CIMEGS-SEJ

DIAMOND OPEN ACCESS · ISSN 2819-6252 (ONLINE)

CIMEGS-SEJ

Socio-Economic Journal

journal homepage: journal.cimeg.ca

VOLUME 2
ISSUE 2
YEAR 2026

CONCEPTUAL PAPER

Blockchain and Environmental Trust in Green Value Chains in the Middle East and North Africa

Tebra Mokaddem*, Abdelkarim Bestani

Mustapha Stambouli University, Mascara, Algeria

ARTICLE INFO

Article history
Received 17 April 2026
Revised 6 July 2026
Accepted 21 August 2026
Published 1 October 2026

Keywords
Blockchain
Environmental trust
Green value chains
Middle East and North Africa
Traceability
Accountability
Governance

JEL classification
O33, Q56, L14, Q58

ABSTRACT

Environmental claims in green value chains depend on information that buyers, investors and regulators may find difficult to verify. This article examines how blockchain could support the recording and review of that information in the Middle East and North Africa (MENA). It uses a conceptual narrative synthesis of research on organisational trust, supply chain governance and blockchain, together with selected policy material and published studies concerning the United Arab Emirates and Jordan. The proposed framework connects five trust-related problems with possible ledger functions and the conditions needed for their use. Shared records may improve access to evidence, provenance tracking and the detection of later changes. They do not establish the accuracy of physical measurements or environmental claims at the point of entry. Smart contracts can execute coded rules, while certification, data assurance and institutional responsibility remain necessary. The regional survey studies describe associations within particular samples; a separate supply chain model illustrates how incentives may differ among actors. These sources do not constitute a validation of the framework or proof of environmental improvement. The article proposes that organisations evaluate data quality, access rights, governance, interoperability and total costs before adopting blockchain for environmental purposes.

* Corresponding author: Tebra Mokaddem, m.tebra@univ-mascara.dz

E-mail addresses: m.tebra@univ-mascara.dz (T. Mokaddem), abdelkarim.bestani@univ-mascara.dz (A. Bestani)

Cite this article: Mokaddem, T., & Bestani, A. (2026). Blockchain and Environmental Trust in Green Value Chains in the Middle East and North Africa. *CIMEGS-SEJ*, *2*(2), 40–47. https://doi.org/10.68808/ge48hj86

CC BY 4.0

© 2026 The Author(s). Published by the Canadian Institute for Middle East and Gulf Studies (CIMEGS), Canada. This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), https://creativecommons.org/licenses/by/4.0/, which permits unrestricted use, distribution and reproduction in any medium, provided the original author(s) and source are credited.

1. Introduction

Green value chains seek to connect production and exchange with environmental objectives. Their credibility depends on how organisations measure, communicate and verify their impacts. The United Nations Environment Programme (UNEP, 2021) places economic activity within the connected climate, biodiversity and pollution crises, while Schaltegger and Burritt (2018) distinguish the motivations underlying corporate sustainability practices. An environmental claim therefore needs to be assessed through its evidence and scope, as well as the organisation's stated aims.

We use environmental trust to mean stakeholders' confidence that claims about environmental practices and outcomes are credible and open to scrutiny. Attributes such as carbon intensity, material origin and recycled content may be difficult for a downstream buyer to assess directly. The problem concerns access to reliable measurements, the basis of a claim and the responsibility for checking it.

Lyon and Montgomery (2015) review forms of misleading environmental communication. Darnall et al. (2018) examine how certification and sponsor trust relate to consumers' ecolabel use. These studies help explain why environmental claims require assurance; they do not

imply that every certification or reporting arrangement fails.

The question has practical relevance for MENA value chains. Lelieveld et al. (2016) examine projected heat extremes in the region, illustrating the need for credible assessment of environmental change. Blockchain-related research and policy material also address selected regional settings, including energy and industrial supply chains. These settings provide context for the present analysis without representing all MENA countries.

Blockchain provides a shared ledger whose records can be resistant to, and reveal evidence of, alteration under defined operating conditions. Access and control depend on the network's design. Tapscott and Tapscott (2016) discuss its wider business possibilities, while technical reviews describe its mechanisms and limitations (Yli-Huumo et al., 2016; Zheng et al., 2018). Yaga et al. (2018) distinguish tamper resistance from absolute immutability and explain the difficulty of checking external inputs.

For environmental purposes, a ledger could link records to products, materials or transactions and make the history available to authorised participants. Smart contracts could execute actions when specified digital conditions are met. These functions may support assurance processes, but the reliability of environmental measurements, input providers and organisational controls remains essential (Saberi et al., 2019; Centobelli et al., 2022).

Adoption also involves costs, coordination and institutional arrangements. Kouhizadeh et al. (2021) analyse barriers to sustainable supply chain adoption, and Kshetri (2021) examines applications in developing-country settings. Neither technical capability nor adoption alone establishes that an organisation has achieved an environmental benefit.

This article asks how blockchain could support environmental trust, which conditions would make the records useful, and which responsibilities remain outside the ledger. We focus on a conceptual framework and use selected studies concerning the United Arab Emirates (UAE) and Jordan as contextual evidence. We do not estimate the causal effect of blockchain or undertake a comprehensive comparison of national legal systems.

2. Theoretical background and literature review

2.1. *Environmental trust and green value chains*

Organisational trust provides a useful starting point, but trust and trustworthiness are distinct concepts. Mayer et al. (1995) identify ability, benevolence and integrity as dimensions of perceived trustworthiness. Pirson and Malhotra (2011) show that the dimensions relevant to trust vary with stakeholder relationships. We apply these perspectives to environmental claims as an analytical interpretation, rather than treat either study as a ready-made measure of environmental trust.

Several information problems affect the assessment of green value chains. Producers and other upstream actors may know more about processes than buyers. Some environmental attributes are difficult to observe through a purchase or ordinary product use. Effects may also occur at a different place or time from the transaction. O'Rourke (2014) discusses the measurement and information challenges of sustainable supply chains.

Responsibility is also distributed among organisations with different roles and bargaining power. Gereffi et al. (2005) analyse forms of global value chain governance. Ponte (2020) examines business, sustainability management and capital accumulation within global value chains. These perspectives suggest that access to environmental information should be considered alongside control over decisions and the distribution of costs.

Certification, reporting and audits can help address information problems, although their quality and incentives vary. Darnall et al. (2018) find that third-party certification can matter where consumers distrust business-sponsored ecolabels. Dauvergne and Lister (2013) critically examine corporate uses of sustainability. The appropriate question is how a ledger might complement assurance and oversight, rather than assume that digital records can replace them.

2.2. *Blockchain as a recording and coordination infrastructure*

A blockchain records transactions in linked blocks and uses agreed procedures to maintain a shared history. In a permissionless network, participation is relatively open; in a permissioned network, designated actors control participation and validation. Distribution of the ledger does not necessarily imply an equal distribution of organisational power (Yaga et al., 2018).

Decentralisation can reduce reliance on a single record holder, but control may remain concentrated among operators, validators or a consortium. Governance rules determine who may join, write records, change software and resolve disputes. These choices affect resilience and the opportunity for manipulation.

Transparency also depends on access rights. A shared ledger may allow authorised participants to inspect relevant records, while sensitive commercial or personal information may require restricted access. Visibility of a transaction history is different from independent confirmation of the environmental claim attached to it.

Tamper resistance can help preserve an audit trail after information is recorded. It does not make the original information true or prevent every attack, software change or governance failure. Environmental data may originate in human reports, sensors or other external systems. Checking these inputs remains a separate task (Yaga et al., 2018).

A smart contract executes programmed rules using information available to it. Network consensus concerns agreement on transactions and ledger state; it is not a measurement of pollution or compliance. A program using external environmental information relies on an

input mechanism, often called an oracle, whose reliability needs separate assessment (Yaga et al., 2018).

Kouhizadeh and Sarkis (2018) discuss opportunities and caveats for greener supply chains. Centobelli et al. (2022) examine trust, traceability and transparency in circular supply chains. These contributions motivate possible applications, including tracking material provenance and recording evidence for environmental claims. They do not remove the need to establish the physical connection between an asset and its digital record.

2.3. *Reengineering assurance processes*

We use reengineering to describe redesigning how organisations record, share and review environmental information. Hammer and Champy (1993) provide the broader process-redesign concept. Its application to environmental assurance here is our conceptual extension.

Some reconciliation or verification tasks could be automated, potentially changing the role of intermediaries. Organisations would still need people or institutions to define environmental criteria, inspect physical processes and address disputes. Any saving should be assessed against implementation, data assurance and coordination costs (Saberi et al., 2019; Kshetri, 2021).

Shared records can help identify who supplied information and which actions followed. Accountability also requires assigned responsibilities, access to explanations and a means of correcting or contesting a decision. A distributed ledger alone does not distribute legal responsibility or establish effective oversight.

A token may represent an asset or an environmental attribute within a digital system. The representation does not by itself establish a valid environmental benefit, exclusive ownership or a liquid market. Systems need rules connecting issuance, transfer and retirement to the underlying asset or claim. This is a design and assurance requirement, rather than an automatic outcome of tokenisation.

2.4. *Selected empirical studies and policy context*

The sources considered here provide different kinds of evidence. The UAE and Jordan studies use cross-sectional survey data. A separate circular supply chain study uses mathematical models, and official policy material describes aims and implementation considerations. These sources should be interpreted according to their methods.

Mothafar et al. (2024) analyse blockchain technology enablers and sustainable supply chain outcomes using interviews and a survey of 462 employees in UAE firms. Their structural model reports positive social and environmental coefficients. The direct economic coefficient is negative but not statistically supported, so it should not be read as evidence of economic harm. The study also reports indirect pathways involving green hydrogen acceptance. These are sample-specific model results, not an evaluation of measured emissions before and after deployment.

AlMaaitah (2026) examines blockchain-based financial technology and environmental, social and governance (ESG) compliance in Jordanian energy supply chains using a cross-sectional survey and partial least squares structural equation modelling. The study reports a positive adoption-compliance relationship, but the proposed moderating role of supply chain governance is not supported. That result does not establish that institutions are unnecessary; it limits the evidence for the particular moderation relationship tested.

Akbarzadeh Sarabi et al. (2026) model a circular closed-loop supply chain using Stackelberg and evolutionary game approaches. Their results illustrate how blockchain costs, consumer responses and carbon-policy incentives can affect participants differently under the model's assumptions. This is theoretical evidence about incentives, rather than an observed MENA implementation or a finding that subsidies always fail.

The Emirates Blockchain Strategy 2021, launched in April 2018, provides historical context for UAE government interest in blockchain (UAE Government, n.d.). Its transaction-conversion and savings statements are policy aims, not environmental outcomes established here. The United Nations Economic and Social Commission for Western Asia (ESCWA, 2024) discusses digital infrastructure, skills and institutional conditions in its report on the Arab region's sustainable energy transition. Such policy material helps identify questions for implementation; it does not validate the present framework.

3. Research questions and analytical propositions

The central question is how blockchain could support credible environmental information and accountable decision-making in MENA green value chains. We consider the relationship between the information problem, the proposed ledger function and the institutional conditions needed for its use.

Four questions guide the analysis:

1. Which recording and coordination functions could address particular environmental trust deficits?
2. Which data, institutional and infrastructure conditions are necessary for these functions to be useful?
3. How could provenance records and programmed actions support traceability and accountability?
4. Which costs, risks and governance problems could limit their contribution?

3.1. *Analytical propositions*

The propositions organise conceptual enquiry. They are conditional expectations for future investigation, rather than hypotheses statistically tested in this article.

P1. Shared access to relevant, reliable records may reduce information asymmetry and help stakeholders assess environmental claims.

P2. The contribution of a ledger depends on data assurance, governance, institutional arrangements and usable digital infrastructure.

P3. Provenance records, tamper-resistant histories and programmed checks may support accountability when responsibilities and procedures for challenge are clear.

P4. Fragmented systems, incompatible standards, unequal incentives and limited organisational capacity may increase costs and constrain useful adoption.

4. Methodology

We use a conceptual qualitative design based on a narrative synthesis of literature and selected policy material. We relate trust and governance concepts to blockchain functions, then consider published studies concerning the UAE and Jordan. The article collects no new interviews, survey responses or operational measurements.

4.1. *Conceptual synthesis*

The synthesis starts with difficulties in accessing, checking and assigning responsibility for environmental information. It maps five analytical problem areas to possible ledger functions: information asymmetry, hard-to-observe environmental attributes, audit vulnerability, fragmented accountability and verification costs. These categories organise the framework and are not empirically validated latent constructs.

The analysis distinguishes record integrity from input accuracy and environmental performance. A consistent transaction history may assist an audit, while the claim itself still depends on measurement and assurance. This distinction applies throughout the framework.

4.2. *Policy and institutional context*

We use the UAE strategy and ESCWA report to discuss policy objectives and implementation conditions. The UAE and Jordan survey studies offer context for selected organisational relationships. We do not rank national institutional quality or infer a country's entire regulatory position from one study.

The policy discussion considers questions about access rights, responsibility, evidence, data protection, interoperability and dispute handling. It identifies matters for project design and jurisdiction-specific assessment. It does not constitute a comprehensive legal analysis or establish that records and smart contracts lack recognition throughout MENA.

4.3. *Use of published studies*

Mothafar et al. (2024) and AlMaaitah (2026) provide contextual survey evidence. Akbarzadeh Sarabi et al. (2026) provide a theoretical comparison of incentives. We consider the sources' research designs and the outcomes they examine before relating them to the propositions.

These sources are illustrations drawn from the literature, rather than a newly assembled sample of operational blockchain projects. A survey of adoption perceptions, a government strategy and a mathematical model do not by themselves document a live environmental application. We therefore make no claim to an independent deployment or impact audit.

4.4. *Sources and analytical approach*

Sources include research on organisational trust, sustainability and supply chain governance; blockchain studies and technical guidance; and selected official policy material. We compare the proposed mechanism with the evidence needed to support its environmental interpretation. The technical overview from the National Institute of Standards and Technology (NIST) provides a basis for distinguishing ledger functions from claims about external data (Yaga et al., 2018).

The synthesis is purposive and interpretive. It does not use a documented systematic search protocol, exhaustive screening process or formal quality-scoring procedure. We do not calculate pooled effects or treat agreement among sources using different methods as an independent validation of the framework.

The analytical sequence is to identify a trust-related problem, describe a relevant ledger function, specify necessary data and governance conditions, and distinguish a possible information benefit from an environmental outcome. Table 1 summarises these relationships.

4.5. *Limitations*

The narrative selection of sources may omit relevant evidence. The regional discussion concentrates on selected UAE and Jordan studies and cannot represent the diversity of MENA countries or sectors. The article offers no estimate of the prevalence of blockchain deployment across the region.

The framework has not been tested against new field data. Survey associations, mathematical model results and policy aims answer different questions and cannot be combined as a causal estimate of blockchain effectiveness. In particular, perceived ESG compliance is not equivalent to independently measured environmental improvement.

Published descriptions may also give more attention to proposed benefits than to failed implementations, operating costs or distributional effects. Further research needs independent project evidence, baseline comparisons and information about data quality, governance and lifecycle resource use.

5. Analytical findings

5.1. *Potential contributions to environmental assurance*

The conceptual mapping identifies ways to make environmental information easier to trace and review. A shared history may reduce duplicated reconciliation, link claims to evidence and help reveal later changes. Each contribution depends on the completeness of records, access rights and the credibility of the data source.

Distributing validation may reduce dependence on one record holder. It does not eliminate collusion, unequal influence or dependence on a platform operator. Decisions about participation, permissions and software changes remain important to the quality of assurance.

A tamper-resistant history can help an auditor identify which information was entered and when. It cannot correct a faulty sensor reading or a misleading original report. An environmental claim still requires a defined measurement method and checks on the underlying process.

Shared visibility can help users inspect evidence where they have access and the skills to interpret it. It should not be equated with open public access or guaranteed market discipline. The relevant design question is whether the intended user can examine sufficient evidence to assess the claim.

Blockchain can therefore change the way participants organise information and assurance. Trust remains directed towards data providers, technical operators, governance rules and the institutions responsible for environmental standards. The ledger complements these relationships.

5.2. *Institutional and infrastructure requirements*

The literature raises implementation questions concerning rules, infrastructure and organisational capacity. These are conditions for evaluating a project, rather than findings from a comprehensive survey of national legal systems. Kouhizadeh et al. (2021) and Kshetri (2021) discuss adoption barriers and institutional context, while ESCWA (2024) considers regional energy-transition requirements.

Participants need clear arrangements for who submits data, who reviews it, which evidence supports a decision and how an error or dispute is handled. Recognition and enforceability require assessment in the relevant jurisdiction and application. A coded action does not settle questions of responsibility.

Operational systems also need reliable connectivity, compatible data definitions and a practical means of linking actors, assets and records. Digital identification can be one component, but a particular national identity architecture is not a universal prerequisite for every blockchain design. Interoperability concerns the meaning and quality of shared data as well as technical connections.

Staff need sufficient capability to manage records, security, environmental measurement and the rules governing automated actions. Technical installation alone does not establish that an organisation can maintain or challenge the resulting decisions. Training and continuing oversight are therefore proposed implementation priorities.

5.3. *Traceability and accountability*

Provenance records may help follow products, materials and claims across stages of a value chain. Their value depends on maintaining the connection between the physical asset and its record, recording relevant transformations and identifying information providers. Traceability describes the history available for review; it does not establish a favourable environmental outcome (Centobelli et al., 2022).

Smart contracts could trigger a payment or reporting action when defined digital conditions are met. The program's output depends on its code and inputs. Environmental certification may still require an authorised assessment outside the program. Program execution, technical transaction validation and environmental assurance are separate functions.

The UAE and Jordan surveys offer contextual evidence of relationships between blockchain-related practices and perceived sustainability or compliance. They do not isolate ledger provenance or automation as the causal mechanism. The unsupported governance moderation in AlMaaitah (2026) also cautions against claiming that every governance relationship in the framework has empirical support.

5.4. *Costs and risks*

Implementation can require investment in integration, security, data collection, assurance and coordination. Some costs may fall on smaller suppliers or actors with limited influence over the system. Adoption needs a comparison with feasible alternatives, including a conventional shared database, rather than an assumption that blockchain is always necessary (Saberi et al., 2019).

Energy use depends on consensus and network design. Proof-of-work can require substantial computation, while other mechanisms can use less energy. Permissioned access is an access-control arrangement, not itself a consensus algorithm or a guarantee of environmental efficiency. Evaluation should include the wider system and its operating requirements (Yaga et al., 2018; ESCWA, 2024).

Governance risks include concentrated control, exclusion from records, weak arrangements for correction and uncertainty about responsibility. Sensitive information also requires suitable access and security controls. A permanent shared history can create practical difficulties where information is wrong or should no longer be widely accessible.

Incentives may differ among participants. Akbarzadeh Sarabi et al. (2026) show within their model that the distribution of costs and policy incentives can affect adoption and profitability differently across supply chain members. These conditional results motivate attention to cost sharing; they do not establish that fragmentation has a particular probability or that a national strategy guarantees scalability.

6. Discussion

6.1. *Proposed framework for environmental trust*

Table 1 connects five trust-related problems with potential recording or coordination functions and their limits. It is a conceptual guide for designing questions and evaluating projects. The proposed contributions require evidence in each application.

Table 1 Environmental trust problems and potential blockchain contributions

Trust problem	Potential function	Possible contribution	Conditions and limits
Information asymmetry	Shared ledger access	Users can inspect relevant evidence and its history.	Access rights, completeness and user capability determine what can be checked.
Hard-to-observe attributes	Provenance records	Claims can be linked to identified materials, assets or transactions.	Physical links, measurement and independent assurance remain necessary.
Audit vulnerability	Tamper-resistant history	Later alterations may be harder to conceal.	The original input may still be wrong; security and governance remain relevant.
Fragmented accountability	Attributed records and coded checks	Contributors and programmed actions can be traced.	Responsibilities, external inputs, review and dispute procedures must be defined.
Verification costs	Automated reconciliation and rule execution	Some repeated processing may require less manual work.	Net savings depend on integration, assurance, operating and coordination costs.

Source: Authors' conceptual synthesis of the literature discussed in the text, including Yaga et al. (2018), Saberi et al. (2019), Kouhizadeh et al. (2021) and Centobelli et al. (2022).

The framework separates information access, record integrity, physical verification and responsibility. An organisation could improve one of these while leaving others unchanged. Evaluation should therefore specify which problem the project addresses and which outcome would demonstrate improvement.

6.2. *Assessment of the analytical propositions*

The synthesis provides a rationale for investigation rather than a statistical test of P1-P4.

P1 is plausible where participants can access relevant evidence and have confidence in its source. The literature motivates shared visibility, but this article does not measure a reduction in information asymmetry or an increase in environmental trust.

P2 identifies data assurance and institutional arrangements as design conditions. It is not confirmed as a universal moderation relationship. In particular, AlMaaitah (2026) does not support the specific supply chain governance moderation tested in that study.

P3 distinguishes a record of actions from effective accountability. Provenance and programmed checks may help an investigation, while responsibility, meaningful review and reliable inputs remain necessary. No direct accountability or environmental-performance effect is estimated here.

P4 draws attention to compatibility, capacity and the distribution of incentives. Adoption-barrier research and the circular supply chain model motivate these concerns. Comparative project evidence is needed to establish how they affect implementation in particular MENA settings.

6.3. *Implications for policy and practice*

The proposed implications concern project evaluation and governance. They should be adapted to the relevant sector and jurisdiction and assessed against measurable objectives. A decision to use blockchain should follow a clear information problem and a comparison of alternatives.

6.3.1. Rules and responsibilities

Before implementation, participating organisations should specify data ownership and access, submission and review roles, security responsibilities and procedures for errors and disputes. The applicable treatment of digital evidence and automated agreements requires a jurisdiction-specific assessment.

Controlled experimentation could help evaluate the process before expansion. An assessment should examine whether participants can question a record or decision, how incorrect information is addressed and which environmental evidence supports a claim. These are proposed safeguards, rather than a finding that any particular country lacks them.

6.3.2. Infrastructure and interoperability

Projects need compatible identifiers, data definitions and evidence requirements across participating systems. A shared ledger is useful only if participants can interpret the records and connect them with the underlying activity. Infrastructure decisions should account for suppliers with limited technical capacity.

Interoperability planning should include data quality, permissions and the continuity of records across systems. Regional cooperation could help where chains cross borders, but its benefits need to be assessed against sector-specific requirements and existing arrangements.

6.3.3. Organisational capacity

Training should connect ledger operation and cybersecurity with environmental measurement and assurance. Firms, auditors and relevant public bodies need to understand the limits of automated checks as well as their possible uses. Responsibility for reviewing inputs and maintaining the system should remain explicit.

Project evaluation also needs participation from technical, environmental and governance specialists, together with those who bear the costs of collecting data. This

would help identify practical burdens and the evidence needed to assess a proposed benefit.

6.3.4. Integration with environmental objectives

Organisations should define an environmental objective before choosing the technology. A project intended to reduce emissions, improve recovery or verify material origin needs indicators appropriate to that objective and a credible baseline.

Operating costs, energy requirements, participation and information quality should be assessed alongside the target outcome. Greater transaction visibility is an information result; an environmental gain requires evidence about the physical process or impact.

Coordination with wider digital and environmental policies may help avoid duplicate systems and clarify responsibilities. Pilot evaluation and independent scrutiny should determine whether expansion is warranted. The appropriate scale and governance model depend on the application.

7. Conclusion

Blockchain may support environmental trust by helping participants share records, trace provenance and detect later changes. Its contribution depends on reliable inputs and an appropriate connection between digital records and physical processes. It does not establish the truth of an environmental claim simply by recording it.

The proposed framework links five trust-related problems with possible ledger functions and the conditions needed for their use. The selected UAE and Jordan surveys provide contextual associations, while the circular supply chain model illustrates conditional incentives. Together, these sources motivate further investigation but do not validate the framework or demonstrate a regional environmental effect.

Future research could compare operational projects with feasible alternatives, examine data-assurance arrangements and track costs and environmental outcomes over time. Customer, supplier and regulator perspectives would help determine whether more accessible records improve trust and accountability in practice. For policy and management, the main task is to match the information problem with a proportionate technical and institutional response.

Declarations

Funding. This research received no external funding.

Conflicts of Interest. The author(s) declare no conflicts of interest.

References

Akbarzadeh Sarabi, M., Taleizadeh, A. A., & Bhattacharya, A. (2026). Towards blockchain-enabled circular closed-loop supply chain and impact of consumers' distrust in price, product greenness sensitivity and carbon tax and subsidy. European Journal of Operational Research, 328(1), 105–121. https://doi.org/10.1016/j.ejor.2025.06.030

AlMaaitah, N. (2026). Blockchain-based FinTech and ESG compliance in energy supply chains: The moderating role of supply chain governance. International Journal of Energy Economics and Policy, 16(2), 1290–1297. https://doi.org/10.32479/ijeep.23057

Centobelli, P., Cerchione, R., Del Vecchio, P., Oropallo, E., & Secundo, G. (2022). Blockchain technology for bridging trust, traceability and transparency in circular supply chain. Information & Management, 59(7), Article 103508. https://doi.org/10.1016/j.im.2021.103508

Darnall, N., Ji, H., & Vázquez-Brust, D. A. (2018). Third-party certification, sponsorship, and consumers' ecolabel use. Journal of Business Ethics, 150(4), 953–969. https://doi.org/10.1007/s10551-016-3138-2

Dauvergne, P., & Lister, J. (2013). Eco-business: A big-brand takeover of sustainability. MIT Press.

Gereffi, G., Humphrey, J., & Sturgeon, T. (2005). The governance of global value chains. Review of International Political Economy, 12(1), 78–104. https://doi.org/10.1080/09692290500049805

Hammer, M., & Champy, J. (1993). Reengineering the corporation: A manifesto for business revolution. HarperBusiness.

Kouhizadeh, M., & Sarkis, J. (2018). Blockchain practices, potentials, and perspectives in greening supply chains. Sustainability, 10(10), Article 3652. https://doi.org/10.3390/su10103652

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

Kshetri, N. (2021). Blockchain and sustainable supply chain management in developing countries. International Journal of Information Management, 60, Article 102376. https://doi.org/10.1016/j.ijinfomgt.2021.102376

Lelieveld, J., Proestos, Y., Hadjinicolaou, P., Tanarhte, M., Tyrlis, E., & Zittis, G. (2016). Strongly increasing heat extremes in the Middle East and North Africa (MENA) in the 21st century. Climatic Change, 137(1–2), 245–260. https://doi.org/10.1007/s10584-016-1665-6

Lyon, T. P., & Montgomery, A. W. (2015). The means and end of greenwash. Organization & Environment, 28(2), 223–249. https://doi.org/10.1177/1086026615575332

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of Management Review, 20(3), 709–734. https://doi.org/10.5465/amr.1995.9508080335

Mothafar, N. A., Zhang, J., Alsoffary, A., Aslam, M. A., AL-Barakani, A., Alhady, O. S., Esangbedo, C. O., & Kone, S. D. (2024). Effecting the adoption of blockchain technology enablers in supply chain sustainability with green hydrogen acceptance role as a mediator: Evidence from complex decarbonization industries in the United Arab Emirates. International Journal of Hydrogen Energy, 84, 1085–1100. https://doi.org/10.1016/j.ijhydene.2024.08.243

O'Rourke, D. (2014). The science of sustainable supply chains. Science, 344(6188), 1124–1127. https://doi.org/10.1126/science.1248526

Pirson, M., & Malhotra, D. (2011). Foundations of organizational trust: What matters to different stakeholders? Organization Science, 22(4), 1087–1104. https://doi.org/10.1287/orsc.1100.0581

Ponte, S. (2020). Green capital accumulation: Business and sustainability management in a world of global value chains. New Political Economy, 25(1), 72–84. https://doi.org/10.1080/13563467.2019.1581152

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

Schaltegger, S., & Burritt, R. (2018). Business cases and corporate engagement with sustainability: Differentiating ethical motivations. Journal of Business Ethics, 147(2), 241–259. https://doi.org/10.1007/s10551-015-2938-0

Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world. Portfolio/Penguin.

UAE Government. (n.d.). Emirates Blockchain Strategy 2021. https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/strategies-plans-and-visions-untill-2021/emirates-blockchain-strategy-2021

United Nations Economic and Social Commission for Western Asia. (2024). The role of blockchain in the sustainable energy transition in the Arab region (E/ESCWA/CL1.CCS/2023/TP.1). https://www.unescwa.org/sites/default/files/pubs/pdf/role-blockchain-sustainable-energy-transition-arab-region-english.pdf

United Nations Environment Programme. (2021). Making peace with nature: A scientific blueprint to tackle the climate, biodiversity and pollution emergencies. https://www.unep.org/resources/making-peace-nature

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain technology overview (NISTIR 8202). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8202

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? A systematic review. PLOS ONE, 11(10), Article e0163477. https://doi.org/10.1371/journal.pone.0163477

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