Methodologies: Introductory Tutorials in Optimization and Decision Support Techniques*; Burke, E.K., Kendall, G., Eds.; Springer: Boston, MA, USA, 2005; pp. 97–125. [CrossRef]
67. Glover, F.; Laguna, M. Tabu Search. In *Handbook of Combinatorial Optimization: Volume 1–3*; Du, D.Z., Pardalos, P.M., Eds.; Springer: Boston, MA, USA, 1998; pp. 2093–2229. [CrossRef]
68. Muhammad, M.N.; Cavus, N. Fuzzy DEMATEL method for identifying LMS evaluation criteria. *Procedia Comput. Sci.* **2017**, *120*, 742–749. [CrossRef]