LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 24, NO. 1(2026)

Blockchain Technology in Management: Opportunities, Risks and Governance Challenges

Dr Patryk Chmielarz

University of the National Education Commission, Krakow, Poland

ORCID: 0000-0003-0286-741X

e-mail: chmielarzp13@gmail.com

Abstract

The idea of using blockchain seems to be gaining support as a way to facilitate transactions between organizations which don't have a shared database or administration. The importance of its management, however, is subject to debate. This article provides a critical assessment of the opportunities, risks and governance issues of organizations taking up blockchain technology. Research is synthesized into a focused narrative organized by three themes—Organizational Value, Implementation Constraints and Institutional Governance Responsibilities—that are grounded in the foundational research, further developed by management and information-systems scholarship, and then extended by institutional guidance. Several potential benefits are suggested in the literature: record reconciliation, traceability of the supply chain, auditing and rule-based transaction processing. This is only achievable by partner willingness to share, the validity of the source information and the appropriateness of blockchain over traditional databases. Potential gains might be offset by technical risks, privacy issues, organizational challenges, and uncertainties regarding regulations. In arguing this, the article does not suggest that you can forgo identifiable decision responsibilities, human responsibility or good dispute resolution when you decentralize record validation. Strategic fit, network design, accountability, information stewardship and performance review are the elements of an integrated governance framework. The paper provides an action-oriented consideration of blockchain adoption, considering benefits not as inherent properties of blockchain but rather possibilities that are likely to occur when blockchain is adopted.

Keywords: blockchain; organizational management; digital transformation; risk; governance; distributed ledger

1. Introduction

The challenge of organisations having to harmonise information across departments, suppliers, financial institutions and regulators is common. Each participant can have an internal record and may be in disagreement with other participants regarding delivery, ownership, authorization or payment. It takes up management time and can damage the trust of potentially strong working partners between the different views(Yaga et al., 2018). As a result, blockchain has brought itself into this issue and provided a solution to allow a history of transactions to be shared under rules agreed by all. However, the buzz surrounding blockchain in technology discussion does not necessarily correlate to better management.

The inspiration for modern blockchains came from electronic payments designed by Nakamoto (2008) for use without relying on a third party. Following applications include digital identity, provenance tracking and procurement and automated agreements. Technically, a blockchain is a distributed book that holds completed records that are chained together using cryptographic techniques and that cannot be altered without detection (Yaga et al., 2018). There is a wide range of arrangements that determine who can enter, validate and modify the network. A permissioned supply-chain consortium, however, leads to very different management concerns than a public cryptocurrency network.

Many of the early references were on transparency, immutability and the elimination of intermediaries. Those expressions need to be modified. A persistent record can accurately record wrong information; shared visibility can reveal commercially sensitive information; and reduction in verification intermediaries can introduce new dependencies upon software developers, platform administrators and data suppliers. De Filippi et al. (2020) suggest that the current level of trust in blockchain functioning relies on the general governance framework. The problem of trust must then also be considered, and institutional relationships are a subject of managers' scrutiny, rather than cryptography being assumed as it were to solve the problems.

Although research offered some insights, it has not found a general business case. Casino et al (2019) surveyed a multitude of uses but noted a host of questions remaining unanswered throughout the scope of the field. The relevance of blockchain is also found to vary based on the coordination needs and characteristics of the supply chain (Treiblmaier, 2018). These observations generate a practical puzzle: when is blockchain adding a real value for organizations and how is management to control the risks brought on by its use?

This article poses the question: How can organizations take advantage of the opportunities of blockchain while dealing with the challenges of technological, organizational and governance adoption? It provides a brief overview of the management rationale, explores major applications and limitations and then offers a governance model. The rationale behind this is that blockchain is a choice of institution and information system, not a necessary step in digital transformation.

2. Conceptual and theoretical background

Blockchain systems ensure a synchronized record by means of sets of rules for what constitutes proposed transactions as the accepted entry. Cryptographic hashing can connect records to each other and can detect changes if the records are changed in an unauthorized way. Consensus Mechanisms determine

what operations in a network will be considered successful. But they vary in terms of their performance expectations, energy consumption, access conditions and participant failure rate (Yaga et al., 2018). For managers, the principal design question is not if a system has a blockchain but who can take what actions in the system?

Unlike private or consortium networks, public networks allow for sharing of information with a wide audience of people. This difference is important as there are often situations where access needs to be restricted for confidentiality reasons or because of regulation. A consortium can give suppliers and customers the freedom to validate milestones while only sharing all the commercial terms with key stakeholders. Many questions arise in deciding which parties have the right to read, validate or amend operational rules, which is also a governance question. There may also be a blockchain where everyone in the network has permission to use it and it may be very close to a replicated database, where managers want to find evidence of its added value.

Applying the lens of transaction cost economics to adoption is one way of evaluating adoption. Williamson (1985) studied the choice of governance structures for transacting under uncertainty and opportunism. If a shared ledger is used and the cost of reconciliation and verification are high, due to organizations frequently challenging each other, then it can reduce these expenses. Rather, it might raise technical set-up costs, membership negotiation expenses, and maintenance expenses for the system. The comparison is therefore not between a “blockchain” and a “ Status quo if there was no blockchain”.

The institutional approach provides an explanation for decisions not completely based on efficiency. DiMaggio and Powell (1983) demonstrated the pressures that can lead to the similarity of organizations. The firms may take up blockchain projects as a result of a need to meet up with their partners or to keep up with the industry leaders or to demonstrate their innovativeness to investors. These are legitimate reasons but can lead to a low strategic value of systems. governance scholarship provides a third perspective: Beck et al. (2018) identify blockchain governance in terms of rights, accountability and incentives. These lenses serve to link technical design and managerial decision making and institutional action.

3. Review approach

A focused narrative literature review and conceptual synthesis are used in the article. It is based on existing information systems scholarship, management and supply-chain research, as well as a technical report in the US National Institute of Standards and Technology. Studies cited were chosen because they were directly relevant to the central question and their capacity to represent both the proposed benefits and identified conceptual limitations. Although these disciplines have made significant contributions, foundational research elucidates the potential of the blockchain, management research investigates applications to organizations and the governance studies examines how authority and responsibility will be structured.

The analysis was continued by comparing the claims and qualifications in this literature under three organizing categories: opportunities for managerial coordination; risk results that occur in adoption and

operation and governance mechanisms for responsible implementation. The framework that emerges is an interpretive one about those themes, not a model run against organizational data. This paper is not a systematic review since no database search, screening protocol or quality appraisal was performed. It also does not provide effect sizes estimates or make any assumption that all the benefits that may be expected have been proven empirically.

4. Managerial opportunities

4.1 Common records and administrative cooperation

A significant issue in interorganisational relations is duplication of the same information and that information needs to be repeated again and again. Each manufacturer and carrier and buyer may have separate proof of dispatch, receipt and acceptance. If these records vary, the employees will look into the difference and approve payment or transaction closure if there was no fault. A shared ledger can help to streamline some exchanges, as it can store a shared history of agreed-upon transactions. This capability of organizing information across various applications scenarios have been identified by Casino et al. (2019) as an important driver for experimenting with blockchain.

The saving which can be made should not be exaggerated. Workers still need to check on the delivery or service itself and many reconciliations can still be automated regardless of being blockchain based. The best-case scenario is when parties are institutionally independent but often require a dependable common history. Generally, it is not worthwhile for a single organization with good internal controls to disseminate records among various internal departments.

4.2 Traceability & Quality Control in the supply chain

Product provenance is difficult and is a characteristic of supply chains that are firm-specific, border crossing and technological platform crossing. Blockchain could provide a uniform evidence trail for such selected events as batch creation, inspection, transfer and delivery. Kshetri (2018) relates such applications to management goals such as dependability, flexibility and risk mitigation. Saberi et al (2019) also talk about the possibilities of distributed records and sustainable supply-chain management, and minimizing technical and organizational hurdles.

Project a food processor which relies on inputs from multiple suppliers. Having batch identifiers, certificates and handover events recorded on a shared system may assist investigators to know the recorded route of a contaminated consignment. However, a ledger is not able to tell if the supplier falsified an inspection. Reliable labelling, sampling, physical checks and incentives will continue to be key for traceability. The integrity of an electronic record should not be confused with the truthfulness of a claim in the real world.

4.3 Financial controls, procurement and smart contracts

Authorisation, delivery and settlement documentation might be needed for financial and procurement teams in an auditable way. Recorded transactions could help to eliminate discrepancies among parties and

simple rules could automate regular portions once certain requirements are met. In this context, a smart contract is a piece of software that executes specific functions, but not necessarily a legally binding contract. According to Yaga et al. (2018), smart contracts are one of the significant application features, where smart contracts rely on the code, rules of the network and the input data.

For instance, in procurement, an agreed payment may be made post a confirmed receipt event. This can possibly reduce some of the administrative processing time, but could possibly bring about an improper result if there are errors in the recevoir system. Managers should maintain exception handling and approvals, and thresholds: automated processes should be suspended if there are any disagreements. While auditors might find blockchain records useful, they cannot and do not straighten out independent audit judgments or financial-reporting duties.

4.4. Administrative and financial relationship with other organisations

A consortium ledger can be beneficial for multiple partners who would like to share a process, but do not want to hand over all operations to one entity Peng et al. (2025). If necessary, joint buyers or cross-border sellers can jointly agree on common definitions of data, common access rules, and common procedures for validating events. Treiblmaier (2018) states that the process should be analyzed in terms of network theories and theoretical concepts of interfirm coordination, not only based on technological aspects.

The opportunity is one of the organization, not just the computation. Regardless of the type of database technology chosen, having common procedures can help to improve coordination. The analyst thus has to determine if benefits come from the attributes of blockchain or from the activity of getting information standardized with partners (Iqbal et al., 2025). This is also meant to safeguard managers from attributing to the logistics what may have been done more cost effectively by the redesign of processes**.**

4.5 Skills and expertise of products and services

Another less obvious, but potentially valuable use is credentials or document provenance. Employers can verify that third parties have provided an attestation, which is verified by an education or professional body without having to ask for a manual attestation to be repeated. The same concepts can help facilitate tracking of records like certifications, maintenance records, or intellectual-property transfers. The record of employees and commercially sensitive documents, however, pose confidentiality issues Peng et al. (2025). The least information necessary for verification should be made public and private information may be kept apart from the chain. Just because there is a technical possibility does not mean that this makes a sound human-resource policy. Consent, data correction and equitable access are still a managerial necessity.

5. Risks and constraints

5.1 Infrastructure, scale and integration

A blockchain's distributed architecture might make validation, communication and storage unnecessary, compared to a traditional database. The overall processing speed and transaction confirmation times vary by architecture and are not necessarily the same for all networks. Yaga et al. (2018) describe the trade-offs to consensus approaches. Managers should consider realistic transaction volumes, tolerance for interruption to that activity, recovery of the system following an interruption, loss of data between the platforms, and interoperability with existing enterprise apps before selecting a platform.

The challenge of integration is usually the short term challenge. To adopt the accounting, inventory and customer-management systems to a shared ledger without generating conflicting versions of the same transaction, a company already employing accounting systems will need to map records to that ledger. Ambiguous ownership of such interfaces can result in an expensive maintenance liability for a potentially successful pilot program. The barriers are not only within the firms, but also between the collaborating organizations, as noted by Saberi et al. (2019).

5.2 Informative, interpretive, and critical reading

Blockchain architectures can be configured to make the changes to accepted records visible, but it is not possible to prevent the changes in all the surrounding elements. Potential failures are caused by stolen private keys, vulnerable applications, weak access controls and the wrong smart-contract code. The data received from external sources could also be inaccurate, delayed or manipulated. For example, a false temperature reading from the sensor to the ledger can be considered a correct reading by the ledger.

These security arrangements need to go beyond the chain. Independent testing still needed, access reviews, back up procedures, incident response/controls over external data sources. It is well known that saying a blockchain is 'tamper-proof' is too much to ask for any decision making process you are going to make: For a management process (Yaga et al., 2018), the security of the whole process depends on the weakest relevant part of the process.

5.3 Privacy and confidentiality

Participants can view critical information on an important record, which can be a positive aspect of a shared ledger system but can also clash with privacy and commercial confidentiality. Confidential or information that is to be kept forever or widely reproduced can be problematic, if there is an expectation by the person that the information can be corrected or if the business needs to safeguard prices and supplier arrangements. De Filippi et al. (2020) warn that this is not a replacement for institutional set-up and processes on which trusting relationships are built.

While none of these actions can eliminate the need for a case-specific legal analysis, a combination of permissioned access and careful data minimization and off-chain storage can help limit exposure. Managers will need to decide what information is actually required for participants, who has the authority to disclose data, how to correct errors and how data will be handled with regard to retention.

5.3 costs, uncertain benefits and organizational readiness

Instituting a blockchain is a much more than software acquisition. Organizations may need to spend money to get going with integration, help with network membership agreements, administration of governance, employee training, and ongoing technical support. Interest rates for participation in L2L projects can be higher for small firms or large reliance on key network partners (Iqbal et al., 2024). If the financial case is split, even further, or if the majority of counterparties still work on a process level, it becomes weaker.

The skills of managers and employees are important. There is resistance from staff to systems that change the roles they have established, or make work more visible, particularly when no expertise exists on the leadership's side of being able to question vendor promises (Kampoowale et al., 2026). The pressures from the institutions may make the adoption of the idea more for looks than for worth (DiMaggio & Powell, 1983). A defensible business case must first establish the problem, then explore options and state measurable success indicators prior to implementation (Zhang et al, 2024).

5.4 Ambiguity of regulation and contract

Requirements relating to data, financial transaction, consumer protection and dispute resolution may be difficult to manage when they cut across jurisdictions with the help of networks. Most notably, the software's rule, which is executed automatically, might not represent the full intent of the parties involved in the contract (Agi & Jha, 2022). If the code is wrong, or if information from outside of the code causes an inappropriate transfer, responsibility may be disputed. There are problems that can't be solved with just technical documentation. Governance should start from an early stage, including legal oversight, negotiated remedies and identifying responsible parties (Beck et al., 2018).

6. Governance challenges

3 What is the relationship between the two?

It is sometimes particularly easy to mix up decentralized managerial authority with decentralized validation. A network can share record maintenance and centralize admission, upgrades and emergency controls to a few actors. A point that Beck et al. (2018) make that is relevant for our discussion is defining decision rights, accountability and incentives. A consortium needs to establish the authority for new additions to its membership, clarify data standards, adopt software changes and resolve conflicts over records. Otherwise, an open ledger will perpetuate coordination problems it was designed to overcome.

6.2 Taking responsibility for failure

In a typical traditional system, it's usually a particular organization that runs a database. Consortium failures can be those of the developers, of the participating firms, network administrators and third party information services. It is important to think about a shipment payment, because the payment is carried out based on statement of delivery, but the statement of delivery is incorrect (Rahman et al., 2024). The payment history is unalterable, and could be used to determine what transpired, but it can't be used to determine who is liable for compensation to the wronged party. Governance agreements need to then allocate responsibility for validation, system errors, remedial transactions and disputes. The point to be

made with regard to confidence in this context is that it is maintained through governance relationships and not just through process automation, as De Filippi et al. (2020) seems to argue.

6.3 Incentives, participation and unequal power

Shared network may provide different benefits to members. SMEs can have an extra burden on their reporting expenses while larger companies can have more supervision over their suppliers. The standards and priorities of a consortium may be declared as being decentralised in fact, but really under the dominance of the most powerful member. The costs and benefits and the participation rules need to be reasonable and transparent, and opportunities to challenge decisions need to be proportionate, if governance is to be effective (Shah et al., 2025). Incentives are especially important because if people are not too motivated to put in consistent data into the system, if there is little consequence of doing wrong, it is unlikely to happen. (Beck et al., 2018)

6.4 Transparency – not too much transparency

Not everything is a good thing when it comes to info visibility. Partners must have confidence in relevant transactions but also they must safeguard their trade secrets and personal information. Governance ought therefore to make sure that there is a distinction between the right to confirm that an event has taken place, and the right to inspect all underlying aspects. Access controls and privacy-protecting design can help with this distinction, but it needs to be accompanied with policies for data correction, retention and authorized investigation. These setups must be examined based on real business needs and not technically for ease of use.

6.5 Institutional and public accountability

Private governance arrangements do not create obligations to anyone else. There may be a way still be an accountable party and comprehensible records that regulators, courts and auditors can demand. If a network extends beyond national boundaries, rules should establish which institution can be dealt with in the case of requests made by regulators and how conflicting needs will be addressed (Sumra et al., 2022). Governance also needs to review how smaller participants are able to be excluded, and the environmental footprint of the chosen consensus mechanism. However, to minimize sweeping generalizations of the sustainability of different blockchain networks, it is better to evaluate them through a lens of their architecture (Yaga et al., 2018).

7. Discussion & proposed governance framework

The review states that blockchain is most secure when the organization has experienced frequent coordination issues with numerous separate actors, disagreement over who's recording what, a requirement to verify the transaction, etc. The best rationale for its use is that it is a plausible improvement over the other procedures (Kampoowale et al., 2026). This is a clear-cut comparison in terms of transaction cost economics: the cost of verifying the KPIs will need to be less than the cost of developing, coordinating and maintaining the KPIs (Williamson, 1985). On the flip-side, institutional

theory suggests that strong feelings of peer adoption or of reputational risk might reduce the rigor of the assessment (DiMaggio & Powell, 1983).

The strategic fit is a good place to begin a practical governance approach. Management should clearly outline the exact breakdown in the process and determine if the shared database is the right way to solve the problem or if an audited interface or contractual changes would be more to the point. Should blockchain prove to be a valuable added value, it is now time to consider network design, which includes the setting of permissions, the forms of validation, privacy protection, and the integration standards that meet the relevant requirements (Peng et al., 2025). Actually, organizational roles should then be delineated for data entry, system administration, security, legal compliance and resolution of conflicts.

The fourth one is information stewardship. All networks must have a set of rules governing data quality, data correction, credential management and external information source usage. Last but not least, comparing actual results with agreed performance indicators like reconciliation time, exceptions, operating costs, tracing time and complaints of the stakeholders. Only a pilot that is proven to be effective under realistic circumstances should be scaled. This is indicative of the challenges identified with governance by Beck et al. (2018) and organizational hurdles by Saberi et al. (2019).

The difference is illustrated by an example of a managerial decision. Imagine that there are three distributors competing who need to independently verify the shipment of temperature-sensitive products through their own warehouses. A permissioned shared history may be helpful if they are having ongoing conflicts regarding custody and inspections. It would first be compared by the managers to a typical database that is jointly managed. They would then determine who can enter a shipment, who can confirm the physical receipt of a shipment, which records are available to the competitors, and how to deal with a "mistaken entry" (Iqbal et al., 2025). Design of governance would have to explicitly record procedures for revocation of access and there would have to be an independent verification of the data coming from the temperature sensors, while documenting any liability for any loss as a result of incorrect data being entered. If technology does not decrease the extent of disagreement and increase the speed of tracing and the lower overall cost of coordination, it would be hard to justify investing in such technology in the future (Iqbal et al., 2025). This example clearly demonstrates the importance of institutional arrangements, like cryptographic architecture.

The framework is “conditional” on purpose. In the case of food distributor, traceability and verification of the physical inputs could be highlighted, while for a procurement consortium, authorization and dispute handling can be emphasized. Professional credentialing service may view privacy and correction processes as core (Iftikhar et al., 2026). The same type of architecture and supervision will not naturally be adequate in both scenarios. Rather than that there is a generalizable management responsibility to relate network design to accountable institutional choices.

This synthesis also uncovers one of the important research gaps. The focus is not so much on what blockchain would allow as on what forms of governance would make for good outcomes over time. Implementation costs could be compared across different organizational units, and actual rates of disputes

and effects of different allocations of decision rights could be compared in cross-sectional studies done longitudinally. Comparative studies on smaller companies would help to better understand the effects of blockchain on the distribution of value across networks rather than the more likely, but distinct, impact on the power of dominant actors.

8. Conclusion

Selected records, verification and coordination of transactions across organizations can be supported with the help of blockchain technology. Where a series of participants have reconciliation issues due to common information infrastructure, but none of them can credibly manage the common infrastructure, its relevance becomes more relevant. However, the literature does not provide any reason to believe that decentralisation tends to lead to greater efficiency or trust in itself. Adoption might be limited by technology limitations, source data quality, privacy requirements, integration requirements, and unequal bargaining power. Governance will never be replaced: There is a need for someone to decide who is allowed to be involved and who records what and what happens if there is an error and who is blamed if things go wrong in the system. This paper, therefore, proposes an assessment based on strategic fit and network design, accountability, information stewardship and performance evaluation. The framework is an abstract, hypothetical approach which needs to be tested empirically. Its main implication for practitioners is simple: blockchain should only be used when it offers a better solution than alternatives for a management problem that can be identified and is clearly only going to be solved by blockchain.

References

1. Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. Journal of the Association for Information Systems, 19(10), 1020–1034. https://doi.org/10.17705/1jais.00518
2. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55–81. https://doi.org/10.1016/j.tele.2018.11.006
3. De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. Technology in Society, 62, Article 101284. https://doi.org/10.1016/j.techsoc.2020.101284
4. Iqbal, M. S., Abdul Rahim, Z., Alshammari, A. M. K., & Iftikhar, H. (2024). Innovative strategies for overcoming barriers to technology adoption in small and medium-sized enterprises. Journal of the International Council for Small Business, 5(4), 331–344. https://doi.org/10.1080/26437015.2024.2367440
5. Iqbal, M. S., Abdul Rahim, Z., Omerkhel, Q., Iftikhar, H., & Khan, M. F. (2025). Leveraging AI and TRIZ for sustainable innovation in advanced manufacturing. Discover Applied Sciences, 7, Article 589. https://doi.org/10.1007/s42452-025-06847-z

6. DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147–160. https://doi.org/10.2307/2095101
7. Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80–89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005
8. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
9. Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261
10. Treiblmaier, H. (2018). The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. Supply Chain Management: An International Journal, 23(6), 545–559. https://doi.org/10.1108/SCM-01-2018-0029
11. Williamson, O. E. (1985). The economic institutions of capitalism: Firms, markets, relational contracting. Free Press.
12. Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain technology overview (NIST Interagency/Internal Report 8202). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8202
13. Kampoowale, I., Hussien Musa, A. M., Adam Abdalla, A. A., Iftikhar, H., Abdelraheem, A. A. E., & Elamin Elboukhari, Y. A. (2026). Assessing the mediating role of human capital in the relationship between digital transformation and firm performance. Journal of Manufacturing Technology Management, 37(1), 1–22. https://doi.org/10.1108/JMTM-02-2025-0122
14. Peng, D., Iftikhar, H., Kampoowale, I., Ali Hussin, H. A. A., & Mohammed Ali, N. B. (2025). Linking big data analytics to firm performance: Exploring the mediating effects of data-driven culture and networking capability. Business Process Management Journal, 1–23. https://doi.org/10.1108/BPMJ-07-2025-1232
15. Sumra, K. B., Alam, M., Mohd Noor, K. B., Hali, S. M., & Iftikhar, H. (2022). Factors affecting artificial intelligence and management of institutional response to the event of coronavirus in Pakistan. Pertanika Journal of Social Sciences & Humanities, 30(4), 1451–1472. https://doi.org/10.47836/pjssh.30.4.01
16. 2. Shah, U., Fayyaz, A. B., Iftikhar, H., & Hayat, R. S. (2025). Exploring stakeholder perspectives on barriers to green financing in Pakistan's transportation sector. Asian Journal of Water, Environment and Pollution, 22(4), 111–122. https://doi.org/10.36922/AJWEP025160121

17. 3. Iftikhar, H., Shah, U. L., Iqbal, S., Fayyaz, A. B., & Hayat, R. S. (2026). Rethinking green finance for sustainable transportation in Pakistan: Institutional barriers, policy misalignments, and pathways for climate-compatible mobility. Asian Journal of Water, Environment and Pollution, 23(3), Article 026060033. https://doi.org/10.36922/AJWEP026060033
18. Agi, M. A. N., & Jha, A. K. (2022). Blockchain technology in the supply chain: An integrated theoretical perspective of organizational adoption. International Journal of Production Economics, 247, Article 108458. https://doi.org/10.1016/j.ijpe.2022.108458
19. Zhang, Y., Tavalaei, M. M., Parry, G., & Zhou, P. (2024). Evolution or involution? A systematic literature review of organisations' blockchain adoption factors. Technological Forecasting and Social Change, 208, Article 123710. https://doi.org/10.1016/j.techfore.2024.123710
20. Rahman, M. H., Yeoh, W., & Pal, S. (2024). Exploring factors influencing blockchain adoption's effectiveness in organizations for generating business value: A systematic literature review and thematic analysis. Enterprise Information Systems, 18(8), Article 2379830. https://doi.org/10.1080/17517575.2024.2379830