

Towards Using Feasible Blockchain Technology in Enterprise Processes

Tomass Zags* and Marite Kirikova

Institute of Applied Computer Systems, Riga Technical University, 6A Kipsalas Street, Riga, LV-1048, Latvia

Abstract

Over the past decade, blockchain technology has developed significantly in technical and conceptual aspects. The goal of the paper is to provide guidelines for choosing a blockchain technology option that are suitable for the processes they support. The paper explores how blockchain is currently implemented in enterprise processes, what benefits it provides, and how organizations can evaluate technology upon its integration. It proposes using the Systems of Systems (SoS) perspective to select blockchain technology options and introduces a five-dimensional roadmap for feasibility evaluation. The paper focuses on how feasible blockchain technology can be for enterprise processes by considering structural environment compatibility, organizational readiness, technology suitability, regulatory and environmental suitability and capability-need alignment. To demonstrate the practical use of the roadmap, it is applied to an administrative user action auditing process in a financial platform. The application identifies the process closest to acknowledged SoS and selects consortium permissioned blockchain as the most suitable architecture. A local Hyperledger Fabric prototype is used to demonstrate audit record creation and hash-based verification.

Keywords

Blockchain, SoS, blockchain readiness, blockchain use cases

1. Introduction

Blockchain technology has gained popularity across many industries in recent years. Many enterprises are moving towards the digital transformation of their systems and the adoption of technologies that offer new opportunities [1]. Blockchain, as a technology that has mainly been associated with cryptocurrencies, has caught the interest of enterprises, and they often aim to integrate it into their workflow because of the popularity and hype of this technology. However, without sufficient research and understanding of blockchain capabilities, the term is often misunderstood and used and implemented inappropriately [2]. Many enterprises operate in interconnected and data-sensitive environments, which do not comply with the traditional approach of centralized systems; therefore, there is an increasing interest in such decentralized technologies as blockchain, which can support secure information sharing [3].

As already mentioned, enterprise adoption of blockchain technology remains inconsistent. Many studies highlight the benefits of blockchain implementation, such as traceability, reduced transaction costs, and trust among stakeholders, but others suggest that there are many technological and organizational challenges that must be overcome to create a proper adoption of blockchain technology [4]. Existing literature on blockchain adoption focuses on specific industries and edge cases, without clear guidelines or a structured approach to adoption, which makes it difficult for enterprises to understand how blockchain can deliver value to them. In many cases, these implementations are misaligned [5].

To address the previously mentioned gap, the goal of this paper is to develop a structured roadmap for evaluating the suitability of blockchain in organizational processes. The roadmap aims to support enterprises in determining whether blockchain provides tangible benefits compared to traditional centralized architectures, based on structural, organizational, technological, regulatory, and capability-related factors. Special attention is given to the structural factors. The hypothesis is that

Baltic DB&IS 2026 Conference Forum and Doctoral Consortium, 28 June - 1 July 2026, Tartu, Estonia

*Corresponding author. / These authors contributed equally.

✉ tomass.zags@edu.rtu.lv (T.Zags), marite.kirikova@rtu.lv (M.Kirikova)

ORCID [0000-0002-1678-9523](https://orcid.org/0000-0002-1678-9523) (M. Kirikova)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

different types of processes require corresponding types of blockchain technology. To achieve the defined goal, the following tasks (research method) are defined:

- analyze main organizational, technological, and regulatory challenges and benefits associated with blockchain adoption to identify common blockchain suitability dimensions
- investigate the Systems-of-Systems (SoS) paradigm and classify different SoS types in relation to blockchain compatibility
- identify key structural characteristics influencing blockchain feasibility
- develop a multi-dimensional blockchain technology selection roadmap
- Apply the proposed roadmap to an administrative user action auditing process and provide preliminary validation through a prototype implementation

The paper is structured as follows. Section 2 discusses the related work. Section 3 introduces a new blockchain evaluation dimension that is based on the SoS perspective. Section 4 presents the proposed roadmap, its practical application to an administrative user action auditing process, and the prototype-based preliminary validation. Section 5 concludes the paper.

2. Related work

This section briefly discusses what challenges and benefits regarding blockchain technology in organizational processes have been reported in related work. Concerning challenges, three main groups of challenges that can lead to three dimensions in blockchain suitability identification were identified and are shown in Table 1.

Table 1

Influence of blockchain challenge categories on roadmap dimensions

Challenge category	Main issue	Influence on roadmap
Organizational [2], [4], [6], [7]	Lack of governance	Leads to the Organizational Readiness dimension
Technological [1], [6], [8], [9]	Scalability, latency, integration complexity	Leads to the Technological Suitability dimension
Regulatory [7]	Compliance uncertainty, privacy, and jurisdiction	Leads to the Regulatory and Environmental dimension

To observe the interplay between the challenges and reported benefits in the adoption of blockchain technology, the overview of domains found in the literature review sources is presented in Table 2. The benefits and challenges are organized by the domain of process operation.

Table 2

Reported benefits and challenges of blockchain adoption

Domain	Key benefits	Key challenges	Examples of studies used
Supply chain	Traceability, waste reduction, transparency	Integration complexity, scalability	[10], [11]
Human resources	Secure data, trust, efficiency	Governance, skills shortage	[1], [12]
Finance	Security, settlement efficiency	Regulatory uncertainty	[9]
Industry 4.0	Automation, transparency	Latency, performance constraints	[1]

It is important to note that the practical benefits listed in the table are those companies have reported after implementing blockchain technology. We can see that the benefits and challenges differ among the domains.

Regarding the technological dimension, the perceived benefits of the use of blockchain technology can depend on the actual blockchain design approach. Table 3 summarizes the main blockchain

design approaches identified in the related work. The main goal of the table is to show which design choices have been most associated with which practical enterprise use cases (processes).

Permissioned blockchain architectures differ from publicly available and permissionless networks such as Bitcoin or Ethereum. Alternative designs adjust consensus mechanisms, access control, and governance models, which help to match industry-based and enterprise-based requirements such as privacy and regulatory compliance [13]. It helps enterprises to take more control of the design and the technology they are supposed to implement in their processes. As shown in Table 3, controlled access to the permissioned blockchain makes the technology appropriate for enterprises. In other words, enterprises are adopting frameworks where only authorized nodes validate transactions, and smart contracts are executed within a controlled environment [12].

Table 3

Classification of blockchain design approaches in enterprise contexts

Classification group	Design approach	Key characteristics	Suitable Use Cases	Examples of Sources
Governance and access approach	Permissioned blockchain	Controlled access, high throughput	Supply chain, Human resources	[13]
Platform example	Hyperledger Fabric	Private channels, configurable consensus	Logistics, enterprise	[2]
Consensus example	Proof-of-Authority	Energy-efficient, predictable	Small and medium-sized enterprise ecommerce	[14]
Governance and access approach	Public blockchain	High transparency, decentralization	Limited enterprise use	[8]
Architecture combination	Hybrid blockchain	Restricted and open characteristics	Internal control	[18]

Some of the examples found in the literature mention *Hyperledger Fabric*, which is a platform example of permissioned enterprise blockchain, as one of the open-source frameworks that uses configurable consensus mechanisms and private channels between participants [13]. This design allows supply chain-related actions to share transaction data within relevant subgroups, and it still lets an enterprise benefit from immutability, which is one of the blockchain's main qualities. Furthermore, such permissioned designs help to deliver higher throughput and more flexible privacy controls for supply chain management rather than using the Ethereum network, which is available publicly [13].

One more example worth noting is the *Proof-of-Authority* design approach mentioned in the context of small or medium-sized enterprise (SME) e-commerce platforms. In Table 3, it is mentioned as a consensus example because it is suited for controlled business settings. Furthermore, it is described as an energy-efficient process for number generation and validator rotation, as a limited number of approved validators create new blocks [14]. This approach represents the opposite of the Proof-of-Work approach, which is energy inefficient and is not as transparent when it comes to meeting the needs of enterprises for lower operational costs and predictable performance.

Hybrid blockchain is also included in Table 2.2 as an architectural combination, combining restricted internal control with selected openness. As discussed in the reviewed literature, Hybrid architectures can be useful in enterprise contexts where sensitive data must remain protected, but selected information may still need to be verified outside the internal environment [18], [19].

In summary, the reviewed literature indicated that sectors, such as supply chain management and SME e-commerce, benefit the most from alternative blockchain architectures, particularly Permissioned frameworks and Proof-of-Authority consensus mechanisms. Furthermore, similar architectural principles are also applicable in human resources management, where sensitive employee data is managed through authorized organizational roles [1]. These findings provide an enterprise-oriented view of blockchain design choices.

To summarize the differences between blockchain design approaches, Figure 1 was created as a conceptual matrix.

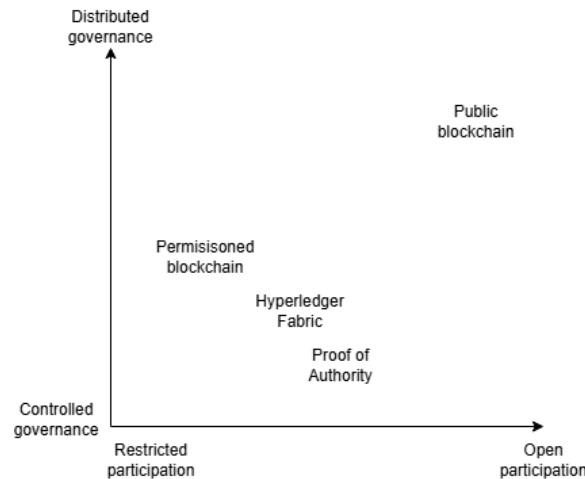


Figure 1: Conceptual summary of blockchain design approaches in enterprise contexts.

Figure 1 presents a conceptual positioning of blockchain design approaches discussed in this section according to two main dimensions: *openness of participation* and *distribution of governance*. Public blockchain is positioned in the upper-right corner of the matrix because it is characterized by open participation and decentralized validation. On the other hand, the other three design approaches examined in this section are placed below it. Permissioned blockchain is located on the left side of the figure, because participation is restricted to authorized actors and governance remains more controlled. Hyperledger Fabric is placed close to a Permissioned blockchain, as it represents the enterprise platform and is a part of the Permissioned blockchain. Proof-of-Authority was earlier mentioned as a consensus mechanism, which has predictable performance, but limited validators, which means that in Figure 1, it is shown in the middle between restricted and open participation.

The figure illustrates that enterprise-oriented blockchain solutions tend to have limited participation and controlled governance, whereas the public blockchain model shows the opposite. This suggests that Public blockchain, as the technology, can be used better in enterprise process adoption, to create an easier implementation, but Permissioned blockchain will have more controlled governance and restricted participation.

3. Structural issues of blockchain technology

In the previous section, three dimensions of blockchain adoption were considered: organizational, technological, and regulatory. It was also seen that different technological solutions are suitable in various enterprise settings. To get closer to organizational processes in particular, the question remains how to identify which kind of blockchain is more suitable for the process expected to benefit from the application of blockchain technology. To answer this question, in this paper, the SoS classification is applied. SoS is a standardized paradigm [15] suitable for distributed systems. We can assume that each agent participating in the process is a system, while all participating agents form a system of systems.

ISO/IEC/IEEE 21841:2019 standard provides a taxonomy of System of Systems to promote communication and reasoning among stakeholders by classifying SOS into four main types of systems: directed, acknowledged, collaborative, and virtual [15].

Directed SoS is the type of system where the central authority, which in this case is stakeholders or the enterprise board, is responsible for coordination and can make decisions on constituent systems, which are part of the SoS [15]. In this case, trust mechanisms are already centralized; adding an additional blockchain layer may introduce unnecessary architectural overhead rather than creating an optimized solution and solving the coordination problem. A representative example of a directed SoS in the NexGen US Air Traffic Management System, where constituent systems operate under centrally managed requirements and coordination [16]. In directed SoS, blockchain's

feasibility is lower, useful only if external stakeholders or systems must share coordination among the SoSs.

In addition, directed SoS are usually associated with the environment, in which the overall purpose, operation priorities, and system evolution are governed by one dominant entity [16]. In these specific cases, constituent systems will have technical independence due to not having any external entities that may conflict with each other [16]. On the other hand, with centrally defined requirements and operational logic, directed SoS may become a subject of a larger SoS [16]. This means that coordination, accountability, and conflict resolution are managed through hierarchy in the organization, without using trust mechanisms that blockchain may provide. In addition, for enterprise process analysis, this part becomes important because blockchain generally provides less additional value in single-authority environments, as coordination and trust are already managed through centralized governance. *Therefore, in directed SoS, blockchain should be considered when a centralized structure governed by a single authority interacts with external actors that require shared verification and transparency.*

Acknowledged SoS differs from directed by two core parts – constituent systems need to have managerial independence, and the central authority lacks complete control of the systems, even though objectives are recognized at the SoS level [15]. A smart city can be considered an acknowledged SoS because a central coordinating body may define city-level objectives, while, e.g., transport, health, and energy systems remain independently managed [16]. This governance structure aligns with the previously mentioned Permissioned architectures, which give enterprises stronger control over the current systems. Maintaining a shared state among independent parties is one of the key benefits of acknowledged SoS in the blockchain context. In feasibility assessment terms, this type of SoS reflects supply-chain and regulated multi-organizational networks, where blockchain can provide shared integrity without full commitment to a centralized approach.

One more feature of acknowledged SoS is that coordination depends on influence and negotiated agreements, rather than on absolute authority [16]. Although a central manager exists and goals in the context of SoS are defined, the participating constituent systems still operate based on their own defined ownership structures and strategic interests [16]. This creates a governance environment in which shared decision-making is required to control all processes. From the blockchain feasibility perspective, such environments are relevant because they require a mechanism that enables trusted coordination without excluding participant independence. This is one of the main reasons why *acknowledged SoS are one of the most suitable contexts for enterprise blockchain adoptions, especially where several organizations share a common view of the processes and, at the same time, are independent in maintaining their own local systems.*

Collaborative SoS lacks a single central authority; most constituent systems cooperate voluntarily to achieve agreed-upon goals while maintaining operational and managerial independence [15]. The global finance system represents a collaborative SoS, as multiple organizations coordinate through shared standards and protocols without being dependent on a single authority [16]. This structure aligns with blockchain's distributed governance, especially when participants do not fully trust any external parties as intermediaries. In this context, blockchain will act as a shared trust layer that supports reliable data exchange and reduces reliance on external systems in cross-organizational processes [17]. In addition, this layer of SoS would benefit the supply chain and human resources fields, as sensitive data is being transferred to fulfill the organizational cycle.

In inter-organizational environments, collaborative SoS are important because participants are mostly in equal positions and none of them can impose a unified governance structure on the others [16]. In this case, interaction is maintained through mutually accepted agreements that allow constituent systems to cooperate while still pursuing their local objectives [16]. When coordination in collaborative SoS becomes more difficult, no single authority enforces shared process rules. Blockchain can become valuable precisely because it provides a distributed mechanism for shared validation, traceability, and rule governance. As a result, *collaborative SoS represents one of the strongest justifications for blockchain adoption in enterprise contexts.* Based on the previous mention, financial and cross-organizational verification processes are the most applicable.

Virtual SoS are characterized by the absence of centralized governance and the lack of clearly shared objectives [15]. Blockchain, by its nature, can operate in decentralized conditions, but when

the system is chaotic, feasibility is limited, because there is no stable governance structure defining responsibilities and participation. A crisis management system illustrates a virtual SoS, because participating systems and actors interact dynamically without a stable central governance structure or predefined system composition [16]. In the organizational process context, a weak governance baseline can prevent blockchain from delivering practical and theoretical value. This issue was mentioned in Section 2, where governance was stated as a required part for positive blockchain adoption.

Another important aspect of virtual SoS is that large-scale behavior may still emerge even though no central authority and objectives exist [16]. The absence of a governance structure creates a mismatch in the adoption of blockchain. Virtual systems in this context may seem like unstructured systems, but a better explanation would be that coordination mechanisms are invisible, and protocols are loosely recognized when systems interact through them [16]. However, from the perspective of enterprise blockchain feasibility, this type of system is problematic. Enterprise processes, generally, require ownership of decisions, responsibility boundaries, and a clear governance structure for effective blockchain technology implementation. Blockchain can create decentralization, but it might not create meaningful organizational value. *Technically, in virtual SoS, it will be hard to use an enterprise process with blockchain technology*, but it can be useful to consider this type of SoS to understand the differences between other types of SoS.

Figure 2 summarizes the above-discussed issues, showing the line of reasoning for the suitability of blockchain technology, in general, for processes corresponding to specific types of SoSs.

The strongest compatibility arises in situations where SoS and blockchain architecture governance models align with each other. The whole comparison reflects that the governance structure is the main factor influencing blockchain suitability. Acknowledged SoS and collaborative SoS are the main types of successful blockchain implementation, due to their support for shared or decentralized coordination among independent actors. On the other hand, directed SoS and virtual SoS are less suitable for blockchain feasibility, as they rely on centralized governance, and clearly defined responsibilities are absent.

In summary, the figure illustrates that blockchain feasibility increases as the need for distributed coordination grows but decreases when governance is fully centralized or insufficiently defined. To be more specific, the different factors characterizing SoS can be analyzed in more detail with respect to the features of different types of blockchain technologies.

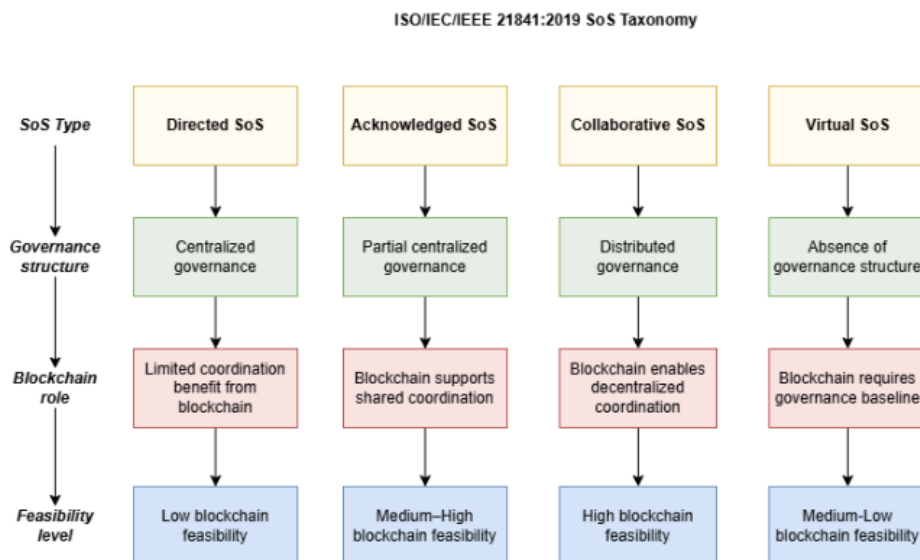


Figure 2: SoS taxonomy and blockchain compatibility (governance).

A common classification in the literature distinguishes between public, private, and consortium blockchains [18], while more recent work also identifies hybrid blockchain as an additional category [19]. Public blockchains are generally characterized as open and permissionless, Private blockchains as centrally controlled and permissioned, and Consortium blockchains as partially decentralized, governed by multiple actors [18]. Hybrid architectures, on the other hand, combine public and

private blockchain models to overcome scalability and usability limitations [18]. Figure 3 illustrates compatibility between the types of SoS and the types of blockchain technology. Deeper discussion regarding the shown strengths of compatibility is beyond the scope of this paper.

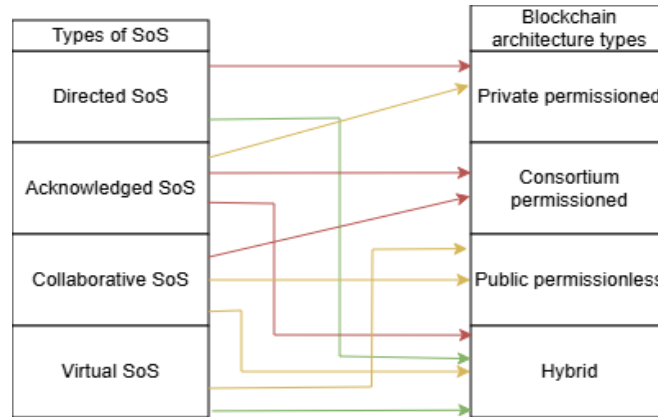


Figure 3: Conceptual compatibility mapping between SoS types and blockchain architecture types (Green – weak compatibility, Yellow – moderate compatibility, Red – strong compatibility).

4. Towards the roadmap for choosing the feasible blockchain technology

Respecting the related work on blockchain adoption discussed in Section 2 and considering the SoS perspective in analyzing blockchain suitability for organizational processes, we propose a roadmap for analyzing blockchain feasibility for selected organizational processes that considers the feasibility via the following 5 dimensions:

- Dimension 1 – Structural environment compatibility
- Dimension 2 – Organizational readiness
- Dimension 3 – Technology suitability
- Dimension 4 – Regulatory or Environmental suitability
- Dimension 5 – Capability and Need alignment

Dimensions 2 to 4 were derived from related work discussed in Section 2 as well as from additional sources such as [20]–[22]. Dimension 1 emerged when analyzing Dimension 3, considering not just blockchain technology as such, but looking closer at possible technological solutions. This revealed a new essential dimension of the feasibility that requires specific analysis of the processes supposed to be supported by the blockchain technology first, and only then consider the rest of the factors, keeping in mind the potential feasibility of specific technological solutions. Thus, the roadmap prescribes.

Regarding *Dimension 1– Structural environment compatibility*, the issues reflected in Figs. 2 and 3 shall be considered, and the processes analyzed regarding the factors reflected in the rows (basic characteristics of SoS) of Table 4. For easier identification of the type of SoS the process belongs to, the model reflected in Figure 4 can be used.

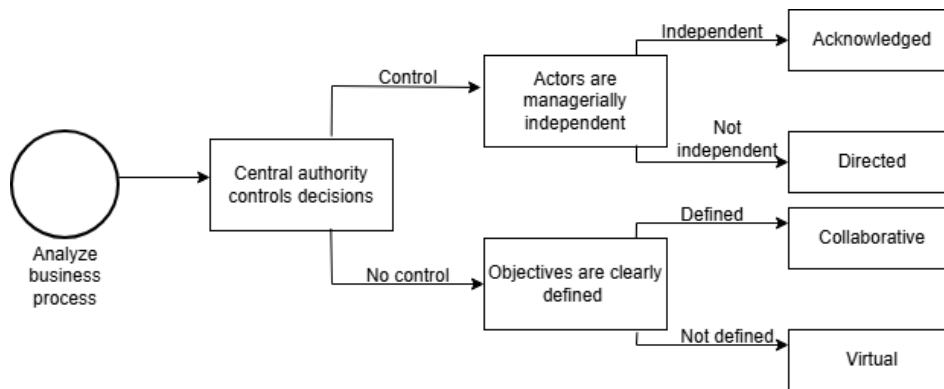
Regarding *Dimensions 2 – Organizational readiness*, based on the literature review [16], [20], the following evaluation factors were selected because they reflect the most frequently emphasized organizational conditions for successful blockchain adoption:

- Strategic alignment
- Clear governance structures
- Financial and human resources
- Proven technical expertise
- Willingness to adapt existing processes

Table 4

Structural characteristics of SoS and implications for blockchain compatibility

Structural characteristic	Description in SoS context [16]	Coordination challenge	Blockchain Implication
Operational independence	Constituent systems operate independently, provide value without central coordination	Autonomous actors complicate centralized coordination and data control.	Distributed consensus mechanisms allow agreement without a single authority.
Managerial independence	Systems are governed by different organizations with their own objectives	Multiple governance structures obstruct decision-making	Permissioned blockchain networks enable shared governance and controlled participation.
Geographic distribution	Systems are physically and logically dispersed across locations	Distributed actors require reliable synchronization and trusted data exchange	Shared distributed ledgers ensure consistent records across participants.
Emergent behavior	System-level outcomes arise from interactions between constituent systems	Dynamic interactions are difficult to coordinate centrally.	Smart contracts can automate cross-organizational interactions.
Evolutionary development	Constituent systems evolve independently over time	Continuous system evolution can affect interoperability.	Blockchain governance mechanisms must support upgrades and adaptability.

**Figure 4:** SoS classification decision model.

Dimension 3 – Technology suitability, evaluates whether the technical requirements of a given enterprise process align with the capabilities and limitations of blockchain systems. The evaluation aspects in this dimension were derived from the recurring technological limitations identified in the literature [23], [24], especially performance constraints, security risks, smart contract complexity, and integration requirements [21]. These aspects provide the basis for the consideration of the following assessment factors:

- Required transaction throughput and system scalability
- Necessity for immutable and auditable records
- Data security and data integrity requirements
- Smart contract automation relevance
- Complexity of integration with existing enterprise systems

Dimension 4 – Regulatory or Environmental suitability reflects that regulatory and environmental conditions significantly influence blockchain feasibility. In the related work, it was highlighted that regulatory uncertainty and compliance complexity are major barriers in the fields of supply-chain and finance [6]. Compliance requirements may limit the implementation of fully decentralized architectures [22]. The following assessment factors can be used in this dimension:

- Clarity of applicable legal frameworks

- Data protection and privacy compliance implications
- Specific field regulatory requirements
- Cross-border operational considerations
- Risk exposure

Dimension 5 – Capability and Need alignment is needed as Blockchain technology offers distinct capabilities, such as decentralization, immutability, transparency, and programmable automation, are mutually related and may not generate value if concrete operational needs are not aligned [20], [24]. The evaluation factors in this dimension were selected to test whether blockchain technology's usefulness is unclear, resources are limited, or current systems are sufficient [20]:

- Dependence on intermediaries for transaction validation
- Benefits of automation through smart contract implementation
- Requirement for immutable records
- Need for increased transparency and traceability
- Presence of distrust between actors

The dimensions are intended to be applied in a particular sequence rather than as a general checklist. The structural environment compatibility dimension is evaluated first, because it determines whether blockchain is structurally justified for the process. If the process does not involve multiple actors, partial independence, or shared coordination needs, blockchain should not be treated as the primary solution. If the process satisfies these structural conditions, the remaining dimensions are used to compare feasible blockchain architecture options.

Table 5 clarifies how the roadmap can be used in practice. Each phase has a guiding question and produces an output that becomes the input of the following phase. The roadmap functions as a filtering mechanism; it can lead to the selection of a blockchain architecture, but it can also indicate that blockchain is not recommended for a given process. Phases 1-3 refer to Dimension 1, Dimensions 2-3 are applied in Phase 4, and Dimension 3 refers to Phase 5.

The proposed roadmap was applied to an administrative user action auditing process on a financial platform. The process was selected because audit information was distributed across several mechanisms, and no single canonical audit record was available. That led to a problem, as historical integrity could not be fully verified. The application followed the roadmap phases from structural assessment to final architecture selection, as summarized in Table 6.

A prototype of an audit layer was then implemented using a local Hyperledger Fabric test network. The prototype stored audit metadata and a payload hash on the ledger while keeping detailed operational data off-chain. Two administrative user actions were tested: completion of email verification and disabling two-factor authentication. For each action, the backend created a local audit reference in the database and submitted the corresponding payload hash to the ledger. During verification, the system compared the payload hash stored in the database with the hash stored on the ledger. The verification result was positive when both values matched, confirming that the local audit reference matched the ledger proof. The next step was testing tamper-evidence. The payload hash in the database was manually changed, and the verification was repeated. In this case, the database hash no longer matched the ledger hash, and the verification returned a negative result. This shows that the prototype does not make the database impossible to modify, but it does make such modifications detectable by comparing them with the ledger record. This preliminary validation shows that the roadmap can lead to a concrete architecture decision and that the selected architecture can support tamper-evident audit verification.

5. Conclusion

The goal of the paper was to establish a background for creating a roadmap to support process owners in their decisions regarding blockchain technology adoption.

Table 5

Practical application logic of the roadmap

Phase	Main question	Output
Phase 1. Structural assessment	Does the process involve multiple actors or systems with shared coordination needs?	SoS-like or primarily centralized process
Phase 2. SoS classification	Which SoS type best describes the process?	Dominant SoS type
Phase 3. Architecture narrowing	Which blockchain architectures fit the identified SoS type?	Retained architecture candidates
Phase 4. Feasibility evaluation	Do retained architectures fit organizational, technical, regulatory, and capability needs?	Comparative suitability result
Phase 5. Final selection	Which architecture provides the strongest overall fit?	Selected architecture or decision not to use blockchain

Table 6

Preliminary application of the roadmap to administrative user action auditing

Roadmap Phase	Result in the application example
Structural assessment	The process was treated as SoS-like because it involves business-side administrators, backend services, database storage, and technical maintenance roles contributing to a shared audit outcome.
SoS classification	The process was classified as closest to acknowledged SoS because a central business environment exists, but technical and operational actors have partial independence
Architecture narrowing	Consortium permissioned and hybrid blockchain were retained as compatible candidates
Feasibility evaluation	Consortium permissioned blockchain showed stronger alignment with controlled participation, auditability, data protection and historical integrity verification.
Final selection	Consortium permissioned blockchain was selected as the most suitable architecture

The key findings show that blockchain technology brings vital benefits in supply chain management, human resource management, and e-commerce processes. Traceability, enhanced transparency, efficiency, and strengthened trust mechanisms are among the key benefits. However, some benefits can be expected only in specific cases, where process requirements and organizational objectives are clearly defined.

The review of related work highlights that, alongside the benefits, there are many challenges to adopting blockchain technology. The challenges include evaluating capabilities and limitations, addressing governance issues, and assessing enterprise readiness before deployment. It is also problematic to evaluate implementation options without proper research beforehand, and using the wrong option may make the technology's use irrelevant. Not addressing these challenges can lead to poor performance and the incorrect application of blockchain capabilities.

Given these challenges, the paper proposes a preliminary roadmap for selecting a feasible blockchain technology, comprising 5 evaluation dimensions. The main scientific contribution of the paper is the introduction of the first dimension, which considers the process from the SoS perspective. The other four dimensions are derived from the results reflected in related work.

The roadmap was initially applied to an administrative user action auditing process in a financial platform. The application selected consortium permissioned blockchain as the most suitable architecture, and a local Hyperledger Fabric prototype demonstrated audit record creation and hash-based verification. Further research should apply the roadmap to a larger set of organizational processes.

Declaration on Generative AI

The author has not employed any Generative AI tools in the writing of this paper.

References

- [1] M. Javaid, A. Haleem, R.P. Singh, R. Suman, Blockchain technology applications for Industry 4.0: A literature-based review, *Blockchain: Research and Applications* 2(4) (2021) 1–15. doi:10.1016/j.bcra.2021.100027.
- [2] K. Zile, R. Strazdiņa, Blockchain use cases and their feasibility, *Applied Computer Systems* 23(1) (2018) 12–20. doi:10.2478/acss-2018-0002.
- [3] H. Axelsen, J. Jensen, O. Ross, When is a DAO decentralized?, *Complex Systems Informatics and Modeling Quarterly* 31 (2022) 51–75. doi:10.7250/csimq.2022-31.04.
- [4] M. Kouhizadeh, S. Saberi, J. Sarkis, Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers, *International Journal of Production Economics* 231 (2021) 107831. doi:10.1016/j.ijpe.2020.107831.
- [5] P. Dutta, T.M. Choi, S. Somani, R. Butala, Blockchain technology in supply chain operations: Applications, challenges and research opportunities, *Transportation Research Part E: Logistics and Transportation Review* 142 (2020) 102067. doi:10.1016/j.tre.2020.102067.
- [6] M. Abdelhamid, L. Sliman, R. Ben Djemaa, G. Perboli, A review on blockchain technology, current challenges, and AI-driven solutions, *ACM Computing Surveys* 57(3) (2024) 73. doi:10.1145/3700641.
- [7] B. Biswas, R. Gupta, Analysis of barriers to blockchain adoption in industry, *Computers & Industrial Engineering* 136 (2019) 225–241. doi:10.1016/j.cie.2019.07.005.
- [8] M.N.M. Bhutta, A.A. Khwaja, A. Nadeem, H.F. Ahmad, M.K. Khan, M. Hanif, H. Song, A survey on blockchain technology: Evolution, architecture and security, *IEEE Access* 9 (2021) 61048–61073. doi:10.1109/ACCESS.2021.3072849.
- [9] A. Bauvars, M. Kirikova, Blockchain-based securities settlement: Opportunities and challenges, *Complex Systems Informatics and Modeling Quarterly* 28 (2021) 53–60. doi:10.7250/csimq.2021-28.03.
- [10] S. Kamble, A. Gunasekaran, R. Sharma, Modeling the blockchain enabled traceability in agriculture supply chain, *International Journal of Information Management* 52 (2020) 101967. doi:10.1016/j.ijinfomgt.2019.05.023.
- [11] Y. Zhang, V. Gupta, H. Karimi, Y. Wang, M.A. Yusoff, H. Vatanparast, J. Pan, M. Aghbashlo, M. Tabatabaei, A. Rajaei, Synergizing blockchain and internet of things for enhancing efficiency and waste reduction in sustainable food management, *Trends in Food Science & Technology* 156 (2025) 104289. doi:10.1016/j.tifs.2025.104873.
- [12] D. Indiyati, U. Rahardja, U. Rusilowati, S. Millah, A. Faturahman, A. Fitriani, Enhancing human resources management with blockchain technology: A case study approach, in: *Proceedings of the 3rd International Conference on Creative Communication and Innovative Technology (ICCIT)*, IEEE, 2024, pp. 1–6. doi:10.1109/ICCIT62134.2024.10701187.
- [13] M. Rakhra, R. Nagpal, P. Singh, P. Kumar, G.S. Cheema, A. Kumar, Blockchain technology's potential in supply chain management, in: *Proceedings of the 2024 International Conference on Electrical, Electronics and Computing Technologies (ICEECT)*, IEEE, 2024, pp. 1–7. doi:10.1109/ICEECT61758.2024.10739315.
- [14] S. Asaithambi, L. Ravi, M. Devarajan, A.S. Almazyad, G. Xiong, A.W. Mohamed, Enhancing enterprises trust mechanism through integrating blockchain technology into e-commerce platforms for SMEs, *Egyptian Informatics Journal* 25 (2024) 100443. doi:10.1016/j.eij.2024.100444.
- [15] International Organization for Standardization, ISO/IEC/IEEE 21841:2019, *Systems and Software Engineering—Taxonomy of Systems of Systems* (2019).
- [16] C. Ncube, S.L. Lim, On systems of systems engineering: A requirements engineering perspective and research agenda, in: *Proceedings of the 2018 IEEE 26th International Requirements Engineering Conference (RE)*, IEEE, 2018, pp. 112–123. doi:10.1109/RE.2018.00021.
- [17] S.M. Loss, Using blockchain to provide trusted interoperability to system-of-systems in smart cities context, in: *Proceedings of the 22nd International Middleware Conference: Doctoral Symposium*, ACM, 2021, pp. 17–18. doi:10.1145/3491087.3493679.

- [18] H.O. Ohize et al., Blockchain for securing electronic voting systems: A survey of architectures, trends, solutions, and challenges, *Cluster Computing* 28(2) (2025). doi:10.1007/s10586-024-04709-8.
- [19] L. Marchesi, M. Marchesi, R. Tonelli, M.I. Lunesu, A blockchain architecture for industrial applications, *Blockchain: Research and Applications* 3(4) (2022). doi:10.1016/j.bcra.2022.100088.
- [20] S. Balasubramanian, V. Shukla, J.S. Sethi, N. Islam, R. Saloum, A readiness assessment framework for blockchain adoption: A healthcare case study, *Technological Forecasting and Social Change* 165 (2021) 120536. doi:10.1016/j.techfore.2020.120536.
- [21] H. Chu, P. Zhang, H. Dong, Y. Xiao, S. Ji, W. Li, A survey on smart contract vulnerabilities: Data sources, detection and repair, *Information and Software Technology* 159 (2023) 107221. doi:10.1016/j.infsof.2023.107221.
- [22] O. Akanfe, D. Lawong, H.R. Rao, Blockchain technology and privacy regulation: Reviewing frictions and synthesizing opportunities, *International Journal of Information Management* 76 (2024) 102753. doi:10.1016/j.ijinfomgt.2024.102753.
- [23] T. Guggenberger, J. Sedlmeir, G. Fridgen, A. Luckow, An in-depth investigation of the performance characteristics of Hyperledger Fabric, *Computers & Industrial Engineering* 173 (2022). doi:10.1016/j.cie.2022.108716.
- [24] E. Kanepajs, M. Kirikova, Centralized vs. decentralized procurement: A literature review, in: *Joint Proceedings of BIR 2018 Workshops and Doctoral Consortium, CEUR Workshop Proceedings*, vol. 2218, CEUR-WS.org, 2018, pp. 217–232.