

Blockchain e Segurança de Indicadores Ambientais

Gustavo Leite¹, Bernardo Alcalde¹, Thiago Rossi¹,
Carlos Oliveira², Victor Souza², Wilson Melo²

¹Instituto Ecosis
Porto Alegre – RS

²Instituto Nacional de Metrologia, Qualidade, e Tecnologia (Inmetro)
Duque de Caxias – RJ

E-mail contato: gustavo.leite@ecosis.com.br

Abstract. *Never before has so much environmental data been produced — and never has it been so difficult to trust it. This article presents a solution developed by the Ecosis Institute that manages the recording of environmental indicators using blockchain and digital signatures at the data generation. The proposed architecture is flexible enough to accept data from both autonomous devices and user-provided information. This solution is innovative for adopting a hybrid on-chain/off-chain storage model and utilizing smart contracts to verify the digital signatures of the data, thereby ensuring security, scalability, and auditability.*

Resumo. *Nunca se gerou tanto dado ambiental — e nunca foi tão difícil confiar neles. Este artigo apresenta uma solução desenvolvida pelo Instituto Ecosis que gerencia o registro de indicadores ambientais com uso de blockchain e assinatura digital na origem do dado. A arquitetura proposta é flexível para aceitar tanto dados de dispositivos autônomos como informações providas diretamente por um usuário. Tal solução é inovadora por adotar armazenamento híbrido on-chain/off-chain e empregar contratos inteligentes na verificação da assinatura digital dos dados, garantindo segurança, escalabilidade e auditabilidade.*

1. Introdução

O planeta enfrenta uma crise ambiental sem precedentes, caracterizada por mudanças climáticas aceleradas, perda de biodiversidade e níveis críticos de poluição. O conceito dos “limites planetários” indica que diversas fronteiras ecológicas já foram ultrapassadas, colocando em risco a estabilidade dos sistemas que sustentam a vida humana [Rockström et al. 2009]. Relatórios recentes do Painel Intergovernamental sobre Mudanças Climáticas reforçam a urgência de ações coordenadas e integradas para mitigar esses impactos e promover sustentabilidade [IPCC 2021].

Atrelada ao contexto de crise, a multiplicação de sistemas de monitoramento, o maior desafio não é mais obter informação, mas garantir sua rastreabilidade, legitimidade, segurança e padronização, sem comprometer a capacidade de agir em tempo hábil. Governos, empresas e comunidades enfrentam um paradoxo: quanto mais dados se acumulam, maior o risco de ineficiência decisória, sobrecarga operacional e desconfiança sistêmica.

Desafios estruturais, como a falta de transparência, a dificuldade de auditoria e a assimetria de informações em projetos ambientais persistem e comprometem a

confiança de investidores, reguladores e comunidades locais. Tecnologias digitais emergentes surgem como alternativas promissoras para garantir rastreabilidade, integridade e automação no monitoramento ambiental [Tapscott and Tapscott 2016, Fang et al. 2020, Zhou et al. 2023, Safeer et al. 2025], promovendo modelos mais confiáveis e inclusivos de governança sustentável.

A literatura tem explorado o uso de tecnologias blockchain como solução promissora para garantir a integridade, autenticidade e rastreabilidade de indicadores ambientais [Carrières et al. 2021, Nygaard and Silkoset 2023]. A blockchain tem despertado crescente interesse em setores como a indústria, academia e órgãos reguladores [AlShamsi et al. 2022]. Sua adoção pode constituir uma base consistente para empresas e organizações que buscam modelos de negócio orientados a dados [Gschnaidtner et al. 2024]. Diferentes trabalhos demonstram seu potencial em cenários diversos, por exemplo na prevenção de fraudes de dados na indústria alimentícia [Boller et al. 2024], na gestão de frotas veiculares e controle de emissões [Melo et al. 2022], e no monitoramento de infraestruturas críticas que envolvem risco ambiental [Melo Jr et al. 2022]. Além disso, o uso de assinaturas digitais na origem do dado, especialmente em ambientes que envolvem dispositivos autônomos, mostra-se eficaz para validar informações de forma descentralizada e eficiente [Moni et al. 2021, Meisami et al. 2025], reforçando a importância de estudos aplicados que integrem essas abordagens.

Este artigo apresenta uma solução desenvolvida pelo Instituto Ecosis, em parceria com pesquisadores do Inmetro, para o registro confiável de indicadores ambientais utilizando blockchain e assinatura digital na origem dos dados. A arquitetura é flexível para incluir diferentes tipos de clientes, desde dispositivos IoT autônomos, até usuários utilizando ferramentas de coleta de dados, como *tablets* e *handhelds*. A solução permite ainda que o cliente agregue uma assinatura de chave pública ao registro de dados, introduzindo um mecanismo adicional de segurança. Deste modo, o diferencial da proposta reside na verificação automatizada da origem, integridade e autenticidade dos dados, eliminando intermediários e aumentando a confiabilidade do sistema. Todo o processo de armazenamento e auditoria dos indicadores ambientais envolve ainda um *trade-off* entre implementação *on-chain* e *off-chain*, o que contribui para que a solução mantenha a escalabilidade e auditabilidade, promovendo maior transparência, rastreabilidade e segurança em projetos e soluções de monitoramento ambiental, com potencial de ampliar a confiança de atores públicos, privados e comunitários envolvidos.

2. Trabalhos Relacionados

A coleta, disponibilização e divulgação de dados e indicadores ambientais por parte da indústria é de grande importância para construir e manter a confiança da sociedade, incluindo consumidores e investidores. Tal prática é vital para a transição verde dos mercados, uma vez que dados confiáveis permitem medir e gerenciar iniciativas ambientais de forma eficaz e combater práticas ilícitas que comprometam o avanço sustentável. Entretanto, a literatura especializada sobre o tema mostra que a confiabilidade desses indicadores nem sempre pode ser atestada [Howe et al. 2025]. Dada a pressão pela conformidade regulatória e a necessidade de criar uma imagem positiva, muitas organizações podem recorrer a práticas irregulares, como o *greenwashing* [Nygaard and Silkoset 2023], por exemplo. Em outros cenários, relatórios de indicadores apresentados de forma voluntária

podem focar aspectos limitados, omitindo informações indesejadas, e não provendo detalhes sobre estratégias de negócio ou obrigações legais, além da falta de padronização e consistência no uso destes indicadores pela indústria [Mengistu and Panizzolo 2023].

Neste contexto, blockchains podem constituir soluções técnicas que contribuam significativamente para a confiabilidade de indicadores ambientais, especialmente em relação à integridade, autenticidade e rastreabilidade desses dados [Carrières et al. 2021, Nygaard and Silkoset 2023]. Embora uma originalmente vinculada a aplicações associadas à emissão e negociação de criptomoedas, esta tecnologia tem se expandido significativamente nos últimos anos, despertando o interesse não apenas da comunidade acadêmica, mas também da indústria e de organismos de regulação [AlShamsi et al. 2022]. Tal interesse caracteriza inclusive uma grande oportunidade de negócio, uma vez que de acordo com [Gschnaidtner et al. 2024], apenas 0,88% das organizações utilizam *blockchain* atualmente, mesmo com os dados dos últimos anos indicando uma tendência de crescimento constante.

Diversos estudos exploram o potencial do *blockchain* em aplicações voltadas à segurança das informações armazenadas. Por exemplo, [Boller et al. 2024] investiga como tecnologias de registro distribuído (DLTs) podem contribuir para a prevenção de fraudes em sistemas de dados que gerenciam cadeias de suprimento associados à produção de alimentos orgânicos. Na área veicular, [Gaba et al. 2024] discute as vantagens do uso de *blockchain* ao gerenciar informações geradas por veículos conectados, algo que pode ser inclusive empregado em sistemas que registram emissões em tempo real [Melo et al. 2022]. Já [Melo Jr et al. 2022] avalia o uso de plataformas blockchain como o Ethereum e o Hyperledger Fabric no monitoramento de infraestruturas críticas, exemplificando o uso dessa tecnologia na gestão de indicadores associados a integridade física de elementos como barragens e taludes.

Nas aplicações que empregam blockchains para armazenamento de informações, o desempenho e escalabilidade é sempre um aspecto desafiante. Buscando soluções que conciliem estes requisitos com segurança e confiabilidade, diferentes estratégias de armazenamento podem ser pensadas. Muitos autores optam por um modelo híbrido que combina armazenamento *on-chain* e *off-chain* [Eren et al. 2025]. Enquanto o armazenamento *on-chain* garante a imutabilidade e segurança de informações consideradas mais críticas, o *off-chain* oferece menor custo, maior eficiência de acesso e recuperação de dados, e também maior capacidade de armazenamento. Essa abordagem híbrida supera as limitações de custo e escalabilidade do *blockchain* convencional, sendo particularmente eficaz em aplicações que lidam com grandes volumes de dados.

Além disso, com o avanço das aplicações descentralizadas (DApps) na Web 3.0, a prática de assinatura de mensagens *off-chain* tem se consolidado como uma alternativa eficiente à assinatura tradicional de transações *on-chain*, especialmente nos cenários onde a informação é gerada por algum dispositivo de medição inteligente, ou mesmo um IoT, de forma autônoma [Moni et al. 2021]. Nesse modelo, o cliente gera ainda na camada de aplicação uma assinatura de chave pública que pode ser agregada por serviços intermediários e, posteriormente, validada por contratos inteligentes. Tal abordagem oferece ganhos significativos em desempenho, usabilidade e redução de custos operacionais [Meisami et al. 2025].

3. Modelo de Negócio e Solução de Segurança do Instituto Ecosystems

A tecnologia *blockchain* desponta como uma abordagem promissora frente aos desafios de governança e confiabilidade de dados ambientais por proporcionar transparência, descentralização e rastreabilidade em sistemas de informação. Essas características permitem maior visibilidade e verificação ao longo de cadeias de valor complexas, assegurando a procedência de produtos e o cumprimento de padrões socioambientais. No setor alimentício, por exemplo, a plataforma IBM Food Trust demonstrou como é possível rastrear itens “da fazenda ao prato”, aumentando a confiança dos consumidores e a eficiência em recalls [Tapscott and Tapscott 2016].

Entretanto, a credibilidade de qualquer solução baseada em *blockchain* depende da integridade dos dados coletados. A arquitetura de referência desenvolvida pelo Instituto Ecosystems ilustra essa dinâmica: dispositivos remotos assinam digitalmente cada leitura, enviam-nas via API a um repositório *off-chain* e registram apenas *hashes* ou eventos-chave no *blockchain* para garantir imutabilidade e auditabilidade [Fang et al. 2020]. Esse modelo “Device-as-a-Service” integra módulos criptográficos nos dispositivos, criando um serviço de assinatura digital que alinha incentivos para manutenção contínua e atualização de *firmware* seguro [Zhou et al. 2023].

A *tokenização* de ativos ambientais, por sua vez, converte resultados mensuráveis — créditos de carbono, hectares reflorestados ou cotas de energia renovável — em *tokens* digitais negociáveis. Contratos inteligentes vinculados a esses *tokens* automatizam a liberação de fundos conforme metas verificadas por dispositivos sejam atingidas, assegurando auditoria em tempo real e evitando dupla contagem de benefícios [Zhou et al. 2023, Tapscott and Tapscott 2016]. Esse modelo de negócio viabiliza capital de impacto de forma mais ágil e transparente, reduzindo dependência de intermediários e ampliando a liquidez do mercado socioambiental. Em última instância, essa infraestrutura convergente conecta governos, empresas, ONGs e comunidades locais num ecossistema de confiança compartilhada, reduzindo assimetrias de informação e promovendo equidade na distribuição de benefícios — de modo que populações vulneráveis possam comprovar e monetizar suas ações de conservação diretamente no ledger público, sem intermediários [Tapscott and Tapscott 2016].

Em última análise, o uso de *blockchain* em iniciativas ambientais promete conectar atores de múltiplos setores — governos, empresas, organizações não governamentais e comunidades locais — em uma infraestrutura comum de confiança. Como todos os participantes passam a compartilhar registros transparentes e imutáveis, reduz-se a assimetria de informação e estabelece-se uma responsabilidade compartilhada pelos resultados. Isso promove maior equidade nas relações: comunidades de base, por exemplo, podem comprovar suas ações de conservação ou de redução de emissões diretamente no ledger público e, assim, receber recompensas ou pagamentos por desempenho de forma justa e sem intermediários. Paralelamente, órgãos reguladores e investidores globais ganham visibilidade em tempo real das atividades e impactos, alinhando os incentivos locais com as metas globais de sustentabilidade. Em síntese, a tecnologia *blockchain* atua como um elo de confiança distribuída entre o âmbito local e o global, catalisando ações colaborativas com potencial de impacto positivo amplificado [Tapscott and Tapscott 2016, Safeer et al. 2025, Muthu 2022].

4. Modelo de Implementação usando Hyperledger Fabric

Para por em prática o modelo de negócio descrito, o Instituto Ecosis desenvolveu em parceria com pesquisadores do Inmetro uma solução baseada em blockchain para registro confiável de indicadores ambientais. A solução emprega o conceito de assinatura de chave pública na origem da informação, de modo a permitir que diferentes clientes (desde sensores inteligentes instalados em campo até usuários preenchendo informações em um *tablet* ou *smartphone*) agreguem ao registro de dados um resumo criptográfico que garante a integridade e autenticidade das informações. Uma vez que essa assinatura pode estar baseada em dados heterogêneos, sua verificação é feita por meio de contratos inteligentes no blockchain, podendo incluir a validação dos ativos digitais escritos diretamente no *ledger* (i.e., *on-chain*) ou ainda em serviços de armazenamento externo (i.e., *off-chain*).

O projeto foi desenvolvido utilizando a plataforma Hyperledger Fabric [Androulaki et al. 2018], que é uma opção eficiente para constituição de redes permissionadas que atendem requisitos de *throughput* elevado, como é o caso de aplicações que envolvem IoT. O ambiente correspondente à rede do Fabric é gerenciada por meio do Kubernetes, sendo o *K3s*¹ a distribuição utilizada, por ser uma versão mais leve. Para auxiliar nesta implementação, utilizamos a ferramenta *Bevel Operator Fabric*, que simplifica a configuração do *Fabric* em um ambiente Kubernetes.

A aplicação desenvolvida implementa os mecanismos de segurança explicitamente na comunicação entre um módulo cliente e o contrato inteligente executado dentro do blockchain, que no Fabric é referido como *chaincode*. Este *chaincode* possui duas funções principais: *StoreFileData* e *CheckSignature*. O cliente é responsável pela geração dos dados, assinatura de chave pública e envio de transações. Para isso, o cliente deve possuir um par de chaves (i.e., pública e privada) ECDSA (*Elliptic Curve Digital Signature Algorithm*), que deve ser único por dispositivo. Com esses dados, o cliente pode submeter transações usando a primeira função do *chaincode* (i.e., *StoreFileData*), que permite o envio dos dados de indicadores ambientais juntamente com o *digest* correspondente à assinatura de chave pública desses dados, representada em *base64*. Esta assinatura é calculada a partir do resumo criptográfico (i.e., *hash*) dos dados, que é cifrado utilizando a chave privada do cliente. Os dados são então enviados para o blockchain com um ID que identifica o cliente. A auditoria dos indicadores ambientais, por sua vez, é obtida através da função *CheckSignature*. Por meio dela, o *chaincode* verifica se uma transação contendo dados de indicadores ambientais foi de fato assinada pelo cliente que possui aquele ID, através de sua chave pública registrada na rede.

Os testes com a plataforma desenvolvida foram executados por meio de dados simulados por um dispositivo IoT em bancada. Para isso, foi utilizado um sensor de temperatura DHT-22, conectado a um Raspberry 3B+ através de uma *protoboard*. Este dispositivo executa uma aplicação cliente, capaz de ler os valores de temperatura periodicamente, reportando-os ao blockchain como indicadores ambientais. O par de chaves ECDSA é gerado automaticamente pelo dispositivo, utilizando a curva elíptica NIST P-256, e armazenado no formato *Privacy-Enhanced Mail* (PEM). As chaves são mantidas em arquivos separados, nomeados de acordo com o ID do dispositivo. Este ambiente serviu como prova de conceito para a avaliação de desempenho da solução, de modo a simular um conjunto variado de dados durante períodos longos de tempo, e a verificação

¹<https://k3s.io>

e auditoria desses dados no blockchain.

5. Discussões e conclusão

A implementação prática da solução blockchain apresentada revela avanços significativos em relação à segurança e integridade dos dados ambientais coletados em campo. A arquitetura híbrida, combinando armazenamento on-chain e off-chain, demonstrou-se eficaz ao lidar com grandes volumes de dados provenientes de dispositivos IoT, conciliando requisitos críticos de segurança e escalabilidade [Eren et al. 2025]. Nesse modelo, informações sensíveis, como os hashes dos dados coletados e assinaturas digitais, são armazenadas diretamente na blockchain, enquanto dados detalhados são mantidos em bancos off-chain. Isso viabiliza a redução de custos operacionais sem comprometer a integridade e auditabilidade necessárias para aplicações críticas.

O uso da assinatura digital baseada em curvas elípticas (ECDSA com curva NIST P-256), aplicada diretamente nos dispositivos de coleta (e.g., sensores conectados via Raspberry Pi), fortalece o modelo de segurança ao assegurar que cada dado coletado tenha proveniência verificável. Esse mecanismo evita adulterações e permite a identificação da origem da informação, essencial para auditorias ambientais, conformidade regulatória e validação de créditos ambientais tokenizados [Zhou et al. 2023]. Além disso, a assinatura digital possibilita um modelo de negócio sustentável: o conceito de “Device-as-a-Service” permite monetizar a infraestrutura tecnológica através de licenciamento ou assinatura mensal, garantindo não apenas a segurança contínua, mas também o financiamento do desenvolvimento e manutenção da tecnologia ao longo do tempo.

Adicionalmente, a integração com tecnologias emergentes como IoT e IA amplia as possibilidades práticas do blockchain, permitindo análises preditivas e monitoramento ambiental em tempo real. O emprego de algoritmos inteligentes potencializa a capacidade preditiva e responsiva dos sistemas, promovendo respostas ágeis e automatizadas a eventos críticos ambientais. Essa sinergia reforça o argumento para a adoção do blockchain como infraestrutura tecnológica robusta e confiável em cenários industriais e ambientais complexos [Safeer et al. 2025].

Finalmente, destaca-se o impacto socioeconômico deste modelo tecnológico integrado. Ao possibilitar o registro seguro e transparente das ações ambientais e sua verificação pública, cria-se um ambiente de confiança compartilhada entre múltiplos atores — governos, empresas, comunidades locais e entidades reguladoras. Esse contexto de confiança distribuída favorece uma governança ambiental mais democrática, equitativa e eficaz, permitindo que comunidades historicamente excluídas tenham acesso direto e justo aos recursos gerados pelos mercados ambientais globais. Em última análise, o modelo proposto neste estudo ilustra um caminho pragmático para superar desafios tradicionais de segurança e confiança, abrindo portas para uma gestão ambiental mais eficiente, inclusiva e sustentável.

Apendice - Figuras

Agradecimentos

Este trabalho contou com recursos financeiros do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), termos de outorga 303373/2023-7 e 405531/2022-2; e do Programa Pronametro.

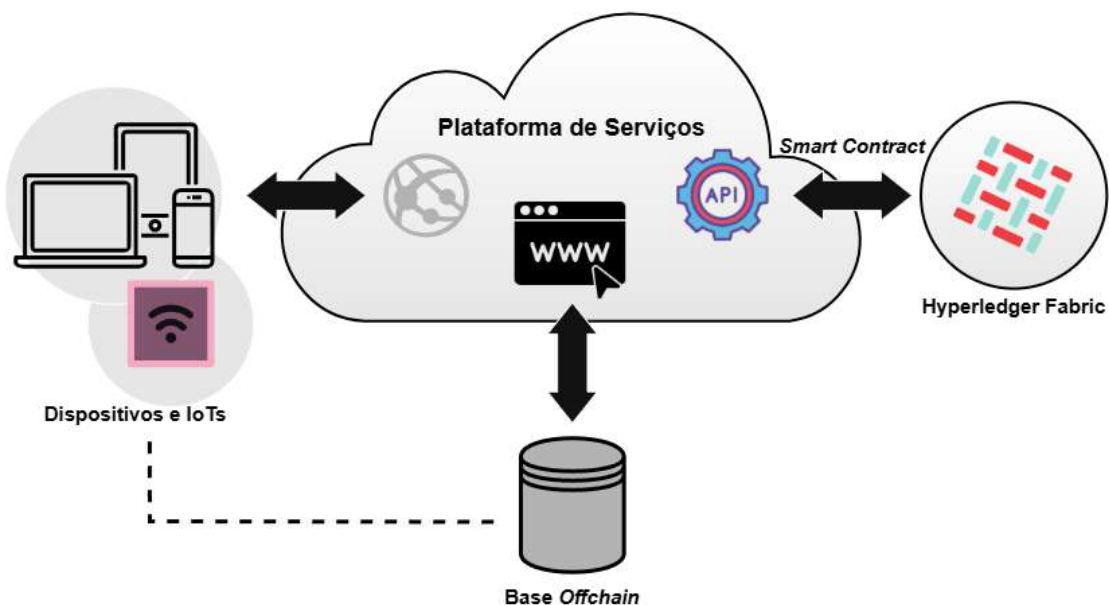


Figura 1. Arquitetura da solução de segurança de indicadores ambientais proposta pelo Instituto Ecosystems.

Referências

- AlShamsi, M., Al-Emran, M., and Shaalan, K. (2022). A systematic review on blockchain adoption. *Applied Sciences*, 12(9):4245.
- Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., Caro, A. D., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Cocco, S. W., and Yellick, J. (2018). Hyperledger fabric: A distributed operating system for permissioned blockchains. *Proceedings of the Thirteenth EuroSys Conference*, pages 1–15.
- Boller, M. L., Zurwehme, A., and Krupitzer, C. (2024). Qualitative assessment on the chances and limitations of food fraud prevention through distributed ledger technologies in the organic food supply chain. *Food Control*, 158:110247.
- Carrières, V., Lemieux, A.-A., and Pellerin, R. (2021). Opportunities of blockchain traceability data for environmental impact assessment in a context of sustainable production. In *IFIP International Conference on Advances in Production Management Systems (APMS)*, pages 124–133, Nantes, France.
- Eren, H., Karaduman, Ö., and Gençoğlu, M. T. (2025). Security challenges and performance trade-offs in on-chain and off-chain blockchain storage: A comprehensive review. *Applied Sciences*, 15(6):3225.
- Fang, W., Chen, W., Zhang, W., Pei, J., Gao, W., and Wang, G. (2020). Digital signature scheme for information non-repudiation in blockchain: a state of the art review. *EURASIP Journal on Wireless Communications and Networking*, 2020(1):1–12.
- Gaba, P., Raw, R. S., Kaiwartya, O., and Aljaidi, M. (2024). B-safe: Blockchain-enabled security architecture for connected vehicle fog environment. *Sensors*, 24(5):1515.

- Gschnaidtner, C., Dehghan, R., Hottenrott, H., and Schwierzy, J. (2024). Adoption and diffusion of blockchain technology. Technical report, ZEW Discussion Papers.
- Howe, L., Johnston, S., and Côte, C. (2025). How reliable is environmental management in mining? learnings through analysis of sustainability reports. *Corporate Social Responsibility and Environmental Management*, 32(2):2664–2680.
- IPCC (2021). *Climate Change 2021: The Physical Science Basis*. Cambridge University Press.
- Meisami, S., Dabadie, H., Li, S., Tang, Y., and Duan, Y. (2025). Sigscope: Detecting and understanding off-chain message signing-related vulnerabilities in decentralized applications. In *Proceedings of the ACM on Web Conference 2025*, pages 4284–4299.
- Melo, W., Nascimento, P., Gomes, K., Oliveira, M., and Machado, R. (2022). Crowdsourcing and monetization as a strategy to reduce vehicular greenhouse gases emissions. In *2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall)*, pages 1–5.
- Melo Jr, W. S., Santos, L. S. D., Bento, L. M., Nascimento, P. R., Oliveira, C. A., and Rezende, R. R. (2022). Using blockchains to protect critical infrastructures: a comparison between ethereum and hyperledger fabric. *International Journal of Security and Networks*, 17(2):77–91.
- Mengistu, A. T. and Panizzolo, R. (2023). Analysis of indicators used for measuring industrial sustainability: a systematic review. *Environment, Development and Sustainability*, 25:1979–2005.
- Moni, M., Melo Jr, W., Peters, D., and Machado, R. (2021). When measurements meet blockchain: On behalf of an inter-nmi network. *Sensors*, 21(5):1564.
- Muthu, S. S., editor (2022). *Blockchain Technologies for Sustainability, Environmental Footprints and Eco-design of Products and Processes*. Springer.
- Nygaard, A. and Silkoset, R. (2023). Sustainable development and greenwashing: How blockchain technology information can empower green consumers. *Business Strategy and the Environment*, 32(6):3801–3813.
- Rockström, J. et al. (2009). Planetary boundaries: Exploring the safe operating space for humanity. *Ecology and Society*.
- Safeer, S., Gallo, P., and Pulvento, C. (2025). Agri-farming with computer vision, iot and blockchain towards climate smart cultivation. *SSRN Electronic Journal*.
- Tapscott, D. and Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Portfolio.
- Zhou, Y. et al. (2023). A blockchain-based privacy-preserving and fair data transaction framework. *Applied Sciences*, 13(22):12389.