



Prioritizing Key Performance and Security Criteria of Blockchain Platforms: A FUCOM-Based Approach

Iliya Mirzaei^{1,*}, Amirhossein Khanlari¹

¹ Computer Science, Department of Computer Science, Stony Brook University, NY, USA

ARTICLE INFO

Article history:

Received 2 September 2026

Received in revised form 5 October 2026

Accepted 19 October 2026

Available online 25 October 2026

Keywords:

Blockchain Platforms; Blockchain Security; Performance Evaluation; Multi-Criteria Decision-Making (MCDM); Full Consistency Method (FUCOM)

ABSTRACT

Performance evaluation of blockchain platforms is essential for understanding their relative strengths and limitations and for establishing a systematic basis for comparing and prioritizing the criteria that characterize their performance and security. In this study, the Full Consistency Method (FUCOM), a Multi-Criteria Decision-Making (MCDM) method, was employed to weight and rank 13 key criteria for evaluating the performance and security-related dimensions of blockchain platforms, which were identified and extracted from the relevant literature. The study is applied in terms of its objective and descriptive-analytical in nature. Data were collected through specialized questionnaires and the judgments of an expert panel. FUCOM was employed because it requires $n - 1$ sequential comparisons to rank n criteria and provides a means of assessing the consistency of expert judgments. The consistency of the judgments was evaluated based on the deviation measure calculated using FUCOM. The results indicated that "Transaction speed (C_{10})", with a weight of 0.1035, ranked first. "Network robustness (C_1)", with a weight of 0.0996; "Consensus mechanism (C_4)", with a weight of 0.0957; and "Transaction-ordering fairness (C_{13})", with a weight of 0.0917, ranked second to fourth, respectively. The remaining structural, security-related, and operational criteria occupied the subsequent positions. These findings provide a systematic basis for prioritizing performance and security criteria in blockchain platform evaluation and can support system architects and technology managers in making more informed decisions about platform design and selection.

1. Introduction

Blockchain-based platforms and Distributed Ledger Technology (DLT) have introduced a new paradigm for establishing trust and transparently recording events by eliminating centralized intermediaries and replacing them with cryptographic mechanisms [1], [2]. This technology has evolved beyond its origins as a purely financial innovation in the form of Bitcoin and is now used as an infrastructure for developing smart contracts, decentralized financial markets, and transparent supply chains [3]. As architectural designs have diversified and industrial implementations have

* Corresponding author.

E-mail address: imirzaei@cs.stonybrook.edu

expanded, the focus of researchers and software engineers has shifted from demonstrating the theoretical feasibility of this technology to rigorously evaluating the performance, security, and operational stability of these systems under real-world conditions. This shift is particularly important because selecting or implementing an inefficient platform can result in severe and irreversible financial and security losses [4].

However, performance evaluation in blockchain environments is inherently multidimensional and challenging, as platform performance metrics are interdependent and often involve conflicting trade-offs, a phenomenon commonly described in the literature as the Blockchain Trilemma [5]. On one side of this trade-off is the need to increase processing throughput and transaction confirmation speed. Achieving these improvements often requires modifying the consensus mechanism and restricting the number of validating nodes. Such changes can directly reduce the degree of decentralization and increase the risk of centralized governance [6]. Furthermore, computationally intensive data validation processes and the use of traditional consensus algorithms can lead to excessive energy consumption and waste of hardware resources, posing a barrier to the sustainable development of these networks [7].

At the other end of this interplay lies a fundamental tension between structural transparency and data protection. Distributed ledger architectures are designed to ensure the immutability, authenticity, and traceability of records through cryptographic links [8]. However, this inherent transparency and public access to block contents can create significant challenges for protecting participants' privacy. To address these challenges, some blockchain platforms incorporate advanced cryptographic techniques, including zero-knowledge proofs, which enable the verification of certain claims without disclosing sensitive information. Although these techniques can enhance privacy, their implementation may increase computational overhead [9]. Furthermore, a platform's resilience to failures and attacks, is influenced by validator behavior and the fairness of transaction ordering, since incentives to manipulate block ordering for personal gain can undermine the stability of the entire system [10]. Therefore, evaluating a platform's performance cannot be limited to considering isolated metrics; rather, it requires a comprehensive approach to assessing the relative priorities of these competing criteria and the extent to which they influence one another.

Despite the growing body of research on blockchain technology, there remains scope for further investigation from both thematic and methodological perspectives. From a thematic perspective, some studies have focused on specific aspects of blockchain platform performance. However, evaluating these aspects alongside security and governance criteria may provide a more comprehensive picture of platform performance. From a methodological perspective, Multi-Criteria Decision-Making (MCDM) methods provide a means of evaluating different criteria based on their relative weights and importance [11]. Nevertheless, determining criterion weights generally relies on expert judgment and may be influenced by differences in experts' opinions and the consistency of their assessments. In some conventional methods, particularly those requiring pairwise comparisons between all criteria, the number of required comparisons increases with the number of criteria. A larger number of comparisons can make the assessment process more time-consuming for experts and complicate the management of judgment consistency [12]. Accordingly, jointly examining the technical, performance, and security criteria of blockchain platforms and employing a weighting method that reduces the number of required comparisons while accounting for the consistency of expert judgments may help extend existing research in this area.

To address these limitations, the Full Consistency Method (FUCOM) provides an alternative approach for determining criterion weights while accounting for consistency in expert judgments [11]. FUCOM enables the determination of criterion weights within a hierarchical level and

incorporates consistency conditions into the weighting process. A key advantage of this method is that weighting n criteria requires only $n - 1$ sequential comparisons between ranked criteria. This reduces the number of judgments required from experts and may help mitigate the effects of judgment fatigue [12]. The method also accommodates integer and decimal values to express comparative priorities and uses a mathematical optimization model to minimize deviations from full consistency between the assigned priorities and the ratios of the resulting weights [13]. In addition, FUCOM quantifies deviations from full consistency, with a value of zero indicating full consistency under the model. This provides a means of assessing the consistency of the resulting weights and supports the systematic prioritization of criteria.

Accordingly, the present study aims to address this combined research gap by prioritizing 13 key criteria for blockchain platforms and determining their relative weights using the FUCOM method. The remainder of the paper is organized into five sections. Section 2 presents the theoretical foundations and related studies under two main themes: the scalability–decentralization trade-off and the transparency–data protection dilemma. It also summarizes previous research and provides a comparative table of the criteria. Section 3 describes the research methodology, conceptual model, and mathematical steps of the FUCOM algorithm. Section 4 presents the empirical findings and the resulting criterion weights. Finally, Section 5 discusses the conclusions, managerial implications, and directions for future research.

2. Literature Review

This section reviews the theoretical foundations and related literature on blockchain platform evaluation. Previous studies are reviewed to identify the criteria used to evaluate blockchain platforms and the methodological approaches adopted in the existing literature. Finally, the research gaps are discussed to establish the rationale for the present study and its application of the FUCOM method to prioritize key performance and security criteria.

2.1 The Scalability–Decentralization Trade-off

The consensus mechanism is a core component of a blockchain network that enables network nodes to agree on the validity of transactions and the order in which they are recorded [2]. In blockchain system design, the well-known concept of the Blockchain Trilemma refers to the challenge of balancing scalability, security, and decentralization. From this perspective, improving all three properties simultaneously involves technical constraints and design considerations, and achieving an appropriate balance depends on the architecture and requirements of each platform [5]. The choice of consensus mechanism can affect a network's operational performance, including transaction throughput, confirmation time, and resource consumption. For example, Proof of Work (PoW) increases the computational cost of altering transaction history through competition among miners, thereby contributing to network security. However, the extensive computational work required by PoW, particularly in networks such as Bitcoin, entails considerable energy consumption. In addition, network design constraints can affect transaction throughput and confirmation times [7]. By contrast, mechanisms such as Proof of Stake (PoS) and Byzantine fault-tolerant protocols, including Practical Byzantine Fault Tolerance (PBFT), use different approaches to achieve consensus rather than relying on the computational competition characteristic of PoW. Under suitable conditions, these approaches can reduce energy consumption or the cost of reaching consensus and may support higher transaction throughput. Their performance, however, depends on factors such as the number

of validators, the network communication structure, and protocol implementation [14], [15]. Furthermore, some designs that rely on a smaller set of validators or require more powerful hardware may increase barriers to participation and affect the degree of decentralization [6].

In addition to the choice of consensus mechanism, distributed network architecture plays an important role in determining the operational limitations and performance of blockchain platforms. Many of these platforms are built on peer-to-peer (P2P) networks, in which transactions and blocks are distributed among nodes through information propagation mechanisms to maintain consistent copies of the ledger across the network [16]. In practice, however, variations in communication latency, bandwidth, and node processing times may prevent information from reaching all parts of the network at the same rate. These delays can increase the likelihood of competing blocks and temporary forks, particularly in protocols where new blocks may be produced before previously generated blocks have been fully propagated. Such forks may reduce block propagation efficiency and increase the network's vulnerability to certain attacks, although the extent of these effects depends on the consensus mechanism and the network's design characteristics [17]. To improve scalability, some blockchain architectures employ approaches such as sharding or structures based on Directed Acyclic Graphs (DAGs) [18]. Sharding can facilitate parallel processing by distributing computational or validation tasks across multiple network partitions. DAG-based structures, in contrast, allow transactions or blocks to be organized in a structure that is not restricted to a single linear chain. However, the performance benefits of these approaches depend on their implementation, and they may introduce challenges related to coordination across network partitions, cross-shard communication, and the security of consensus. In sharding-based architectures, for example, validator allocation and each shard's resilience to collusion are important security considerations [19].

2.2 The Transparency–Data Protection Dilemma

The foundations of trustworthiness and technical reliability in distributed ledger platforms depend on the combination of cryptography-based data structures, consensus mechanisms, and methods for verifying data provenance. Immutability, as an important design property of blockchain, uses one-way hash functions to enable the detection of changes to recorded data and increase the cost or difficulty of tampering with confirmed records. However, the degree of resistance to modification also depends on the consensus mechanism and the rules governing the network [2]. This property alone does not guarantee the factual accuracy of recorded information or the real-world identities of those who submit it. By contrast, mechanisms such as digital signatures can be used to verify a signature and establish its association with the corresponding public key, although this does not necessarily prove the real-world identity of the key holder or the truthfulness of the information itself [8]. Together, these mechanisms can enhance the traceability of transactions and recorded events, thereby supporting information transparency, oversight, and auditing. In this context, public-key cryptography, including schemes based on elliptic curves, plays a role in verifying digital signatures; however, authentication procedures and the degree of assurance regarding users' real-world identities depend on the platform's design and complementary mechanisms [9]. On the other hand, the public visibility of transactions on public ledgers can conflict with the protection of users' privacy, as analyses of address relationships and transaction timing patterns may enable the identification of users or the inference of their activities [8]. To address these concerns, some platforms and protocols employ privacy-preserving techniques, including zero-knowledge proofs and stealth addresses, to enable information verification or transaction receipt while disclosing less

sensitive information. Nevertheless, the level of protection provided depends on the specific technique and its implementation.

At the structural and technical governance level, evaluating a blockchain platform requires examining network robustness, defined as its ability to maintain acceptable operation in the presence of faults, disruptions, and attacks. Relevant threats may include communication failures, unintended forks, and coordinated attacks. However, a network's resistance to these threats depends on its architecture, consensus mechanism, and defensive measures. The robustness of a distributed ledger system is not determined solely by the strength of its cryptographic algorithms; protocol design, the distribution of power among participants, and the economic incentives of block producers or validators can also affect it [20]. This issue is particularly relevant when assessing fair transaction ordering, as block producers or builders may, depending on their authority and the network's governing mechanisms, exploit their ability to include, exclude, or reorder transactions for economic gain. Such behavior can, under certain conditions, disadvantage users, lead to discriminatory transaction processing, or concentrate profit-generating opportunities [10]. Accordingly, multi-criteria analysis of blockchain platforms requires privacy-preserving mechanisms, data integrity and authenticity, and record immutability to be evaluated alongside fair transaction ordering and operational network robustness as related but distinct criteria.

A review of previous studies and a comparison of the criteria examined in them (Table 1) indicate that the level of attention devoted to different dimensions of blockchain performance evaluation has varied across the selected studies. Among the criteria examined, consensus mechanisms, decentralization, and immutability appeared most frequently. By contrast, privacy protection and energy consumption were addressed in fewer of the studies reviewed. Furthermore, criteria related to cryptography and access management, including cryptographic algorithms, authentication, and traceability, were examined less frequently. Overall, this pattern indicates that the coverage of different criteria varied across the selected studies and that transaction-ordering fairness received less attention than the more frequently examined criteria.

From a methodological perspective, the studies examined employed a range of approaches, including literature reviews, comparative analyses, and conceptual and structural investigations. Among the selected sources, [2], [3], [8], [9], [21], [22], [23] are among the studies that may be classified as review-based or comparative investigations, depending on the nature and purpose of their analyses. Other studies, including [4], [5], [7], [16], [24] examine conceptual, structural, or technical aspects of blockchain technology. By contrast, specific quantitative and empirical methods, including empirical behavioral analysis [10] and panel-data analysis [25], were identified in fewer studies within the comparative matrix. This pattern may indicate an opportunity to expand quantitative and systematic research on blockchain evaluation criteria. In particular, MCDM methods can facilitate the simultaneous assessment of the relative importance and prioritization of technical, performance, and security criteria, an approach that warrants further examination within the scope of the studies considered here.

In response to the thematic and methodological limitations identified in the selected studies, the present study proposes a framework for evaluating and prioritizing 13 performance and security criteria for blockchain platforms. Within this framework, the criteria identified from the relevant literature are examined simultaneously, and their relative weights are determined and ranked using FUCOM. One feature of FUCOM is that it reduces the number of required comparisons relative to approaches based on complete pairwise comparisons and incorporates the consistency of expert judgments into a mathematical optimization model.

3. Methodology

MCDM is a well-established approach in operations research and decision science, developed to support decision-making in complex, multidimensional problems [26], [27]. By providing a systematic framework, this approach enables the simultaneous evaluation of quantitative and qualitative criteria, the analysis of decision-makers' preferences, and the examination of potential trade-offs among criteria [28], [29]. In terms of their functions, MCDM methods encompass a broad range of techniques for determining criterion weights, ranking alternatives, and analyzing preference relations [30], [31], [32]. Among these functions, criterion weighting is a fundamental stage of the decision-making process, as the relative importance assigned to each criterion can substantially influence evaluation outcomes and prioritization results. Weighting methods can be broadly classified into three categories: subjective, objective, and integrated methods. Subjective methods rely on expert judgments and preferences, objective methods are based on the statistical and informational characteristics of the data, and integrated methods combine these two sources of information. With the development of newer MCDM approaches, methods such as FUCOM, BWM, and BCM have also attracted attention in studies concerned with determining criterion importance, each employing a different computational mechanism to derive criterion weights. Within this framework, the selection of an appropriate method should be aligned with the nature of the problem, the type of information available, the number of criteria, and the requirements for consistency in decision-makers' judgments [27].

The present study is applied in terms of its purpose and descriptive-analytical in terms of its research approach, as it seeks to examine the key performance and security dimensions and criteria of blockchain platforms in a systematic and practical manner. In addition to identifying and precisely defining the various performance and security dimensions and criteria, the study assesses their relative importance to develop a more comprehensive and in-depth understanding of the architecture and current state of blockchain platforms. The primary focus of this research is to determine the optimal weights and establish priorities among performance and security dimensions and criteria. To achieve this objective, and given the structural complexity of blockchain platforms and the large number of technical criteria involved, the FUCOM method was employed. FUCOM is a relatively recent approach in the field of MCDM. Its key advantage lies in its ability to derive precise and consistent weights through sequential pairwise comparisons of criteria while minimizing deviations and inconsistencies in the resulting calculations.

3.1 FUCOM Method

In real-world decision-making problems, criteria do not generally carry equal weights or levels of importance. Therefore, it is necessary to determine the relative importance of each criterion by assigning weights such that their sum equals one. Determining the relative weights of criteria within MCDM models has long been regarded as a critical issue, particularly because it is often influenced by expert judgment and subjectivity [33]. This stage plays a vital role in the evaluation framework and directly affects the final decision-making outcomes, as weighting coefficients are instrumental in ranking alternatives and selecting optimal solutions across evaluation approaches. In this context, the FUCOM method enables the highly precise determination of numerical weights for all elements being compared at a given level of the hierarchical structure, while simultaneously ensuring that the mathematical consistency requirements of the comparisons are fully satisfied [11].

Table 1

Summary of previous studies on blockchain platform

Paper	Approach	Privacy protection	Encryption algorithm	Authentication	Consensus mechanism	Decentralization	Distributed network architecture	Immutability	Data authenticity and validity	Traceability	Transaction speed	Network robustness	Energy consumption	Transaction ordering fairness
Agag and Alboqami [25]	Panel Data Empirical Study	-	-	-	-	✓	-	-	-	-	-	-	-	-
Sathio et al. [22]	Systematic Review	✓	-	-	✓	-	✓	-	-	-	✓	✓	✓	-
Zimba et al. [21]	Systematic Literature Review	-	-	-	✓	✓	✓	-	-	-	-	✓	✓	-
Sabbagh et al. [36]	Systematic Literature Review	-	-	-	-	-	✓	✓	✓	-	-	-	-	-
Galati et al. [37]	PRISMA-Based Review	-	-	-	-	-	-	-	✓	✓	-	-	-	-
Daian et al. [10]	Empirical Assessment of Validator Behavior	-	-	-	✓	-	-	-	-	✓	✓	✓	-	✓
Hafid et al. [5]	Systematic Review of Scalability Techniques	-	-	-	✓	✓	✓	-	-	-	✓	✓	-	-
Sedlmeir et al. [7]	Critical Review and Clarification	-	-	✓	✓	-	-	-	-	-	-	-	✓	-
Kannengießer et al. [4]	Analysis of DLT Trade-offs	-	✓	✓	✓	✓	✓	-	-	-	-	-	-	-
Xiao et al. [16]	Structural Analysis of Consensus Protocols	-	-	-	✓	-	✓	-	✓	-	✓	✓	✓	-
Feng et al. [8]	Review Focusing on Privacy Assessment	✓	✓	-	-	-	✓	✓	✓	-	-	-	-	-
Monrat et al. [3]	Comparative Survey	✓	-	-	✓	✓	✓	✓	-	-	-	-	✓	-
Conti et al. [9]	Systematic Review	✓	-	-	✓	-	✓	✓	-	-	-	✓	-	-
Zheng et al. [2]	Systematic Review of Blockchain Architecture	✓	-	-	✓	✓	✓	✓	✓	-	-	-	-	-
Present Study	Multi-Criteria Evaluation Using FUCOM	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

In practice, pairwise comparison values, $a_{ij} = w_i/w_j$, where a_{ij} represents the relative preference of criterion i over criterion j , are not exact but are based on subjective judgments. Consequently, the values of a_{ij} may deviate from the ideal ratios w_i/w_j , where w_i and w_j denote the weights of criteria i and j , respectively. For example, if criterion A is considered much more important than B, B is considered more important than C, and C is considered more important than A, the resulting judgments are inconsistent, reducing the reliability of the results. This issue becomes particularly pronounced when a large number of pairwise comparisons must be made among criteria.

The FUCOM method minimized the probability of judgment errors in pairwise comparisons for two main reasons. First, its weighting procedure requires only the minimum number of comparisons ($n - 1$). Second, the method incorporates a set of precise optimization constraints to determine the optimal weighting coefficients. FUCOM also enables the model to be validated by calculating the deviation from full consistency [13]. In contrast, other widely used weighting methods, such as the Best–Worst Method (BWM) and the Analytic Hierarchy Process (AHP), involve redundant pairwise comparisons, making evaluations more susceptible to cognitive and judgmental errors. By eliminating this redundancy, FUCOM provides greater computational accuracy and robustness [12], [34].

3.2 Steps of the FUCOM Method

This section describes the procedural steps of the FUCOM method for determining and deriving the optimal weighting coefficients of the criteria [11], [12].

Step 1. In the first step, the set of defined criteria $C = \{C_1, C_2, \dots, C_n\}$, is ranked according to their importance, from the most important to the least important. The criteria are ordered according to Equation 1.

$$C_{j(1)} > C_{j(2)} > \dots > C_{j(k)} \quad (1)$$

where k denotes the rank of the criterion under consideration. If two or more criteria are considered equally important, the “<” sign in Equation 1 is replaced with the “=” sign.

Step 2. In the second step, the ranked criteria are compared to determine their relative priorities, denoted by $\varphi_{k/(k+1)}$ where $k = 1, 2, \dots, n$. Accordingly, the vector of relative priorities is obtained using Equation 2.

$$\Phi = (\varphi_{1/2}, \varphi_{2/3}, \dots, \varphi_{k/(k+1)}) \quad (2)$$

where $\varphi_{k/(k+1)}$ represents the preference of the criterion $C_{j(k)}$ over the criterion $C_{j(k+1)}$.

To determine the relative priorities of the criteria, a scale ranging from 1 to 9 is used. For example, if this scale is used to compare criterion A with criterion B, and their respective importance ratings are estimated to be 7 and 6, then:

$$\varphi_{A/B} = \frac{7}{6} = 1.17$$

This indicates that criterion A has a relative priority of 1.17 over criterion B. Following the same procedure, experts determine the relative priorities of the identified criteria. As a result, the relative importance of each criterion, $vC_{j(k)}$, is established for all criteria ranked in Step 1. Since the highest-ranked criterion is compared with itself ($vC_{j(1)} = 1$), the total number of comparisons is $n - 1$. If an expert considers criteria $C_{j(k)}$ and $C_{j(k+1)}$ to be equally important, the value of $\varphi_{k/(k+1)}$ is set to 1.

Step 3. In the third step, the final weighting coefficients, $(w_1, w_2, \dots, w_n)^T$, are calculated. These coefficients are determined such that the ratios between the calculated weights correspond to the relative priorities established among the criteria using Equations 3 and 4.

$$\frac{w_k}{w_{k+1}} = \varphi_{k/(k+1)} \quad (3)$$

$$\frac{w_k}{w_{k+2}} = \varphi_{k/(k+1)} \otimes \varphi_{(k+1)/(k+2)} \quad (4)$$

Step 4. In the fourth step, the final nonlinear programming model is formulated to derive and calculate the optimal weighting coefficients for the evaluation criteria, as expressed in Equation 5.

$$\begin{aligned} &\min \chi \\ &\text{s.t.} \\ &\left| \frac{w_{j(k)}}{w_{j(k+1)}} - \varphi_{k/(k+1)} \right| \leq \chi, \quad \forall j \\ &\left| \frac{w_{j(k)}}{w_{j(k+2)}} - \varphi_{k/(k+1)} \otimes \varphi_{(k+1)/(k+2)} \right| \leq \chi, \quad \forall j \\ &\sum_{j=1}^n w_j = 1, \quad \forall j \\ &w_j \geq 0, \quad \forall j \end{aligned} \quad (5)$$

In this study, the FUCOM method was implemented by first identifying and defining the key criteria affecting the performance and security of blockchain platforms through a thorough review of the relative literature. 13 fundamental criteria representing the core performance dimensions and critical security aspects were identified and selected for the final evaluation. Subsequently, the prioritization process and pairwise comparisons among these 13 criteria were carried out to incorporate their relative importance coefficients into the FUCOM mathematical model. This process established an ordered preference matrix for the 13 criteria, providing a basis for optimal weighting and security assessment of blockchain platforms by minimizing deviations from full consistency.

The empirical data required for the pairwise comparisons were collected using a comparison questionnaire and a preference matrix, which were provided to a panel of experts and professionals in blockchain technology, cybersecurity, and distributed systems architecture. After the expert judgments had been collected and screened, the resulting data were incorporated into the FUCOM optimization model, and the final weights of the performance and security criteria were calculated. By incorporating full-consistency constraints, FUCOM offered a more rigorous approach to

consistency assessment than conventional methods such as AHP and BWM, ensuring that the resulting weights exhibited a high degree of accuracy and internal consistency while minimizing judgment errors [35]. Figure 1 illustrates the methodological framework of the study, outlining the process of identifying and extracting evaluation criteria from the relevant literature, applying the FUCOM method to rank the criteria and determine their optimal weights, and deriving the final ranking of the criteria.

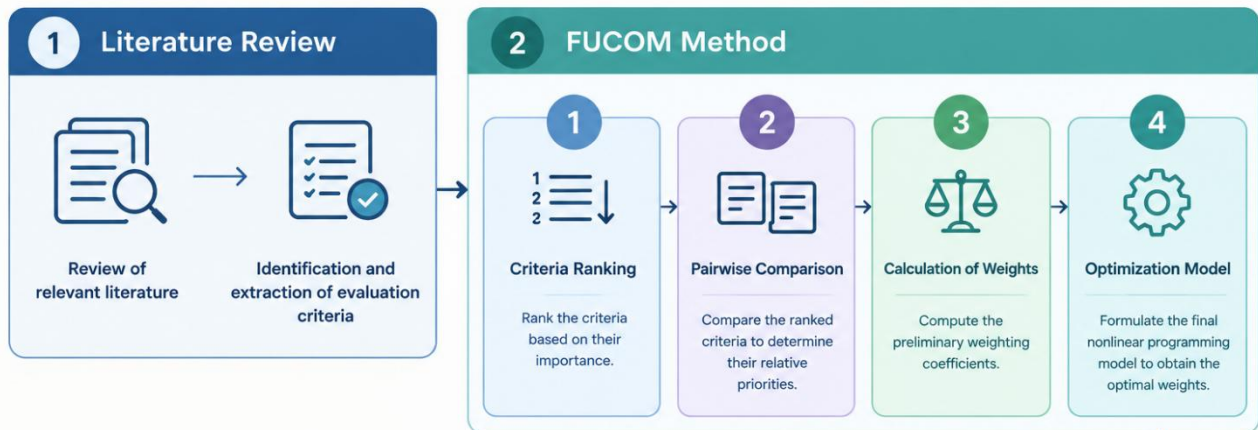


Fig. 1. Methodological framework of the study

4. Results

This section presents the findings from the identification of key performance and security criteria for blockchain platforms based on relevant literature, as well as the results of prioritizing and ranking these criteria using the FUCOM method. First, the criteria related to the performance and security of blockchain platforms were identified and extracted from relevant academic sources. Subsequently, expert judgments and the FUCOM method were employed to determine the weights and rankings of the criteria. The objective was to calculate their relative weights and obtain consistent and reliable results. To this end, the procedure was carried out in accordance with the steps of the FUCOM method. Table 2 presents the identified criteria along with the corresponding academic references supporting each one.

Table 2

Key identified criteria for the blockchain platforms

Symbol	Criteria	Reference
C1	Privacy protection	[2], [3], [8], [9], [22]
C2	Encryption algorithm	[4], [8]
C3	Authentication	[4], [7]
C4	Consensus mechanism	[2], [3], [4], [5], [7], [9], [10], [16], [21], [22]
C5	Decentralization	[2], [3], [4], [5], [21], [25]
C6	Distributed network architecture	[2], [3], [4], [5], [8], [9], [16], [21], [22], [36]
C7	Immutability	[2], [3], [8], [9], [36]
C8	Data authenticity and validity	[2], [8], [16], [36], [37]
C9	Traceability	[10], [37]
C10	Transaction speed	[5], [10], [16], [22]
C11	Network robustness	[5], [9], [10], [16], [21], [22]

C12	Energy consumption	[3], [7], [16], [21], [22]
C13	Transaction ordering fairness	[10], [37]

Following the steps of the FUCOM method, experts were first asked to assess the importance and establish the priority order of the key performance and security criteria for blockchain platforms. Based on the aggregated expert preferences, the criteria were ranked in order of priority, as presented in Equation 6.

$$C_{10} > C_{11} > C_4 > C_{13} > C_7 > C_6 > C_8 > C_{12} > C_5 > C_9 > C_3 > C_2 > C_1 \quad (6)$$

In the next step, the experts evaluated the importance of each key performance and security criterion for blockchain platforms using a numerical scale ranging from 1 to 9. The mean score for each criterion was then calculated and used in the FUCOM calculations. Table 3 presents the mean importance scores of the criteria based on the experts' assessments.

Table 3

Mean importance scores of the key blockchain criteria

Symbol	Criteria	Mean Importance Score
C10	Transaction speed	8.80
C11	Network robustness	8.47
C4	Consensus mechanism	8.13
C13	Transaction ordering fairness	7.80
C7	Immutability	7.27
C6	Distributed network architecture	7.07
C8	Data authenticity and validity	6.87
C12	Energy consumption	6.40
C5	Decentralization	6.00
C9	Traceability	5.40
C3	Authentication	5.07
C2	Encryption algorithm	4.47
C1	Privacy protection	3.40

Next, the relative importance of each criterion with respect to the other was calculated using Equation 3, as presented in Table 4. For example, the relative importance of "Transaction speed" compared with "Network robustness" was calculated by dividing 8.80 by 8.47.

Table 4

Direct relative importance of key blockchain criteria

Symbol	Description	$\varphi_{k/(k+1)}$
C10/C11	Relative importance of "Transaction speed" to "Network robustness"	1.039
C11/C4	Relative importance of "Network robustness" to "Consensus mechanism"	1.041
C4/C13	Relative importance of "Consensus mechanism" to "Transaction ordering fairness"	1.043
C13/C7	Relative importance of "Transaction ordering fairness" to "Immutability"	1.073
C7/C6	Relative importance of "Immutability" to "Distributed network architecture"	1.028
C6/C8	Relative importance of "Distributed network architecture" to "Data authenticity and validity"	1.029
C8/C12	Relative importance of "Data authenticity and validity" to "Energy consumption"	1.084
C12/C5	Relative importance of "Energy consumption" to "Decentralization"	1.056
C5/C9	Relative importance of "Decentralization" to "Traceability"	1.111
C9/C3	Relative importance of "Traceability" to "Authentication"	1.066
C3/C2	Relative importance of "Authentication" to "Encryption algorithm"	1.152

C2/C1	Relative importance of "Encryption algorithm" to "Privacy protection"	1.294
-------	---	-------

As explained in the methodology section, the weights calculated for each criterion must also satisfy Equation 5. Accordingly, the relative importance of each criterion with respect to the criterion ranked two positions below it was calculated, and the results are presented in Table 5. At this stage, the relative importance values were determined indirectly by multiplying the values obtained in the previous step. For example, the indirect relative importance of "Transaction speed" with respect to the "Consensus mechanism" in Table 5 (1.082) was obtained by multiplying the relative importance of "Transaction speed" with respect to "Network robustness" (1.039) by the relative importance of "Network robustness" with respect to the "Consensus mechanism" (1.041).

Table 5
Indirect relative importance of key blockchain criteria

Symbol	Description	$\varphi_{k/(k+2)}$
C10/C4	Relative importance of "Transaction speed" to "Consensus mechanism"	1.082
C11/C13	Relative importance of "Network robustness" to "Transaction ordering fairness"	1.085
C4/C7	Relative importance of "Consensus mechanism" to "Immutability"	1.119
C13/C6	Relative importance of "Transaction ordering fairness" to "Distributed network architecture"	1.104
C7/C8	Relative importance of "Immutability" to "Data authenticity and validity"	1.058
C6/C12	Relative importance of "Distributed network architecture" to "Energy consumption"	1.116
C8/C5	Relative importance of "Data authenticity and validity" to "Decentralization"	1.144
C12/C9	Relative importance of "Energy consumption" to "Traceability"	1.173
C5/C3	Relative importance of "Decentralization" to "Authentication"	1.184
C9/C2	Relative importance of "Traceability" to "Encryption algorithm"	1.227
C3/C1	Relative importance of "Authentication" to "Privacy protection"	1.490

Finally, the mathematical model for calculating the optimal weights of the criteria was formulated using the obtained values and based on Equation 5, as shown in Equation 7.

$$\begin{aligned}
 & \min \chi \\
 & \text{s.t.} \\
 & \left| \frac{w_{10}}{w_{11}} - 1.039 \right| \leq \chi, \quad \left| \frac{w_{11}}{w_4} - 1.041 \right| \leq \chi, \quad \left| \frac{w_4}{w_{13}} - 1.043 \right| \leq \chi \\
 & \left| \frac{w_{13}}{w_7} - 1.073 \right| \leq \chi, \quad \left| \frac{w_7}{w_6} - 1.028 \right| \leq \chi, \quad \left| \frac{w_6}{w_8} - 1.029 \right| \leq \chi \\
 & \left| \frac{w_8}{w_{12}} - 1.084 \right| \leq \chi, \quad \left| \frac{w_{12}}{w_5} - 1.056 \right| \leq \chi, \quad \left| \frac{w_5}{w_9} - 1.111 \right| \leq \chi \\
 & \left| \frac{w_9}{w_3} - 1.066 \right| \leq \chi, \quad \left| \frac{w_3}{w_2} - 1.152 \right| \leq \chi, \quad \left| \frac{w_2}{w_1} - 1.294 \right| \leq \chi \\
 & \left| \frac{w_{10}}{w_4} - 1.082 \right| \leq \chi, \quad \left| \frac{w_{11}}{w_{13}} - 1.085 \right| \leq \chi, \quad \left| \frac{w_4}{w_7} - 1.119 \right| \leq \chi \\
 & \left| \frac{w_{13}}{w_6} - 1.104 \right| \leq \chi, \quad \left| \frac{w_7}{w_8} - 1.058 \right| \leq \chi, \quad \left| \frac{w_6}{w_{12}} - 1.116 \right| \leq \chi \\
 & \left| \frac{w_8}{w_5} - 1.114 \right| \leq \chi, \quad \left| \frac{w_{12}}{w_9} - 1.173 \right| \leq \chi, \quad \left| \frac{w_5}{w_3} - 1.184 \right| \leq \chi \\
 & \left| \frac{w_9}{w_2} - 1.227 \right| \leq \chi, \quad \left| \frac{w_3}{w_1} - 1.490 \right| \leq \chi
 \end{aligned} \tag{7}$$

$$\begin{aligned}
 & w_1 + w_2 + w_3 + w_4 + w_5 + w_6 + w_7 + w_8 + w_9 + w_{10} + w_{12} + w_{13} = 1 \\
 & w_1 \geq 0, w_2 \geq 0, w_3 \geq 0, w_4 \geq 0, w_5 \geq 0, w_6 \geq 0, w_7 \geq 0, w_8 \geq 0, w_9 \geq 0, w_{10} \geq 0, w_{11} \\
 & \geq 0, w_{12} \geq 0, w_{13} \geq 0
 \end{aligned}$$

Solving the above mathematical model yielded an objective function value of zero, indicating that the calculated weights were fully consistent with the experts' preferences. Finally, the final weights and corresponding rankings of the performance and security criteria of blockchain platforms were determined. The results are presented in Table 6.

Table 6

Final weights and rankings of key blockchain criteria

Symbol	Criteria	Final Weight of Each Criterion	Final Ranking
C1	Privacy protection	0.0400	13
C2	Encryption algorithm	0.0518	12
C3	Authentication	0.0596	11
C4	Consensus mechanism	0.0957	3
C5	Decentralization	0.0706	9
C6	Distributed network architecture	0.0831	6
C7	Immutability	0.0855	5
C8	Data authenticity and validity	0.0808	7
C9	Traceability	0.0635	10
C10	Transaction speed	0.1035	1
C11	Network robustness	0.0996	2
C12	Energy consumption	0.0745	8
C13	Transaction ordering fairness	0.0917	4

Figure 2 presents a visual representation of the final weights and rankings of the 13 blockchain evaluation criteria obtained using the FUCOM method.

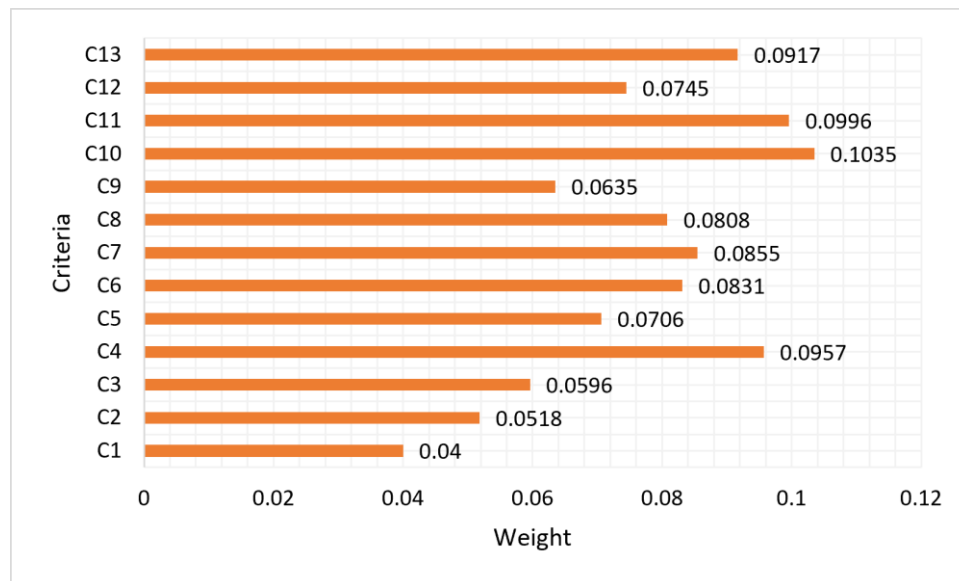


Fig. 2. Final weights and rankings of the criteria

To provide an integrated overview of the study, Figure 3 presents a graphical summary of the main research findings.

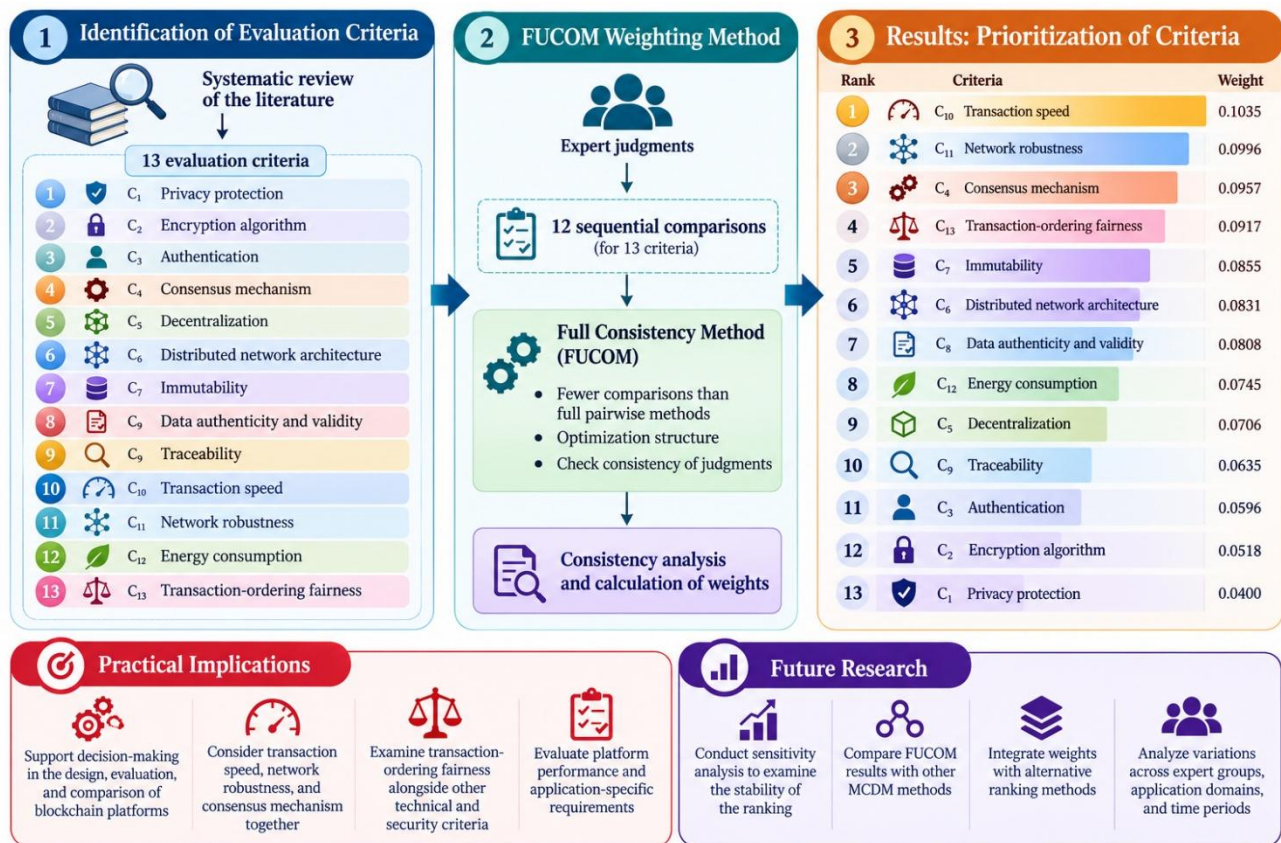


Fig. 3. Research Framework and Key Findings

5. Conclusions

The present study aimed to identify the criteria for evaluating the performance of blockchain platforms and determine their relative importance using an MCDM approach. To this end, a review of the relevant literature was conducted, taking into account the technical, structural, security, and performance-related dimensions of blockchain technology. Thirteen criteria were identified: "Privacy protection (C_1)", "Encryption algorithm (C_2)", "Authentication (C_3)", "Consensus mechanism (C_4)", "Decentralization (C_5)", "Distributed network architecture (C_6)", "Immutability (C_7)", "Data authenticity and validity (C_8)", "Traceability (C_9)", "Transaction speed (C_{10})", "Network robustness (C_{11})", "Energy consumption (C_{12})", and "Transaction ordering fairness (C_{13})". Subsequently, the FUCOM method, was employed to determine the relative weights and prioritize these criteria. For 13 criteria, this method requires 12 sequential comparisons, thereby reducing the number of comparisons required compared with approaches based on complete pairwise comparisons. Moreover, the optimization structure of the FUCOM method enables full consistency among expert judgments to be achieved.

The results obtained from applying FUCOM indicated that "Transaction speed (C_{10})", with a weight of 0.1035, ranked first. "Network robustness (C_{11})", with a weight of 0.0996, and "Consensus mechanism (C_4)", with a weight of 0.0957, ranked second and third, respectively. These findings indicate that, in the judgments of the experts participating in this study, transaction processing speed, network robustness, and the consensus mechanism were relatively more important. Furthermore, "Transaction ordering fairness (C_{13})", with a weight of 0.0917, ranked fourth. This

position reflects the experts' recognition of the relative importance of this criterion alongside other evaluation dimensions. Transaction-ordering fairness may play a role in analyzing opportunistic behavior in transaction ordering. In the remainder of the ranking, "Immutability (C_7)", with a weight of 0.0855; "Distributed network architecture (C_6)", with a weight of 0.0831; "Data authenticity and validity (C_8)", with a weight of 0.0808; "Energy consumption (C_{12})", with a weight of 0.0745; and "Decentralization (C_5)", with a weight of 0.0706, ranked fifth through ninth, respectively. "Traceability (C_9)", with a weight of 0.0635; "Authentication (C_3)", with a weight of 0.0596; "Encryption algorithm (C_2)", with a weight of 0.0518; and "Privacy protection (C_1)", with a weight of 0.0400, occupied the tenth through thirteenth positions. This ranking reflects the relative priorities of the criteria within the model and according to the expert judgments obtained in this study. It should not, however, be interpreted as indicating that lower-ranked criteria are inherently less important or need not be considered in the design and evaluation of blockchain platforms. For example, the lower weights assigned to privacy protection and cryptographic algorithms do not necessarily imply that these dimensions can be disregarded, as their practical importance may vary depending on the application, security requirements, and architectural characteristics of each platform.

From a practical perspective, the findings can serve as an analytical basis for supporting decision-making in the design, evaluation, and comparison of blockchain platforms. The ranking of "Transaction speed (C_{10})", "Network robustness (C_{11})" and "Consensus mechanism (C_4)" among the top three criteria highlights the need to consider throughput, network resilience, and the consensus process simultaneously when evaluating blockchain platforms. Moreover, the fourth-place ranking of "Transaction ordering fairness (C_{13})" underscores the importance of examining this dimension alongside other technical and security criteria. Nevertheless, the weights obtained are not, by themselves, sufficient to select a particular platform as the best option. Such a decision also requires an assessment of the actual performance of candidate platforms, their technical limitations, their application-specific requirements, and the extent to which each platform meets the criteria under consideration.

Furthermore, given the continuous evolution of blockchain technology, including the development of consensus protocols, Layer 2 solutions, and novel cryptographic methods, the relative importance of evaluation criteria may change over time and across application contexts. Periodically reviewing the criteria and their weights may therefore help maintain the relevance of the evaluation framework in light of technological developments. Accordingly, future research is encouraged to examine the stability of the ranking through sensitivity analysis and compare FUCOM results with those obtained using other MCDM methods. The resulting weights could also be integrated with alternative-ranking methods to enable the empirical evaluation and comparison of specific blockchain platforms. In addition, examining variations in criterion weights across different expert groups, application domains, and time periods could provide a more detailed understanding of the factors influencing the prioritization of blockchain performance and security criteria.

Author Contributions

Conceptualization, I.M. and A.Kh.; methodology, I.M.; software, I.M.; validation, I.M. and A.Kh.; formal analysis, I.M.; investigation, A.Kh.; data curation, I.M.; writing—original draft preparation, I.M. and A.Kh.; writing—review and editing, I.M.; visualization, A.Kh.; supervision, I.M. All authors have read and agreed to the published version of the manuscript.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

This research was not funded by any grant.

References

- [1] Pishdar, M., Lei, Y., Harfoush, K., & Manzoor, J. (2025). Denial-of-Service Attacks on Permissioned Blockchains: A Practical Study. *Journal of Cybersecurity and Privacy*, 5(3), 39. <https://doi.org/10.3390/jcp5030039>
- [2] Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14(4), 352–375. <https://doi.org/10.1504/IJWGS.2018.095647>
- [3] Monrat, A. A., Schelén, O., & Andersson, K. (2019). A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities. *IEEE Access*, 7, 117134–117151. <https://doi.org/10.1109/ACCESS.2019.2936094>
- [4] Kannengießer, N., Lins, S., Dehling, T., & Sunyaev, A. (2020). Trade-offs between Distributed Ledger Technology Characteristics. *ACM Computing Surveys (CSUR)*, 53(2), 42:1-42:37. <https://doi.org/10.1145/3379463>
- [5] Hafid, A., Hafid, A. S., & Samih, M. (2020). Scaling Blockchains: A Comprehensive Survey. *IEEE Access*, 8, 125244–125262. <https://doi.org/10.1109/ACCESS.2020.3007251>
- [6] Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., & Mohaisen, D. (2020). Exploring the Attack Surface of Blockchain: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*, 22(3), 1977–2008. <https://doi.org/10.1109/COMST.2020.2975999>
- [7] Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The Energy Consumption of Blockchain Technology: Beyond Myth. *Business & Information Systems Engineering*, 62(6), 599–608. <https://doi.org/10.1007/s12599-020-00656-x>
- [8] Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2019). A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications*, 126, 45–58. <https://doi.org/10.1016/j.inca.2018.10.020>
- [9] Conti, M., Sandeep Kumar, E., Lal, C., & Ruj, S. (2018). A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys & Tutorials*, 20(4), 3416–3452. <https://doi.org/10.1109/COMST.2018.2842460>
- [10] Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., & Juels, A. (2020). Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability. 2020 IEEE Symposium on Security and Privacy (SP), 910–927. <https://doi.org/10.1109/SP40000.2020.00040>
- [11] Pamučar, D., Stević, Ž., & Sremac, S. (2018). A New Model for Determining Weight Coefficients of Criteria in MCDM Models: Full Consistency Method (FUCOM). *Symmetry*, 10(9), 393. <https://doi.org/10.3390/sym10090393>

- [12] Pamucar, D., & Ecer, F. (2020). PRIORITIZING THE WEIGHTS OF THE EVALUATION CRITERIA UNDER FUZZINESS: THE FUZZY FULL CONSISTENCY METHOD – FUCOM-F. *Facta Universitatis, Series: Mechanical Engineering*, 18(3), 419–437. <https://doi.org/10.22190/FUME200602034P>
- [13] Yürüyen, A. A., Ulutaş, A., Demirhan, A., & Ozsalkan, E. (2025). Environmental considerations in the selection of transport vehicles: A fuzzy FUCOM method. *Management of Environmental Quality: An International Journal*, 36(6), 1650–1669. <https://doi.org/10.1108/MEQ-10-2024-0437>
- [14] Castro, M., & Liskov, B. (2002). Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems (TOCS)*, 20(4), 398–461. <https://doi.org/10.1145/571637.571640>
- [15] Saleh, F. (2021). Blockchain without Waste: Proof-of-Stake. *The Review of Financial Studies*, 34(3), 1156–1190. <https://doi.org/10.1093/rfs/hhaa075>
- [16] Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A Survey of Distributed Consensus Protocols for Blockchain Networks. *IEEE Communications Surveys & Tutorials*, 22(2), 1432–1465. <https://doi.org/10.1109/COMST.2020.2969706>
- [17] Decker, C., & Wattenhofer, R. (2013). Information propagation in the Bitcoin network. *IEEE P2P 2013 Proceedings*, 1–10. <https://doi.org/10.1109/P2P.2013.6688704>
- [18] Pervez, H., Muneeb, M., Irfan, M. U., & Haq, I. U. (2018). A Comparative Analysis of DAG-Based Blockchain Architectures. *2018 12th International Conference on Open-Source Systems and Technologies (ICOSST)*, 27–34. <https://doi.org/10.1109/ICOSST.2018.8632193>
- [19] Wang, G., Shi, Z. J., Nixon, M., & Han, S. (2019). SoK: Sharding on Blockchain. *Proceedings of the 1st ACM Conference on Advances in Financial Technologies, AFT '19*, 41–61. <https://doi.org/10.1145/3318041.3355457>
- [20] Mirzaei, I., Patel, H., Wu, C., & Amiri, M. J. (2026). Competition, Collusion, and Corruption: The Spectrum of MEV Attacks on DAG-Based BFT Consensus Protocols (arXiv:2609.20069). *arXiv*. <https://doi.org/10.48550/arXiv.2609.20069>
- [21] Zimba, A., Phiri, K. O., Mulenga, M., & Mukupa, G. (2025). A systematic literature review of blockchain technology and energy efficiency based on consensus mechanisms, architectural innovations, and sustainable solutions. *Discover Analytics*, 3(1), 14. <https://doi.org/10.1007/s44257-025-00041-6>
- [22] Sathio, A. A., Rind, M. M., Chowdhry, R., Ahmed, G., & Awan, S. A. (2026). Evolving BFT from Byzantine Logic to Green Ledgers—A Systematic Review of Energy-Efficient Voting-Based Consensus for Sustainable Private DeFi Systems. *Research Consortium Archive*, 4(1), 1682–1723.
- [23] Navaei, R. L., Safarzadeh, M., & Sobhani, S. M. J. (2025). Optimizing Flamelet Generated Manifold Models: A Machine Learning Performance Study (arXiv:2507.01030). *arXiv*. <https://doi.org/10.48550/arXiv.2507.01030>
- [24] Amiri, N., Honarmand, M., Dizani, M., Moosavi, A., & Kazemzadeh Hannani, S. (2021). Shear-thinning droplet formation inside a microfluidic T-junction under an electric field. *Acta Mechanica*, 232(7), 2535–2554. <https://doi.org/10.1007/s00707-021-02965-y>
- [25] Agag, G., & Alboqami, H. (2026). From blocks to bookings: How blockchain lifts customer satisfaction and hotel performance using textual analytics and panel evidence from hotels. *International Journal of Hospitality Management*, 138, 104726. <https://doi.org/10.1016/j.ijhm.2026.104726>

- [26] Haseli, G., Sheikh, R., & Sana, S. S. (2020). Base-criterion on multi-criteria decision-making method and its applications. *International Journal of Management Science and Engineering Management*, 15(2), 79–88. <https://doi.org/10.1080/17509653.2019.1633964>
- [27] Nazarian-Jashnabadi, J., Haseli, G., Hajiaghaei-Keshteli, M., Deveci, M., & Tomaskova, H. (2026). Chapter 17 - Nonadditive BWM: Nonadditive best-worst method for multi-attribute decision-making. In G. Haseli, M. Deveci, & M. Hajiaghaei-Keshteli (Eds.), *Encyclopedia of Multi-Attribute Decision Making (MADM)* (pp. 257–271). Morgan Kaufmann. <https://doi.org/10.1016/B978-0-443-33275-3.00065-8>
- [28] Nazarian-Jashnabadi, J., Sepahi, T., & Pamucar, D. (2026). Chapter 29 - Nonadditive BCM: Nonadditive base-criterion method for multi-attribute decision-making. In G. Haseli, M. Deveci, & M. Hajiaghaei-Keshteli (Eds.), *Encyclopedia of Multi-Attribute Decision Making (MADM)* (pp. 435–449). Morgan Kaufmann. <https://doi.org/10.1016/B978-0-443-33275-3.00028-2>
- [29] Nazarian-Jashnabadi, J., & Yousefi, S. (2026). Chapter 27 - Stratified BCM: Stratified base criterion method for multi-attribute decision-making. In G. Haseli, M. Deveci, & M. Hajiaghaei-Keshteli (Eds.), *Encyclopedia of Multi-Attribute Decision Making (MADM)* (pp. 403–419). Morgan Kaufmann. <https://doi.org/10.1016/B978-0-443-33275-3.00008-7>
- [30] Nezhad, M. Z., Zamani, A., Sepahi, T., Mehraeen, M., & Nazarian-Jashnabadi, J. (2026). A Knowledge-Driven Framework for Privacy Personalization in Smart Cities: Integrating Meta-Synthesis, Fermatean Fuzzy SWARA, and Clustering Approach. *Journal of Decision Science and Applications*, 1, 1–41. <https://jdesa.org/index.php/jdesa/article/view/340>
- [31] Nazarian Jashnabadi, J., Pooya, A., & Bagheri, R. (2023). Provide a Model for Budget Policy in University-Community Communication Programs with a System Dynamics Approach (Case Study: Ferdowsi University of Mashhad). *Journal of Industrial Management Perspective*, 13(1), 9–40. <https://doi.org/10.48308/jimp.13.1.9>
- [32] Nezhad, M. Z., Nazarian-Jashnabadi, J., Mehraeen, M., & Rezazadeh, J. (2024). PERAM: An Efficient Readiness Assessment Model for the Banking Industry to Implement IoT – A Systematic Review and Fuzzy SWARA Methods. *Journal of Intelligent Decision Making and Information Science*, 1, 120–155. <https://doi.org/10.59543/jidmis.v1i.12617>
- [33] Nazarian-Jashnabadi, J., & Tirkolaee, E. B. (2026). Chapter 28 - BCM tradeoff (BCT): Base criterion tradeoff for multi-attribute decision-making. In G. Haseli, M. Deveci, & M. Hajiaghaei-Keshteli (Eds.), *Encyclopedia of Multi-Attribute Decision Making (MADM)* (pp. 421–434). Morgan Kaufmann. <https://doi.org/10.1016/B978-0-443-33275-3.00085-3>
- [34] Haseli, G., Nazarian-Jashnabadi, J., Hajiaghaei-Keshteli, M., Deveci, M., & Tomaskova, H. (2026). Chapter 18 - BWT: Best-worst tradeoff for multi-attribute decision-making. In G. Haseli, M. Deveci, & M. Hajiaghaei-Keshteli (Eds.), *Encyclopedia of Multi-Attribute Decision Making (MADM)* (pp. 273–287). Morgan Kaufmann. <https://doi.org/10.1016/B978-0-443-33275-3.00043-9>
- [35] Stević, Ž., & Brković, N. (2020). A Novel Integrated FUCOM-MARCOS Model for Evaluation of Human Resources in a Transport Company. *Logistics*, 4(1), 4. <https://doi.org/10.3390/logistics4010004>
- [36] Sabbagh, P., Morkūnas, M., & Galati, A. (2024). Applications and impacts of blockchain-based solutions in the wine supply chain: A systematic literature review. *Digital Policy, Regulation and Governance*, 27(3), 261–277. <https://doi.org/10.1108/DPRG-03-2024-0044>
- [37] Galati, A., Adamashvili, N., Sabbagh, P., & Fiore, M. (2024). Do Blockchain-Based Innovative Solutions Improve Wine Brand Loyalty? A Case Study of a Winery in Mendoza, Argentina. In

A. Galati, D. Vrontis, A. Thrassou, & M. Fiore (Eds.), *Agribusiness Innovation and Contextual Evolution, Volume II: Technological, Societal and Channel Advancements* (pp. 235–257). Springer International Publishing. https://doi.org/10.1007/978-3-031-45742-5_10