International Journal of Management and Commerce Innovations ISSN 2348-7585 (Online)
Vol. 14, Issue 2, pp: (83-90), Month: October 2026 - March 2027, Available at: www.researchpublish.com

Blockchain Management: Strategic Applications, Governance, Challenges and Future Directions

Dr. Chong Kuan Git[1], Dr. P. Ravindran Pathmanathan[2], Dr. Venkatesh Karanam[3]

[1,2,3] UNIES Business School

DOI: https://doi.org/10.5281/zenodo.23684743

Published Date: 21-October-2026, Amendment Date: 27-October-2026

Abstract: **Blockchain is no longer discussed only in connection with cryptocurrencies. Firms, public agencies and industry consortia now examine it as a way of recording, verifying and coordinating transactions that involve several independent parties. The managerial value of a blockchain, however, is not inherent in the technology. It depends on whether a shared ledger solves a real coordination problem, whether participants accept the rules that govern the network, and whether the expected gains outweigh the cost of building and running it. This conceptual review organises the topic around five linked dimensions: strategic fit, organisational and inter-organisational governance, operational applications, risk management, and implementation capability. Drawing on published reviews of blockchain applications, supply-chain integration, adoption barriers and sustainability, the paper explains how distributed ledgers and smart contracts can support traceability, common records, process automation and accountability. It also sets out the constraints that managers routinely underestimate, including the quality of data entering the ledger, scalability, privacy, interoperability, regulatory uncertainty, energy use, skills shortages and the uneven bargaining power of network members. The paper argues that blockchain should be managed as a socio-technical, ecosystem-level investment rather than as a self-contained information technology project. A six-stage adoption framework is proposed, moving from problem definition and suitability testing through consortium design, controlled piloting and selective scaling to continuous assurance. The review closes with a research agenda on realised value, consortium governance, adoption by small and medium-sized enterprises (SMEs), and the link between blockchain and sustainable business performance.**

Keywords: **Blockchain management; distributed ledger technology; organisational governance; smart contracts; supply chain management; digital transformation; risk management; sustainability.**

I. INTRODUCTION

Most organisations today do business through networks of suppliers, customers, banks, logistics firms, regulators and technology partners. Work in these networks depends on information moving quickly between parties and on each party being confident that the records it receives are accurate, complete and properly authorised. Conventional information systems tend to hold data in separate organisational databases, so the same transaction is often recorded several times in slightly different ways. Reconciling those records takes time and money, and it frequently produces disputes, especially when no participant is accepted by the others as the legitimate keeper of the master record. Blockchain proposes a different arrangement: authorised participants maintain a synchronised copy of one ledger and follow agreed procedures for validating new entries (Iansiti & Lakhani, 2017; Nakamoto, 2008).

In technical terms, a blockchain is a type of distributed ledger in which transactions are grouped into blocks, each block is cryptographically linked to the one before it, and new blocks are accepted through a consensus mechanism (Zheng et al., 2018). Designs vary considerably. Public, permissionless networks allow anyone to read and validate transactions, whereas private or permissioned networks restrict participation to known entities. Permissioned designs are usually better suited to commercial settings, where participants need identifiable access, clearly assigned responsibilities and control over what is disclosed to whom (Belotti et al., 2019). Smart contracts add the ability to execute pre-programmed actions once specified

conditions are met, although the outcome is only as sound as the data and assumptions written into the code (Casino et al., 2019; Iansiti & Lakhani, 2017).

For managers, then, the relevant question is not whether blockchain is novel. It is whether a distributed ledger is the best available way to deal with a clearly defined business problem. Systematic reviews document applications in finance, supply chains, healthcare, government records and data management, yet they consistently report that value depends on context (Casino et al., 2019; Hughes et al., 2019; Xu et al., 2019). Iansiti and Lakhani (2017) describe blockchain as a foundational rather than a disruptive technology, one whose adoption is likely to be gradual because it requires coordination among many actors. Supply chains illustrate the point. A shared ledger may make product movements more visible and easier to trace, but it cannot by itself confirm that the information entered at the point of origin is true (Pournader et al., 2020; Wang et al., 2019).

This paper offers a management-centred account of blockchain adoption, focusing on the decisions executives and managers face before, during and after implementation. It pursues three objectives: (a) to explain the strategic and operational implications of blockchain for organisations; (b) to identify the governance, organisational and technological conditions that shape adoption outcomes; and (c) to propose a practical framework for evaluating and managing blockchain initiatives. The contribution is conceptual. The paper synthesises existing literature and derives managerial guidance; it does not report new empirical data.

II. REVIEW APPROACH AND CONCEPTUAL FOUNDATION

The manuscript follows an integrative conceptual-review approach. It draws on foundational accounts of blockchain architecture and on peer-reviewed reviews of business applications, supply-chain integration, adoption barriers and sustainability. Sources were examined thematically, and no claim is made to exhaustive coverage. Themes were retained when they bore directly on management decisions, namely business value, governance, process design, adoption barriers and organisational outcomes. Readers should therefore treat the paper as a synthesis and a managerial framework. It is not a systematic review with a reproducible search strategy, a formal screening protocol or a quantitative meta-analysis.

A. Blockchain as a Socio-Technical System

A blockchain is made up of technical components and of rules that govern who participates and how decisions are taken. The technical layer may include digital signatures, consensus protocols, replicated data storage and smart-contract code. The institutional layer determines who can join the network, who validates transactions, how software changes are approved, what information each party can see, how disputes are settled and who is liable when something goes wrong. Beck et al. (2018) frame these questions in terms of decision rights, accountability and incentives, and they argue that governance in a blockchain economy cannot be separated from the design of the ledger itself. Viewing the ledger as a purely technical artefact therefore misses the arrangements that decide whether organisations will actually use it.

Three properties matter most from a management perspective. First, a shared ledger can give participating organisations a common history of transactions. Second, cryptography and consensus make unauthorised changes harder to carry out and easier to detect. Third, programmable logic allows selected transactions to be automated. Babich and Hilary (2020) describe related strengths in terms of visibility, aggregation, validation, automation and resilience. None of these properties should be mistaken for absolute truth, complete security or automatic legal enforceability. A blockchain can faithfully preserve incorrect data, reveal sensitive metadata, contain coding errors, or run under governance arrangements that favour its most powerful members (Casino et al., 2019; Zheng et al., 2018).

B. Strategic Fit and the Business Case

Blockchain is most likely to add value when several independent parties must update or check a common record, when reconciling separate records is expensive, and when no single party can credibly be trusted to control the shared database. Catalini and Gans (2020) explain the economic logic in terms of two costs that blockchain can lower: the cost of verifying transaction attributes and the cost of operating a network without a central intermediary. Where one trusted organisation already runs the process efficiently, a conventional database will usually be cheaper, faster and simpler to govern. Wüst and Gervais (2018) make this point through a structured decision sequence that asks whether multiple writers are involved, whether they are known and trusted, and whether a trusted third party is available. Managers should accordingly compare a blockchain proposal against realistic alternatives such as process redesign, application programming interfaces (APIs), a jointly managed database or independent audit arrangements.

A credible business case starts by quantifying the current cost of the problem and stating the outcomes the network is expected to deliver. Useful measures include transaction-processing time, reconciliation effort, error and dispute rates,

product-recall time, audit-preparation cost, exposure to fraud and customer confidence. Intangible benefits such as trust and transparency should be converted into observable indicators wherever possible. The cost side should be equally complete, covering systems integration, cybersecurity, legal review, training, network administration and long-term maintenance. Treiblmaier (2018) shows that established theories, including transaction cost economics, principal-agent theory, the resource-based view and network theory, offer useful lenses for specifying where these costs and benefits are likely to arise.

III. STRATEGIC APPLICATIONS OF BLOCKCHAIN MANAGEMENT

A. Supply Chain Visibility and Traceability

Supply-chain management is among the most widely studied business applications. A shared ledger can record events such as manufacture, certification, shipment, transfer of custody, storage and delivery. When participants use consistent product identifiers and agreed data standards, these records can improve a firm's ability to trace goods across organisational boundaries. Prior reviews link blockchain-enabled supply chains with greater visibility, traceability, data security and scope for smart contracts (Pournader et al., 2020; Wang et al., 2019). Kshetri (2018) connects these capabilities to core supply-chain objectives, including cost, speed, dependability, risk reduction, sustainability and flexibility. The potential is greatest in food safety, pharmaceuticals, high-value goods, responsible sourcing and complex cross-border logistics, where documentation is heavy and multiple intermediaries are involved (Chang et al., 2020).

Traceability, however, is only as reliable as the process that captures physical events. A ledger entry cannot prove that a container holds the goods described in the digital record. Organisations therefore need complementary controls, for example tamper-evident packaging, sensors, physical inspections, third-party certification, supplier audits and clear responsibility for each data entry. Managers should also ask whether smaller suppliers can afford the technology and whether the lead firm is shifting costs or risks onto weaker network members. Research on sustainable supply chains groups adoption barriers into intra-organisational, inter-organisational, system-related and external categories (Saberi et al., 2019), and later work confirms that these barriers interact rather than operate in isolation (Kouhizadeh et al., 2021). Empirical evidence from India and the United States further suggests that adoption drivers differ across national contexts, so findings from one market should not be assumed to transfer directly to another (Queiroz & Fosso Wamba, 2019).

B. Financial Services and Transaction Management

In financial services, distributed ledgers can support shared transaction records, clearing and settlement, tokenisation of assets and some forms of programmable finance. The managerial attractions include less reconciliation, stronger audit trails and the opportunity to redesign processes that currently pass through several intermediaries (Xu et al., 2019). Yermack (2017) adds that ledger-based records of ownership could change corporate governance practice by making share registers more transparent and settlement faster. These benefits do not follow automatically. Financial applications must still deal with identity verification, consumer protection, operational resilience, market integrity, legal finality of settlement and compliance obligations. A permissioned ledger can restrict access, but it does not remove the need for strong internal controls or for supervision by regulators.

C. Contracting, Procurement and Process Automation

Smart contracts can encode selected business rules, such as releasing a payment once an approved delivery is confirmed or sending an alert when a service-level threshold is breached. They can cut manual hand-offs where the triggering information is reliable and the process is sufficiently standardised. Managers need to separate two questions here: whether a rule can be automated, and whether the rule is fair, commercially sensible and legally enforceable. Werbach and Cornell (2017) caution that smart contracts do not replace contract law, because commercial agreements depend on interpretation, remedies and flexibility that code cannot easily capture. Exceptions, disputed events and ambiguous performance conditions still call for human judgement. Smart-contract design should therefore build in exception handling, authorisation controls, thorough testing, an audit trail and a defined route for resolving disputes.

D. Records, Credentials and Inter-Organisational Assurance

Blockchain can also be used to verify qualifications, licences, certificates, provenance records and other institutional documents. A verifier may be able to confirm that a credential was issued by an authorised body and that it has not since been revoked or altered (Casino et al., 2019). In education and professional services, this could reduce the repeated manual checks that employers and regulators currently perform. Sensitive personal data, though, should not be written to an immutable ledger as a matter of course. A privacy-conscious design keeps only cryptographic proofs or references on-chain

and holds the underlying personal data in controlled systems, in line with applicable data-protection law and retention rules (Finck, 2018).

IV. GOVERNANCE AND ORGANISATIONAL MANAGEMENT

A. Network Governance and Accountability

A blockchain consortium needs explicit governance well before it moves into production. A governance charter should set out membership criteria, participant roles, validation rights, data-access rules, voting thresholds, procedures for software changes, service levels, cost sharing, liability, audit rights and exit arrangements. Without such rules, a network that works technically can still break down over disputes about control, access or responsibility (Beck et al., 2018). Governance matters most where competitors, suppliers and customers share the same infrastructure, since each will be wary of giving rivals an informational or commercial advantage.

Decision-making arrangements must balance speed with legitimacy. A small group of dominant firms can take decisions quickly, but other members may come to see the network as serving those firms rather than the consortium as a whole. A requirement for unanimous approval, on the other hand, can make software upgrades and incident response unworkably slow. One practical answer is to match decision rights to risk. Routine operational changes can be handled under delegated authority, while changes that affect data rights, membership or financial exposure should require a higher level of approval.

B. Leadership, Culture and Change Management

Implementing a blockchain changes people's responsibilities as well as the systems they use. Procurement teams may have to agree common supplier-data standards; legal teams have to review digital contracting and liability; information-technology staff must handle integration and security; and frontline employees must follow new data-capture routines. Senior leaders should explain the business problem being addressed, the benefits expected and the limits of what the technology can do. Training should be tailored to each role and should cover how to correct errors, escalate incidents and manage exceptions.

Organisational readiness covers executive sponsorship, clear process ownership, digital capability, partner commitment and funding for ongoing operation. Clohessy and Acton (2019) found that top-management support and organisational readiness are significant influences on whether firms adopt blockchain. Projects tend to fail when they are run as isolated technology experiments with no accompanying change to incentives or workflows. Managers should therefore establish early who benefits, who pays and who takes on extra work. Where costs and benefits fall unevenly, participants may hold back data or drift away from the network altogether.

C. Data Governance, Privacy and Cybersecurity

Immutability strengthens auditability, but it creates a design problem whenever information has to be corrected, restricted or erased. Finck (2018) shows that this tension is particularly acute under data-protection regimes such as the European Union's General Data Protection Regulation, which grants individuals rights of rectification and erasure and requires a clearly identifiable data controller. Organisations should classify their data before choosing an architecture and should keep confidential or personally identifiable information off the ledger unless there is a clear legal basis and a suitable technical design. Access controls, encryption, cryptographic key management, secure interfaces, identity management, independent code review and incident-response procedures all remain necessary (Zheng et al., 2018). The ledger should also sit within the organisation's wider information-security and business-continuity programmes rather than being managed as a separate system.

V. IMPLEMENTATION CHALLENGES AND RISK MANAGEMENT

A. Technical Performance and Interoperability

Blockchain platforms differ in their consensus mechanisms, data models, identity systems and smart-contract languages (Belotti et al., 2019). Linking these networks to enterprise resource planning systems, legacy databases, sensors and partners' platforms can be difficult, and the lack of common standards is a recurring obstacle in cross-border trade (Chang et al., 2020). Performance also varies with transaction volume, network topology and validation requirements. Before deployment, managers should test throughput, latency, availability, recovery, storage growth and integration effort under realistic operating conditions. Scalability claims need to be demonstrated in the intended environment, not assumed on the strength of a vendor demonstration.

B. Data Quality and the 'Oracle' Problem

A ledger can keep a durable record of whatever is submitted to it, but it cannot independently establish that an external event happened as recorded. Data may be incomplete, entered late, manipulated before submission or generated by faulty sensors. The gap between real-world events and on-chain records is widely known as the oracle problem (Caldarelli, 2020). Babich and Hilary (2020) describe the same weakness more bluntly as a "garbage in, garbage out" risk. Management controls should therefore specify the source of every data item, the party accountable for its accuracy, the evidence required to support it and the procedure for challenging a disputed entry.

C. Legal, Regulatory and Ethical Considerations

Legal questions can arise over contractual enforceability, the status of electronic evidence, data protection, intellectual property, jurisdiction, consumer protection, financial regulation and cross-border data transfers. Because the legal position varies by sector and country, organisations should obtain jurisdiction-specific advice before processing regulated or personal information on a ledger (Finck, 2018; Werbach & Cornell, 2017). Ethical concerns include unequal access, surveillance, the exclusion of smaller participants, automated decisions that are hard to contest and the environmental cost of certain consensus mechanisms. The energy demand of proof-of-work networks such as Bitcoin has been estimated to rival that of some national economies (de Vries, 2018). Permissioned networks and less energy-intensive consensus designs can ease some of these concerns, but they do not remove the need for a proper assessment.

D. Cost, Skills and Vendor Dependence

Implementation costs include platform development or licensing, systems integration, cybersecurity, legal advice, consortium administration, training and user support. Organisations can also become dependent on a single technology provider or a small pool of specialists, a risk that is greater where blockchain skills are scarce in the local labour market. A total-cost assessment should cover initial and recurring costs, exit costs, data portability, software maintenance and the practical ability to change providers. Procurement contracts should address service continuity, security obligations, audit access, ownership of intellectual property and transition assistance at the end of the contract.

VI. A STAGED FRAMEWORK FOR BLOCKCHAIN ADOPTION

Drawing on the themes discussed above, this paper proposes a six-stage framework for blockchain adoption (Table 1). It is meant as a decision aid that managers can adapt to their own circumstances, not as a universal implementation recipe. Each stage ends with a decision point at which the initiative can be continued, redesigned or stopped.

Table 1: Six-Stage Framework for Managing Blockchain Adoption

Stage	Key managerial question	Principal activities and outputs
1. Define the business problem	What process failure or coordination cost are we trying to fix?	Document the problem, identify affected stakeholders and establish measurable baseline performance. Avoid starting with a technology purchase.
2. Test blockchain suitability	Does this problem genuinely require a shared, distributed ledger?	Confirm that multiple parties need a common record and that trust, reconciliation or audit problems justify a ledger. Compare the proposal with a conventional database and with process redesign (Wüst & Gervais, 2018).
3. Design the ecosystem and governance	Who participates, on what terms, and who decides?	Specify participants, incentives, data rights, validation roles, decision procedures, liability, funding and exit rules. Secure firm partner commitment before building (Beck et al., 2018).
4. Build a controlled pilot	Does the solution work under realistic conditions?	Select a bounded use case, use representative data, integrate only essential systems, and test security, performance, usability, exception handling and legal assumptions.
5. Evaluate and scale selectively	Is there evidence that benefits exceed costs?	Compare pilot results with the baseline. Scale only when benefits are demonstrated, governance is workable, participants are ready and the operating model is funded.
6. Assure and improve continuously	Is the network still delivering value safely?	Monitor security, data quality, participation, cost, regulatory change and business outcomes. Review smart contracts and governance rules as processes change.

Note. Framework developed by the authors from the literature reviewed in Sections II to V.

Performance measurement should combine technical and organisational indicators across four levels (Table 2). Indicators should be chosen and baselined before the pilot begins, so that the organisation can tell genuine improvement apart from enthusiasm based on anecdote. Kshetri (2018) and Babich and Hilary (2020) both stress that claims about blockchain value need to be tied to specific operational objectives rather than to general statements about trust or transparency.

Table 2: Illustrative Indicators for Evaluating Blockchain Initiatives

Level	Example indicators
Technical	Transaction completion time; system availability; error rates; security incidents; recovery time
Process	Reconciliation hours; dispute frequency; traceability (trace-back) time; administrative and audit-preparation cost
Network	Active-participant rate; data completeness; time taken to approve changes; partner retention
Strategic	Customer confidence; supplier participation; audit readiness; measurable sustainability outcomes

VII. DISCUSSION AND FUTURE RESEARCH DIRECTIONS

The literature reviewed here points to blockchain as infrastructure for coordination, verification and rule execution across organisational boundaries. Reviews of applications identify a wide range of possible uses, but the presence of a technical capability does not by itself establish a positive business case (Casino et al., 2019; Hughes et al., 2019; Xu et al., 2019). Supply-chain research similarly highlights visibility, traceability and trust while drawing attention to the conditions and barriers that shape adoption (Pournader et al., 2020; Saberi et al., 2019; Wang et al., 2019). The central management issue is therefore one of conditional value: which processes benefit, under which governance arrangements, and at what cost?

Several research priorities follow. First, studies should measure realised rather than expected value. Many claimed benefits are framed as anticipated gains in transparency, efficiency or trust, and longitudinal case studies comparing performance before and after implementation, including the ongoing cost of governance and maintenance, would help to test these claims. Second, more work is needed on consortium governance, in particular on how voting rights, data ownership and liability are shared among organisations with unequal resources (Beck et al., 2018). Third, researchers should examine the experience of SMEs, which may bear disproportionate integration, skills and compliance costs and which are often the weakest members of a supply network (Kouhizadeh et al., 2021).

Fourth, research should look at how blockchain interacts with complementary technologies such as the Internet of Things, artificial intelligence and digital identity systems. These combinations may strengthen data capture and decision support, yet they can also add new points of failure and blur accountability. Fifth, sustainability research should separate the environmental footprint of the underlying network from the sustainability gains that better traceability or reduced waste might bring (de Vries, 2018; Saberi et al., 2019). Finally, comparative studies across jurisdictions and industries could clarify how regulation, institutional trust and market structure influence adoption, building on the cross-country evidence already reported by Queiroz and Fosso Wamba (2019).

For practitioners, the proposed framework stresses disciplined selection and deliberate governance. Organisations should resist the assumption that decentralisation is better in every case. In some settings a shared database run by a trusted intermediary will be the more efficient option. In others, a permissioned blockchain will add value precisely because participants need a common record without handing any single party unilateral control (Catalini & Gans, 2020). The right architecture is the one that best fits the business process, the risk profile and the institutional environment in which it will operate.

VIII. CONCLUSION

Managing blockchain is fundamentally about aligning a distributed digital infrastructure with organisational strategy, operating processes and the interests of the stakeholders who take part in it. The technology can support shared records, traceability, transaction verification and some forms of process automation, and these capabilities can improve coordination where several independent parties rely on a common transaction history. Blockchain does not, however, guarantee truthful input, eliminate cyber risk, resolve legal uncertainty or ensure that every participant benefits equally. Its value depends on data quality, network participation, governance, interoperability, skills and the cost of keeping the system running.

This paper has proposed a six-stage adoption framework that begins with a clearly defined business problem, tests blockchain against alternative solutions, establishes ecosystem governance, pilots a bounded use case and scales only when measurable benefits have been shown. The framework also calls for continuing assurance of security, privacy, compliance and performance. The practical lesson for business leaders is to manage blockchain as a socio-technical, inter-organisational change programme rather than as a technology purchase or a fashionable innovation. Future empirical work should test the framework across industries, assess realised financial and non-financial outcomes, and investigate how different governance structures sustain trust and participation over time. A context-sensitive approach of this kind offers the soundest basis for responsible and effective blockchain adoption.

ACKNOWLEDGEMENT

The authors thank the researchers whose published work informed this conceptual review. This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors. The authors declare no conflict of interest.

REFERENCES

[1] Babich, V., & Hilary, G. (2020). Distributed ledgers and operations: What operations management researchers should know about blockchain technology. *Manufacturing & Service Operations Management, 22*(2), 223–240. https://doi.org/10.1287/msom.2018.0752

[2] 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

[3] Belotti, M., Božić, N., Pujolle, G., & Secci, S. (2019). A vademecum on blockchain technologies: When, which, and how. *IEEE Communications Surveys & Tutorials, 21*(4), 3796–3838. https://doi.org/10.1109/COMST.2019.2928178

[4] Caldarelli, G. (2020). Understanding the blockchain oracle problem: A call for action. *Information, 11*(11), Article 509. https://doi.org/10.3390/info11110509

[5] 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

[6] Catalini, C., & Gans, J. S. (2020). Some simple economics of the blockchain. *Communications of the ACM, 63*(7), 80–90. https://doi.org/10.1145/3359552

[7] Chang, Y., Iakovou, E., & Shi, W. (2020). Blockchain in global supply chains and cross border trade: A critical synthesis of the state-of-the-art, challenges and opportunities. *International Journal of Production Research, 58*(7), 2082–2099. https://doi.org/10.1080/00207543.2019.1651946

[8] Clohessy, T., & Acton, T. (2019). Investigating the influence of organizational factors on blockchain adoption: An innovation theory perspective. *Industrial Management & Data Systems, 119*(7), 1457–1491. https://doi.org/10.1108/IMDS-08-2018-0365

[9] de Vries, A. (2018). Bitcoin's growing energy problem. *Joule, 2*(5), 801–805. https://doi.org/10.1016/j.joule.2018.04.016

[10] Finck, M. (2018). Blockchains and data protection in the European Union. *European Data Protection Law Review, 4*(1), 17–35. https://doi.org/10.21552/edpl/2018/1/6

[11] Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *International Journal of Information Management, 49*, 114–129. https://doi.org/10.1016/j.ijinfomgt.2019.02.005

[12] Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review, 95*(1), 118–127.

[13] Kouhizadeh, M., Saberi, S., & Sarkis, J. (2021). Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers. *International Journal of Production Economics, 231*, Article 107831. https://doi.org/10.1016/j.ijpe.2020.107831

[14] 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

[15] Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf

[16] Pournader, M., Shi, Y., Seuring, S., & Koh, S. C. L. (2020). Blockchain applications in supply chains, transport and logistics: A systematic review of the literature. *International Journal of Production Research, 58*(7), 2063–2081. https://doi.org/10.1080/00207543.2019.1650976

[17] Queiroz, M. M., & Fosso Wamba, S. (2019). Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA. *International Journal of Information Management, 46*, 70–82. https://doi.org/10.1016/j.ijinfomgt.2018.11.021

[18] 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

[19] 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

[20] Wang, Y., Han, J. H., & Beynon-Davies, P. (2019). Understanding blockchain technology for future supply chains: A systematic literature review and research agenda. *Supply Chain Management: An International Journal, 24*(1), 62–84. https://doi.org/10.1108/SCM-03-2018-0148

[21] Werbach, K., & Cornell, N. (2017). Contracts ex machina. *Duke Law Journal, 67*(2), 313–382.

[22] Wüst, K., & Gervais, A. (2018). Do you need a blockchain? In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)* (pp. 45–54). IEEE. https://doi.org/10.1109/CVCBT.2018.00011

[23] Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. *Financial Innovation, 5*, Article 27. https://doi.org/10.1186/s40854-019-0147-z

[24] Yermack, D. (2017). Corporate governance and blockchains. *Review of Finance, 21*(1), 7–31. https://doi.org/10.1093/rof/rfw074

[25] Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services, 14*(4), 352–375. https://doi.org/10.1504/IJWGS.2018.095647