International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A STRUCTURED PRIORITIZATION METHOD FOR SECURE DATA-SHARING WEB APPLICATIONS ON DISTRIBUTED LEDGERS

Rinku Raheja[1*], Prabhash Chandra Pathak[2], Syed Anas Ansar[3]

[1*,2,3]Department of Computer Applications, Babu Banarasi Das University, Lucknow, India
rinkuraheja85@gmail.com[1*],
pathakprabhash2@gmail.com[2], syed000anas@gmail.com[3]

***Corresponding author**: Rinku Raheja
[*]Department of Computer Applications, Babu Banarasi Das University, Lucknow, India
rinkuraheja85@gmail.com

Abstract:
Distributed-ledger technologies (DLTs) have upended the design logic of, data-sharing web architectures, especially within sectors that demand uncompromising transparency, indelible audit trails, and decentralised governance. Yet curating an optimal DLT stack remains an intricate optimisation puzzle involving nuanced trade-offs across cryptographic rigour, elastic scalability, experiential ergonomics, propagation latency, cross-ledger interoperability, and fiscal prudence. To navigate this complexity, we introduce a tiered decision-support framework that welds expert-elicited priorities to empirical performance signals within a rigorous multi-criteria outranking model. The scheme yields transparent, rank-ordered shortlists of candidate ledgers and is demonstrated across healthcare, fintech, and supply-chain provenance scenarios. Results confirm the model's ability to surface context-specific "best fits" even when decision objectives clash, thereby equipping engineers, CIOs, and policy designers with a defensible roadmap for trustworthy, efficient, and governance-aligned blockchain adoption. Future iterations will embed fuzzy logic and live-telemetry feedback to sharpen responsiveness in rapidly evolving operating environments.

Keywords: Blockchain Web Applications, Distributed Ledger Technologies (DLT), Secure Data Sharing, Multi-Criteria Decision Making (MCDM), Decision Support Systems

1. Introduction

Over the last decade, mainstream computing has tilted decisively toward decentralisation, propelled by blockchain and allied distributed-ledger technologies that furnish a cryptographically anchored, trust-minimised substrate for secure web transactions [1]. Although first adopted as the settlement engine for cryptocurrencies such as Bitcoin and Ethereum, the ledger concept has since evolved into a versatile mechanism for safeguarding data sovereignty, automating verification workflows, and enabling fault-tolerant information exchange [2]. By substituting hierarchical control with consensus-driven, tamper-evident networks, these systems deliver immutable audit trails, built-in transparency, and immunity to single-node compromise [3]. Practitioners now leverage these qualities across an expanding array of data-sensitive arenas—most notably in healthcare [4] (e.g., interoperable electronic health records), but also in capital markets, supply-chain provenance, public-sector identity and voting registries, and the security fabric of the Internet of Things.
As companies retrofit old stacks to meet today's expectations for provably transparent operations, strict privacy, and increasingly stringent regulatory requirements, they face a rapidly expanding list of blockchain platforms each characterized by a distinct combination of scalability limits, consensus algorithms, per-second transaction profiles, privacy protections,

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

smart-contract toolchains, and integration channels. Open, permissionless chains like Ethereum and Solana provide maximal decentralisation and auditability but remain susceptible to fee surges and network overload; permissioned ledgers like Hyperledger Fabric provide confidentiality and administrative control but require more sophisticated governance and onboarding structures [5]. This diversity, alongside the absence of widely adopted test suites or benchmarks, makes platform choice a daunting exercise for technologists, CIOs, and public-policy guardians with competing goals to balance—security versus cost, latency versus data integrity, and interoperability versus governance complexity.

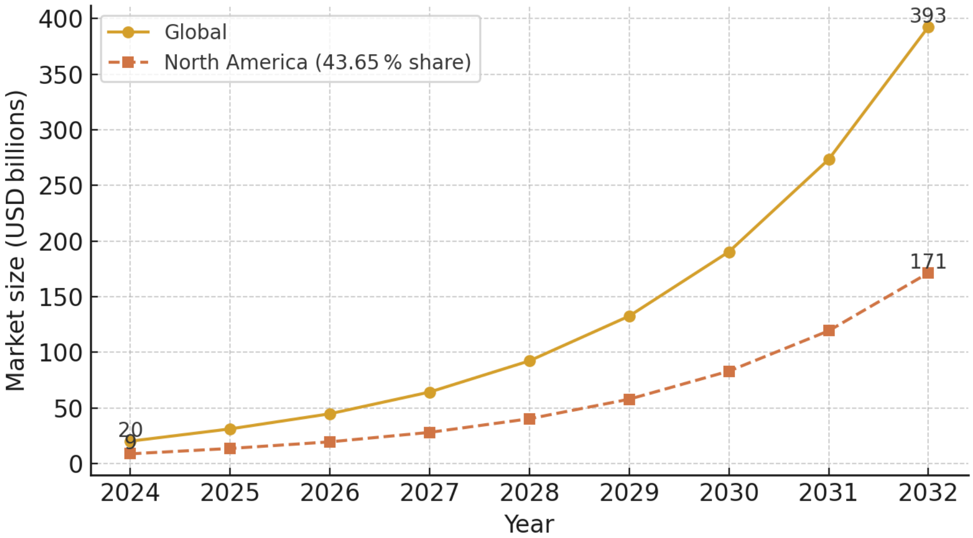

Fig 1. Projected Blockchain Market Size Growth (2024–2032), Global vs. North America.

Industry reports highlight the magnitude of the choice: Figure 1 estimates worldwide blockchain revenues to increase at a 43.6 % compound annual rate to around USD 393 billion by 2032, with North America alone set to claim some USD 170 billion if its current 43.65 % share continues (Fortune Business Insights, 2025) [6]. Such explosive growth highlights the need for highly organized evaluation frameworks that can trace strategic demands to the most context-relevant ledger. Even with blockchain's revolutionary potential, real-world roll-outs are hindered by a congested ecosystem whose platforms vary exceedingly in throughput, consensus architecture, privacy-preserving additions, cost models, and developer-community maturity. The intricate trade-offs among performance, security, and decentralisation therefore demand a standardised, multi-dimensional assessment methodology to guide stakeholders toward judicious, application-specific choices.

To bridge the foregoing methodological void, the present study advances four principal contributions:

- **Structured evaluation architecture.** It formulates an explicit prioritisation schema for appraising secure, data-sharing web services constructed atop distributed-ledger substrates.
- **Quantitative trade-off calculus.** It operationalises a computational, multi-criteria decision model that renders the tensions among technical soundness, security posture, and user experience as tractable, quantifiable scores.
- **Empirical validation.** It showcases the framework on production-grade blockchain platforms, generating rank-ordered insights that inform platform choice in real-world settings.
- **Extensibility blueprint.** It supplies a modular template readily adaptable to emergent arenas such as decentralised finance, provenance-driven supply-chain oversight, and digital-health infrastructures.

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The remainder of this article is organised as follows. Section 2 surveys pertinent scholarship on blockchain-enabled web systems and decision-support techniques. Section 3 delineates the computational architecture and prioritisation workflow. Section 4 furnishes a case-study implementation, while Section 5 interprets the findings, situates them within practice, and flags residual limitations. The paper closes with an agenda for future research aimed at enriching adaptive decision models within decentralised environments.

2. Vetting Research Work

2.1. Blockchain in Web Applications and Secure Data Sharing

The maturation of distributed-ledger technologies has catalysed a new generation of web applications that privilege tamper-evidence, fine-grained access control, and transparent audit trails. Contemporary scholarship chronicles blockchain's efficacy across domains as disparate as healthcare, smart-city orchestration, and electoral governance. Abo-Akleek et al. (2025) architected a blockchain-backed e-voting platform that embeds decision integrity through a fully decentralised tallying workflow [7]. Bonagiri and Deepalakshmi (2025) demonstrated blockchain's utility as a cryptographic backbone for Internet-of-Things (IoT) ecosystems, fortifying data confidentiality and provenance [8]. Complementing these efforts, Malarvizhi and Anusuya (2025) fused blockchain, IoT, and AI to construct a trusted middleware layer for smart-city services, thereby underscoring the ledger's role as secure connective tissue for distributed applications [9].

2.2. Challenges in Platform Evaluation and Decision-Making

The expanding universe of blockchain platforms compels adopters to deal with complex trade-offs in matching use-case requirements to platform functionality. Eido and Zeebaree (2025) surveyed e-business and marketing implementations and suggested comparative heuristics that balance trust, transparency, and scalability—criteria that vary strongly across Ethereum, Hyperledger, and Solana [10]. Themistocleous (2025) described the blockchain ecosystem as highly fragmented and promoted adaptive decision structures to align technical characteristics with organisational strategy [11]. Supporting this appeal, Hadfi et al. (2025) presented an anomaly-detection-based decision approach for decentralised autonomous organisations, heralding a transition to smart, context-aware evaluation frameworks [12].

2.3. Multi-Criteria Evaluation and Computational Techniques

More recent research turns towards quantitative multi-criteria decision-making (MCDM) and AI-facilitated analytics to give preference to blockchain alternatives in diverse domains. Srinivasan and Senthilkumar (2025) engineered a hybrid intrusion-detection and prevention scheme for industrial IoT that intertwines blockchain safeguards with computational risk scoring—exemplifying the need for multifactor assessment [13]. Zeng (2025) embedded deep-reinforcement logic into a cross-platform web crawler anchored by blockchain audit trails, illustrating how autonomic decision policies can be natively integrated within distributed systems [14]. In a complementary vein, Peddi *et al.* (2025) employed fuzzy-logic MCDM to appraise blockchain-enabled IoT infrastructures, mirroring the field's gravitation toward nuanced, criteria-rich evaluation paradigms [15].

A consolidated synopsis of extant research appears in Tables 1–3: Table 1 catalogues seminal blockchain-evaluation studies by application vertical, Table 2 juxtaposes the MCDM methodologies they deploy, and Table 3 enumerates the evaluation criteria most frequently invoked across the literature.

Table 1. Recent Applications of MCDM Methods in Blockchain Platform Evaluation (2022–2025)

Author(s)/ Outlet	Yr	Decision Method(s)	Focus Area	Key Insight
Nguyen et al. (IEEE) [16]	2024	PROMETHEE-PT, Quantum MCDM	Quantum × Blockchain	PROMETHEE fused with fuzzy sets proves more agile for fast-evolving ledger cases.
Muhammad et al. (IEEE) [17]	2023	AHP + PROMETHEE + TOPSIS	Agile-blockchain design	A three-way hybrid ranks non-functional requirements more robustly than single tools.
Muradi (UM Malaysia) [18]	2022	Fuzzy AHP-TOPSIS	Platform short-listing	Expert-weighted fuzzy logic yields a hands-on route to shortlist blockchain options.
Yadav et al. (Emerald) [19]	2025	TOPSIS; PROMETHEE	BRICS Industry 4.0 adoption	Cross-sector test shows combined outranking + distance scoring reveals contextual fit.
Lima-Junior et al. (MDPI) [20]	2023	HFLTS-TOPSIS	Supply Chain Decisions	Hesitant-fuzzy linguistic sets let TOPSIS capture multi-party nuance.
Mizrak & Akkartal (Heliyon) [21]	2024	DEMATEL + PROMETHEE-II	Cybersecurity (Aviation)	Cause–effect mapping plus full outranking clarifies security-critical priorities.
Barahmand & Eikeland (MDPI) [22]	2022	AHP; TOPSIS	Blockchain in LCA evaluation	Traceability metrics improve sustainability-centred MCDM.
Pereira et al. (Sensors, MDPI) [23]	2023	AHP-Gaussian MCDM	IoT + Blockchain	Gaussian scoring refines sensor-to-ledger pairing for resilient infra.

Table 2. Comparative Overview of MCDM Methods for Blockchain Platform Evaluation

Method	Signature Features	Principal Strengths	Notable Limitations	Typical Value for Blockchain Studies
AHP [18]	Pairwise expert weights	Easy hierarchy, transparent	Consistency-ratio sensitive	Good for small criterion sets needing clear weights
TOPSIS [19]	Ideal-/worst-point distance	Fast numeric ranking	Ignores inter-criterion links	Handy when raw performance data dominate
PROMETHEE II [17]	Positive / negative flow outrank	Handles conflicting goals	Needs preference-function tuning	Excels where trade-offs are sharp
DEMATEL [23]	Cause–effect graphing	Maps inter-dependencies	Requires solid expert input	Favours security / risk contexts
Fuzzy AHP [18]	Adds linguistic fuzziness	Captures vagueness	More math overhead	Useful with subjective, imprecise judgements
AHP-TOPSIS [22]	Weight with AHP, rank via TOPSIS	Balanced view	Carries both tools' limits	Common in corporate IT selection
DEMATEL-PROMETHEE [23]	Dependency map + full ranking	Holistic picture	Heavier data + compute load	Chosen for secure-system pick lists

Table 3. Evaluation Criteria Reported in Recent Blockchain-MCDM Studies

Author(s)	Yr	Criteria Highlighted	Methodology	Sector / Use Case
Muradi [18]	2022	Cost, Security, Governance, Interop., Latency	Fuzzy AHP–TOPSIS	Public-sector ledgers
Muhammad et al. [17]	2023	Flexibility, Agility, Performance, Scalability	AHP–PROMETHEE	Agile dev settings
Nguyen et al. [16]	2024	TPS, Quantum-resistance, Fault-tolerance, Flexibility	Quantum PROMETHEE-PT	Quantum–DLT synergy

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Yadav et al. [19]	2025	Interop., Risk, Cost, Ease, Compatibility	AHP–TOPSIS	Industry 4.0 / BRICS adoption
Pereira et al. [23]	2023	Sensor-ledger match, Latency, Redundancy, Power	AHP–Gaussian MCDM	IoT smart infra
Mizrak & Akkartal [21]	2024	Compliance, Control flow, Threat vectors, Trust	DEMATEL–PROMETHEE II	Aviation security
Barahmand & Eikeland [22]	2022	Traceability, Lifecycle, Sustainability	AHP–TOPSIS	Environmental LCA
Lima-Junior et al. [20]	2023	Decision delay, Linguistic agreement, Supply-uncertainty	HFLTS–TOPSIS	Supply chain networks

2.4. Research Gap and Justification

Although recent scholarship positions blockchain as a cornerstone for the next wave of secure, data-sharing web services, a broadly applicable, criteria-driven framework for choosing between rival ledger platforms is still conspicuously scarce. Existing studies tend to be tightly domain-bound, lack defensible ranking engines, or omit any fusion of expert insight with empirical performance evidence. Even investigations that adopt PROMETHEE rarely exploit its full potential—criteria formulation is cursory, and the preference-flow logic remains opaque. These shortcomings signal the need for a computational, rules-based decision aide—the very void this paper seeks to fill.

3. Methodology and Framework Design

3.1. Overview of Computational Approach

Evaluating a distributed-ledger platform for secure data exchange is never a one-note exercise. Engineers must weigh performance signals—block-confirmation speed, fault-recovery tolerance—alongside security guarantees such as cryptographic strength and ledger immutability, while business realities (budget ceilings, interoperability duties, day-to-day usability) tug in the opposite direction. A checklist with a single headline metric—or a narrative built only on gut feeling—cannot deliver a defendable choice [24]. What is needed is a disciplined procedure that blends expert insight with hard numbers and turns that mix into clear priorities.

For that reason, we adopt a MCDM engine that scores blockchain-based web solutions across every dimension that matters [25]. MCDM is tailor-made for thorny technology calls: it pulls together criteria that do not share units, scales, or even the same logic, and yet still produces a result stakeholders can act on. In decentralised settings, where no ledger is best at everything, that capability is indispensable [26].

Inside the MCDM toolbox, outranking algorithms stand out. They rely on direct pair-by-pair comparisons and allow "better-than" relationships that do not need to be perfectly transitive. They also tolerate threshold zones where two options are judged close enough to be treated as ties—something a pure weighted-sum model cannot express [27]. Such flexibility maps nicely to blockchain realities: lightning-fast finality might be non-negotiable for a tele-health portal, while archival strength could trump speed in digital-notary work.

The prioritisation routine presented here therefore:

- Ingests multiple candidate solutions—whether full blockchain platforms or bespoke architectural variants.
- Rates each one on a weighted list of criteria supplied by domain experts.
- Runs pairwise preference tests to gauge how strongly one option outranks another.
- Builds a net outranking score that produces an ordered list of best-fit choices [27].

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Designed for adaptability, the model can absorb new criteria, overlay fuzzy logic where inputs are uncertain, and map to domain-specific regulations or constraints. As the later case study shows, the same scaffold can be repurposed for finance, logistics, digital identity, and beyond—furnishing a reusable, transparent roadmap for blockchain platform prioritisation

3.2. Criteria Selection and Modeling Logic

Establishing a defensible criterion set constitutes the fulcrum of any MCDM investigation, as the chosen variables govern the architecture, sensitivity, and epistemic credibility of subsequent rankings. In the arena of blockchain-mediated web services for secure data exchange, those variables must integrally reflect the technological, economic, and operational strata that determine system performance, user trust, and long-run scalability. Guided by a triangulation of recent scholarship, sector-specific regulatory mandates, and iterative consultations with domain specialists, this study synthesizes a cross-sector criterion portfolio intentionally crafted to be reusable yet re-weightable—enabling, for example, amplified privacy salience in healthcare or heightened cost sensitivity in fintech deployments [28]. The list is grouped into three overarching lenses—Technical Performance, Security & Privacy, and Operational Feasibility—with detailed sub-criteria shown in Table 4. Each item is flagged as either

- Beneficial—higher values are better (e.g., Scalability, Ledger Integrity)
- Non-Beneficial—lower values are preferred (e.g., Latency, Implementation Cost)

Relative importances are encoded on a normalised 0 – 1 scale whose weights collectively sum to unity, thereby preserving comparability while reflecting domain-specific salience [26]. This structured yet flexible scaffold ensures that subsequent outranking analyses rest on a criterion set both comprehensive and defensible, safeguarding the rigor and transparency of the entire decision-support pipeline.

Table 4. Evaluation Criteria for Blockchain-Based Secure Web Applications

Dimension	Criterion	Description	Code	Weight	Type
Technical Performance	**Scalability**	Ability to absorb a growing transaction load or user base with no material drop in throughput or responsiveness	C1	0.12	Beneficial
	Latency	End-to-end interval required to validate and permanently record a transaction or update	C2	0.08	Non-Beneficial
	Interoperability	Degree to which the ledger can interface or exchange data with external systems and heterogeneous blockchains	C3	0.07	Beneficial
	Consensus Efficiency	Computational and time efficiency of the consensus algorithm in achieving finality	C4	0.08	Beneficial
Security & Privacy	**Data Integrity**	Assurance that on-chain data cannot be altered, deleted, or inserted undetected	C5	0.10	Beneficial
	Access Control	Breadth and granularity of mechanisms to restrict, grant, and audit data access	C6	0.07	Beneficial
	Immutability Guarantees	Strength of resistance to retrospective tampering with previously committed records	C7	0.10	Beneficial
	Anonymity/Confidentiality	Availability of privacy-enhancing features (e.g., encryption layers, zero-knowledge proofs)	C8	0.08	Beneficial
Operational Feasibility	**Deployment Cost**	Aggregate expenditure for implementation, operation, and scaling of the platform	C9	0.08	Non-Beneficial

Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

	Developer Ecosystem	Maturity and accessibility of tooling, libraries, documentation, and community support	C10	0.06	Beneficial
	Usability / Integration Ease	Effort required to incorporate the platform into existing IT infrastructure and workflows	C11	0.08	Beneficial
	Regulatory Compliance Readiness	Capability of the platform to satisfy prevailing data-protection and governance statutes	C12	0.08	Beneficial

3.3. Evaluation Mechanism and Ranking Procedure

The decision framework is articulated as a four-tier hierarchy (Figure 2). At its apex sits the global objective—selection of the most suitable blockchain platform. This goal decomposes into the three criterion clusters enumerated in Table 4, which in turn branch into the twelve operational indicators and, finally, the competing platform alternatives. The same hierarchy governs every stage of the PROMETHEE II workflow, from weight allocation through pair-wise preference elicitation to net-flow synthesis.

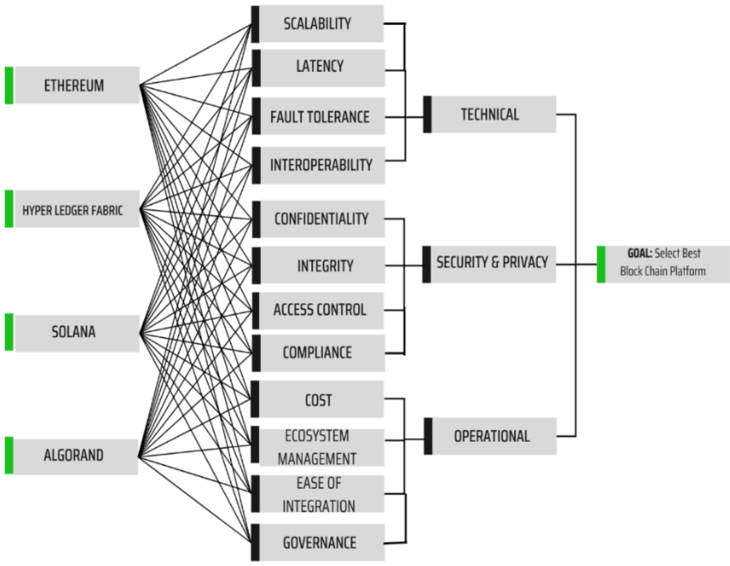

Fig 2. Hierarchical multi-criteria decision structure for evaluating blockchain platforms.

Each candidate platform A_i receives an initial rating $x_{ij} \in [0,10]$ for every criterion C_j. To render the scales commensurable, scores are rescaled by min–max normalisation [29]:

$$x_{ij}^{norm} = \begin{cases} \dfrac{(x_{ij} - \min(x_j))}{(\max(x_j) - \min(x_j))}, & beneficial\ criteria \\ \dfrac{(\max(x_j) - x_{ij})}{(\max(x_j) - \min(x_j))}, & non-beneficial\ criteria \end{cases} \quad (1)$$

Each pair of platforms (A_i, A_j) is compared across all criteria. The **usual preference function** is applied:

$$\pi_k(a_i, a_j) = \begin{cases} 1, & if\ x_{ik}^{norm} > x_{jk}^{norm} \\ 0, & otherwise \end{cases} \quad (2)$$

The global preference index for each pair is computed as:

Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$P(a_\mathrm{i}, a_\mathrm{j}) = \sum_{k=1}^{n} w_\mathrm{k} \cdot \pi_\mathrm{k}(a_\mathrm{i}, a_\mathrm{j}) \quad (3)$$

Finally, for each platform A_i:
- Positive Flow (Φ^+): How much A_i outranks others
- Negative Flow (Φ^-): How much A_i is outranked by others
- Net Flow (Φ): $\phi(a_i) = \phi^+(a_i) - \phi^-(a_i)$ (4)

The platform with the highest Φ is considered the most favorable overall.

4. Case Study and Numerical Analysis

To validate the utility of the proposed prioritisation apparatus, we executed a PROMETHEE II analysis on four widely cited ledger platforms that underpin secure, data-sharing web services. The quartet—Ethereum, Hyperledger Fabric, Solana, and Algorand—spans both permissionless and permissioned architectures and therefore offers a representative cross-section of design philosophies, performance envelopes, and ecosystem maturity levels.

4.1. Case Study Setup

Platform selection. Candidates were shortlisted according to three filters: (i) demonstrable production use, (ii) sustained industry adoption, and (iii) coverage of both public-chain and consortium-chain paradigms.
- **Ethereum (P1)**: Public, highly decentralised ledger distinguished by Turing-complete smart contracts and an extensive developer toolkit [30].
- **Hyperledger Fabric (P2)**: Permissioned, modular ledger engineered for enterprise deployments that require compartmentalised data visibility and configurable governance [31, 32].
- **Solana (P3)**: High-throughput public network that employs a proof-of-history clock to compress block times and minimise confirmation delay [33].
- **Algorand (P4)**: Public ledger running a rapid Byzantine-agreement protocol; adoption is rising in payments and identity projects [34, 35].

All four alternatives were scored against the twelve criteria identified in Section 3, which bundle technical performance, security/privacy, and operational feasibility attributes into a single analytic frame.

4.2. Performance Scoring

Each candidate ledger was scored on a 0 – 10 scale for all twelve-evaluation metrics. Table 5 lists the pre-normalized performance ratings for every platform across these criteria. These preliminary scores stem from expert judgement informed by vendor documentation, published benchmarks, and the platforms' deployment contexts. The resulting decision matrix constituted the input for subsequent min–max scaling and PROMETHEE II ranking. Ratings were synthesised from
- Official whitepapers and technical documentation
- Empirical benchmarks reported in the scholarly literature
- Expert approximations where quantitative evidence was unavailable

Table 5. Decision Matrix

Alternative/ Criteria	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12

P1	8.0	6.0	8.5	7.0	9.0	8.0	9.5	8.0	4.0	9.0	7.5	7.0
P2	6.5	7.5	7.0	6.0	8.5	9.0	9.0	9.0	5.0	8.0	8.5	9.5
P3	9.0	4.5	6.5	9.0	7.5	7.0	8.0	6.5	3.5	7.5	6.0	6.0
P4	7.5	6.0	8.0	8.0	8.0	8.5	9.0	7.5	4.5	8.5	7.0	8.0

4.3. Normalization and Weighting

To place the platforms on a common footing, every initial score was re-scaled with a min–max transformation. Converting each metric to the closed interval [0 , 1] eliminates unit disparities and range effects, thereby safeguarding comparability across the heterogeneous criteria outlined in Section 3.2. The resulting normalised matrix—used as the input for the subsequent PROMETHEE II computations—appears in Table 6.

Table 6. Normalized Decision Matrix

Alternative/ Criteria	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**C9**	**C10**	**C11**	**C12**
P1	0.60	0.50	1.00	0.333	1.000	0.50	1.000	0.60	0.667	1.000	0.60	0.286
P2	0.00	0.00	0.25	0.000	0.667	1.00	0.667	1.00	0.000	0.333	1.00	1.000
P3	1.00	1.00	0.00	1.000	0.000	0.00	0.000	0.00	1.000	0.000	0.00	0.000
P4	0.40	0.50	0.75	0.667	0.333	0.75	0.667	0.40	0.333	0.667	0.40	0.571

4.4. Aggregated Preference Flows and Decision Scores

With the scaled data and predefined weights, pairwise preference indices were computed for every platform dyad. PROMETHEE II subsequently produced the extent to which a platform dominates its peers, the extent to which it is dominated by others, and the overall preference score.

Table 7. Final Preference Flow Scores and Platform Rankings

Rank	**Platform**	**Φ^+ (Positive Flow)**	**Φ^- (Negative Flow)**	**Φ (Net Flow)**
1	Ethereum	0.6733	0.3000	**+0.3733**
2	Algorand	0.4533	0.4867	–0.0333
3	Hyperledger	0.4533	0.5133	–0.0600
4	Solana	0.3600	0.6400	**–0.2800**

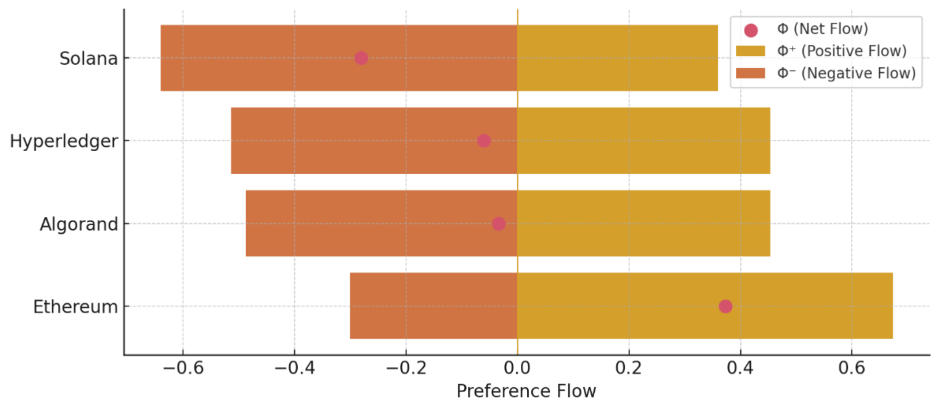

Fig 3. Positive vs Negative Preference Flows

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

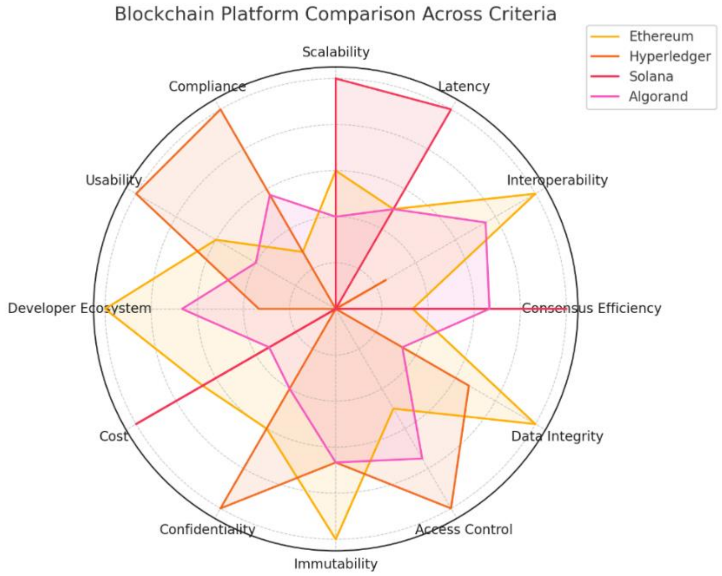

Fig 4. Radar Chart: Blockchain Platform Comparison Across 12 Criteria

The PROMETHEE II net-flow ranking and a radial criterion profile for each ledger are displayed in Fig. 4, providing an at-a-glance comparison of how each candidate aligns with the multi-dimensional decision mandate and as elaborated in Table 8.

Table 8. Performance Synopsis (visualised in Fig. 4)

Platform	Relative Strengths	Relative Weaknesses
Ethereum	Ecosystem breadth, scalability, data-integrity assurances	Mid-range latency, moderate compliance readiness
Hyperledger Fabric	Robust security stack, granular access control, strong regulatory alignment	Limited horizontal scalability, moderate consensus efficiency
Solana	Exceptional throughput and low latency driven by PoH–PoS hybrid	Weaker privacy/compliance profile
Algorand	Balanced scores; notable in access control, interoperability, and consensus speed	No pronounced deficiencies but marginally trails top performer on ecosystem depth

5. Results and Discussion

A PROMETHEE II outranking analysis was carried out on four mainstream ledger platforms—Ethereum, Hyperledger Fabric, Solana, and Algorand—rated against twelve criteria. After min–max scaling, the decision matrix blended beneficial factors (e.g., scalability, data integrity, interoperability) with non-beneficial factors (e.g., latency, deployment cost), each criterion weighted according to expert consensus.

The computed net flows (Table 7, Fig. 3) place Ethereum at the top with $\Phi = +0.3733$, reflecting consistent superiority across most indicators. Algorand ($\Phi = -0.0333$) and Hyperledger Fabric ($\Phi = -0.0600$) follow, each showing solid scores in operational feasibility and privacy-related metrics. Solana, despite excellent raw throughput and consensus speed, records the lowest net flow ($\Phi = -0.2800$) due to the limited access-control features, modest privacy safeguards, and incomplete compliance tooling.

5.1. Performance Insights

The radar plot in Figure 3 depicts each platform's position on the full criterion set. Ethereum combines strong scalability, robust immutability, and a mature development ecosystem—properties that suit public, high-volume deployments. Hyperledger Fabric excels in privacy, fine-

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

grained access control, and regulatory conformity, making it well matched to enterprise and health-sector applications. Algorand delivers a balanced scorecard, with notable results in interoperability and consensus efficiency, yielding versatility for hybrid public–private scenarios. Solana excels in transaction throughput but lags in governance, privacy, and compliance—key characteristics in trust-sensitive environments.

5.2. Trade-Offs and Use-Case Alignment

Ranking depicts ongoing trade-offs between decentralisation, operating expenditure, and governance. Public chains like Ethereum have widespread community support and robust fault tolerance but network charges and verification latency that may increase under load. Permissioned models (e.g., Hyperledger Fabric) allow for fine-grained control and regulatory compliance at the cost of complete openness. Algorand offers a middle ground, and Solana's plain speed incurs additional compliance effort.

5.3. Implications for Decision-Makers

By converting heterogeneous platform characteristics and domain expert preferences into a uniform, transparent ranking, the PROMETHEE II methodology provides a reproducible decision support tool for choosing blockchain infrastructure within multi-dimensional limits. The procedure can be easily extended to other domains—finance, healthcare, logistics—where data-sharing must be secure and auditable, and performance, security, and compliance trade-offs need to be made explicit.

6. Conclusion

The paper presents a methodical computational framework for ranking distributed-ledger systems that enable secure web services with data sharing. Through combining multi-criteria decision analysis with weights from subject-matter experts, the framework addresses the complex challenge of evaluating blockchain alternatives. Using the PROMETHEE II outranking approach, it balances technological ability and operational feasibility with privacy protection, cost considerations, and regulatory compliance.

The comparative exercise puts Ethereum in first place, thanks to its mature ecosystem, high scalability, and robust security stance. Hyperledger Fabric and Algorand both fill useful niches: their increased controls over privacy and compliance preparedness make them appealing for enterprise or highly regulated environments. Solana, although unrivaled in throughput and consensus speed, scores lower in governance and confidentiality.

The tool thus provides engineers, strategists, and policymakers an open, reproducible process for selecting a suitable ledger. Since the weights of the criteria are adjustable for each user and the model can consume fuzzy inputs, real-time telemetry, or feedback loops, it can be tailored for varied industries. Further work will generalize the framework to dynamic spaces—decentralised finance, intelligent-city services, and digital-health infrastructures—where performance benchmarks and stakeholder values change over time.

References

1. Rana, M. (2025). Impact of Blockchain and Big data on Global Economy.
2. Banerjee, B. (2024). Blockchain 2030: Revolutionizing the Future of Digital Trust. *International Research Journal of Scientific Studies*, *1*(1), 13-18.

Received: August 08, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3. Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019, April). Blockchain technology in healthcare: a systematic review. In *Healthcare* (Vol. 7, No. 2, p. 56). MDPI.
4. Anita, N., & Soundar, K. R. (2024). Secure blockchain framework for high-value financial transaction management. In *Applications of Blockchain and Artificial Intelligence in Finance and Governance* (pp. 14-27). CRC Press.
5. Yadav, R., Mishra, U., & Gupta, R. (2024, August). A Review of Blockchain Technology: Its Benefits, Challenges, and Functionalities. In *2024 International Conference on Electrical Electronics and Computing Technologies (ICEECT)* (Vol. 1, pp. 1-6). IEEE.
6. Fortune Business Insights, "Blockchain Technology Market Size, Share & Industry Analysis … Regional Forecast, 2025–2032," May 26 2025. [Online]. Available: https://www.fortune businessinsights.com/industry-reports/blockchain-market-100072
7. Abo-Akleek, F., Mowafi, M., & Taqieddin, E. S. (2025). *Leveraging blockchain for robust and transparent E-voting systems*. Journal of Cybersecurity and Applications.
8. Bonagiri, K., & Deepalakshmi, P. (2025). *Cybersecurity With Blockchain in IoT*. IEEE Xplore.
9. Malarvizhi, B., & Anusuya, S. (2025). *Integrating Blockchain with IoT and AI for Smart Cities*. Taylor & Francis.
10. Eido, W. M., & Zeebaree, S. (2025). *A Review of Blockchain in Digital Marketing*. HAL.
11. Themistocleous, M. (2025). *Handbook of Blockchain Technology*. Edward Elgar.
12. Hadfi, R., Ito, T., & Fujihara, A. (2025). *Anomaly Detection in DAOs Using AI*. AI & Society, Springer.
13. Srinivasan, M., & Senthilkumar, N. C. (2025). *Hybrid Blockchain-Based IDPS*. IEEE Access.
14. Zeng, W. (2025). *Blockchain Audit Logging in Cross-Platform Crawling Systems*. IJAI4S.
15. Peddi, S., Valivarthi, D. T., & Narla, S. (2025). *Fuzzy Decision-Making in Blockchain-IoT*. World Scientific.
16. Nguyen, P. H., Pham, T. V., & Nguyen, L. A. T. (2024). *Analysis of Quantum Computing's Applicability in Data Analysis: Utilizing a Hybrid MCDM Approach With Quantum Spherical Fuzzy Sets*. IEEE.
17. Muhammad, A., Siddique, A., & Mubasher, M. (2023). *Prioritizing Non-Functional Requirements in Agile Process Using Multi Criteria Decision Making Analysis*. IEEE.
18. Muradi, S. B. (2022). *Systematic Selection of Blockchain Platforms Using Fuzzy AHP-TOPSIS*. Malaysian Journal of Computer Science.
19. Yadav, A., Yadav, G., & Desai, T. N. (2025). *Unlocking the Potential of Industry 4.0 in BRICS Nations: A Systematic Literature Review and Meta-Analysis*. International Journal of Quality & Reliability Management.
20. Lima-Junior, F. R., Oliveira, M. E. B., & Resende, C. H. L. (2023). *Applications of Hesitant Fuzzy Linguistic Term Sets in Supply Chain Management: A State-of-the-Art Review*. Mathematics, 11(13), 2814.
21. Mizrak, F., & Akkartal, G. R. (2024). *Prioritizing Cybersecurity Initiatives in Aviation: A DEMATEL-QSFS Methodology*. Heliyon, 10(6), e22504.
22. Barahmand, Z., & Eikeland, M. S. (2022). *Life Cycle Assessment Under Uncertainty: A Scoping Review*. World, 3(3), 455–476.
23. Pereira, R. C. A., da Silva Jr, O. S., & de Mello Bandeira, R. A. (2023). *Evaluation of Smart Sensors for Subway Electric Motor Escalators Through AHP-Gaussian Method*. Sensors, 23(8), 4131.
24. Liu, J., Zhang, Q., Xie, M., Lin, M., & Xu, Z. (2024). A blockchain platform selection method with heterogeneous multi-criteria Decision-Making based on hybrid distance measures and an AHP-EWM weight method. *Expert Systems with Applications*, *256*, 124910.

25. Larbani, M., & Aouni, B. (2025). A generalized approach for multi-criteria decision aid methods. *Annals of Operations Research*, 1-29.
26. Mishra, A. R., & Rani, P. (2025). Evaluating and Prioritizing Blockchain Networks using Intuitionistic Fuzzy Multi-Criteria Decision-Making Method. *Spectrum of Mechanical Engineering and Operational Research*, *2*(1), 78-92.
27. Liu, X., & Liu, Y. (2024). Sensitivity analysis of the parameters for preference functions and rank reversal analysis in the PROMETHEE II method. *Omega*, *128*, 103116.
28. Tatar, V., & Ayvaz, B. (2024, August). A Spherical Fuzzy SWARA-Based Methodology for Prioritizing Selection Criteria of Blockchain Software. In *Global Joint Conference on Industrial Engineering and Its Application Areas* (pp. 307-318). Cham: Springer Nature Switzerland.
29. Larbani, M., & Aouni, B. (2025). A generalized approach for multi-criteria decision aid methods. *Annals of Operations Research*, 1-29.
30. Grayscale Research. (2025, March 20). Ethereum: The OG Smart Contract Blockchain. https://research.grayscale.com/reports/ethereum-the-og-smart-contract-blockchain
31. Joshi, P., & Mahajan, P. (2025). Secure and interoperable EHR management via Hyperledger Fabric: The MrBlock framework. *Peer-to-Peer Networking and Applications, 18*, 133.
32. Melo, C., Gonçalves, G., Silva, F. A., & Soares, A. (2024, June). Performance Modeling and Evaluation of Hyperledger Fabric: An Analysis Based on Transaction Flow and Endorsement Policies. In *2024 IEEE Symposium on Computers and Communications (ISCC)* (pp. 1-6). IEEE.
33. Panda Academy. (2025, April 15). In-depth analysis of Solana RPC providers: A 2025 developer's guide. https://academy.pandatool.org/en_US/solana/305
34. Genfinity. (2025, May 28). Algorand May 2025 recap: RWA and DeFi expansion. https://genfinity.io/2025/05/28/algorand-may-2025-recap/
35. Algorand Foundation. (2025, Apr 15). *Algorand 2025 ecosystem surge: Major upgrades, staking rewards & project highlights*. https://genfinity.io/2025/04/15/algorand-2025-ecosystem-updates/