Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.042379

ARTICLE

Analyzing the Impact of Blockchain Models for Securing Intelligent Logistics through Unified Computational Techniques

Mohammed S. Alsaqer[1], Majid H. Alsulami[2,*], Rami N. Alkhawaji[3] and Abdulellah A. Alaboudi[2]

[1]College of Computer Science, King Khalid University, Abha, 62529, Saudi Arabia

[2]Applied College, Shaqra University, Shaqra, 11961, Saudi Arabia

[3]University College of Umluj, University of Tabuk, Umluj, 48335, Saudi Arabia

*Corresponding Author: Majid H. Alsulami. Email: malsulami@su.edu.sa

Received: 28 May 2023 Accepted: 12 August 2023 Published: 26 December 2023

ABSTRACT

Blockchain technology has revolutionized conventional trade. The success of blockchain can be attributed to its distributed ledger characteristic, which secures every record inside the ledger using cryptography rules, making it more reliable, secure, and tamper-proof. This is evident by the significant impact that the use of this technology has had on people connected to digital spaces in the present-day context. Furthermore, it has been proven that blockchain technology is evolving from new perspectives and that it provides an effective mechanism for the intelligent transportation system infrastructure. To realize the full potential of the accurate and efficacious use of blockchain in the transportation sector, it is essential to understand the most effective mechanisms of this technology and identify the most useful one. As a result, the present work offers a priority-based methodology that would be a useful reference for security experts in managing blockchain technology and its models. The study uses the hesitant fuzzy analytical hierarchy process for prioritizing the different blockchain models. Based on the findings of actual performance, alternative solution A1 which is Private Blockchain model has an extremely high level of security satisfaction. The accuracy of the results has been tested using the hesitant fuzzy technique for order of preference by similarity to the ideal solution procedure. The study also uses guidelines from security researchers working in this domain.

KEYWORDS

Intelligent transportation system; security engineering; smart systems; decision making

1 Introduction

Digital solutions play a critical role in changing the world in several industries. They can improve efficiency and productivity by providing services to be available at any time and from anywhere. The revolution of technology has come up with emerging technologies such as blockchain, cloud computing, the Internet of Things, Artificial Intelligence, etc. These emerging technologies can play a significant impact on different sectors [1].

Blockchain technology uses a decentralized mechanism that allows data to be secured while ensuring that their integrity is not breached [2]. Every data transaction operated through blockchain technology has a verified copy and history within the blocks, making it a more secure and well-managed technology [3,4]. With the help of blockchain technology, a transaction can be conducted in a decentralized manner. According to many experts, blockchain has the potential to significantly lower costs while also improving the performance of transactions [5–7]. Various industries [8–10] have adopted blockchain technology as their major information technology-related assignments. The use of blockchain technology in transportation can resolve a variety of problems, such as management strategies and data security. The transportation sector creates fresh information each day, such as facts about the user, test information, accounting systems, scientific investigations, and tending systems, as well as other records that are often pushed into several divided, inconsistent databases [11–13]. Further, blockchain may possibly control the flow of data to enhance their value for various public services through modernizing transportation records, safeguarding classified information from attackers, and offering users better control over their data.

Most industries now rely on blockchain technology because of its advancements in security [14,15]. The reliance on blockchain technology is likely to grow even more in the near future. Gartner, a prominent systematic work and business consulting firm, has predicted that blockchain technology will generate a business value of USD 3.1 trillion by 2030 [16]. The four categories that make up the Blockchain Spectrum are decomposed by the traits and components they have, several of which will only partially appear for a while. Through these stages, each present opportunities and threats. Gartner's real blockchain representation is shown in Fig. 1.

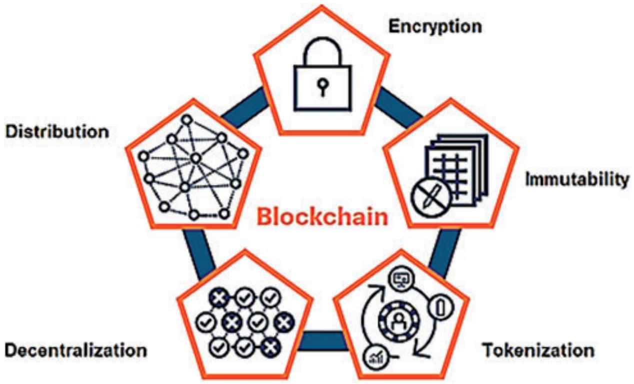

Figure 1: Real blockchain representation by Gartner

Enterprises have quickly recognized the disruptive potential of blockchain technology. The increasing use of this technology makes it a trending technology in the transportation industry. A good deal of research on blockchain technology exists due to the industry's expanding adoption of blockchain techniques. One study reported more than 500 data breaches in the transportation sector from 2009 to 2019 [17–20]. In the transportation industry, these breaches led to the disclosure, theft, destruction, or illegal release of 230, 954, 151 records [21–23]. This number compares to approximately 69.78 percent of the population of the United States. Thus, the gravity of the matter cannot be negated, and it calls for the prompt implementation of safeguards and countermeasures. In 2019, data breaches in transportation occurred at a rate of 1.4 per day [24,25]. The transportation sector has, however, finally started to prioritize blockchain design and implementation [26–28]. Blockchain technology aids businesses in keeping track of transportation systems. Transportation industries use blockchain technologies to minimize fraudulent activities, enabling all activities to be traced [29]. Blockchain assists in determining the source of the fraudulent activity [30–32]. More relevantly, the market size for blockchain technology in the transportation and logistics industries is increasing. Fig. 2 illustrates the market scope [33–35].

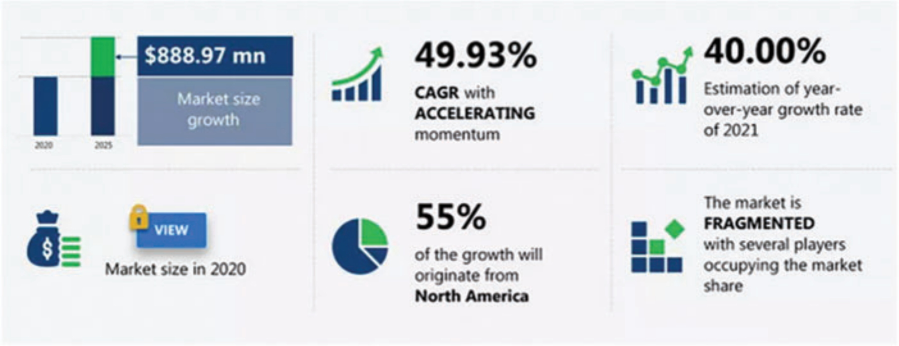
$888.97 mn
Market size growth
2020
2025
49.93%
CAGR with ACCELERATING momentum
40.00%
Estimation of year-over-year growth rate of 2021
VIEW
Market size in 2020
55%
of the growth will originate from North America
The market is FRAGMENTED with several players occupying the market share

Figure 2: Future of blockchain technology in transportation and logistics industries

Blockchain systems are gaining a lot of attention as a tool to increase financial transactions, commerce, and transparency while streamlining supply chains. A significant portion of this interest was sparked by the speculative craze surrounding Bitcoin, which is built on outdated blockchain architecture with issues with speed and energy usage. In order to get beyond these restrictions and provide useful value for various commercial purposes and applications, advanced blockchain systems have been built. The transportation industry has suffered from security breaches for a decade. Therefore, security management is the biggest challenge for the current digital transportation domain [36–40]. Managing transportation data with less investment and higher production can produce a practical framework [41–43]. The transportation industry has undergone a digital transformation using blockchain technology, which creates a single dataset by gathering transportation data from various databases [44,45]. Evaluation and selection of an efficient blockchain model is always a challenging task. Therefore, this study uses the hesitant fuzzy AHP to prioritize the different blockchain models. The authors have used the hesitant fuzzy TOPSIS process to test the accuracy of the results. Well-classified data facilitate quick and accurate decision-making, especially in terms of data that are cost related. Therefore, it is important to categorize the various blockchain models in a manner that allows the easy recognition of which model is preferable and which is not. To facilitate secure transportation policies, it is essential to categorize various blockchain models and their impact in a systematic, pre-validated manner. As such, the writers have utilized multi-criteria decision-making (MCDM) to calculate the effects of various blockchain technologies examined in this study. Several MCDM approaches can be used to solve this type of problem [42,43,46,47]. However, this study implements a practical MCDM approach called the hesitant fuzzy analytical hierarchy process (AHP) technique for order preference by similarity to the ideal solution (TOPSIS) approach has also been used in our work to obtain a hierarchical structure that is based on prioritizing the different blockchain tools models in the descending order of “highest” to “lowest” [41,42,48]. Although extensive research has been done on the use of blockchain technology in the area of transportation [43,44,49], very few studies have focused on the role of different blockchain model and what it can offer for managing big data in transport.

This study compares the estimated impacts of the current research and those of earlier methods to show how valuable the current contributions are. Therefore, the goal of this paper is to (1) conduct an in-depth study of the security of information software systems, i.e., from the standpoint of blockchain technology, security influences are analyzed in terms of weakness as well as strength;

(2) run implementations through hesitant fuzzy AHP to figure out which features of blockchain technology models are most important; and (3) use hesitant fuzzy TOPSIS to estimate how well the blockchain technology models work in different transportation systems. The rest of this work is organized as follows: materials and methods are described in Section 2. In Section 3, the results are discussed. The data were compared, and a sensitivity analysis was performed in Section 4 of this research. Finally, conclusions and future recommendations are given in Section 5.

2 Materials and Methods

2.1 Model Classification

The types of blockchain models are public, hybrid, private, and permissioned blockchain, and decentralized application and consortium blockchain. We categorize and associate these models with our study in the following sections.

2.1.1 Private Blockchain

This is an encrypted data repository that works as a personal blockchain. This model operates exclusively within a closed hierarchy and has no constraints or permissions. With this type of model, the end-users are private employees that have access to the blocks. Read permissions can be public or constrained, and the access to modify the originality of blocks is controlled by a centralized system [40,41]. It simply allows approved users or groups to enter, view, and display data in the ledger. Further, the type of blockchain model works in an environment opposite to its actual nature, where every entity in the blockchain model can see the data over blocks. However, it can restrict the users [16].

2.1.2 Public Blockchain

A public blockchain is open to anyone who wishes to connect with it. It is an open-source distributed ledger with no permissions. With this type of model, any compatible entity on the web can perform a partner role in blockchain technology and enact operations over it. Public blockchain technology allows all of the participants in a transaction to communicate with one another. It has a record of transactions that cannot be changed. Anyone who follows a set of established rules and participates in the hierarchy can report a transaction. Any type of transaction that is applied over blocks is anonymous, and no mutual shareholders know about each other until the transaction has been completed [17].

2.1.3 Hybrid Blockchain

A hybrid blockchain mixes private and public models. This combines the features of both types of blockchains, allowing for both private and public consent hierarchies. With this type of model, the owner of the block can control the access management of the approaches, as well as restrict the information flow as needed. Hybrid blockchain has the potential to benefit both highly regulated corporations and governments. It offers consistency and flexibility, including the ability to keep or disseminate information on a public ledger. In the current world, there are numerous hybrid blockchain implementations. There are various models of blockchain available that are widely used across industries [18]. This model confers high security with fast data management speed [42–44].

2.1.4 Permissioned Blockchain

This model facilitates an advanced mechanism where every block verifier needs standard access permission before implementing any operation. This is useful for enterprises, financial institutions, and organizations that are confident in their ability to comply with most of the constraints while also being aware of the importance of maintaining complete record monitoring [45–47]. This type of layered security mechanism provides an advanced benefit to the model. Permissioned blockchains operate in a very different way from private and public blockchains. They are designed to take advantage of blockchains without risking the authority of a centrally regulated system.

2.1.5 Consortium Blockchain

This is a perfect example of a semi-decentralized blockchain model with which many businesses operate. It is different from a private ledger managed by a single entity, as more than one organization can operate on the network under this kind of blockchain. A consortium blockchain combines aspects of both private and public chains. The most significant departure from either system is that rather than being open where anyone can authenticate blocks or a locked stage where only one individual can designate block providers, a consortium sequence has a collection of similar companies acting as validators [47–49].

2.1.6 Decentralized Blockchain

This is a model that operates over a non-singular framework model in which there are various node-to-node entities available with permissions and access controls. Popcorn Time, BitTorrent, and Tor are some names of tools and software that work on this type of model where the standard authorities are not centralized, and access permission distribution is allocated throughout the whole peer-to-peer network. There are many pieces of software and cryptocurrencies that are not part of any centralized control authority and work freely in the public domain [12–17]. Fig. 3 shows the hierarchical structure for the assessment of different blockchain models.

The research examines several blockchain models and their impact on logisticss. The hesitant fuzzy analytical hierarchy process (AHP) is used in the research report to prioritize the various blockchain models. AHP is a decision-making technique that aids in the systematic evaluation and comparison of alternatives based on a variety of criteria. The evaluation criteria used to analyze the effectiveness and applicability of blockchain technology in logistics are presented in Table 1 of the report. Based on these characteristics, the table presents a framework for assessing and contrasting the various blockchain models.

Table 2 concentrates on the sub-criteria used to determine the impact of each blockchain model at tier 2. These sub-criteria go deeper into the precise components that determine each model's overall assessment. These sub-criteria aid in further breaking down and analysing each blockchain model's prospective effect on intelligent logistics.

MCDM is considered an effective method for resolving a variety of real-world problems and making the best decisions. AHP is a well-organized strategy for MCDM operations. To answer the problem of picking the best assessment approach, this study proposes an effective strategy that uses AHP to analyze decision criteria and TOPSIS to identify the most relevant functions [7–10]. This study also uses the hesitant fuzzy approach to generate highly accurate results. MCDM offers some complicated algorithms, but TOPSIS is useful because of its straightforward computation. To decide the value of the specified sub-techniques or strategies, the following measures are summarized:

Step 1: Create a tree structure for the numerous layers of the problem.

Step 2: Manage the linguistic technologies using pair comparison matrixes [16].

Step 3: Convert assessments with hesitant fuzzy wrappers [16] using Eq. (1):

$$Or\,WA\,(A_1, A_2, \ldots A_n) = \sum_{j=1}^{n} W_j B_j \tag{1}$$

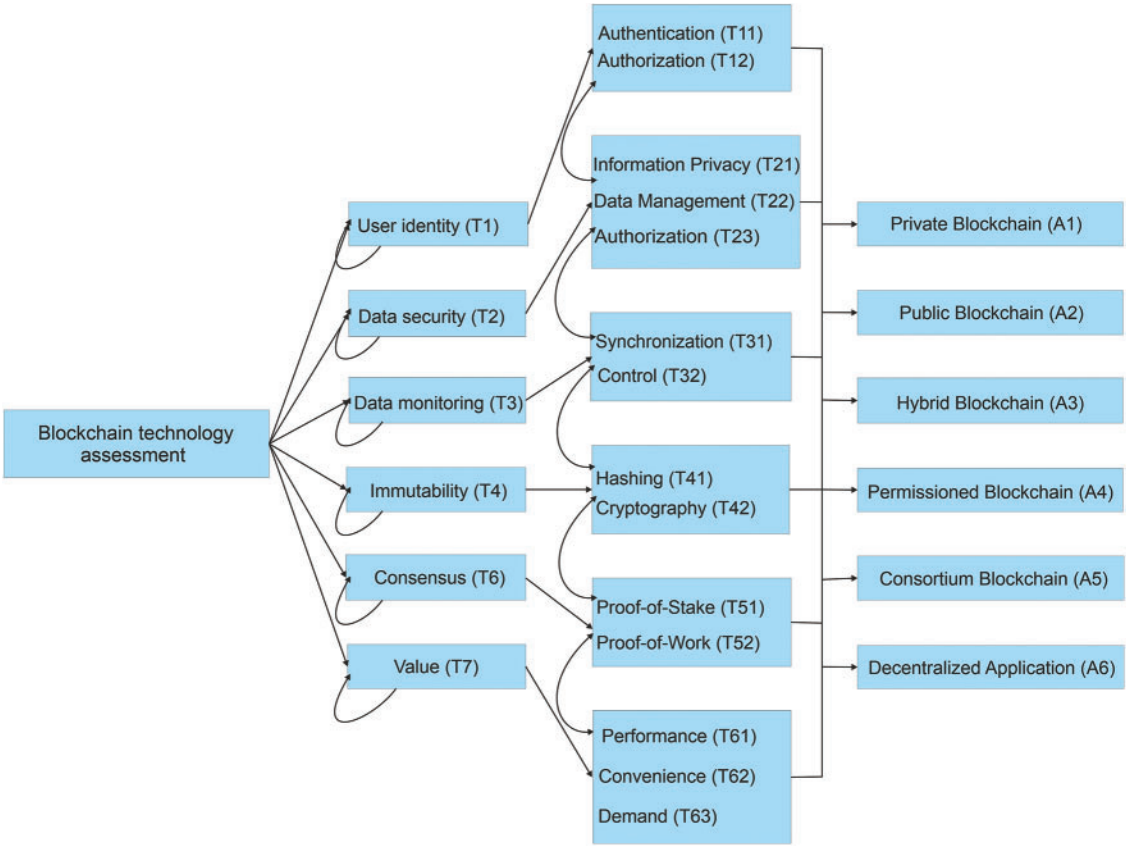

Figure 3: Hierarchical structure for the assessment of different blockchain models

Table 1: Evaluation criteria

Criteria	Description
User identity (T1)	In this criterion, the blockchain gives a special concept of key distribution. Every blockchain theory, as part of the transportation application, provides a public key to every user. By using this key, the users can control the flow of their data and its access management.

(Continued)

Table 1 (continued)

Criteria	Description
Data security (T2)	To make the user's data more secure and integrated, this technology provides a key management concept. Along with that, the technology can also associate a smart contract with it for an extra layer of security.
Data monitoring (T3)	In a transportation blockchain system, the ledger keeps track of data at each step along the process, such as who controlled them and where they were kept before reaching the proper user. Each user's data are appropriately regulated and synchronized in real-time to all interested events for efficient data monitoring.
Immutability (T4)	By giving appropriate security standards and policies such as audit and security checks, this technology has an effective data management scenario in the current situation.
Consensus (T5)	The provided technology has effective data security mechanisms, and by using these mechanisms, this technology provides an effective anti-data theft scenario.
Value (T6)	This mechanism has the potential to become a main platform for professionals, delivering tremendous value to the industry. The utility of this mechanism in the transportation sector can be assessed by looking at its performance, ease, and demand.

Table 2: Different sub-criteria for estimating the influence at tier 2

Sub-criteria	Description
Authentication (T11)	Verifying a user's or process's identification is a procedure or activity. Blockchain authentication refers to systems that validate users of the resources present in Bitcoin and other digital currencies' underlying technology.
Authorization (T12)	The process of allowing a user permission to access a specific resource or function in a system is known as authorization. Client privilege and access control are two phrases that are commonly used interchangeably.
Information privacy (T21)	Information privacy is the interaction between data collection and dissemination, technology, the public expectation of privacy, and the legal and political considerations that surround it. Data security or data privacy are other terms for it.
Data management (T22)	There is an administrative process called "data management". It includes obtaining important data and keeping it safe, validating it, and processing it to make sure its users can access, use, and update it.

(Continued)

Table 2 (continued)

Sub-criteria	Description
Authorization (T23)	The process of allowing a user permission to access a specific resource or function in a system is known as authorization. Client privilege and access control are two phrases that are commonly used interchangeably.
Synchronization (T31)	The act of ensuring that a group of data or files is the same in several locations.
Control (T32)	The ability to manage a machine, vehicle, or other moving objects.
Hashing (T41)	This is an approach that is used in managing the integrity of files and information. This technique is used in various datasets and technologies that ensure the attributes of information.
Cryptography (T42)	Cryptography is the use of codes to safeguard data and communications so that only those who are supposed to be able to access and process them can. Because private data can be decoded and accessed by the authorized person or the targeted person, cryptography is a two-way procedure. Hence, the best method of encrypted transmission is cryptography. Nevertheless, it only works one way in hashing.
Proof-of-Stake (T51)	According to the Proof of Stake (PoS) theory, a person's ability to mine or validate block transactions is proportionate to the number of coins possessed. This means that as the quantity of Bitcoins or altcoins a miner holds grows, so does his or her mining power.
Proof-of-Work (T52)	This is called Proof of Work (PoW), and it is a kind of zero-knowledge cryptographic proof. One party, the prover, proves to others (the verifiers) that a certain amount of computational work has been performed for a certain reason. Following that, with no effort on their part, verifiers can authenticate this expenditure.
Performance (T61)	The act or process of carrying out a task or function.
Convenience (T62)	This is the state of being able to complete a task without trouble.
Demand (T63)	Insistent and peremptory request made as of right now.

W = (w1, w2, wn)S is used here. Which is the corresponding balance vector that follows the $\sum_{i=1}^{n} W = 1$rule, and Bj has the same importance as the goal of A1, A2, and An. The hesitant fuzzy restrictions of the trapezoidal figures C = (A, B, C, D), for instance, in Eq. (2), is calculated after this calculation (5).

$$A = min\left\{A_L^i, A_M^i, A_M^{i+1}, \ldots\ldots A_M^j, A_R^j\right\} = A_L^i \tag{2}$$

$$D = max\left\{A_L^i, A_M^i, A_M^{i+1}, \ldots\ldots A_M^j, A_R^j\right\} = A_R^j \tag{3}$$

$$B = \left\{ \begin{array}{c} A_M^i, if\ i+1=j \\ Or\,WA_{\underset{w}{2\left(A_m^j,\ldots\ldots A_m^{\frac{i+j}{2}}\right),ifi+jiseven}} \\ Or\,WA_{\underset{w}{2\left(A_m^j,\ldots\ldots A_m^{\frac{i+j+1}{2}}\right),ifi+jisodd}} \end{array} \right\} \tag{4}$$

$$C = \left\{ \begin{array}{c} A_M^{i+1}, if\ i+1=j \\ Or\,WA_{\underset{w}{2\left(A_m^j A_m^{j-1},\ldots\ldots A_m^{\frac{(i+j)}{2}}\right),ifi+jiseven}} \\ Or\,WA_{\underset{w}{2\left(A_m^j, A_m^{j-1}\ldots\ldots A_m^{\frac{(i+j+1)}{2}}\right),ifi+jisodd}} \end{array} \right\} \tag{5}$$

After that, by using Eqs. (6) and (7) separately, the authors need to find priority and secondary weights for attributes.

$$w_1^1 = \mu_2, w_2^1 = \mu_2\left(1-\mu_2\right), \ldots\ldots.w_n^1\mu_2(1-\mu_2)^{n-2} \tag{6}$$

Second type weights ($W2 = (w_1^2, w_2^2, \ldots, w_n^2)$):

$$w_1^2 = \mu_1^{n-1}, w_2^2 = \left(1-\mu_1\right)\mu_1^{n-1} \tag{7}$$

With the support of the equations $\mu_1 = \dfrac{r-(j-1)}{r-1}$s and $\mu_2 = \dfrac{r-(j-1)}{r-1}$, where r represents the priority number, and i and j show secondary numbers.

Step 4: Use Eqs. (8) and (9) to complete the pairwise comparison matrix.

$$\tilde{a} = \begin{bmatrix} 1 & \cdots & \tilde{c}_{1n} \\ \vdots & \ddots & \vdots \\ \tilde{c}_{n1} & \ldots & 1 \end{bmatrix} \tag{8}$$

$$\tilde{c}_{ji} = \left(\frac{1}{cij_u}, \frac{1}{cij_{m2}}, \frac{1}{cij_{m1}}, \frac{1}{cij_1}\right) \tag{9}$$

Step 5: Use Eq. (10) in the process of defuzzification.

$$\eta_x = \frac{l+2m_1+2m_2+h}{6} \tag{10}$$

Estimate the consistency ratio (CR) using Eqs. (11) and (12) [16,19].

$$CI = \frac{\gamma_{max}-n}{n-1} \tag{11}$$

$$CR = \frac{CI}{RI} \tag{12}$$

Step 6: Use Eq. (13) to calculate the geometric mean (GM).

$$\tilde{g}_i = \left(\tilde{c}_{i1} \bigotimes \tilde{c}_{i2} \ldots\ldots \bigotimes \tilde{c}_{in}\right)^{\frac{1}{n}} \tag{13}$$

Step 7: Evaluate the assumed weights by using Eq. (14).

$$\tilde{w}_i = \tilde{g}_1 \bigotimes \left(\tilde{g}_1 \bigoplus \tilde{g}_2 \ldots\ldots.\tilde{g}_n\right)^{-1} \tag{14}$$

Step 8: Use Eq. (15) to further clarify the defuzzification of hesitant fuzzy figures.

$$\eta_x = \frac{l + 2m_1 + 2m_2 + h}{6} \tag{15}$$

Step 9: Normalize the weights using Eq. (16).

$$\frac{\tilde{w}_i}{\sum_i \sum_j \tilde{w}_j} \tag{16}$$

The next stage uses (hesitant fuzzy) HF-TOPSIS to discover the optimal choice. As a frequently used MADM (Multiple attribute decision-making) strategy, TOPSIS supports specialists in selecting the most favorable solution for real-world problems [16]. Sahu et al. [22] made use of TOPSIS. TOPSIS is the principle that selected alternatives must have the farthest distance from the negative ideal solution and the shortest to the positive ideal solution. In this proposed work, the HF-TOPSIS approach is used to prioritize characteristics used to define the mechanism [31–33]. The technique is centered on the customization of wrappers to determine distances in the middle of envelopes G1s and G2s. The distance is specified as envelop (G1s) = [Lp, Lq] and envelop (G2s) = [L p*, L q*] when the envelopes are given.

$$d\,(G1s, G2s) = |q^* - q| + |p^* - p| \tag{17}$$

The technique can be described as follows:

Step 10: Adopt the following at the preliminary stage:

Select the below concern taking Q alternatives ($C = \{C_1, C_2, \ldots, C_E\}$) and n criteria or characteristics ($C = \{C_1, C_2, \ldots, C_n\}$)

The specialists are stated using e_x, and the number of practitioners is K.

$\tilde{X}^l = \left[H^l_{S_{ij}}\right]_{Q\times n}$ is a hesitant fuzzy-assessment matrix in which $H^l_{S_{ij}}$ is the approximation mark for an alternative I (Ci) against criteria j (aj) stated by experts e_x.

The HF-TOPSIS process scale is as follows:

Let Scale = Nothing, Very Bad, Bad, Medium, Good, Very Good, Perfect be a demonstrated or textual term set, and CH be the context-free syntax used to generate its comparative linguistic variables. Accordingly, now consider two experts, e1 and e2, who will provide their priority for two attributes, R1 and R2.

g^1_1 = between Medium as well as Good (b/w M&G)

g^1_2 = at most Medium (am M)

g^2_1 = at least Good (al G)

g^2_2 = between Very bad and Medium (b/w VB&M)

The following is the hesitant fuzzy wrapper for the corresponding comparative linguistic statement [19]:

env_F(EGH (btM&G)) = T (0.34, 0.51, 0.68, 0.84)

env_F(EGH (amM)) = T (0.00, 0.00, 0.36, 0.68)

env_F(EGH (alG)) = T (0.51, 0.86, 1.00, 1.00)

env_F(EGH (btVB&M)) = T (0.00, 0.31, 0.38, 0.68)

Step 11: Combine the specific calculations of practitioners $\left(\tilde{X}^1, \tilde{X}^2, \ldots, \tilde{X}^K\right)$ in the following phase and construct a combined assessment matrix X = [xij], where xij represents the calculations of Ci in contradiction of aj and accurately presented as xij = [Lpij, Lqij], for instance, in Eq. (18),

$$L_{pij} = min\left\{min_{i=1}^{K}\left(maxH_{t_{ij}}^{x}\right), max_{i=1}^{K}\left(minH_{t_{ij}}^{x}\right)\right\}$$
$$L_{qij} = max\left\{min_{i=1}^{K}\left(maxH_{t_{ij}}^{x}\right), max_{i=1}^{K}\left(minH_{t_{ij}}^{x}\right)\right\} \tag{18}$$

Step 12: Let αb stand for help characteristic or criteria, with higher values in aj indicating higher preference, and αc for cost criteria, with lower values in aj indicating higher preference. Now, adopting the significant hesitant fuzzy linguistic set the positive ideal solution (indicated with $\tilde{C}^+$) and scientifically symbolized as $\tilde{C}^+ = (\tilde{F}_1^+, \tilde{F}_2^+, \ldots, \tilde{F}_n^+)$, where $\tilde{F}_j^+ = \left[F_{pj}^+, F_{qj}^+\right] (j = 1, 2, 3, \ldots, n)$ and the Hesitant Fuzzy Linguistic Term Set (HFLTS) negative ideal solution is indicated as $\tilde{C}^-$ and scientifically symbolized as $\tilde{C}^- = \left(\tilde{F}_1^-, \tilde{F}_2^-, \ldots, \tilde{F}_n^-\right)$, where $\tilde{F}_j^- = \left[F_{pj}^-, F_{qj}^-\right] (j = 1, 2, \ldots, n)$.

Additionally, we describe $\tilde{V}_{pj}^+, \tilde{V}_{qj}^+$, $\tilde{V}_{pj}^-$, and $\tilde{V}_{qj}^-$ for cost and benefit criteria such that

$$\tilde{F}_{pj}^+ = max_{i=1}^{K}\left(max_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_b$$

and

$$min_{i=1}^{K}\left(min_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_c \tag{19}$$

$$\tilde{F}_{qj}^+ = max_{i=1}^{K}\left(max_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_b$$

and

$$min_{i=1}^{K}\left(min_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_c \tag{20}$$

$$\tilde{F}_{pj}^- = max_{i=1}^{K}\left(max_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_c$$

and

$$min_{i=1}^{K}\left(min_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_b \tag{21}$$

$$\tilde{F}_{qj}^- = max_{i=1}^{K}\left(max_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_c$$

and

$$min_{i=1}^{K}\left(min_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_b \tag{22}$$

Step 13: Use Eqs. (22) and (23) to make the positive and negative ideal difference matrixes (V^+, V^-), respectively.

$$V^+ = \begin{bmatrix} d\left(x_{11}, \tilde{F}_1^+\right) + & d\left(x_{12}, \tilde{F}_2^+\right) + & \ldots + d\left(x_{1n}, \tilde{F}_n^+\right) \\ d\left(x_{21}, \tilde{F}_1^+\right) + & d\left(x_{22}, \tilde{F}_2^+\right) + & \ldots + d\left(x_{21}, \tilde{F}_n^+\right) \\ d\left(x_{m1}, \tilde{F}_1^+\right) + & d\left(x_{m2}, \tilde{F}_1^+\right) + & \ldots + d\left(x_{mn}, \tilde{F}_n^+\right) \end{bmatrix} \tag{23}$$

$$V^{-}=\begin{bmatrix} d\left(x_{11},\tilde{F}_1^{-}\right)+ & d\left(x_{12},\tilde{F}_2^{-}\right)+ & \ldots+d\left(x_{1n},\tilde{F}_n^{-}\right) \\ d\left(x_{21},\tilde{F}_1^{-}\right)+ & d\left(x_{22},\tilde{F}_2^{-}\right)+ & \ldots+d\left(x_{21},\tilde{F}_n^{-}\right) \\ d\left(x_{m1},\tilde{F}_1^{-}\right)+ & d\left(x_{m2},\tilde{F}_1^{-}\right)+ & \ldots+d\left(x_{mn},\tilde{F}_n^{-}\right) \end{bmatrix} \tag{24}$$

Step 14: Use Eq. (24) to compute the comparative closeness score for the options under deliberation.

$$CS\left(a_i\right)=\frac{V_i^{+}}{V_i^{+}+V_i^{-}}, i=1,2,\ldots.m \tag{25}$$

where

$V_i^{+}=\sum_{j=1}^{n} d\left(x_{ij},F_j^{+}\right)$ and

$$V_i^{-}=\sum_{j=1}^{n} d\left(x_{ij},F_j^{-}\right) \tag{26}$$

Step 15: Order the possibilities according to their relative proximity ratings.

The next section uses HF-AHP-TOPSIS to analyze data and produce outcomes.

3 Findings

Securing intelligent logistics is a significant concern in today's quickly changing corporate market. Because supply chains are becoming more complicated and reliant on technology, strong and efficient security measures are required. Blockchain technology has emerged as a possible answer to logistics security concerns. We defined the assessment attributes in this research based on a thorough literature survey that included analyzing various existing studies on blockchain models, intelligent logistics, as well as unified computational methodologies. We found significant parameters that are critical in determining the influence of blockchain models on intelligent logistics. We used a mixed-method strategy to acquire pertinent data during the data gathering procedure. To begin, we interviewed industry experts, logistics specialists, and blockchain specialists to gain qualitative understanding and expert viewpoints on the matter. These interviews provided us with a better grasp of the real-world implications and potential problems of implementing blockchain in intelligent logistics. Furthermore, we acquired quantitative data through questionnaires sent to logistics firms and organisations who have used blockchain in their operations. The survey questionnaire was created with the goal of gathering precise metrics and quantitative data connected to the influence of blockchain models on multiple facets of logistics safety and effectiveness.

Several measures were used to assure the reliability and authenticity of our data. To begin, we built our survey questionnaire using established measuring scales and industry-recognized metrics, that helped ensure the data's dependability and consistency. Furthermore, we ran a pilot study with a small sample size to polish the questionnaire and tackle any potential survey challenges. Further, we made every effort during the interviews to make sure that the queries were clear, unbiased, and concentrated on relevant areas of the study in order to minimise any potential researcher bias. In order to determine convergent validity, we cross-referenced the qualitative insights received from the interviews using the quantitative data collected by the questionnaires. In this section, the authors classify these models with some of their attributes in order to evaluate the priority for the selected blockchain models. To evaluate the priority of the models, the authors select them as T1 to T6 at the first tier (T) of the hierarchy. They also perform the AHP approach steps on them one by one. The hierarchy discussed in the previous section of this paper portrays the arrangements of selected technologies and their respective inherited sub-layered attributes for clear understanding. The authors of this research intended to examine the influence of blockchain-based models on transportation information records and their security by using a hierarchical structure created from current literature and the AHP technique. The hierarchical structure enabled the organization and prioritisation of evaluation criteria and sub-criteria. The AHP approach allowed for a systematic investigation of the blockchain-based models, allowing for a comparison of their usefulness in improving the security of transportation data records. Decision-makers allocated weights to each criterion and sub-criterion using pairwise comparisons, indicating their relative importance in the context of transportation data security. The AHP method enabled the weights to be aggregated in order to estimate the overall impact of every model on the security of transportation data records.

The comparative matrix interpretation is represented by a haphazard index of less than 0.1 in some similarity measures. The combined hesitant fuzzy pairwise comparison matrix (FPCM) at tier 1 is shown in Table 3 of the research paper. This matrix is utilised at the highest level of the analytical hierarchy process to contrast and assess the various criteria. The FPCM includes decision-makers' viewpoints and preferences to establish the relative significance of each criterion in the setting of ensuring intelligent logistics. Table 4 includes the aggregated hesitant FPCM from tier 1 to tier 6, including the criteria and their corresponding sub-criteria. This thorough matrix offers a full view of the review process, taking into consideration all levels and aspects of the evaluation. The table, which employs the hesitant fuzzy technique, aids in systematically reviewing and prioritising blockchain models according to their performance across many criteria and sub-criteria. The total weights determined from the analysis are presented in Table 5 of the research publication. These weights represent the relative significance or value allocated to each criterion as well as sub-criterion in the assessment process. The table gives a quantitative representation of the impact of each factor on the selection of the most acceptable blockchain model for securing intelligent logistics by aggregating decision-makers' opinions and preferences. A4, A5, and A6 were chosen as six distinct blockchain technologies [34,35]. As these six technologies represent diverse segments, the evaluation and assessment effects can be seen in distinct ways.

Table 3: At tier 1, combined hesitant fuzzy pairwise comparison matrix (FPCM)

	T1	T2	T3	T4	T5	T6	DE fuzzified and local weights
T1	1.000, 1.000, 1.000, 1.000	1.000, 1.000, 3.000, 5.000	0.300, 1.000, 1.100, 3.000	1.000, 1.200, 3.000, 5.000	0.300, 1.000, 1.000, 3.000	0.330, 1.000, 1.000, 3.000	0.050, 0.160, 0.280, 1.014
T2	0.200, 0.300, 1.000, 1.000	1.000, 1.000, 1.000, 1.000	0.200, 0.330, 1.000, 1.000	0.330, 1.000, 1.000, 3.000	1.000, 1.000, 3.000, 5.000	0.300, 1.000, 1.000, 3.000	0.035, 0.166, 0.225, 0.625
T3	0.330, 1.000, 1.000, 3.000	1.000, 1.000, 3.000, 5.000	1.000, 1.000, 1.000, 1.000	0.330, 1.000, 1.000, 3.000	1.000, 1.000, 3.000, 5.000	0.330, 1.000, 1.000, 3.000	0.050, 0.200, 0.348, 1.263

(Continued)

Table 3 (continued)

	T1	T2	T3	T4	T5	T6	DE fuzzified and local weights
T4	0.200, 0.330, 1.000, 1.000	0.330, 1.000, 1.000, 3.000	0.200, 0.300, 1.000, 1.000	1.000, 1.000, 1.000, 1.000	0.330, 1.000, 1.000, 3.000	0.200, 0.330, 1.000, 1.000	0.050, 0.133, 0.280, 0.940
T5	0.330, 1.000, 1.000, 3.000	0.200, 0.330, 1.000, 1.000	0.200, 0.330, 1.000, 1.000	0.330, 1.000, 1.000, 3.000	1.000, 1.000, 1.000, 1.000	0.330, 1.000, 1.000, 3.000	0.030, 0.080, 0.180, 0.498
T6	0.300, 1.000, 1.000, 3.000	0.330, 1.000, 1.000, 3.000	0.200, 0.330, 1.000, 1.000	1.000, 1.000, 3.000, 5.000	0.200, 0.330, 1.000, 1.000	1.000, 1.000, 1.000, 1.000	0.048, 0.157, 0.271, 1.030

Table 4: At tier 1 to tier 6, combined hesitant FPCM with the criteria

Criteria		T11	T12		Defuzzified and local weights
User identity (T1)	T11	1.000, 1.000, 1.000, 1.000	0.330, 1.000, 1.000, 3.000		0.033, 0.120, 0.212, 0.781
	T12	0.330, 1.000, 1.000, 3.000	1.000, 1.000, 1.000, 1.000		0.064, 0.240, 0.426, 1.214
Data security (T2)		T21	T22	T23	Defuzzified and local weights
	T21	1.000, 1.000, 1.000, 1.000	0.330, 1.000, 1.000, 3.000	1.000, 1.000, 3.000, 5.000	0.054, 0.133, 0.281, 0.948
	T22	0.330, 1.000, 1.000, 3.000	1.000, 1.000, 1.000, 1.000	0.330, 1.000, 1.000, 3.000	0.033, 0.086, 0.181, 0.498
	T23	0.200, 0.330, 1.000, 1.000	0.330, 1.000, 1.000, 3.000	1.000, 1.000, 1.000, 1.000	0.048, 0.157, 0.271, 1.025
Data monitoring (T3)		T31	T32		Defuzzified and local weights
	T31	1.000, 1.000, 1.000, 1.000	0.200, 0.330, 1.000, 1.000		0.052, 0.159, 0.290, 1.030
	T32	1.000, 1.000, 3.000, 5.000	1.000, 1.000, 1.000, 1.000		0.020, 0.073, 0.113, 0.500
Immutability (T4)		T41	T42		Defuzzified and local weights

(Continued)

Table 4 (continued)

Criteria		T11	T12		Defuzzified and local weights
	T41	1.000, 1.000, 1.000, 1.000	1.000, 1.000, 3.000, 5.000		0.030, 0.078, 0.121, 0.391
	T42	0.200, 0.330, 1.000, 1.000	1.000, 1.000, 1.000, 1.000		0.149, 0.276, 0.723, 1.509
Consensus (T5)		T51	T52		Defuzzied and local weights
	T51	1.000, 1.000, 1.000, 1.000	0.200, 0.330, 1.000, 1.000		0.035, 0.097, 0.198, 0.514
	T52	1.000, 1.000, 3.000, 5.000	1.000, 1.000, 1.000, 1.000		0.032, 0.079, 0.122, 0.392
Value (T6)		T61	T62	T63	Defuzzied and local weights
	T61	1.000, 1.000, 1.000, 1.000	0.200, 0.330, 1.000, 1.000	0.330, 1.000, 1.000, 3.000	0.033, 0.129, 0.212, 0.782
	T62	000, 1.000, 3.000, 5.000	1.000, 1.000, 1.000, 1.000	1.000, 1.000, 3.000, 5.000	0.064, 0.240, 0.426, 1.214
	T63	0.200, 0.330, 1.000, 1.000	0.200, 0.330, 1.000, 1.000	1.000, 1.000, 1.000, 1.000	0.053, 0.159, 0.298, 1.026

Table 5: Overall weights

First tier attributes	Local weights	Second tier attributes	Local weights	Global weights	Orders
T1	0.050, 0.160, 0.280, 1.014	T11	0.033, 0.120, 0.212, 0.781	0.080, 0.040, 0.164, 1.353	10
		T12	0.064, 0.240, 0.426, 1.214	0.004, 0.022, 0.105, 0.710	2
T2	0.035, 0.166, 0.225, 0.625	T21	0.054, 0.133, 0.281, 0.948	0.006, 0.040, 0.157, 1.462	13
		T22	0.033, 0.086, 0.181, 0.498	0.006, 0.030, 0.164, 1.353	14
		T23	0.048, 0.157, 0.271, 1.025	0.004, 0.022, 0.105, 0.711	12
T3	0.050, 0.200, 0.348, 1.263	T31	0.052, 0.159, 0.290, 1.030	0.006, 0.040, 0.157, 1.462	9
		T32	0.020, 0.073, 0.113, 0.500	0.004, 0.033, 0.123, 1.114	6

(Continued)

Table 5 (continued)

First tier attributes	Local weights	Second tier attributes	Local weights	Global weights	Orders
T4	0.050, 0.133, 0.280, 0.940	T41	0.030, 0.078, 0.121, 0.391	0.008, 0.062, 0.248, 1.732	11
		T42	0.149, 0.276, 0.723, 1.509	0.006, 0.030, 0.164, 1.353	3
T5	0.030, 0.080, 0.180, 0.498	T51	0.035, 0.097, 0.198, 0.514	0.004, 0.022, 0.105, 0.711	7
		T52	0.032, 0.079, 0.122, 0.392	0.006, 0.040, 0.157, 1.462	1
T6	0.048, 0.157, 0.271, 1.030	T61	0.033, 0.129, 0.212, 0.782	0.004, 0.033, 0.123, 1.114	8
		T62	0.064, 0.240, 0.426, 1.214	0.008, 0.062, 0.248, 1.732	5
		T63	0.053, 0.159, 0.298, 1.026	0.006, 0.041, 0.173, 1.462	4

We converted language concepts into quantitative values using the standardized Satya scale [12] and Eqs. (1)–(9), and then aggregated triangular fuzzy numeric (TFN) values. We then used Eqs. (10) and (11) to calculate the consistency and random indices.

The researchers determined the impacts of blockchain methods on various aspects after calculating the final or reliance weights of security mechanisms. As indicated in Table 6, Eqs. (1)–(5) and Step 10 have been used to gather feedback from the procedural data of the three tasks.

Table 6: Subjective cognition outcomes

	A1	A2	A3	A4	A5	A6
T11	3.550, 5.550, 7.450, 8.730	3.550, 5.550, 7.450, 8.730	3.550, 5.550, 7.450, 8.730	1.640, 3.550, 5.550, 6.730	1.450, 3.180, 5.180, 7.720	2.450, 4.270, 6.270, 8.620
T12	2.900, 4.800, 6.700, 7.640	2.900, 4.800, 6.700, 7.640	2.900, 4.800, 6.700, 7.640	2.500, 4.450, 6.400, 7.840	3.550, 5.550, 7.450, 8.700	2.090, 3.730, 5.730, 6.450
T21	2.900, 4.800, 6.700, 7.640	3.550, 5.550, 7.450, 8.730	2.900, 4.800, 6.700, 7.640	3.550, 5.550, 7.450, 8.730	2.900, 4.800, 6.700, 7.640	1.640, 3.550, 5.550, 6.730
T22	1.820, 3.730, 5.730, 6.730	2.900, 4.800, 6.700, 7.640	1.820, 3.730, 5.730, 6.730	3.550, 5.550, 7.450, 8.730	2.900, 4.800, 6.700, 7.640	3.550, 5.550, 7.450, 8.730
T23	2.820, 4.640, 6.640, 6.640	2.900, 4.800, 6.700, 7.640	2.820, 4.600, 6.640, 6.640	2.900, 4.800, 6.700, 7.640	1.820, 3.730, 5.730, 6.730	2.900, 4.800, 6.700, 7.640
T31	2.450, 4.500, 6.450, 7.730	1.800, 3.730, 5.700, 6.730	2.450, 4.450, 6.450, 7.730	2.900, 4.800, 6.700, 7.640	2.820, 4.640, 6.640, 6.640	2.900, 4.800, 6.700, 7.640

(Continued)

Table 6 (continued)

	A1	A2	A3	A4	A5	A6
T32	2.900, 4.800, 6.700, 7.640	2.500, 4.450, 6.400, 7.840	3.550, 5.550, 7.450, 8.700	2.900, 4.800, 6.700, 7.640	2.500, 4.450, 6.400, 7.840	3.550, 5.550, 7.450, 8.700
T41	2.900, 4.800, 6.700, 7.640	2.500, 4.450, 6.400, 7.840	3.550, 5.550, 7.450, 8.700	2.900, 4.800, 6.700, 7.640	3.550, 5.550, 7.450, 8.730	2.900, 4.800, 6.700, 7.640
T42	2.900, 4.800, 6.700, 7.640	3.550, 5.550, 7.450, 8.730	2.900, 4.800, 6.700, 7.640	1.820, 3.730, 5.730, 6.730	3.550, 5.550, 7.450, 8.730	2.900, 4.800, 6.700, 7.640
T51	1.820, 3.730, 5.730, 6.730	3.550, 5.550, 7.450, 8.730	2.900, 4.800, 6.700, 7.640	2.820, 4.600, 6.640, 6.640	2.900, 4.800, 6.700, 7.640	1.820, 3.730, 5.730, 6.730
T52	2.820, 4.600, 6.640, 6.640	2.900, 4.800, 6.700, 7.640	2.900, 4.800, 6.700, 7.640	2.450, 4.450, 6.450, 7.730	2.900, 4.800, 6.700, 7.640	2.820, 4.640, 6.640, 6.640
T61	2.450, 4.450, 6.450, 7.730	2.900, 4.800, 6.700, 7.640	1.820, 3.730, 5.730, 6.730	3.550, 5.550, 7.450, 8.730	3.550, 5.550, 7.450, 8.730	3.550, 5.550, 7.450, 8.730
T62	3.550, 5.550, 7.450, 8.730	3.550, 5.550, 7.450, 8.730	2.820, 4.600, 6.640, 6.640	2.900, 4.800, 6.700, 7.640	1.820, 3.730, 5.730, 6.730	3.550, 5.550, 7.450, 8.730
T63	2.820, 4.640, 6.640, 6.640	2.900, 4.800, 6.700, 7.640	2.450, 4.450, 6.450, 7.730	2.900, 4.800, 6.700, 7.640	2.820, 4.640, 6.640, 6.640	2.900, 4.800, 6.700, 7.640

The contributors calculated the standardized hesitant fuzzy-based judgment matrix and weighted the standardized and weighted normalized hesitant fuzzy judgment matrix using Eqs. (16)–(18), as illustrated in Tables 7 and 8.

Table 7: The normalized hesitant fuzzy-assessment matrix

	A1	A2	A3	A4	A5	A6
T11	0.639, 0.816, 0.589, 0.967	0.639, 0.816, 0.589, 0.967	0.639, 0.816, 0.589, 0.967	0.639, 0.816, 0.589, 0.967	0.639, 0.816, 0.589, 0.967	0.620, 0.872, 0.936, 0.989
T12	0.554, 0.804, 0.880, 0.958	0.611, 0.772, 0.856, 0.945	0.554, 0.804, 0.880, 0.958	0.611, 0.772, 0.856, 0.945	0.380, 0.574, 0.722, 0.080	0.275, 0.456, 0.533, 0.733
T21	0.372, 0.565, 0.693, 0.835	0.639, 0.816, 0.589, 0.967	0.370, 0.565, 0.690, 0.835	0.639, 0.816, 0.589, 0.967	0.630, 0.816, 0.589, 0.967	0.639, 0.816, 0.589, 0.967
T22	0.604, 0.812, 0.858, 0.969	0.550, 0.800, 0.880, 0.950	0.600, 0.812, 0.858, 0.969	0.554, 0.804, 0.880, 0.958	0.611, 0.772, 0.850, 0.945	0.380, 0.574, 0.722, 0.082
T23	0.554, 0.804, 0.880, 0.958	0.370, 0.550, 0.690, 0.850	0.550, 0.804, 0.880, 0.958	0.372, 0.565, 0.693, 0.835	0.570, 0.725, 0.792, 0.896	0.249, 0.413, 0.532, 0.741
T31	0.639, 0.816, 0.589, 0.967	0.630, 0.810, 0.580, 0.960	0.630, 0.816, 0.589, 0.967	0.639, 0.816, 0.589, 0.967	0.630, 0.816, 0.580, 0.967	0.231, 0.381, 0.548, 0.736
T32	0.554, 0.800, 0.880, 0.950	0.611, 0.772, 0.856, 0.945	0.554, 0.804, 0.880, 0.958	0.639, 0.816, 0.589, 0.967	0.639, 0.816, 0.580, 0.967	0.639, 0.816, 0.589, 0.967

(Continued)

Table 7 (continued)

	A1	A2	A3	A4	A5	A6
T41	0.372, 0.565, 0.693, 0.835	0.639, 0.816, 0.589, 0.967	0.639, 0.816, 0.589, 0.967	0.370, 0.565, 0.690, 0.835	0.639, 0.816, 0.589, 0.967	0.630, 0.816, 0.589, 0.967
T42	0.604, 0.812, 0.858, 0.969	0.550, 0.800, 0.880, 0.950	0.550, 0.800, 0.880, 0.950	0.600, 0.812, 0.858, 0.969	0.554, 0.804, 0.880, 0.958	0.611, 0.772, 0.850, 0.945
T51	0.639, 0.816, 0.589, 0.967	0.370, 0.550, 0.690, 0.850	0.370, 0.550, 0.690, 0.850	0.550, 0.804, 0.880, 0.958	0.372, 0.565, 0.693, 0.835	0.570, 0.725, 0.792, 0.896
T52	0.554, 0.804, 0.880, 0.950	0.639, 0.816, 0.589, 0.967	0.370, 0.565, 0.690, 0.835	0.639, 0.816, 0.589, 0.967	0.630, 0.816, 0.589, 0.967	0.639, 0.816, 0.589, 0.967
T61	0.639, 0.816, 0.589, 0.967	0.550, 0.800, 0.880, 0.950	0.600, 0.812, 0.858, 0.969	0.554, 0.804, 0.880, 0.958	0.611, 0.772, 0.850, 0.945	0.380, 0.574, 0.722, 0.082
T62	0.554, 0.800, 0.880, 0.958	0.370, 0.550, 0.690, 0.850	0.550, 0.804, 0.880, 0.958	0.372, 0.565, 0.693, 0.835	0.570, 0.725, 0.792, 0.896	0.249, 0.413, 0.532, 0.741
T63	0.372, 0.565, 0.693, 0.835	0.630, 0.810, 0.580, 0.960	0.630, 0.816, 0.589, 0.967	0.639, 0.816, 0.589, 0.967	0.630, 0.816, 0.580, 0.967	0.231, 0.381, 0.548, 0.736

Table 8: The subjective normalized hesitant fuzzy-assessment matrix

	A1	A2	A3	A4	A5	A6
T11	0.032, 0.053, 0.072, 0.098	0.032, 0.047, 0.053, 0.063	0.142, 0.179, 0.198, 0.219	0.058, 0.085, 0.090, 0.180	0.047, 0.074, 0.092, 0.112	0.044, 0.051, 0.066, 0.069
T12	0.061, 0.101, 0.117, 0.154	0.112, 0.144, 0.163, 0.195	0.016, 0.082, 0.099, 0.122	0.032, 0.050, 0.072, 0.090	0.032, 0.047, 0.053, 0.063	0.142, 0.179, 0.198, 0.219
T21	0.037, 0.066, 0.079, 0.110	0.061, 0.101, 0.117, 0.154	0.112, 0.144, 0.163, 0.195	0.061, 0.101, 0.110, 0.150	0.112, 0.144, 0.163, 0.195	0.051, 0.082, 0.099, 0.122
T22	0.063, 0.097, 0.114, 0.131	0.032, 0.050, 0.072, 0.098	0.032, 0.047, 0.053, 0.063	0.037, 0.061, 0.070, 0.110	0.061, 0.101, 0.117, 0.154	0.112, 0.144, 0.163, 0.195
T23	0.112, 0.144, 0.163, 0.195	0.061, 0.101, 0.117, 0.154	0.112, 0.144, 0.163, 0.195	0.063, 0.097, 0.114, 0.131	0.037, 0.061, 0.079, 0.110	0.032, 0.053, 0.072, 0.098
T31	0.032, 0.053, 0.072, 0.098	0.032, 0.047, 0.053, 0.063	0.142, 0.179, 0.198, 0.219	0.112, 0.144, 0.163, 0.195	0.061, 0.101, 0.117, 0.154	0.112, 0.144, 0.163, 0.195
T32	0.061, 0.101, 0.117, 0.154	0.112, 0.144, 0.163, 0.195	0.112, 0.144, 0.163, 0.195	0.032, 0.053, 0.072, 0.098	0.030, 0.047, 0.053, 0.063	0.142, 0.179, 0.198, 0.219
T41	0.031, 0.066, 0.070, 0.110	0.061, 0.110, 0.117, 0.150	0.061, 0.110, 0.117, 0.150	0.061, 0.100, 0.117, 0.154	0.032, 0.053, 0.072, 0.098	0.032, 0.047, 0.053, 0.063
T42	0.063, 0.097, 0.114, 0.131	0.032, 0.050, 0.072, 0.098	0.032, 0.050, 0.072, 0.098	0.032, 0.047, 0.053, 0.063	0.037, 0.061, 0.070, 0.110	0.061, 0.101, 0.117, 0.154
T51	0.112, 0.144, 0.163, 0.195	0.061, 0.101, 0.117, 0.154	0.112, 0.144, 0.163, 0.195	0.032, 0.053, 0.072, 0.098	0.030, 0.047, 0.053, 0.063	0.142, 0.179, 0.198, 0.219

(Continued)

Table 8 (continued)

	A1	A2	A3	A4	A5	A6
T52	0.032, 0.053, 0.072, 0.098	0.032, 0.047, 0.053, 0.063	0.061, 0.110, 0.117, 0.150	0.061, 0.100, 0.117, 0.154	0.032, 0.053, 0.072, 0.098	0.032, 0.047, 0.053, 0.063
T61	0.061, 0.101, 0.110, 0.154	0.112, 0.144, 0.163, 0.195	0.032, 0.050, 0.072, 0.098	0.032, 0.047, 0.053, 0.063	0.037, 0.061, 0.070, 0.110	0.061, 0.101, 0.117, 0.154
T62	0.037, 0.066, 0.079, 0.110	0.032, 0.047, 0.053, 0.063	0.142, 0.179, 0.198, 0.219	0.112, 0.144, 0.163, 0.195	0.061, 0.101, 0.117, 0.154	0.112, 0.144, 0.163, 0.195
T63	0.063, 0.097, 0.114, 0.131	0.112, 0.144, 0.163, 0.195	0.112, 0.144, 0.163, 0.195	0.032, 0.053, 0.072, 0.098	0.030, 0.047, 0.053, 0.063	0.142, 0.179, 0.198, 0.219

The closeness coefficients for different alternatives are shown in Table 9. Closeness coefficients are generated as a component of the decision-making process to determine how close each alternative is to the ideal solution. These coefficients reflect the degree to which each alternative meets the study's evaluation criteria and sub-criteria. The proximity coefficients are calculated mathematically by comparing the effectiveness of each alternative to the defined criteria and sub-criteria. The higher an alternative's proximity coefficient, the closer it is to the ideal answer and the more appropriate it is deemed in the context of securing intelligent logistics. The authors premeditated the relative proximity using Eqs. (19)–(26), as shown in Table 9 and Fig. 4.

Table 9: Closeness coefficients of numerous alternatives

Alternatives		d+i	d-i	Gap degree	Satisfaction degree
Alternative 1	A1	0.045	0.027	0.379	0.632
Alternative 2	A2	0.038	0.037	0.499	0.527
Alternative 3	A3	0.037	0.043	0.537	0.464
Alternative 4	A4	0.037	0.027	0.433	0.571
Alternative 5	A5	0.036	0.046	0.550	0.465
Alternative 6	A6	0.031	0.050	0.625	0.405

3.1 Sensitivity Analysis

The responsiveness of the procured weights (different factors) was evaluated throughout this data processing [31]. At the completion of the second phase, 15 relevant factors were taken from the investigative process to ensure that the sensitivities could be evaluated using 14 experimentations. Through both the hesitant fuzzy AHP-TOPSIS technique and the hesitant fuzzy AHP-TOPSIS method, the degree of satisfaction tier (CC-i) was premeditated in every test by adjusting the alternatives, while the values of the different elements continued to be unaffected. The estimated effects are shown in Table 10 and Fig. 5. Based on the actual performance, alternative solution one (A1) has an extremely high level of satisfaction (CC-i). A total of 15 experiments were carried out. The results reveal that alternative one (A1) continues to provide a high level of satisfaction (CC-i) in all of the experiments. A3 is the lowest-weighted option in 13 experiments, and A6 is the lowest-weighted alternative in 2 of them. When the scores of the alternatives are compared to each other, the results show that the options' ratings are weighted.

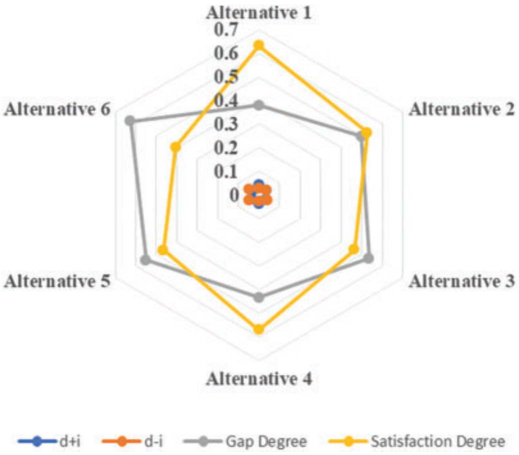

Figure 4: Schematic illustration of the tier of satisfaction

Table 10: Sensitivity examination

		Satisfaction degree (CC-i)					
Scenario	Weights/alternatives	A1	A2	A3	A4	A5	A6
Exp-0	Original weights	0.632	0.527	0.464	0.571	0.465	0.405
Exp-1	T-11	0.632	0.527	0.464	0.571	0.465	0.406
Exp-2	T-12	0.633	0.527	0.466	0.589	0.479	0.397
Exp-3	T-21	0.633	0.527	0.464	0.571	0.466	0.406
Exp-4	T-22	0.637	0.527	0.470	0.571	0.465	0.415
Exp-5	T-23	0.632	0.525	0.464	0.577	0.466	0.415
Exp-6	T-31	0.632	0.527	0.464	0.571	0.465	0.424
Exp-7	T-32	0.645	0.536	0.463	0.572	0.465	0.405
Exp-8	T-41	0.632	0.527	0.464	0.572	0.465	0.406
Exp-9	T-42	0.632	0.527	0.479	0.589	0.479	0.390
Exp-10	T-51	0.632	0.527	0.464	0.571	0.465	0.424
Exp-11	T-52	0.632	0.527	0.464	0.572	0.465	0.406
Exp-12	T-61	0.632	0.525	0.464	0.577	0.466	0.415
Exp-13	T-62	0.633	0.527	0.464	0.571	0.466	0.406
Exp-14	T-63	0.646	0.536	0.478	0.586	0.479	0.415

3.2 Comparative Analysis of the Findings

During this investigation, the researchers employed a variety of symmetrical methods to assess the accuracy of the research's results. To assess the accuracy of the study's findings, the researchers employed a hesitant fuzzy AHP-TOPSIS tactic. In hesitant fuzzy AHP-TOPSIS, the information gathering and computation methods are closely related to those used in conventional AHP-TOPSIS. Fuzzification and defuzzification are permitted in hesitant fuzzy AHP-TOPSIS. Information is compiled in its earliest mathematical terms for hesitant fuzzy AHP-TOPSIS and afterward changed into hesitant fuzzy figures. Fig. 6 depicts the discrepancies between the hesitant fuzzy and traditional AHP-TOPSIS findings.

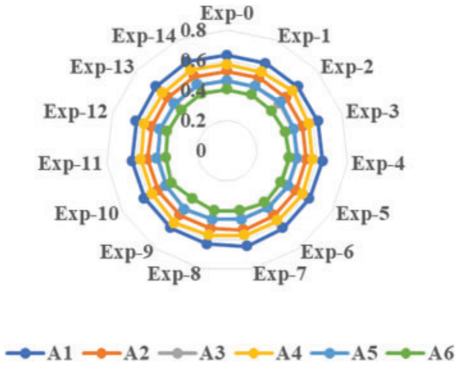

Figure 5: Schematic illustration of sensitivity examination

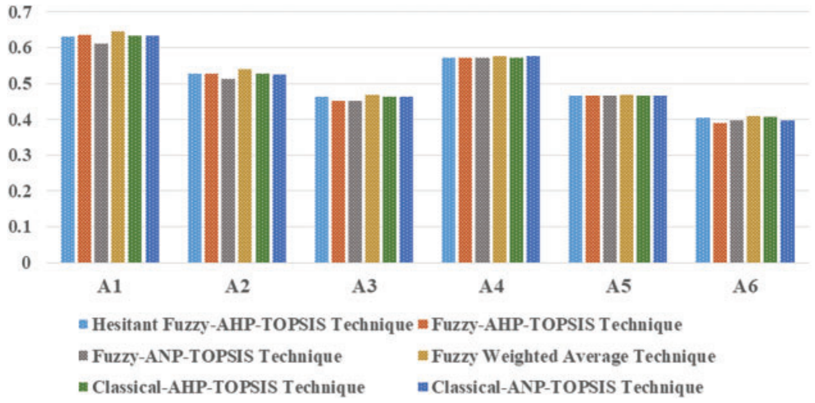

Figure 6: Schematic illustration of different outcomes

The findings of this study are unique, yet they are essentially the same. The Pearson correlation technique was used to evaluate the relationship between the outcomes in this empirical study. The effect of the two-value relationship is demonstrated by the coefficient correlation [32]. The scale spans from –1 to 1. A value close to –1 suggests a weaker relationship between values, whereas a value close to 1 indicates a stronger connection. The Pearson correlation for the hesitant fuzzy AHP results and the classical AHP conclusions is 0.89176, which shows that the outcomes are very similar. As shown in Table 11, studies on the same dataset using different criteria for blockchain technology have previously been created, and all of the findings indicate that the outcomes of hesitant fuzzy AHP and classical AHP are significantly connected.

Our research results also demonstrate that the identified different factors and their correlation to efficient security capabilities are highly relevant to security arrangements. Khan et al. [37] used the hesitant fuzzy AHP-TOPSIS technique in their research. This is because the AHP methodology differs as it uses a hierarchy structure rather than a tree structure. As a result, in the current study, the researchers included design techniques in the hierarchy's initial stage, which effectively improved the outcomes. There is no synchronous method of evaluating system security in the specific scenario of design policy initiatives using the hesitant fuzzy AHP-TOPSIS procedure.

Table 11: Comparative analysis

Approaches/alternatives	A1	A2	A3	A4	A5	A6
Hesitant fuzzy-AHP-TOPSIS technique	0.632	0.527	0.464	0.571	0.465	0.405
Fuzzy-AHP-TOPSIS technique	0.637	0.527	0.450	0.571	0.465	0.389
Fuzzy-ANP-TOPSIS technique	0.612	0.514	0.451	0.572	0.465	0.398
Fuzzy weighted average technique	0.646	0.540	0.469	0.577	0.469	0.409
Classical-AHP-TOPSIS technique	0.633	0.527	0.463	0.573	0.465	0.407
Classical-ANP-TOPSIS technique	0.633	0.526	0.464	0.577	0.466	0.396

4 Discussion

The primary goal of this research is to compute the influence of blockchain technology frameworks on the security of electronic records in the context of a security policy that could aid professionals in identifying and choosing the most effective blockchain model to improve security in the transportation sector. To examine the influence of blockchain technology models, the authors used an MCDM hybrid approach with hesitant fuzzy AHP-TOPSIS. Key characteristics of blockchain technology, such as immutability, decentralization, and security, combine to address several major difficulties now affecting the transportation industry. In this research, the private blockchain model obtained higher weighted choices compared to other blockchain models, which indicates that private blockchain models are more effective than a hybrid, public, consortium, and permissioned blockchains, as well as decentralized systems, in executing secure electronic records transactions in transportation organizations. Zarour et al. [42] created observation networks using a private blockchain framework to encourage and strengthen the distribution of e-transportation information across various European nations and concluded it was the safest method imaginable. The basis of quality transportation is electronic records. As a result, providing consumers with ideal secure transportation structures via a private blockchain model would be highly beneficial to the transportation industry.

The study's findings have important implications for the area of intelligent logistics and the use of blockchain technology. This study effectively analysed different blockchain models by using a static analysis with an integrated hesitant fuzzy AHP-TOPSIS approach. The researchers were able to completely examine and compare the various models of blockchain technology and establish their impact on intelligent logistics by using this MCDM methodology. According to the findings of this research, the private blockchain model is the most significant solution for the transportation business. Implementing a private blockchain approach might potentially revolutionise how logistical operations are carried out. This architecture is well-known for its improved safety capabilities, making it an appealing alternative for businesses looking to protect sensitive information as well as transactions within their logistical networks. When it comes to precious goods, time-critical deliveries, and sensitive information in the transportation business, the safe environment provided by the private blockchain model can be extremely beneficial in preserving data integrity and preventing unauthorised access. Additionally, the study's beneficial implications extend beyond the transportation business. The use of the hesitant fuzzy AHP-TOPSIS methodology proves the relevance and efficacy of such decision-making strategies in evaluating and choosing optimal blockchain models for diverse applications within intelligent logistics. This technique offers decision-makers with a dependable tool for evaluating and prioritising various technology possibilities based on a variety of factors, allowing them to make educated and efficient decisions.

Measuring the impact of blockchain technology frameworks on electronic records security is a technique that can assist developers in determining the performance of blockchain technology. The present study would assist blockchain designers in prioritizing and selecting elements of blockchain technology for building reliable and secure transportation blockchain applications. Currently, electronic record security is a major challenge for both designers and users. While establishing a security feature for electronic records, the current research would provide specialists with plenty of consideration for various techniques rather than using informal and traditional approaches. In addition, as the security of electronic records is both a diverse and complex task in the blockchain technology context, this research may be useful for transportation providers, which limits the applicability of the overall system. Every day, customers and engineers are presented with new issues. Although the combined hesitant fuzzy AHP-TOPSIS method for evaluating the impact of blockchain technology on safeguarding electronic records is effective and relevant, there may be a more viable MCDM symmetrical technology for this challenge.

5 Conclusion

In the era of digital transformation, it is vital to understand concepts that are beneficial to the industry. This study uses static analysis to evaluate the various blockchain models by utilizing an integrated hesitant fuzzy AHP-TOPSIS methodology, which provides an effective outcome. By adopting this MCDM approach, the authors evaluated various models of blockchain technology and applied the adopted integrated mechanism to them to calculate the most impactful approach. The results discussed in this article suggest that the private model of blockchain would have the greatest impact on the transportation industry, and it also provides the most secure environment. As a future direction, this study provides guidelines for developers by simulating the results and expanding on different models and their impact. Furthermore, to make the results more effective and accurate, the authors performed both sensitivity and comparison analyses on the results.

Acknowledgement: The authors would like to thank the Deanship of Scientific Research at Shaqra University for supporting this work.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: Study conception and design: M. S. Alsaqer, M. H. Alsulami; data collection: M. H. Alsulami, R. N. Alkhawaji, A. A. Alaboudi; analysis and interpretation of results: M. S. Alsaqer, M. H. Alsulami, A. A. Alaboudi; draft manuscript preparation: M. S. Alsaqer, M. H. Alsulami, R. N. Alkhawaji, A. A. Alaboudi. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The authors confirm that the data supporting the findings of this study are available within the article.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] CST, "Blockchain as a regulatory tool," 2022. [Online]. Available: https://www.cst.gov.sa/ar/research-innovation/Documents/BlockchainasaRegulatoryTool.pdf

[2] M. S. Rahman, M. A. P. Chamikara, I. Khalil and A. Bouras, "Blockchain-of-blockchains: An interoperable blockchain platform for ensuring IoT data integrity in smart city," *Journal of Industrial Information Integration*, vol. 30, pp. 100408, 2022.

[3] H. Alyami, M. Nadeem, A. Alharbi, W. Alosaimi, M. T. J. Ansari *et al.,* "The evaluation of software security through quantum computing techniques: A durability perspective," *Applied Sciences*, vol. 11, no. 24, pp. 11784, 2021.

[4] M. Crosby, P. Pattanayak, S. Verma and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Applied Innovation*, vol. 71, no. 2, pp. 6–10, 2016.

[5] Z. Zheng, S. Xie, H. N. Dai, X. Chen and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[6] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach *et al.,* "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renewable and Sustainable Energy Reviews*, vol. 100, no. 5, pp. 143–174, 2019.

[7] B. Teufel, A. Sentic and M. Barmet, "Blockchain energy: Blockchain in future energy systems," *Journal of Electronic Science and Technology*, vol. 17, no. 4, pp. 317–331, 2019.

[8] M. Gorodnichev, A. Kukharenko, E. Kukharenko and T. Salutina, "Methods of developing systems based on blockchain," in *Proc. of the 24th Conf. of Open Innovations Association FRUCT*, Helsinki, Uusimaa, Finland, pp. 613–618, 2019.

[9] M. Li, S. Shao, Q. Ye, G. Xu and G. Q. Huang, "Blockchain-enabled logistics finance execution platform for capital-constrained E-commerce retail," *Robotics and Computer-Integrated Manufacturing*, vol. 65, no. 9, pp. 1019–1027, 2020.

[10] F. Damico, "How technology is reshaping financial services: Blockchain use cases in the banking industry," *Symmetry*, vol. 10, no. 3, pp. 352–375, 2020.

[11] S. Ølnes, J. Ubacht and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing," *Government Information Quarterly*, vol. 34, no. 3, pp. 355–364, 2017.

[12] R. Kumar, S. A. Khan and R. A. Khan, "Software security testing: A pertinent framework," *Journal of Global Research in Computer Science*, vol. 5, no. 3, pp. 23–27, 2014.

[13] R. Kumar, S. A. Khan and R. A. Khan, "Fuzzy analytic hierarchy process for software durability: Security risks perspective," in *Proc. of Int. Conf. on Communication and Networks*, Singapore, Springer, pp. 469–478, 2017.

[14] R. Kumar, S. A. Khan and R. A. Khan, "Secure serviceability of software: Durability perspective," in *Int. Conf. on Smart Trends for Information Technology and Computer Communications*, Singapore, Springer, pp. 104–110, 2016.

[15] A. Attaallah, H. Alsuhabi, S. Shukla, R. Kumar, B. K. Gupta *et al.,* "Analyzing the big data security through a unified decision-making approach," *Intelligent Automation and Soft Computing*, vol. 32, no. 2, pp. 1071–1088, 2022.

[16] R. Kandaswamy and D. Furlonger, "Blockchain-based transformation: A gartner trend insight report," 2018. [Online]. Available: https://www.gartner.com/en/doc/3869696-blockchain-based-transformation-a-gartner-trend-insight-report

[17] M. Z. A. Bhuiyan, A. Zaman, T. Wang, G. Wang, H. Tao *et al.,* "Blockchain and big data to transform the transportation," in *Proc. of the Int. Conf. on Data Processing and Applications*, Guangdong, China, pp. 62–68, 2018. https://doi.org/10.1145/3224207.3224220

[18] N. N. Neto, S. Madnick, A. M. G. D. Paula and N. M. Borges, "Developing a global data breach database and the challenges encountered," *Journal of Data and Information Quality (JDIQ)*, vol. 13, no. 1, pp. 1–33, 2021.

[19] C. Arsene, "The global 'blockchain in transportation' report: The 2020 ultimate guide for every executive, Transportation Weekly," 2020. [Online]. Available: https://transportationweekly.com/blockchain-in-transportation-guide/

[20] H. Abusaaq, "Kingdom of Saudi Arabia 2020 budget report, KPMG Professional Services," 2019. [Online]. Available: https://assets.kpmg.com/content/dam/kpmg/sa/pdf/2019/KingdomofSaudi%20Arabia2020BudgetReport.pdf

[21] H. S. M. Lim and A. Taeihagh, "Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications," *Energies*, vol. 11, no. 5, pp. 1062, 2018.

[22] G. Tonn, J. P. Kesan, L. Zhang and J. Czajkowski, "Cyber risk and insurance for transportation infrastructure," *Transport Policy*, vol. 79, no. 1, pp. 103–114, 2019.

[23] R. Kumar, S. A. Khan and R. A. Khanm, "Analytical network process for software security: A design perspective," *CSI Transactions on ICT*, vol. 4, no. 2, pp. 255–258, 2016.

[24] X. Liang, J. Zhao, S. Shetty, J. Liu and D. Li, "Integrating blockchain for data sharing and collaboration in mobile transportation applications," in *Proc. of the 2017 IEEE 28th Annual Int. Sym. on Personal, Indoor, and Mobile Radio Communications*, Montreal, QC, Canada, pp. 1–5, 2017. https://doi.org/10.1109/PIMRC.2017.8292361

[25] R. Kumar, S. A. Khan, A. Agrawal and R. A. Khan, "Measuring the security attributes through fuzzy analytic hierarchy process: Durability perspective," *ICIC Express Letters*, vol. 12, no. 6, pp. 615–620, 2018.

[26] M. Shoaib, M. K. Lim and C. Wang, "An integrated framework to prioritize blockchain-based supply chain success factors," *Industrial Management & Data Systems*, vol. 120, no. 11, pp. 2103–2131, 2020.

[27] Technavio, "Blockchain technology market in transportation and logistics industry analysis," 2022. [Online]. Available: https://www.technavio.com/report/blockchain-technology-market-in-transportation-and-logistics-industry-analysis

[28] A. Agrawal, A. H. Seh, A. Baz, H. Alhakami, W. Alhakami *et al.,* "Software security estimation using the hybrid fuzzy ANP-TOPSIS approach: Design tactics perspective," *Symmetry*, vol. 12, no. 4, pp. 598, 2020.

[29] R. Kumar, S. A. Khan and R. A. Khan, "Durable security in software development: Needs and importance," *CSI Communication*, vol. 39, no. 7, pp. 34–36, 2015.

[30] N. Khoshavi, G. Tristani and A. Sargolzaei, "Blockchain applications to improve operation and security of transportation systems: A survey," *Electronics*, vol. 10, no. 5, pp. 629, 2021.

[31] R. Kumar, S. A. Khan and R. A. Khan, "Revisiting software security risks," *British Journal of Mathematics & Computer Science*, vol. 11, no. 6, pp. 1–10, 2015.

[32] W. Alosaimi, M. T. J. Ansari, A. Alharbi, H. Alyami, S. Ali *et al.,* "Toward a unified model approach for evaluating different electric vehicles," *Energies*, vol. 14, no. 19, pp. 6120, 2021.

[33] R. Kumar, S. A. Khan and R. A. Khan, "Durability challenges in software engineering," *Crosstalk–The Journal of Defense Software Engineering*, vol. 1, pp. 29–31, 2016.

[34] C. Zhang, M. Zhao, L. Zhu, W. Zhang, T. Wu *et al.,* "FRUIT: A blockchain-based efficient and privacy-preserving quality-aware incentive scheme," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 12, pp. 3343–3357, 2022.

[35] H. Alyami, M. T. J. Ansari, A. Alharbi, W. Alosaimi, M. Alshammari *et al.,* "Effectiveness evaluation of different IDSs using integrated fuzzy MCDM model," *Electronics*, vol. 11, no. 6, pp. 859, 2022.

[36] R. Kumar, M. Zarour, M. Alenezi, A. Agrawal and R. A. Khan, "Measuring security durability of software through fuzzy-based decision-making process," *International Journal of Computational Intelligence Systems*, vol. 12, no. 2, pp. 627, 2019.

[37] A. I. Khan, A. S. A. M. ALGhamdi, F. J. Alsolami, Y. B. Abushark, A. Almalawi *et al.,* "Integrating blockchain technology into healthcare through an intelligent computing technique," *Computers, Materials & Continua*, vol. 70, no. 2, pp. 2835–2860, 2022.

[38] A. H. Seh, J. F. Al-Amri, A. F. Subahi, M. T. J. Ansari, R. Kumar *et al.,* "Hybrid computational modeling for web application security assessment," *Computers, Materials & Continua*, vol. 70, no. 1, pp. 469–489, 2022.

[39] A. P. Balcerzak, E. Nica, E. Rogalska, M. Poliak, T. Kliešṫik *et al.,* "Blockchain technology and smart contracts in decentralized governance systems," *Administrative Sciences*, vol. 12, no. 3, pp. 96, 2022.

[40] R. Kumar, S. A. Khan and R. A. Khan, "Revisiting software security: Durability perspective," *International Journal of Hybrid Information Technology*, vol. 8, no. 2, pp. 311–322, 2015.

[41] M. T. J. Ansari, A. Agrawal and R. A. Khan, "DURASec: Durable security blueprints for web-applications empowering digital india initiative," *EAI Endorsed Transactions on Scalable Information Systems*, vol. 9, no. 4, pp. e25, 2022.

[42] M. Zarour, M. T. J. Ansari, M. Alenezi, A. K. Sarkar, M. Faizan *et al.,* "Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records," *IEEE Access*, vol. 8, pp. 157959–157973, 2020.

[43] Q. Yang, Y. Zhao, H. Huang, Z. Xiong, J. Kang *et al.,* "Fusing blockchain and AI with metaverse: A survey," *IEEE Open Journal of the Computer Society*, vol. 3, pp. 122–136, 2022.

[44] Z. Zhou, M. Wang, J. Huang, S. Lin and Z. Lv, "Blockchain in big data security for intelligent transportation with 6G," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 9736–9746, 2021.

[45] S. Alacam and A. Sencer, "Using blockchain technology to foster collaboration among shippers and carriers in the trucking industry: A design science research approach," *Logistics*, vol. 5, no. 2, pp. 37, 2021.

[46] O. Ali, A. Jaradat, A. Kulakli and A. Abuhalimeh, "A comparative study: Blockchain technology utilization benefits, challenges and functionalities," *IEEE Access*, vol. 9, pp. 12730–12749, 2021.

[47] S. Singh, A. S. Hosen and B. Yoon, "Blockchain security attacks, challenges, and solutions for the future distributed IoT network," *IEEE Access*, vol. 9, pp. 13938–13959, 2021.

[48] S. Nanayakkara, M. N. N. Rodrigo, S. Perera, G. T. Weerasuriya and A. A. Hijazi, "A methodology for selection of a Blockchain platform to develop an enterprise system," *Journal of Industrial Information Integration*, vol. 23, no. 4, pp. 100215, 2021.

[49] P. De Filippi, M. Mannan and W. Reijers, "The legality of blockchain technology," *Policy and Society*, vol. 41, no. 3, pp. 358–372, 2022.