Journal of Innovations in Computer Science and Engineering
Shahid Beheshti Unversity

June 2025, Volume 3, Issue 1

A Taxonomy of Blockchain Key Performance Indicators and Measurement Features: A Systematic Review

Kimiya Karimi Dehkordi, **CODE ORCID**: 0009-0002-7120-4548
Master Student, Department of Computer Engineering, Faculty of Engineering, Shahrekord University, Shahrekord, Iran, kimiya.karimi@stu.sku.ac.ir.
Leila Samimi-Dehkordi✉, **CODE ORCID**: 0000-0002-2842-0256
Assistant Professor, Department of Computer Engineering, Faculty of Engineering, Shahrekord University, Shahrekord, Iran, samimi@sku.ac.ir**.**
Abbas Horri, **CODE ORCID**: 0000-0001-7933-9266
Assistant Professor, Department of Computer Engineering, Faculty of Engineering, Shahrekord University, Shahrekord, Iran, horri@sku.ac.ir**.**

ABSTRACT

Blockchain technology has revolutionized various industries by enabling decentralized, transparent, and secure systems for applications such as supply chain management, Internet of Things (IoT), and smart contracts. However, evaluating the performance of diverse blockchain systems remains challenging due to the absence of standardized metrics. This systematic review synthesizes findings from 55 peer-reviewed studies to develop a comprehensive taxonomy of Key Performance Indicators (KPIs). Our analysis reveals a critical trade-off: while Proof-of-Work systems (e.g., Bitcoin) offer superior security with hash rates exceeding 500 EH/s, they consume approximately 700 kWh per transaction—a sustainability gap of nearly two orders of magnitude compared to more efficient alternatives. Furthermore, we identify the IoT domain as the most vulnerable to the lack of standardization, where inconsistent KPIs for latency and throughput currently hinder real-time device coordination. We categorize 30 general KPIs into four dimensions—technical, security, economic, and user-centric—while identifying domain-specific KPIs tailored to applications like supply chain logistic, IoT, and smart contracts. Additionally, we map blockchain features required for measuring these KPIs, ensuring traceability to system properties. Derived from a rigorous systematic review of blockchain performance literature, our findings provide a holistic framework for assessing blockchain performance. This framework bridges technical and application- specific needs, offering actionable insights for researchers, developers, and industry practitioners to optimize blockchain systems across public, private, and hybrid architectures. The taxonomy and measurement features support standardized evaluation, paving the way for scalable and sustainable blockchain adoption in emerging domains like decentralized finance.

KEYWORDS

Blockchain, Key Performance Indicators, Systematic Review, Performance Evaluation, Domain-Specific Metrics.

1. INTRODUCTION

Blockchain technology, initially conceptualized by Nakamoto in 2008 [1], has transformed from a foundational element for cryptocurrencies like Bitcoin into a versatile infrastructure that supports decentralized applications across various industries. Its immutable, distributed ledger fosters transparency and trust, facilitating use cases such as supply chain management [2], [3], Internet of Things (IoT) [5], smart contracts [8], and industrial automation [10]. In contrast to traditional centralized systems, blockchain mitigates single points of failure and enhances security through cryptographic mechanisms [5], [12]. However, the diversity of blockchain architectures—public (e.g., Bitcoin, Ethereum [1], [14], private (e.g., Hyperledger Fabric [15]), and hybrid [3]—presents significant challenges for performance evaluation [18], [19].

Performance assessment is essential to ensure that blockchain systems fulfill application-specific requirements, such as high throughput in IoT networks [21], low latency in real-time monitoring [5], and transparency in supply chains [2]. Key Performance Indicators (KPIs) serve as measurable metrics for evaluating efficiency, security, scalability, and user satisfaction [25], [27]. For instance, Transaction Throughput (TPS) quantifies operational capacity [28], while Hash Rate evaluates security in Proof-of-Work (PoW) systems [29]. Economic KPIs, such as Energy Consumption, highlight sustainability concerns [27], and user-centric KPIs, such as User Adoption Rate, indicate system acceptance [25]. Despite their significance, the blockchain literature lacks a unified taxonomy that integrates both general and domain-specific KPIs, along with the system features required for their measurement [18], [27].

Prior studies frequently concentrate on specific aspects, such as the performance of consensus algorithm [27], or the efficiency of smart contract [8], without offering a holistic framework. For example, general KPIs like TPS and Latency are well-

Submit Date: 2025-09-08
Revise Date: 2026-05-19
Accept Date: 2026-06-01
✉ Corresponding author

documented for public blockchains [18], [28], but domain-specific metrics, such as Delivery Time in supply chains [2], [24] or Access Latency in IoT [5], [34], are less standardized. Furthermore, measuring these KPIs requires specific blockchain features, such as transaction timestamps or audit trails [15], [35], which are seldom mapped systematically. This fragmentation hinders cross-domain comparisons and the development of standardized evaluation tools [3], [19].

Beyond traditional domains such as supply chains, IoT, and industrial systems, emerging blockchain applications—including Decentralized Finance (DeFi), Non-Fungible Tokens (NFTs), Web3 platforms, and the metaverse—have gained significant momentum in recent years. Despite the proliferation of blockchain-based Decentralized Applications (DApps) across gaming, finance, and social media, existing performance evaluation frameworks exhibit a pronounced blind spot. Metrics central to DApp ecosystems—such as Daily Active Users (DAU), Transaction Volume (in USD), Retention Rate, and Total Value Locked (TVL)—are conspicuously absent from prior systematic reviews [26]. Similarly, user-centric indicators like Session Duration or Smart Contract Invocation Frequency, which directly inform tokenomics and user engagement models, remain largely overlooked. This omission raises a critical question: who is the intended audience for blockchain KPI frameworks, and why have researchers and practitioners consistently ignored comprehensive metric sets in favor of one or two simplistic indicators? The answer lies in a fundamental disconnect between academic taxonomy and practical application. Infrastructure-focused metrics (e.g., TPS, Hash Rate) dominate the literature because they are easily instrumented at the node level [28], whereas DApp-level metrics often require off-chain analytics or cross-platform data aggregation, which many blockchain systems do not natively support [23], [36]. Consequently, practitioners default to easily accessible metrics, neglecting holistic evaluation. Our work directly addresses this gap by (1) explicitly defining the intended audience for each KPI category (infrastructure engineers, DApp developers, business analysts, and regulators) and (2) explaining why certain metrics are systematically underutilized—thereby transforming a perceived weakness into a structured research agenda.

These domains introduce unique operational and economic requirements, making existing KPI frameworks insufficient. For instance, DeFi platforms demand indicators for Liquidity and Impermanent Loss, while NFTs emphasize Transaction Uniqueness and Market Volatility. Highlighting these domains underscores the need for extending KPI taxonomies to capture performance in rapidly evolving blockchain ecosystems.

To address these gaps, this study conducts a systematic literature review to answer two research questions (RQs):

- RQ1: What KPIs exist in the blockchain literature for evaluating system performance across general and domain-specific contexts?
- RQ2: What blockchain features are required to measure these KPIs effectively?

We analyzed 58 peer-reviewed studies, citing 55 representative ones (25 for general KPIs and 30 for domain-specific KPIs) to develop a comprehensive taxonomy. The general KPIs encompass technical, security, economic, and user-centric dimensions [18], while domain-specific KPIs pertain to applications like supply chain logistics [2], IoT [5], smart contracts [8], and industrial systems [10]. Additionally, we map the blockchain features required for KPI measurement, facilitating practical evaluation across public, private, and hybrid systems [21], [36]. Our contributions include:

- A taxonomy of 30 general KPIs, providing a standardized framework for blockchain evaluation.
- A set of domain-specific KPIs tailored to critical applications, derived from 30 specialist studies.
- A detailed mapping of blockchain features for KPI measurement, ensuring traceability and reproducibility.
- A holistic framework that bridges technical and application-specific performance needs, supporting researchers and practitioners in optimizing blockchain systems.

As shown in Figure 1, the research process begins with a comprehensive review of the literature, proceeds through the screening of relevant sources, and advances to the development of a taxonomy. The identified categories are then used to map key features, culminating in a discussion of the findings and their broader implications.

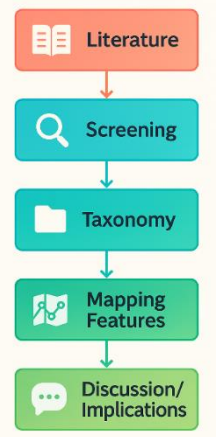

Figure 1. Flowchart of Research Process Stages

This paper is structured as follows: Section 2 describes the review methodology, Section 3 presents the taxonomy and findings, Section 4 analyzes implications and limitations, and Section 5 summarizes contributions and future directions.

2. METHOLOGY

To ensure a rigorous and reproducible review, we adopted the Kitchenham (2007) framework for systematic reviews in software engineering [20]. This framework is particularly well-suited for synthesizing evidence in interdisciplinary fields like blockchain performance evaluation due to its structured approach. Our methodology comprised three key stages: planning the review, conducting the review, and analysis and reporting. This systematic process enabled us to develop a comprehensive taxonomy of blockchain KPIs and their measurement features, addressing both general and domain-specific contexts [18], [19].

2.1. Planning the Review

The planning phase involved defining research objectives, formulating research questions, and establishing the review protocol. Our objective was to identify and categorize blockchain KPIs and their measurement features across general and domain-specific applications. Two research questions (RQs) guided the review:

- RQ1: What KPIs exist in the blockchain literature for evaluating system performance across general and domain-specific contexts?
- RQ2: What blockchain features are required to measure these KPIs effectively?

The review protocol outlined the search strategy, inclusion/exclusion criteria, and data extraction methods. We selected three major databases—Scopus, IEEE Xplore, and Web of Science—for their extensive coverage of computer science, engineering, and blockchain research [3], [20]. The search covered peer-reviewed literature published between 2008 (the inception of blockchain [1]) and April 2024.

To ensure reproducibility, the search strings combined general blockchain terms ("blockchain," "key performance indicators," "performance metrics," "evaluation frameworks") with domain-specific keywords ("supply chain," "Internet of Things (IoT)," "smart contracts," "industrial systems," "consensus algorithms") [10], [27]. Table 1 summarizes the exact keyword combinations and database-specific syntax.

Inclusion criteria: (1) peer-reviewed articles or conference papers, (2) studies explicitly reporting blockchain KPIs or performance metrics, and (3) relevance to either general or domain-specific applications (e.g., supply chain [2], [3], IoT [4], [5], smart contracts [7], [8]).

Exclusion criteria: (1) non-English publications, (2) studies without measurable KPIs, (3) non-peer-reviewed sources (e.g., whitepapers lacking empirical validation), and (4) works unrelated to blockchain performance evaluation.

Table 1. Keyword Combinations and Database-Specific Syntax

Database	Search String (example syntax)
Scopus	TITLE-ABS-KEY("blockchain" AND ("key performance indicator*" OR "performance metric*" OR "evaluation framework*") AND ("supply chain" OR "Internet of Things" OR "IoT" OR "smart contract*" OR "industrial system*" OR "consensus algorithm*"))
IEEE Xplore	("All Metadata": blockchain) AND ("All Metadata": "key performance indicator*" OR "All Metadata": "performance metric*" OR "All Metadata": "evaluation framework*") AND ("All Metadata": "supply chain" OR "All Metadata": "Internet of Things" OR "All Metadata": "IoT" OR "All Metadata": "smart contract*" OR "All Metadata": "industrial system*" OR "All Metadata": "consensus algorithm*")
Web of Science	TS=(blockchain AND ("key performance indicator*" OR "performance metric*" OR "evaluation framework*") AND ("supply chain" OR "Internet of Things" OR "IoT" OR "smart contract*" OR "industrial system*" OR "consensus algorithm*"))

2.2. Conducting the Review

The execution phase involved searching, screening, and selecting relevant studies. After applying the database-specific queries, we initially identified 342 unique records (after duplicate removal). Screening followed a two-phase approach:

1. ***Title and abstract screening:*** applied inclusion/exclusion criteria, reducing the pool to 126 papers.
2. ***Full-text review:*** assessed methodological quality and clarity of KPI definitions, yielding 58 final studies [27].

Of these, 55 were directly cited in the results (25 for general KPIs and 30 for domain-specific KPIs). The remaining three were used only for contextual analysis and KPI validation without direct citation [3].

To enhance transparency, we documented the selection process using a PRISMA flow diagram, which illustrates the number of studies at each stage: identification (n = 342), screening (n = 126), and final inclusion (n = 58). This visual representation supports reproducibility and aligns with best practices for systematic reviews. The PRISMA flow diagram for this systematic review is shown in Figure 2.

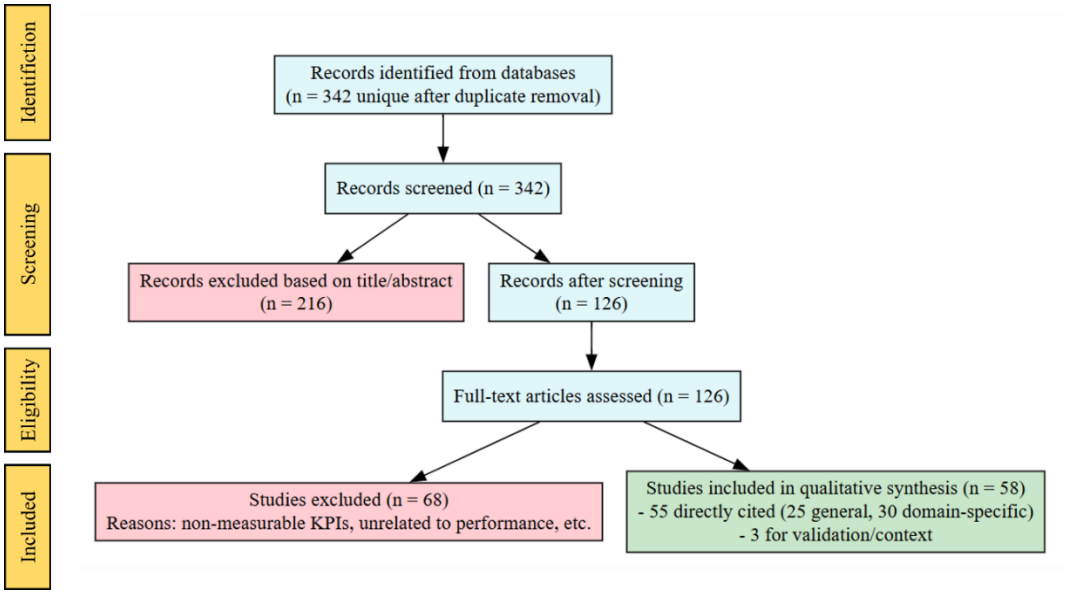

Figure 2. PRISMA Flow Diagram of Systematic Review

2.3. Analysis and Reporting

Data extraction focused on identifying KPIs, their definitions, applicable formulas, and required blockchain features. For general KPIs, we categorized metrics into four dimensions—technical, security, economic, and user- centric—following established frameworks [19], [25]. Examples of these KPIs include Transaction Throughput (TPS) [28], Hash Rate [29], Energy Consumption [30], and User Adoption Rate [25]. For domain-specific KPIs, we extracted metrics from 30 specialist studies, covering applications such as supply chain logistics [3], IoT [5], smart contracts [8], and industrial systems [10]. These metrics included Delivery Time [2], Access Latency [5], and Gas Consumption [41].

We employed both qualitative and quantitative synthesis. Qualitatively, we grouped KPIs by application and blockchain type (public, private, hybrid) to identify patterns and overlaps [15]. Quantitatively, we compiled formulas and measurement approaches to ensure consistency across studies [27]. The extracted data were organized into tables to present general KPIs, domain-specific KPIs, and their measurement features, ensuring traceability and reproducibility [21], [36]. This process resulted in a comprehensive taxonomy addressing RQ1 (identifying KPIs) and RQ2 (mapping measurement features), with findings reported in a structured format suitable for academic and practitioner audiences [20].

3. RESULT

This section presents the findings of our systematic review, addressing RQ1 (identifying blockchain KPIs) and RQ2 (determining measurement features). From an initial pool of 342 papers, 58 met our inclusion criteria. We cited 55 representative studies—25 for general KPIs [25], [36] and 30 for domain-specific KPIs [21], [27]—to ensure comprehensive coverage of unique metrics. The remaining three studies contributed to contextual analysis and KPI validation, enhancing the robustness of our taxonomy [3]. The findings are organized into three subsections: general KPIs, their measurement features, and domain-specific KPIs with corresponding features.

3.1. RQ1: Existing KPIs in Blockchain

Our analysis identified 30 general KPIs, applicable to blockchain systems such as Bitcoin, Ethereum, and Hyperledger Fabric. These KPIs are categorized into four dimensions: technical, security, economic, and user-centric, as shown in Table 2. Each KPI is accompanied by its definition and formula (where applicable), supported by representative studies.

1) Detailed Explanation of General KPIs: The 30 general KPIs in Table 2 provide a robust framework for evaluating blockchain performance across diverse systems. We highlight the most diagnostic KPIs per dimension as below:

- Technical KPIs, such as Transaction Throughput (TPS) and Latency, measure blockchain operational efficiency. TPS quantifies the number of transactions processed per second, while Latency captures the delay between transaction submission and confirmation [1], [28]. Scalability reflects the ability of a blockchain to maintain performance under increasing workload and node participation [18]. Additional indicators, including Block Time, Fork Rate, and Block Propagation Delay, influence responsiveness and network consistency. Shorter block times may reduce latency but increase the probability of temporary forks due to propagation delays [42]. Other KPIs, such as Node Synchronization Time, Chain Growth Rate, and Network Bandwidth Usage, characterize storage, communication, and onboarding overheads in blockchain networks [36], [44], [45]. Collectively, these metrics provide a technical foundation for evaluating blockchain efficiency across public and private architectures.
- Security KPIs evaluate the resilience and integrity of blockchain networks against adversarial behavior. Metrics such as Hash Rate, Attack Cost, and Double-Spending Success Rate quantify the difficulty of compromising consensus mechanisms in public blockchains [12], [42]. Additional indicators, including Orphaned Block Rate, Stale Block Rate, and Consensus Failure Rate, assess network stability and synchronization reliability [42], [47]. Cryptographic Strength and Network Partition Tolerance further characterize the robustness of blockchain protocols under cryptographic or network-level attacks [13], [15]. Together, these KPIs support comparative evaluation of blockchain security across different architectures and consensus mechanisms.
- Economic KPIs assess the financial and sustainability aspects of blockchain systems. Metrics such as Cost per Transaction, Energy Consumption, and Network Operational Cost capture the resource requirements associated with

blockchain deployment and maintenance [19], [30]. Additional indicators, including Mining Reward Efficiency and Gas Fee Variability, reflect the economic dynamics of PoW-based and smart-contract platforms [40], [49]. Transaction Value further measures the economic activity supported by blockchain ecosystems [50]. These KPIs enable assessment of operational efficiency and long-term sustainability across blockchain platforms.

- User-Centric KPIs, User-centric KPIs evaluate blockchain adoption and user engagement. Metrics such as User Adoption Rate, Active Address Count, and User Transaction Frequency measure participation and activity levels within blockchain ecosystems [25], [37]. The NVT Ratio relates market capitalization to transaction volume, supporting analysis of economic utilization and network activity [50], [51]. Unlike technical KPIs, user-centric indicators are highly dependent on application context and measurement assumptions. Collectively, these metrics support evaluation of blockchain acceptance and ecosystem growth, particularly in DApp and decentralized finance environments.

By systematically applying the categories and formulas in Table 2, stakeholders can perform holistic evaluations, supporting comparisons across public (e.g., Bitcoin, Ethereum) and private (e.g., Hyperledger Fabric) blockchains [18], [15], [36]. To address the context-dependency concern raised in prior studies, we additionally classify each KPI according to its applicability across blockchain architectures and consensus mechanisms. This distinction clarifies that certain KPIs (e.g., Hash Rate, Mining Reward Efficiency) are specific to PoW-based systems, whereas others remain universally applicable.

Table 2. Comprehensive Overview of Blockchain KPIs

	KPI	Definition	Formula	Applicable To
Technical	Transaction Throughput (TPS)	Transactions processed per second	$TPS = \frac{Total\ Transactions}{Elapsed\ Time\ (seconds)}$ [1], [28]	All Blockchain Types
	Latency	Time from submission to confirmation	$Latency = T_{confirm} - T_{submit}$ [28]	All Blockchain Types
	Block Time	Average time between consecutive blocks	$Block\ Time = \frac{\sum_{i=0}^{n}(T_i - T_{i-1})}{Number\ of\ Blocks}$ [14]	All Blockchain Types
	Scalability	Capacity to handle increased load	$Scalability\ Index = \frac{\Delta TPS}{\Delta Nodes}$ [18]	All Blockchain Types
	Block Propagation Delay	Time for a block to reach all nodes	$Delay = T_{receive} - T_{broadcast}$ [28]	All Blockchain Types
	Fork Rate	Frequency of temporary chain splits	$Fork\ Rate = \frac{Temporary\ Forks}{Total\ Blocks}$ [42]	PoW-based Systems, Some PoS Systems
	Transaction Finality	Time until a transaction is irreversible	$Finality = T_{irreversible} - T_{submit}$ [43]	All Blockchain Types
	Network Bandwidth Usage	Data rate of network traffic	$Bandwidth = \frac{Total\ Data\ Transferred\ (bytes)}{Time\ (seconds)}$ [36]	All Blockchain Types
	Node Synchronization Time	Time to fully sync a new node	$Sync\ Time = T_{full\ sync} - T_{start}$ [44]	All Blockchain Types
	Chain Growth Rate	Rate of blockchain size increase	$Growth\ Rate = \frac{\Delta Size\ (bytes)}{\Delta Time\ (seconds)}$ [45]	All Blockchain Types
Security	Hash Rate	Computational power securing the network	$Hash\ Rate = \Sigma\ Hashes\ per\ Second$ [12]	PoW-based Systems
	51% Attack Cost	Cost to control majority power	$Attack\ Cost = (Hardware\ Cost + Energy\ Cost) \times Attack\ Duration$ [12]	All Blockchain Types (context-dependent)
	Orphaned Block Rate	Percentage of blocks not in main chain	$Orphan\ Rate = \frac{Orphaned\ Blocks}{Total\ Blocks}$ [46]	PoW-based Systems
	Double-Spending Success Rate	Probability of successful double-spend	$P_{DS} = \left(\frac{q}{p}\right)^k, q: attacker\ power, p: network\ power, k: confirmaions$ [42]	Public Blockchains
	Sybil Attack Resistance	Cost to create fake identities	$Cost_{Sybil} = \Sigma\ Stake\ per\ Fake\ ID$, for pos-based systems [29] $Cost_{Sybil} = Hash\ Rate \times Energy\ Cost\ per\ hash \times Attack\ Duration$, for pow − based systems [29]	All Blockchain Types (context-dependent)
	Consensus Failure Rate	Frequency of consensus breakdowns	$Failure\ Rate = \frac{Failed\ Rounds}{Total\ Rounds}$ [47]	All Blockchain Types
	Cryptographic Strength	Resistance to cryptographic attacks	$Qualitative: Key\ length, Algorithm\ strength$ [13]	All Blockchain Types
	Network Partition Tolerance	Ability to withstand network splits	$Qualitative: \%\ of\ nodes\ isolated\ tolerated$ [15]	All Blockchain Types
	Stale Block Rate	Superseded blocks due to competition	$Stale\ Rate = \frac{Stale\ Blocks}{Total\ Blocks}$ [46]	PoW-based Systems
	Network Disruption Cost	Cost to disrupt network	$Attack\ Cost = Resource\ Cost \times Attack\ Duration$ [48]	All Blockchain Types
Economic	Cost per Transaction	Operational cost per transaction	$Cost/Tx = \frac{Total\ Operational\ Cost}{Total\ Transactions}$ [19]	All Blockchain Types
	Energy Consumption	Power usage per transaction	$Energy/Tx = \frac{Total\ Energy\ (kWh)}{Total\ Transactions}$ [30]	All Blockchain Types
	Mining Reward Efficiency	Reward vs. total cost	$Efficiency = \frac{Reward}{(Energy\ Cost + Hardware\ Cost))}$ [40]	PoW-based Systems
	Gas Fee Variability	Fluctuation in transaction fees	$Variability = \sigma(Gas\ Fees)$ [49]	Smart-Contract Platforms
	Transaction Value	Monetary value of transactions	$Value = \Sigma\ Transaction\ Amounts\ s\ (e.g., BTC)$ [50]	Public Blockchains, DApp Ecosystems
	Network Operational Cost	Network maintenance cost	$Op\ Cost = \Sigma(Node\ Costs + Infrastructure\ Costs)$ [20]	All Blockchain Types
User-Centric	User Adoption Rate	Growth in active users	$Adoption\ Rate = \frac{\Delta Users}{\Delta Time}$ [25]	Public Blockchains, DApp Ecosystems
	Active Address Count	Active addresses per period	$Active\ Count = \Sigma\ Distinct\ Addresses\ in\ period_t$ [25]	Public Blockchains
	NVT Ratio	Market cap vs. transaction volume	$NVT = \frac{Market\ Capitalization}{Transaction\ Volume}$ [50]	Cryptocurrency-based Public Blockchains
	User Transaction Frequency	Avg. transactions per user	$Frequency = \frac{Total\ Transactions}{Active\ Users}$ [37]	Public Blockchains, DApp Ecosystems

3.2. RQ2: Blockchain Features for General KPI Measurement

Three main observations emerge from the mapping between KPIs and blockchain features in Table 3. First, some KPIs rely on directly observable blockchain data, such as timestamps and transaction counts, whereas others require derived metrics or external estimations [42]. Second, several blockchain features are reused across multiple KPIs; for example, timestamps contribute to Latency, Block Time, and Chain Growth Rate measurements. Third, feature requirements vary according to the consensus mechanism. PoW systems depend on metrics such as Hash Rate and mining-related resource usage, whereas PoS systems rely more heavily on validator participation and stake distribution [15], [36]. These observations demonstrate that KPI measurement is strongly influenced by both blockchain architecture and monitoring capabilities.

The features in Table 3 are derived from blockchain protocols and system logs. For example, TPS measurement requires block size and transaction counts [1], [28], while Hash Rate relies on miner computational data [12]. These features ensure that KPIs are measurable across different blockchain types, including public (e.g., Ethereum [14]) and private (e.g., Hyperledger Fabric [15]) systems [36]. The mapping facilitates practical implementation, enabling developers to integrate performance monitoring into blockchain platforms [18], [20]. Figure 3 illustrates the mapping of KPIs to blockchain features using a bipartite graph representation.

Table 3 Blockchain Features Required For General KPI Measurement

Values are approximate and depend on network status; e.g., Bitcoin's hash rate exceeded 500 EH/s in 2023 [12].

KPI	Required Blockchain Features	Applicable To
Transaction Throughput	Block size, transaction count, time interval [1], [28]	All Blockchain Types
Latency	Transaction timestamps (submit, confirm) [28]	All Blockchain Types
Block Time	Block timestamps [14]	All Blockchain Types
Scalability	Node count, TPS under load [18]	All Blockchain Types
Block Propagation Delay	Broadcast and receive timestamps [28]	All Blockchain Types
Fork Rate	Block metadata (temporary forks vs. main chain) [46]	PoW-based Systems, Some PoS Systems
Transaction Finality	Confirmation depth (PoW) or finality time (PoS) [43]	All Blockchain Types
Network Bandwidth Usage	Data transfer logs [36]	All Blockchain Types
Node Synchronization Time	Sync start/end timestamps [44]	All Blockchain Types
Chain Growth Rate	Blockchain size, time [45]	All Blockchain Types
Hash Rate	Miner computational power [12]	PoW-based Systems
Resistance to 51% Attack	Total hash rate, hardware cost, energy cost per hash [12]	All Blockchain Types
Orphaned Block Rate	Block status (orphaned vs. accepted) [46]	PoW-based Systems
Double-Spending Success Rate	Transaction history, chain analysis, attacker's hash power share (q), network power (p), and confirmation count (k). [42]	Public Blockchains
Sybil Attack Resistance	For pos-based systems: Node identity verification data, minimum stake requirement per identity; for pow-based systems: total hash rate, energy cost per hash, attack duration [29]	All Blockchain Types
Consensus Failure Rate	Consensus round logs [47]	All Blockchain Types
Cryptographic Strength	Encryption algorithm, key size [13]	All Blockchain Types
Network Partition Tolerance	Network topology, split logs [15]	All Blockchain Types
Stale Block Rate	Block status (stale vs. accepted) [46]	PoW-based Systems
Attack Cost	Attack type specification (e.g., DoS, 51%), resource usage (computational, financial), time logs [48]	All Blockchain Types
Cost per Transaction	Fee data, operational costs [19]	All Blockchain Types
Energy Consumption	Hash rate (PoW) or node count (PoS), hardware specs [30]	All Blockchain Types
Mining Reward Efficiency	Reward data, energy cost, hardware cost [40]	PoW-based Systems
Gas Fee Variability	Fee history [49]	Smart-Contract Platforms
Transaction Value	Transaction amounts (in native currency) [50]	Public Blockchains, DApp Ecosystems
Network Operational Cost	Node maintenance costs, infrastructure costs [20]	All Blockchain Types
User Adoption Rate	User registration logs [25]	DApp Ecosystems, Public Blockchains
Active Address Count	Address activity logs over time [25]	Public Blockchains
NVT Ratio	Market cap, transaction volume [50]	Cryptocurrency-based Public Blockchains
User Transaction Frequency	Transaction logs, user count [37]	DApp Ecosystems, Public Blockchains

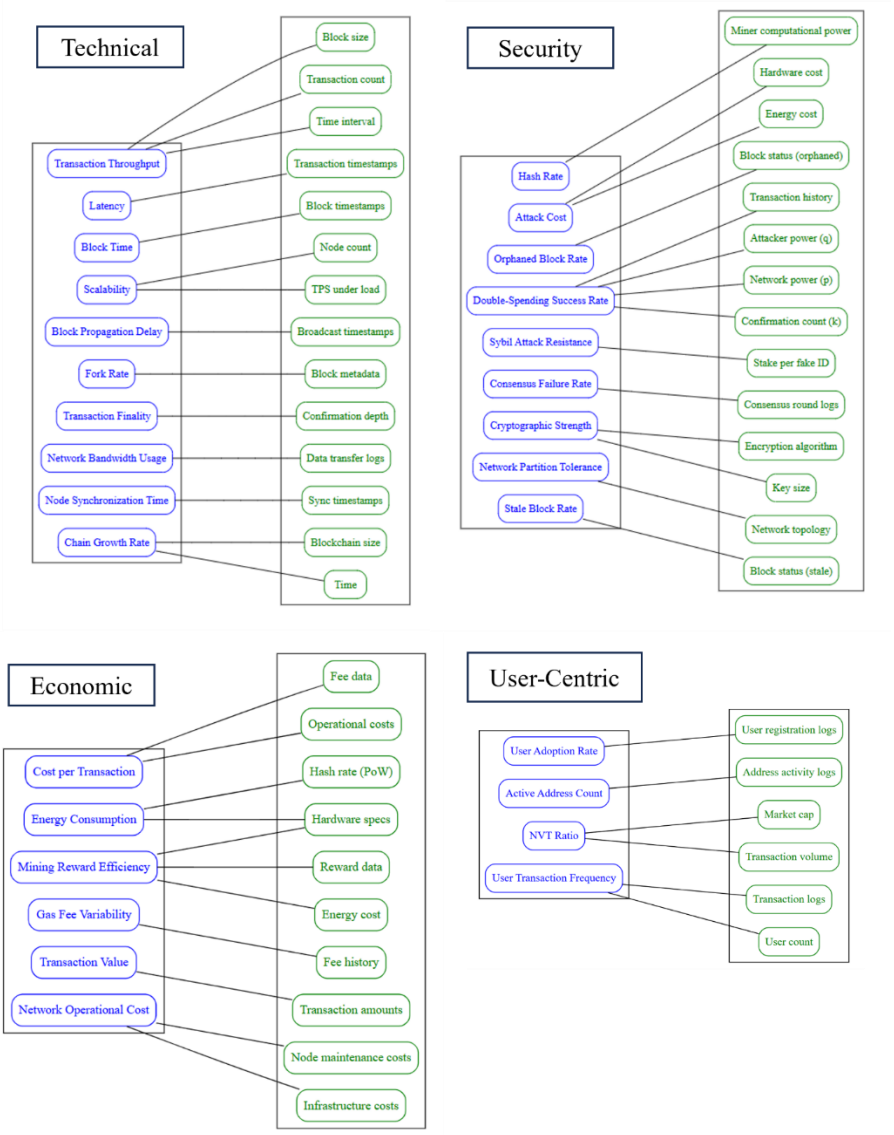

Figure 3 Bipartite Graph for Mapping of KPIs to Blockchain Features

3.3. Domain-Specific KPIs and Features

We analyzed 30 specialist studies to derive domain-specific KPIs tailored to applications such as supply chain management, IoT, smart contracts, and industrial systems. Table 4 lists these KPIs, their formulas or measurement approaches, and contextual details (application, time horizon, blockchain type), addressing RQ1. Table 5 details the blockchain features required for their measurement, addressing RQ2.

We highlight four interpretive patterns that help readers navigate this domain-specific taxonomy.

Pattern 1 – Technical vs. non-technical split: Some KPIs (e.g., Throughput, Gas Consumption) are direct analogs of general KPIs from Table 2; others (e.g., Transparency, User Satisfaction) require qualitative or composite measures. Look for the "Formula / Measurement Approach" column in Table 4 to distinguish quantitative formulas from qualitative checklists.

Pattern 2 – Overlapping KPIs across domains: Throughput appears in IoT, industrial systems, and protocol efficiency studies [35], [51]. Table 4 consolidates such overlaps to avoid redundancy – when you see a KPI labeled "recurring," it means the same measurement approach applies across multiple domains.

Pattern 3 – Time horizon matters: Short-term KPIs (e.g., Access Latency) capture real-time performance; long-term KPIs (e.g., Sustainability Score) require trend data over weeks or months. Table 4's "Time Horizon" column tells you whether to sample second-by-second or aggregate monthly.

Pattern 4 – Emerging vs. established: The bottom rows of Table 4 introduce conceptual KPIs for DeFi, NFTs, and Web3 that lack standardized formulas. These are flagged as "preliminary" – researchers should treat them as research gaps rather than ready-to-use metrics.

1) Discussion of Domain-Specific KPIs: Table 4 presents domain-specific KPIs tailored to blockchain applications such as supply chain management, IoT, smart contracts, industrial systems, and transaction networks. In supply chain applications, metrics such as Delivery Time, Transparency, and Delivery Accuracy support logistics monitoring and traceability [2], [3]. IoT environments emphasize Throughput, End-to-End Delay, and Access Latency to ensure scalable and responsive device coordination [4]. Smart contract platforms rely on KPIs including Gas Consumption, Contract Execution Time, and Vulnerability

Count to evaluate execution efficiency and security [49]. Industrial systems prioritize metrics such as System Reliability and Response Time to support operational stability [11].

Several KPIs recur across domains, particularly Throughput, Latency, and Scalability, although their interpretation varies depending on application context. Technical KPIs are generally associated with measurable protocol behavior, whereas non-technical KPIs, such as Transparency, Sustainability Score, and User Satisfaction, often rely on qualitative or composite assessments [3]. Emerging applications, including mobile gaming and transaction network analysis, introduce additional KPIs reflecting the evolving scope of blockchain ecosystems [21], [52].

Table 5 maps domain-specific KPIs to the blockchain features required for their measurement. Frequently reused features include transaction timestamps, audit trails, smart contract execution logs, and consensus records. Technical KPIs primarily rely on on-chain protocol data, whereas non-technical KPIs often require external or qualitative information, such as user feedback and survey data [21], [32]. This mapping supports traceable KPI measurement across public, private, and hybrid blockchain systems while reducing redundant instrumentation requirements.

Table 4. Domain-Specific Blockchain KPIs
(T: Technical, NT: Non-Technical)

Values are approximate and depend on network status; e.g., Bitcoin's hash rate exceeded 500 EH/s in 2023 [12].

Ref.	Application	Time Horizon	Type	KPI (T/NT)	Formula/Approach
[2], [24]	Supply chain	Short-term	Private	Delivery Time (T)	$T_{confirm} - T_{submit}$
[2], [24]	Supply chain	Short-term	Private	Transaction Success Rate (T)	$(\frac{Successful\ Tx}{Total\ Tx}) \times 100\%$
[2]	Supply chain	Short-term	Private	Confirmation Time (T)	$T_{confirm} - T_{start}$
[26], [27], [31]	Consensus scalability	Long-term	Public	Consensus Speed (T)	$T_{consensus} - T_{proposal}$
[27], [31]	Consensus scalability	Long-term	Public	Fault Tolerance (T)	$(\frac{Tolerated\ Failures}{Total\ Nodes}) \times 100\%$
[27], [31]	Consensus scalability	Long-term	Public	Energy Consumption (T)	$\frac{Total\ Energy}{Total\ Tx}$
[27]	Consensus scalability	Long-term	Public	Scalability (T)	$\frac{\Delta Throughput}{\Delta Nodes}$
[7], [8]	Smart contracts	Short-term	Private	Contract Execution Time (T)	$T_{complete} - T_{start}$
[7]	Smart contracts	Short-term	Private	Code Complexity (T)	$\sum Decision\ Points$
[7], [11], [51]	Smart contracts	Short-term	Private	Transaction Rate (T)	$\frac{Total\ Tx}{Time}$
[41], [8]	Smart contracts	Short-term	Private	CPU Usage (T)	$\frac{CPU\ Cycles}{Tx}$
[41]	Smart contracts	Short-term	Private	Memory Consumption (T)	$\frac{Memory}{Tx}$
[8]	Smart contracts	Short-term	Public	Gas Consumption (T)	$\sum Gas\ Units$
[8]	Smart contracts	Short-term	Public	Vulnerability Count (T)	$\sum Vulnerabilities$
[17], [3], [10]	Industrial systems	Long-term	Public	System Reliability (T)	$(\frac{Uptime}{Total\ Time}) \times 100\%$
[9], [10], [11]	Industrial systems	Long-term	Public	Response Time (T)	$T_{response} - T_{request}$
[35], [51]	Industrial systems	Long-term	Public	Throughput (T)	$\frac{Total\ Tx}{Time}$
[4], [5], [51]	IoT	Short-term	Public	End-to-End Delay (T)	$T_{confirm} - T_{initiate}$
[4], [35]	IoT	Short-term	Public	Throughput (T)	$\frac{Total\ Tx}{Time}$
[34], [5]	IoT	Long-term	Public	Access Latency (T)	$T_{access} - T_{request}$
[34], [5], [21]	IoT	Long-term	Public	Scalability (NT)	$\frac{\Delta Throughput}{\Delta Devices}$
[16]-[3]	Supply chain	Long-term	Hybrid	Transparency (NT)	$(\frac{Auditable\ Tx}{Total\ Tx}) \times 100\%$
[16]	Supply chain	Long-term	Hybrid	Data Integrity (NT)	$(\frac{Unmodified\ Tx}{Total\ Tx}) \times 100\%$
[16], [24]	Supply chain	Long-term	Hybrid	Transaction Success Rate (NT)	$(\frac{Successful\ Tx}{Total\ Tx}) \times 100\%$
[11], [22]	Protocol efficiency	Long-term	Private	Throughput (T)	$\frac{Total\ Tx}{Time}$
[11], [51]	Protocol efficiency	Long-term	Private	Resource Consumption (T)	$\sum CPU, Memory, Bandwidth$
[31], [33]	Consensus performance	Long-term	Private	Consensus Time (T)	$T_{final} - T_{start}$
[31], [33]	Consensus performance	Long-term	Private	Fault Tolerance (T)	$(\frac{Tolerated\ Failures}{Total\ Nodes}) \times 100\%$
[9], [5]	Industrial IoT	Long-term	Private	Energy Efficiency (T)	$\frac{Total\ Tx}{Total\ Energy}$
[9], [5], [11]	Industrial IoT	Long-term	Private	Response Time (T)	$T_{response} - T_{request}$
[22], [51]	Vehicle data	Long-term	Public	Throughput (T)	$\frac{Total\ Tx}{Time}$
[22]	Vehicle data	Long-term	Public	Access Speed (T)	$T_{retrieve} - T_{request}$
[5], [21], [23]	Real-time monitoring	Short-term	Public	Latency (T)	$T_{confirm} - T_{submit}$
[23]	Real-time monitoring	Short-term	Public	System Stability (T)	$\frac{\sigma(Throughput)}{Avg\ Throughput}$
[17], [3]	Supply chain	Long-term	Hybrid	Sustainability Score (NT)	$w_1 \cdot Energy\ Efficiency + w_2 \cdot Reliability$
[17], [3]	Supply chain	Long-term	Hybrid	System Efficiency (NT)	$\frac{Successful\ Operations}{Total\ Operations}$
[24]	Supply chain	Long-term	Hybrid	Delivery Accuracy (NT)	$(\frac{Accurate\ Deliveries}{Total\ Deliveries}) \times 100\%$
[52]	Transaction networks	Long-term	Public	Data Depth (T)	$\sum Unique\ Data\ Points$
[52]	Transaction networks	Long-term	Public	Pattern Detection Accuracy (T)	$(\frac{Correct\ Patterns}{Total\ Patterns}) \times 100\%$
[21], [39]	Platform selection	Long-term	Hybrid	Platform Efficiency (NT)	$\frac{Successful\ Operations}{Resource\ Cost}$
[21]	Mobile gaming	Short-term	Public	User Experience (NT)	$Qualitative: User\ satisfaction\ surveys$
[32]	System adoption	Long-term	Public	User Satisfaction (NT)	$Qualitative: User\ feedback\ scores$

Table 5. Blockchain Features Required for Domain-Specific KPI Measurement

(T: Technical, NT: Non-Technical)

Ref.	KPI (T/NT)	Required Blockchain Features
[2], [24]	Delivery Time (T)	Transaction timestamps (submit, confirm)
[2], [24]	Transaction Success Rate (T/NT)	Transaction status logs, confirmation events
[2]	Confirmation Time (T)	Transaction timestamps (start, confirm)
[26], [27], [31]	Consensus Speed (T)	Consensus round timestamps (proposal, consensus)
[27], [31]	Fault Tolerance (T)	Node status logs, consensus parameters
[27], [31]	Energy Consumption (T)	Hash rate (PoW), node count (PoS), hardware specs
[27]	Scalability (T)	Node count, throughput logs under load
[7], [8]	Contract Execution Time (T)	Gas usage logs, smart contract event timestamps
[7]	Code Complexity (T)	Smart contract source code, gas consumption metrics
[7], [11], [51]	Transaction Rate (T)	Transaction count, time interval
[41], [8]	CPU Usage (T)	Node resource logs (CPU cycles), gas metrics
[41]	Memory Consumption (T)	Node resource logs (memory allocation), gas metrics
[8]	Gas Consumption (T)	Gas usage logs, transaction operation details
[8]	Vulnerability Count (T)	Smart contract audit logs, vulnerability scan reports
[17], [3], [10]	System Reliability (T)	Node uptime logs, failure event records
[9], [10], [11]	Response Time (T)	Transaction request/response timestamps
[11], [22], [51]	Throughput (T)	Block size, transaction count, time interval
[4], [5], [51]	End-to-End Delay (T)	Transaction timestamps (initiate, confirm), network latency data
[35], [51]	Throughput (T)	Block size, transaction count, time interval
[34], [5]	Access Latency (T)	Access request/response timestamps, smart contract logs
[34], [5], [21]	Scalability (NT)	Device count, throughput logs under load
[16]-[3]	Transparency (NT)	Audit trails, transaction history, public ledger data
[16]	Data Integrity (NT)	Transaction hashes, tamper-proof logs
[16], [24]	Transaction Success Rate (NT)	Transaction status logs, confirmation events
[35], [51]	Throughput (T)	Block size, transaction count, time interval
[35], [11], [51]	Resource Consumption (T)	Node resource logs (CPU, memory, bandwidth)
[31], [33]	Consensus Time (T)	Consensus round timestamps, protocol logs
[31], [33]	Fault Tolerance (T)	Node status logs, consensus parameters
[9], [5]	Energy Efficiency (T)	Transaction count, energy consumption logs (kWh)
[9], [5], [11]	Response Time (T)	Transaction request/response timestamps
[11], [22], [51]	Throughput (T)	Block size, transaction count, time interval
[22]	Access Speed (T)	Data request/retrieval timestamps
[5], [21], [23]	Latency (T)	Transaction timestamps (submit, confirm)
[23]	System Stability (T)	Throughput logs, load variation data
[17], [3]	Sustainability Score (NT)	Energy consumption logs, reliability logs, transaction success rate
[17], [3]	System Efficiency (NT)	Operation logs, resource usage data
[24]	Delivery Accuracy (NT)	Delivery confirmation logs, transaction records
[52]	Data Depth (T)	Transaction metadata, unique data point logs
[52]	Pattern Detection Accuracy (T)	Transaction pattern logs, verification records
[21], [39]	Platform Efficiency (NT)	Operation logs, resource cost metrics
[21]	User Experience (NT)	User feedback logs, satisfaction survey data
[32]	User Satisfaction (NT)	User feedback logs, satisfaction score data

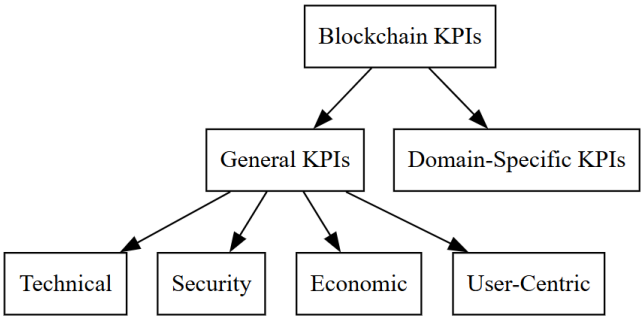

Figure 4. Taxonomy Diagram of Blockchain KPIs

4. DISCUSSION AND RECOMMENDATIONS

4.1. Innovation and Comparison with Prior Work

To our knowledge, this is the first systematic review to integrate both general and domain-specific blockchain KPIs into a unified, traceable taxonomy, addressing a critical gap where prior efforts lacked cross-domain frameworks [19]. The study adopts the Kitchenham (2007) framework with a rigorous two-phase screening and strict inclusion/exclusion criteria, ensuring methodological robustness and reproducibility [20]. Prior surveys have only partially addressed this challenge. For example, Fan et al. [3] provided a systematic survey of blockchain performance evaluation but concentrated mainly on benchmarking methods without offering a structured taxonomy of KPIs. Similarly, Zheng et al. [5] focused on performance and security challenges, yet their KPI coverage remained fragmented and descriptive. Belotti et al. [19] examined a narrow set of consensus-related KPIs, while Tonelli et al. [7] restricted their analysis to smart contract metrics. In contrast, our review synthesizes 30 general KPIs (covering technical, security, economic, and user-centric dimensions) together with domain-specific KPIs from five major application domains (supply chain [3], IoT [5], smart contracts [8], industrial systems [10], and transaction networks [52]).

This dual contribution—a standardized taxonomy of KPIs and their measurable blockchain features—directly addresses RQ1 and RQ2 and provides a more comprehensive and actionable framework than prior reviews. For RQ1, the taxonomy of 30 general

KPIs (technical, security, economic, user-centric) and domain-specific KPIs provides a holistic framework for performance assessment [25]. For RQ2, mapping features like transaction timestamps [24], audit trails [3], and consensus logs [27], ensures practical implementation across public, private, and hybrid systems [21], [36]. This dual contribution establishes a standardized approach for optimizing blockchain design.

4.2. Analysis of Domain-Specific Overlaps and Differences

The interplay between general and domain-specific KPIs reveals context-dependent interpretations rather than redundancy, highlighting the need for tailored prioritization. For instance, supply chain systems studied in [2], adopt Delivery Time as a latency-related KPI to ensure timely logistics, whereas IoT networks emphasize Throughput for large-scale device interaction and scalability [5]. Smart contract platforms like Ethereum [8] instead focus on Gas Consumption, reflecting execution cost efficiency rather than transaction speed.

Although KPIs such as Throughput, Latency, and Scalability appear both in the general taxonomy (Table 1) and in domain-specific contexts (Table 3), their meanings diverge across applications. Transaction Throughput (TPS) generally measures protocol-level performance [28], but in IoT it captures device-driven transaction capacity [5], and in smart contracts it manifests as transaction execution rate [11]. Similarly, Latency is broadly defined as confirmation delay [28], but in supply chains it is expressed as Delivery Time [2], [24], and in consensus mechanisms it corresponds to Consensus Speed [27], [31]. Transparency refers to product traceability in supply chains [16], [24], while in smart contracts it denotes source code availability and auditability [7], [8]. Likewise, Scalability in public blockchains measures node capacity [18], but in IoT it relates to the ability to accommodate growing numbers of connected devices [34]. Finally, Energy Consumption—a critical sustainability KPI in PoW systems (≈700 kWh per transaction [27], [30], with the value varying according to network conditions and time)—is reframed as node-level efficiency in IoT deployments [9].

These variations demonstrate that domain-specific KPIs extend, refine, or reinterpret general metrics rather than duplicating them, underscoring the importance of contextualized KPI frameworks for optimizing blockchain performance in different application domains. Table 6 illustrates this by comparing general blockchain KPIs with their domain-specific adaptations in various sectors. Figure 5 is a comparative visualization of KPI priorities in IoT, Smart Contracts, and Supply Chain domains as a radar graph.

Table 6 Mapping of General KPIs to Domain-Specific Equivalents and Priority Differences

General KPI	Domain-Specific Equivalent	Priority Differences
Transaction Throughput (TPS)	IoT: Throughput [4],[5],[22] Smart Contracts: Transaction Rate [7], [11], [51] Supply Chain: Transaction Success Rate [2], [24]	Critical in IoT for high device transaction volumes; secondary in Smart Contracts, where Gas Consumption is prioritized; moderate in Supply Chain, focusing on reliability.
Latency	IoT: Access Latency [34], [5] Smart Contracts: Contract Execution Time [7], [8] Supply Chain: Delivery Time [2], [24]	Critical in Supply Chain for real-time tracking; moderate in IoT for device responsiveness; lower in Smart Contracts, where execution cost is key.
Transparency	IoT: Not typically emphasized [4], [5] Smart Contracts: Code Transparency [7], [8] Supply Chain: Transaction Transparency [16], [24], [3]	Essential in Supply Chain for traceability; important in Smart Contracts for trust in code; less prioritized in IoT, where scalability dominates.
Scalability	IoT: Device Scalability [34], [5], [21] Smart Contracts: Not typically emphasized [7], [8] Supply Chain: System Efficiency [17], [3]	Critical in IoT for large-scale device networks; moderate in Supply Chain for operational growth; lower in Smart Contracts, where security is prioritized.
Energy Consumption	IoT: Energy Efficiency [9], [5] Smart Contracts: Gas Consumption [41], [8] Supply Chain: Sustainability Score [17], [3]	Critical in IoT for low-power devices; high in Smart Contracts for cost efficiency; moderate in Supply Chain, balancing sustainability with reliability.

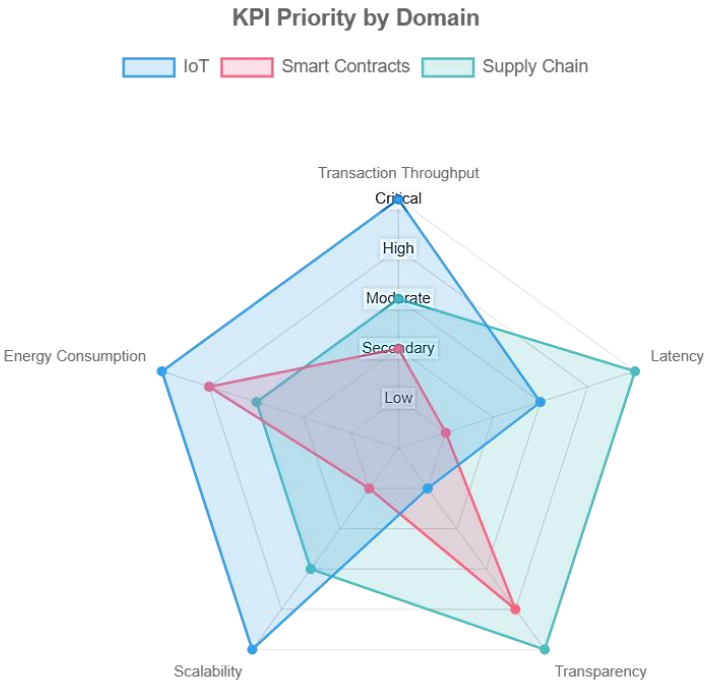

Figure 5. KPI Priorities across IoT, Smart Contracts, and Supply Chain Domains

4.3. Challenges and Needs

Significant challenges remain in applying blockchain KPIs consistently across domains. First, heterogeneous definitions complicate comparability; for instance, Throughput is reported as transactions per second in public blockchains [28], but as operations per second in industrial contexts [10]. Such inconsistencies limit benchmarking reliability and hinder the development of reusable evaluation frameworks. Similarly, Energy Consumption is measured in kWh per transaction for PoW networks [27], yet often approximated at the node level in private systems [10], making cross-system comparisons problematic.

Second, there are measurement limitations. Many KPIs depend on blockchain-internal data (e.g., timestamps, audit trails), but others—such as real-time energy usage—require proprietary logs rarely accessible in private deployments [35]. This restricts reproducibility and calls for collaborative solutions, such as open-source monitoring tools or anonymized data sharing with network operators [21].

Third, some KPIs involve trade-offs that complicate interpretation. For example, maximizing Transaction Throughput in IoT systems [5], can sharply increase Energy Consumption [27], while minimizing Gas Costs in smart contracts [7] [8], may come at the expense of execution latency. Without multi-dimensional evaluation frameworks, such conflicts remain unresolved.

Finally, non-technical KPIs introduce subjectivity and reduce reproducibility. Indicators like Transparency [3], or User Satisfaction [32] often rely on qualitative assessments or surveys, which lack standardized protocols. Similarly, emerging domains such as mobile gaming [21] and transaction networks [52] introduce novel KPIs (e.g., User Experience, Data Depth) without validated measurement models.

Addressing these challenges requires community-driven standardization efforts (e.g., IEEE, ISO) to unify KPI definitions [20], development of automated monitoring tools for real-time measurement, and the design of cross-domain benchmarking frameworks. Moreover, new research should explicitly consider trade-offs among KPIs and expand validated metrics for emerging areas such as DeFi [32], NFTs, and Web3 applications.

Another critical challenge is the lack of standardized KPIs for emerging blockchain domains. Current frameworks predominantly address traditional contexts, leaving DeFi, NFTs, and Web3 applications underexplored. For example, while liquidity and cost efficiency are central to DeFi, no consensus exists on how to measure these indicators uniformly across protocols. NFT performance is similarly fragmented, with studies focusing on market trends rather than reproducible metrics. Without systematic definitions and measurement features, comparisons across emerging platforms remain unreliable. Addressing this gap requires collaborative efforts to establish domain-specific standards and benchmarks.

4.4. Limitations and Scope Constraints

This study has several limitations that should be acknowledged. First, data accessibility posed a challenge, as certain blockchain performance indicators—such as real-time energy consumption or private transaction logs—are rarely available in permissioned systems, limiting reproducibility [15], [35]. Second, KPI definitions across the literature are heterogeneous; for example, *Throughput* is measured either as transactions per second [1], [28] or as operations per second [10], [11], complicating direct comparisons. Third, the scope of our review was restricted to peer-reviewed, English-language publications between 2008 and April 2024, which may introduce selection bias. Moreover, the reliance on three databases (Scopus, IEEE Xplore, and Web of Science) raises the possibility of missing relevant studies outside this scope. Finally, empirical validation remains limited in emerging domains such as DeFi, NFTs, and Web3, where KPIs are still conceptual and lack standardized protocols. These limitations highlight the need for broader datasets, harmonized definitions, and future research dedicated to benchmarking KPIs across both established and emerging blockchain domains.

While our taxonomy addresses key gaps, several limitations remain. First, despite our efforts to include DApp-centric metrics (Section 4.4), the review's search strings prioritized terms like "performance metrics" and "key performance indicators," which may have systematically excluded user experience or business-oriented studies that use alternative terminology (e.g., "engagement," "retention"). Future reviews should employ broader search strategies, including gray literature and industry reports.

Second, the scope of our analysis is necessarily bounded by the peer-reviewed literature. Emerging DApp domains (e.g., Web3 gaming, decentralized social networks) often publish performance data in preprints or technical blogs that do not meet our inclusion criteria. Consequently, metrics such as Social Graph Growth Rate or Gaming Session Length remain preliminary.

Third, and most critically, our study does not empirically validate the utility or feasibility of all 30 general KPIs. The question of whether practitioners *should* use a given KPI—given trade-offs between measurement cost and insight value—is a direction for future research rather than a claim we settle here.

4.5. Filling the Blind Spot and Audience Mapping

Our analysis confirms that existing blockchain KPI taxonomies disproportionately emphasize infrastructure-layer metrics (e.g., TPS, Latency, Block Time) while neglecting application-layer indicators critical to DApp success. Table 7 presents a non-exhaustive list of commonly omitted metrics, their relevance, and the primary audience for each. These metrics are not absent from the literature; rather, they are scattered across domain-specific studies (e.g., mobile gaming [21], DeFi platforms [25]) without integration into a unified framework.

Table 7. DApp-Centric KPIs and Target Audiences

KPI	Definition	Relevance	Primary Audience
Daily Active Users (DAU)	Unique addresses interacting with a DApp per day	User engagement, token velocity	DApp developers, investors
Total Value Locked (TVL)	Aggregate value of assets deposited in DeFi protocols	Financial health, liquidity	DeFi analysts, regulators
Smart Contract Invocation Frequency	Number of times a contract is called per block/interval	Code utility, gas demand	Smart contract auditors
Retention Rate (Day 1, 7, 30)	% of users returning after first interaction	Long-term viability	Product managers
Session Duration	Time spent per user interaction	User experience, stickiness	UX researchers
Transaction Uniqueness	Ratio of distinct senders to total transactions	Sybil resistance, organic activity	Security analysts

The omission of these metrics is not accidental. Unlike node-level KPIs, DApp-level indicators often require:

- **Off-chain indexing**: DAU calculation necessitates tracking addresses across multiple blocks, which many nodes do not store historically [23].
- **Cross-platform correlation**: Retention rate requires linking wallet addresses to session logs, raising privacy concerns [32].
- **Protocol-specific definitions**: TVL calculation varies across DeFi protocols (e.g., Uniswap vs. Aave), hindering standardization [25].

4.6. Barriers to KPI Adoption

A persistent paradox in blockchain performance evaluation is that while taxonomies list dozens of KPIs, empirical studies rarely employ more than two or three [4], [7]. Our review identifies three structural reasons, which also clarify how our framework addresses each:

1. **Instrumentation Overhead**: KPIs such as Attack Cost or Sybil Attack Resistance require adversarial simulation or privileged network data, which are infeasible in live public blockchains [12], [29]. For each KPI in Table 2 and Table 4, we explicitly indicate whether measurement requires basic node logs (accessible to any operator), privileged system access (permissioned blockchains only), or simulation-based estimation (research environments). This allows practitioners to filter KPIs by implementability.
2. **Lack of Standardized Formulas**: As noted in Section 4.3, Throughput is reported inconsistently (TPS vs. operations/second) [10], [11], and Energy Consumption lacks a unified unit (kWh per transaction vs. node-level approximation) [27], [30]. We provide formula templates (Table 2) and recommend units, enabling cross-study replication.
3. **Audience Misalignment**: Infrastructure engineers prioritize TPS and Latency [18], while business stakeholders require Cost per Transaction or User Adoption Rate [25], [37]. Taxonomies that blend these without audience mapping become unusable. We introduce an "Primary Audience" column (expanded from Table 7) and a decision tree (Figure 6) guiding users to relevant KPI subsets based on their role (developer, operator, analyst, regulator).

By systematically diagnosing why most KPIs are ignored—and providing a structured selection mechanism—our framework moves beyond mere enumeration to actionable guidance.

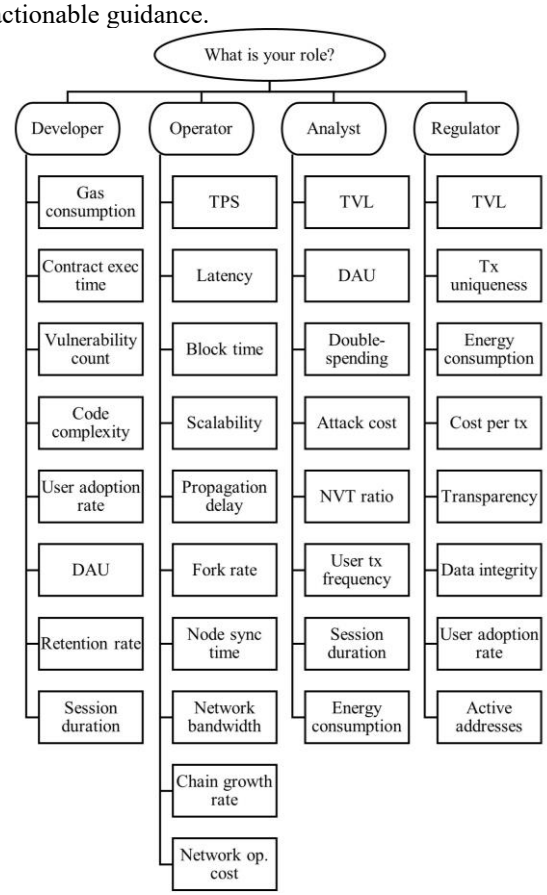

Figure 6. Decision tree for role-based KPI selection

5. CONCLUSION

This systematic review delivers a comprehensive taxonomy of blockchain KPIs, integrating 30 general KPIs and domain- specific KPIs from 55 peer-reviewed studies, addressing RQ1 and RQ2. The general KPIs enable holistic evaluation of systems like Bitcoin [1], Ethereum [14], and Hyperledger Fabric [15], while domain-specific KPIs cater to applications like supply chain [2], [3], IoT [5], [21], smart contracts [8], and industrial systems [10]. The mapped features (e.g., timestamps [2], audit trails [3], [17]) ensure practical measurement across architectures [21], [36]. Our contributions include a standardized framework, tailored domain-specific metrics, and a traceable measurement approach, bridging technical and application-specific needs.

Future research should address several directions, categorized into four areas:

- ***Hybrid Qualitative-Quantitative KPIs:*** Emerging domains such as gaming [21] and healthcare [26] require hybrid metrics that combine quantitative blockchain data (e.g., transaction latency [21], data integrity [16]) with qualitative metrics (e.g., user satisfaction surveys [32], clinical validation). For example, a gaming KPI could integrate latency with player feedback scores, weighted by application goals [21].
- ***Cost-Benefit Analysis Framework:*** Quantifying KPI trade-offs is critical for stakeholders. A framework could weight KPIs (e.g., Throughput vs. Energy Consumption [27]) based on application priorities (e.g., scalability for IoT, reliability for supply chains) and re- source constraints (e.g., hardware costs, energy budgets). For instance, optimizing TPS in IoT may increase energy costs, requiring a balanced cost-benefit model [17].
- ***Automated KPI Monitoring Tools:*** Real-time KPI evaluation requires tools integrated with blockchain nodes, supporting APIs for transaction logs, consensus data, and resource usage [21]. Desired features include scalability, real-time analytics, and cross-platform compatibility. Challenges include data privacy (e.g., anonymizing proprietary logs [35]) and computational overhead. Open-source platforms could accelerate adoption [20].
- ***Cross-Domain Benchmarking Frameworks:*** Standardized benchmarking frameworks should include unified metrics (e.g., aligning TPS [28] with Delivery Time [2]), test scenarios (e.g., stress tests for IoT [5]), and comparison protocols (e.g., public vs. private blockchains [35]). A proposed structure involves a metric repository, standardized testbeds, and open-access datasets, fostering reproducible evaluations [26].
- ***KPIs for Emerging Domains:*** Future work must extend KPI frameworks to fast-growing blockchain applications. In DeFi, this includes formalizing metrics such as *Liquidity Depth*, *Impermanent Loss*, and *Decentralization Index* [32]. For NFTs, indicators like *Transaction Uniqueness*, *Creator Royalties Stability*, and *Market Adoption Rate* are essential. In Web3 and metaverse environments, KPIs such as *Latency*, *Interoperability Index*, and *User Experience* require

rigorous definition and empirical validation. Developing and standardizing these metrics will ensure that performance evaluation frameworks remain relevant as blockchain ecosystems evolve into new digital economies.

These directions collectively address technical and non-technical dimensions—ranging from energy-intensive PoW systems [27], [30], and smart contract security [8] to non-technical KPI standardization [21], [32]—driving more robust, scalable, and user-centric blockchain adoption across both established and emerging industries.

6. ACKNOWLEDGMENT

The authors would like to express sincere gratitude to the editors and anonymous reviewers for their invaluable comments and constructive feedback, which significantly contributed to the improvement of this paper.

Declaration of generative AI in the writing processDuring the preparation of this work, the authors used ChatGPT (OpenAI) to improve the readability and language of the manuscript. After using this tool, the authors reviewed and edited the content as needed and takes full responsibility for the final content of this publication.

7. REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] Y. Madhwal, Y. Borbon-Galvez, N. Etemadi, Y. Yanovich, and A. Creazza, "Proof of delivery smart contract for performance measurements," *Ieee Access,* vol. 10, pp. 69147–69159, 2022.

[3] C. Fan, S. Ghaemi, H. Khazaei, and P. Musilek, "Performance evaluation of blockchain systems: A systematic survey," *Ieee Access,* vol. 8, pp. 126927–126950, 2020.

[4] M. Alaslani, F. Nawab, and B. Shihada, "Blockchain in IoT systems: End-to-end delay evaluation," *IEEE Internet of Things Journal,* vol. 6, no. 5, pp. 8332–8344, 2019.

[5] X. Zheng, Y. Zhu, and X. Si, "A survey on challenges and progresses in blockchain technologies: A performance and security perspective," *Applied Sciences,* vol. 9, no. 22, p. 4731, 2019.

[6] S. Alrubei, J. Rigelsford, C. Willis, and E. Ball, "Ethereum blockchain for securing the Internet of Things: practical implementation and performance evaluation," in *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 2019: IEEE, pp. 1–5.

[7] R. Tonelli, G. Destefanis, M. Marchesi, and M. Ortu, "Smart contracts software metrics: a first study," *arXiv preprint arXiv:1802.01517,* 2018.

[8] A. Pinna, S. Ibba, G. Baralla, R. Tonelli, and M. Marchesi, "A massive analysis of ethereum smart contracts empirical study and code metrics," *Ieee Access,* vol. 7, pp. 78194–78213, 2019.

[9] Y. Liu, K. Wang, Y. Lin, and W. Xu, "$\mathsf {LightChain} $: a lightweight blockchain system for industrial internet of things," *IEEE Transactions on Industrial Informatics,* vol. 15, no. 6, pp. 3571–3581, 2019.

[10] G. Bovenzi, G. Aceto, V. Persico, and A. Pescapé, "Blockchain Performance in Industry 4.0: Drivers, use cases, and future directions," *Journal of Industrial Information Integration,* vol. 36, p. 100513, 2023.

[11] B. Cao *et al.*, "When Internet of Things meets blockchain: Challenges in distributed consensus," *Ieee Network,* vol. 33, no. 6, pp. 133–139, 2019.

[12] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 3–16.

[13] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *2017 IEEE international conference on systems, man, and cybernetics (SMC)*, 2017: IEEE, pp. 2567–2572.

[14] V. Buterin, "Ethereum white paper: a next generation smart contract & decentralized application platform," *First version,* vol. 53, 2014.

[15] E. Androulaki *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the thirteenth EuroSys conference*, 2018, pp. 1–15.

[16] K. Kuhi, K. Kaare, and O. Koppel, "Ensuring performance measurement integrity in logistics using blockchain," in *2018 IEEE international conference on service operations and logistics, and informatics (SOLI)*, 2018: IEEE, pp. 256–261.

[17] A. Park and H. Li, "The effect of blockchain technology on supply chain sustainability performances," *Sustainability,* vol. 13, no. 4, p. 1726, 2021.

[18] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "Blockbench: A framework for analyzing private blockchains," in *Proceedings of the 2017 ACM international conference on management of data*, 2017, pp. 1085–1100.

[19] M. Belotti, N. Božić, G. Pujolle, and S. Secci, "A vademecum on blockchain technologies: When, which, and how," *IEEE Communications Surveys & Tutorials,* vol. 21, no. 4, pp. 3796–3838, 2019.

[20] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," *arXiv preprint arXiv:1906.11078,* 2019.

[21] G. Yang, K. Lee, K. Lee, Y. Yoo, H. Lee, and C. Yoo, "Resource analysis of blockchain consensus algorithms in hyperledger fabric," *IEEE Access,* vol. 10, pp. 74902–74920, 2022.

[22] T. Jiang, H. Fang, and H. Wang, "Blockchain-based internet of vehicles: Distributed network architecture and performance analysis," *IEEE Internet of Things Journal,* vol. 6, no. 3, pp. 4640–4649, 2018.

[23] P. Zheng, Z. Zheng, X. Luo, X. Chen, and X. Liu, "A detailed and real-time performance monitoring framework for blockchain systems," in *Proceedings of the 40th international conference on software engineering: software engineering in practice*, 2018, pp. 134–143.

[24] M. H. Meng and Y. Qian, "A blockchain aided metric for predictive delivery performance in supply chain management," in *2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, 2018: IEEE, pp. 285–290.
[25] Y. Chen and C. Bellavitis, "Blockchain disruption and decentralized finance: The rise of decentralized business models," *Journal of Business Venturing Insights,* vol. 13, p. e00151, 2020.
[26] I. Pittaras, N. Fotiou, V. A. Siris, and G. C. Polyzos, "Beacons and blockchains in the mobile gaming ecosystem: A feasibility analysis," *Sensors,* vol. 21, no. 3, p. 862, 2021.
[27] Y. Merrad *et al.*, "Blockchain: Consensus algorithm key performance indicators, trade-offs, current trends, common drawbacks, and novel solution proposals," *Mathematics,* vol. 10, no. 15, p. 2754, 2022.
[28] K. Croman *et al.*, "On Scaling Decentralized Blockchains: (A Position Paper)," in *International conference on financial cryptography and data security*, 2016: Springer, pp. 106–125.
[29] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Communications of the ACM,* vol. 61, no. 7, pp. 95–102, 2018.
[30] A. De Vries, "Bitcoin's growing energy problem," *Joule,* vol. 2, no. 5, pp. 801–805, 2018.
[31] M. Hayat and H. Winkler, "An analytic hierarchy process for selection of blockchain-based platform for product lifecycle management," *Sustainability,* vol. 14, no. 21, p. 13703, 2022.
[32] M. O. Grida, S. Abd Elrahman, and K. A. Eldrandaly, "Critical success factors evaluation for blockchain's adoption and implementing," *Systems,* vol. 11, no. 1, p. 2, 2022.
[33] Y. Hao, Y. Li, X. Dong, L. Fang, and P. Chen, "Performance analysis of consensus algorithm in private blockchain," in *2018 IEEE Intelligent Vehicles Symposium (IV)*, 2018: IEEE, pp. 280–285.
[34] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE internet of things journal,* vol. 5, no. 2, pp. 1184–1195, 2018.
[35] P. Thakkar, S. Nathan, and B. Viswanathan, "Performance benchmarking and optimizing hyperledger fabric blockchain platform," in *2018 IEEE 26th international symposium on modeling, analysis, and simulation of computer and telecommunication systems (MASCOTS)*, 2018: IEEE, pp. 264–276.
[36] J. Polge, J. Robert, and Y. Le Traon, "Permissioned blockchain frameworks in the industry: A comparison," *Ict Express,* vol. 7, no. 2, pp. 229–233, 2021.
[37] S. Bano, M. Al-Bassam, and G. Danezis, "The road to scalable blockchain designs," *USENIX; login: magazine,* vol. 42, no. 4, pp. 31–36, 2017.
[38] S. Rouhani and R. Deters, "Performance analysis of ethereum transactions in private blockchain," in *2017 8th IEEE international conference on software engineering and service science (ICSESS)*, 2017: IEEE, pp. 70–74.
[39] Z. Zhou, R. Li, Y. Cao, L. Zheng, and H. Xiao, "Dynamic performance evaluation of blockchain technologies," *IEEE Access,* vol. 8, pp. 217762–217772, 2020.
[40] J. Göbel and A. E. Krzesinski, "Increased block size and Bitcoin blockchain dynamics," in *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, 2017: IEEE, pp. 1–6.
[41] N. Ajienka, P. Vangorp, and A. Capiluppi, "An empirical analysis of source code metrics and smart contract resource consumption," *Journal of Software: Evolution and Process,* vol. 32, no. 10, p. e2267, 2020.
[42] M. Rosenfeld, "Analysis of hashrate-based double spending," *arXiv preprint arXiv:1402.2009,* 2014.
[43] J. Göbel, H. P. Keeler, A. E. Krzesinski, and P. G. Taylor, "Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay," *Performance evaluation,* vol. 104, pp. 23–41, 2016.
[44] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper,* vol. 151, no. 2014, pp. 1–32, 2014.
[45] A. Kiayias, E. Koutsoupias, M. Kyropoulou, and Y. Tselekounis, "Blockchain mining games," in *Proceedings of the 2016 ACM Conference on Economics and Computation*, 2016, pp. 365–382.
[46] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *IEEE P2P 2013 Proceedings*, 2013: IEEE, pp. 1–10.
[47] Y. Sompolinsky and A. Zohar, "Secure high-rate transaction processing in bitcoin," in *Financial Cryptography and Data Security: 19th International Conference, FC 2015, San Juan, Puerto Rico, January 26-30, 2015, Revised Selected Papers 19*, 2015: Springer, pp. 507–527.
[48] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, "Bitcoin and cryptocurrency technologies: a comprehensive introduction," ed: Princeton University Press Princeton, NJ, USA, 2018.
[49] M. Bez, G. Fornari, and T. Vardanega, "The scalability challenge of ethereum: An initial quantitative analysis," in *2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)*, 2019: IEEE, pp. 167–176.
[50] C. Burniske and J. Tatar, "Cryptoassets: The innovative investor's guide to Bitcoin and beyond," 2018.
[51] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance analysis of private blockchain platforms in varying workloads," in *2017 26th international conference on computer communication and networks (ICCCN)*, 2017: IEEE, pp. 1–6.
[52] J. Zhu, A. Khan, and C. G. Akcora, "Data depth and core-based trend detection on blockchain transaction networks," *Frontiers in Blockchain,* vol. 7, p. 1342956, 2024.

Kimiya Karimi Dehkordi received the B.S. and the M.Sc. degree in Computer Engineering from Shahrekord University. She is currently the Ph.D. student at Isfahan University. Her research interests include blockchain, smart contracts, and model-driven software engineering.
https://orcid.org/0009-0002-7120-4548
kimiya.karimi@stu.sku.ac.ir
Master graduated, Department of Computer Engineering, Faculty of Technology and Engineering, Shahrekord University, Shahrekord, Iran.

Leila Samimi-Dehkordi is an Assistant Professor in the Department of Computer Engineering at Shahrekord University, Iran. She received her B.Sc. degree in Computer Engineering from Iran University of Science and Technology, her M.Sc. degree in Algorithms and Computation from the University of Tehran, and her Ph.D. degree in Software Engineering from the University of Isfahan. Her primary research interests include model-driven software engineering, software language engineering, Blockchain modeling, and gamification. Recently, her work has extended into leveraging large language models (LLMs) and artificial intelligence for automated software modeling and system verification.
https://orcid.org/0000-0002-2842-0256
samimi@sku.ac.ir
Assistant Professor, Department of Computer Engineering, Faculty of Technology and Engineering, Shahrekord University, Shahrekord, Iran.

Abbas Horri is an Assistant Professor in the Department of Computer Engineering at Shahrekord University, Iran. He received both his M.Sc. and Ph.D. degrees in Computer Engineering (Software) from Shiraz University, Iran. His primary research interests include cloud computing, parallel architectures, green computing, and big data. His recent research also extends to resource optimization, distributed systems, and performance evaluation in cloud-edge and blockchain environments.
https://orcid.org/0000-0001-7933-9266
horri@sku.ac.ir
Assistant Professor, Department of Computer Engineering, Faculty of Technology and Engineering, Shahrekord University, Shahrekord, Iran.