Assessing Blockchain's Suitability for ESG Disclosure: A Risk-Cluster Literature Review

Yiming Wang*

Curtin University, Singapore, Singapore

Abstract. As ESG disclosure requirements tighten, markets and regulators increasingly demand information that is verifiable and traceable. Blockchain is suggested to be a supporting infrastructure because of its decentralization, immutability and traceability. Prior studies have argued that blockchain may reduce information asymmetry, limit greenwashing, and support audit trails. However, blockchain is neither automatically trustworthy nor environmentally friendly; therefore, drawing on a risk-cluster lens, this paper critically reviews the literature and identifies three implementation risk clusters shaped by (A) risks related to monitoring, reporting and verification (MRV) quality and measurement frameworks alignment, (B) risks around privacy, data subject rights and accountability, and (C) risks linked to energy use, cost structures and the inclusion of smaller or weaker actors. This paper integrates these risks and their control conditions, and proposes a suitability assessment framework to determine when blockchain can generate sustainable net benefits in specific ESG disclosure scenarios, and to provide insights for internal control design and regulatory practices.

Keywords: Blockchain; ESG disclosure; MRV (measurement, reporting and verification); Data privacy; Energy use and cost; Internal controls.

1. Introduction

In recent years, firms have faced growing pressure to disclose environmental, social and governance (ESG) information. It is shifting from voluntary participation to a core part of compliance, and external assurance is widely regarded as an important way to enhance the credibility of reports [1]. A core challenge is that ESG data is often produced across departments and supply chains, with inconsistent definitions, and high verification costs. At the same time, the risks of selective disclosure and greenwashing still exist, making it difficult for stakeholders to assess the truthfulness and comparability of ESG information [2]. In this context, blockchain is often promoted as a tool to improve ESG disclosure credibility. Previous reviews and applied studies argue that tamper-resistant records, traceable links, and shared ledgers can strengthen transparency and auditability, especially in supply chain and carbon footprint traceability, ESG reporting, and the transparency of accounting-related information [3-6].

However, the existing literature's discussions on how blockchain "improves the quality of ESG information" are often based on implicit assumptions: reliable data sources before recording, achievable system security and interoperability, privacy and compliance met through both technology and institutions, and consensus mechanisms with sustainable energy and cost characteristics under organizational constraints [7-14]. Due to the differences in these assumptions across various industries, governance structures, and regulatory environments, blockchain features cannot automatically translate into meaningful improvements in the quality of information disclosure. More importantly, existing research provides limited systematic clarification on when these assumptions hold true or fail, which may lead to a gap between technological promises and governance realities.

To address this gap, this paper reviews 14 studies and adopts a risk-cluster logic to critically assess key debates on blockchain-enabled ESG disclosure. It makes three verifiable contributions. First, it classifies the main adoption barriers into three risk clusters: (A) MRV quality and misalignment across measurement frameworks, (B) privacy and regulatory compliance, and (C) energy use, cost, and organizational feasibility. Second, within each cluster, it summarizes the risk mechanisms, widely accepted mitigation conditions, and governance considerations identified in the existing literature. Third, based on these insights, it proposes a conditional evaluation framework to help researchers, regulators, and firms judge when blockchain is likely to deliver net benefits for ESG disclosure and when alternative or hybrid governance arrangements are more appropriate.

* Corresponding author: 22461016@student.curtin.edu.au

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

The rest of this paper is organized as follows: Section 2 summarizes the main claims and their assumptions; Sections 3 to 5 critically evaluate the three risk clusters; and finally proposes a conditional suitability framework and practical impacts.

2. Blockchain and ESG disclosure: main claims and potential risks

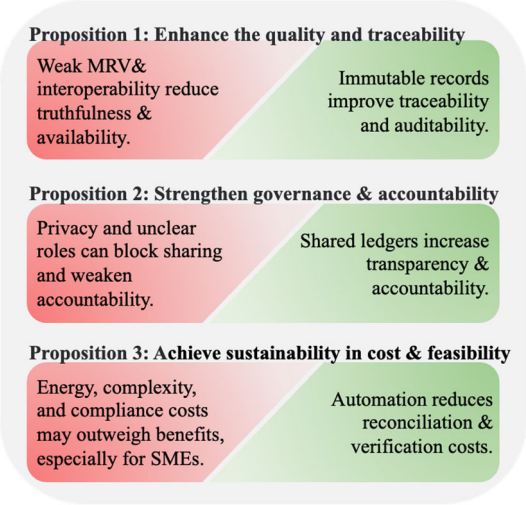

Figure 1. Main claims and potential risks

Existing research generally positions blockchain as a key infrastructure for enhancing the credibility of ESG disclosure, forming three main propositions: (1) improving information quality, (2) strengthening governance and accountability, and (3) achieving sustainable implementation in terms of cost and feasibility [3, 4, 6, 14]. However, whether these claims hold true in practice depends on a set of conditions being met at the same time: robust MRV and data source governance, system security and interoperability, compliance with privacy and data protection requirements, and an energy-cost structure that aligns with the organization's operating capabilities [7-13]. Accordingly, this paper examines each claim and clarifies its supporting conditions and limitations, laying the foundation for the later risk cluster analysis.

Firstly, the information quality claim argues that tamper-proof records, timestamps, and shared ledgers can enhance data integrity, traceability, and auditability, particularly in sustainable supply chain tracking and carbon accounting/offsetting contexts, and thus have an impact on ESG reporting and accounting transparency [3-6]. This claim requires both “pre-chain truthfulness” and “on-chain availability.” If the MRV input is weak or poorly controlled, the blockchain may merely lock in errors or actions; if security and interoperability are limited, end-to-end verification is hard to maintain; and if privacy and data protection rules restrict what can be recorded or shared, the verifiability and audit value will be reduced [7-10, 12, 14].

Secondly, the governance proposition indicates that multi-party maintenance, rule embedding, and attributable records can reduce unilateral control, enhance accountability, and provide stronger evidence trails for external assurance. Meanwhile, previous work emphasized that false reporting and greenwashing are not merely technical issues but are strongly influenced by incentive mechanisms, monitoring, and institutional designs [1-3, 6]. This statement relies on aligned governance and compliance architecture: access control and role design can influence new attack surfaces; interoperability affects the consistency of cross-organizational evidence links; privacy laws (including tensions with immutability) restrict the content that can be shared and audited; and high energy and operating costs can weaken long-term operation and continuous accountability [7-14].

Thirdly, the feasibility claim argues that blockchain may reduce reliance on intermediaries, lower reconciliation frictions, and improve coordination efficiency, thereby reducing verification costs over time and supporting scalable ESG data management [3, 5, 14]. However, different consensus architectures have very different energy and efficiency outcomes, which directly affect adoption thresholds, particularly for participants with limited resources. Moreover, security, interoperability, and privacy compliance will significantly increase implementation and maintenance costs, which means that "technically feasible" is not the same as “organizationally feasible”, especially when considering assurance and audit requirements [1, 6-13].

In conclusion, the value of blockchain in ESG disclosure should be regarded as a conditional benefit. The outcome depends on the comprehensive matching degree of data governance, privacy compliance, system security and interoperability, and energy-cost feasibility, rather than a single technical feature. Therefore, the following sections will assess these boundaries through three risk clusters.

3. Risk Cluster A: How Biased MRV and Fragmented Standards Driving Greenwashing Risk

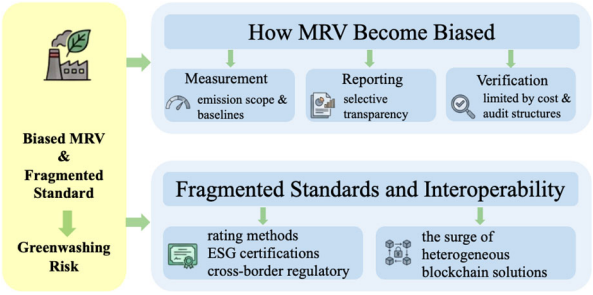

Figure 2. How Biased MRV and Fragmented Standards Driving Greenwashing Risk

3.1 How Measurement, Reporting and Verification (MRV) Become Biased

Studies often argue that recording ESG and carbon data on immutable distributed ledgers, with transparent and traceable audit trails, can reduce fraud and verification problems and thereby increase the credibility of environmental performance claims [3-5]. However,

blockchain enters only at the recording stage. Real environmental effects are first translated into data on physical emissions or social events by firms and their supply chain partners through monitoring and measurement methods, then aggregated and formatted for disclosure, and finally subjected to some level of assurance or regulatory review before being written into on-chain indicators. Blockchain changes how ledgers are organized and shared, but not what is calculated or how it is calculated. If off-chain MRV processes are biased, blockchain immutability will freeze wrong information technically.

The core problem is the choices of MRV design, such as emission boundaries, emission factors, and baselines, are not purely technical; different choices can materially change reported results. In aviation, carbon-footprint tools often rely on assumptions about greenhouse gas boundaries (Scope 1/2/3), which systematically overstate or understate emissions [5]. Once these inaccurate data are uploaded, blockchain records them with high integrity but cannot prevent them from being written to the ledger; data created through human error or collusion can remain permanently stored. Therefore, the reliability of MRV results depends on the quality and governance of off-chain database. If measurement methods leave wide room for managerial discretion, what is put on chain is just a set of numbers that favor the corporate narrative rather than an objective truth. This shows that MRV quality is a core condition for evaluating if blockchain can deliver credible ESG disclosure.

This governance gap can also appear at the reporting stage through selective transparency. Sustainable supply-chain management typically involves multiple standards and certifications, which forces firms to choose what to measure, classify, and disclose across frameworks [4]. In a blockchain setting, firms may choose to only record ESG indicators and projects that are beneficial to themselves on chain, while keeping high-emission activities and uncertainties off-chain or not disclosing at all. In substance, this should be understood as symbolic communication, using technology for greenwashing instead of underlying practices have changed[2]. Therefore, the paper treats selective on-chain recording as a credibility boundary that must be tested when judging blockchain's suitability for ESG disclosure.

At the verification stage, sustainability assurance is often voluntary and costly, and firms' decisions to obtain assurance are shaped by cost–benefit tradeoffs. Accordingly, the literature emphasizes the role of institutional actors, such as registries, standards organizations, and certifiers in constraining managerial discretion over MRV design and disclosure [1, 4]. While blockchain enable auditors to access records directly, increasing efficiency and transparency, this improvement mainly remains at the level of recorded data; emission boundaries, factor choices and carbon accounting methods; assurance scope and depth continue to be limited by cost and agency structures. Without strengthened institutional constraints, on-chain records may remain a beautified output rather than a faithful account of emissions, which may even lead external stakeholders to overestimate the objectivity and verifiability of on-chain data, reducing their willingness to question methodological assumptions and assurance depth. Therefore, it makes institutional assurance a core credibility condition in the paper's suitability assessment.

3.2 Fragmented Standards and Interoperability: Same On-Chain Data, Different Compliance Outcomes

Misalignment between MRV data and fragmented standards further increases greenwashing risks. Carbon management and ESG disclosure operate under various rating methodologies, sustainability certifications, and cross-border regulatory, making outcomes across platforms difficult to compare [3, 4]. Against this background, even the same set of ESG data can be interpreted differently across frameworks, leading to inconsistent compliance assessments. For example, the same on-chain data may be counted as "additional reductions eligible for offsets" in one scheme but treated merely as part of the baseline scenario in another and thus not recognized as additional reductions at all. Thus, blockchain credibility depends not only on data integrity, but also on whether standards allow consistent ESG interpretation.

Moreover, the surge of heterogeneous blockchain solutions makes standardization difficult and interoperability challenging [14]. Importantly, the problem is not only whether data can move from one chain to another, but whether the meaning and governance of that data remain aligned. Belchior, Vasconcelos [7] distinguish technical, semantic, organizational, legal and governance layers of interoperability and stress that existing research largely prioritizes technical cross-chain communication and limited semantic alignment through protocols (e.g., CC-dApps), while regulatory and governance interoperability remain underdeveloped. Even if cross-chain mechanisms enable secure data flow, they often cannot harmonize the regulatory rules.

In short, the current interoperability solutions mainly address "how data flows securely ", rather than "which set of rules these data are interpreted and regulated under different systems". When ESG standards are highly fragmented, and existing interoperability solutions are mainly used to connect data channels between different chains without unifying the compliance rules, the same cross-chain data may be calculated as completely different emission, reduction, or compliance results under different systems. Thus, interoperability is a conditional factor to determine if blockchain can produce comparable ESG outcomes across systems.

4. Risk Cluster B: Privacy, Data Rights and Accountability in ESG Blockchains

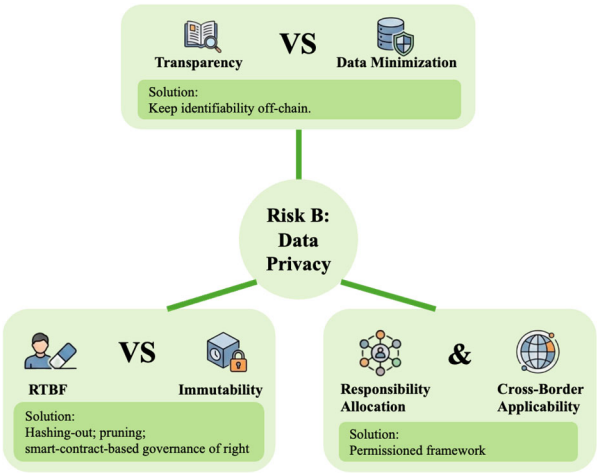

Figure 3. Privacy, Data Rights and Accountability in ESG Blockchains

4.1 The Tension Between Transparency and Data Minimization

There is a contradiction between the transparency of blockchain and the data minimization principle in general data protection laws such as the General Data Protection Regulation (GDPR). GDPR requires controllers to collect and retain only the minimum amount of personal data necessary to achieve a specified purpose [8, 9]. By contrast, many ESG projects adopt blockchain to increase traceability of carbon accounting, thus signaling greener and more responsible [3, 4, 6]. However, encryption alone cannot prevent the risk that transaction metadata, addresses and timestamps may be linked to identifiable individuals. Over time, the accumulation of high-frequency behavioral traces and transaction graphs further increases the risk that adversaries can infer concrete identities [8, 10]. This suggests that transparent blockchain may actually expand the exposure surface of privacy and trigger continuous monitoring risks for employees and community residents. Firms may retain more individual-level data than is necessary for disclosure purposes in order to present a sufficiently transparent ESG performance to external stakeholders, turning ESG reporting that was originally intended to strengthen accountability into a form of surveillance-based governance and eroding the social dimension of respect for dignity and privacy.

To mitigate this tension, research often advocates the principle of keeping verifiability on-chain and identifiability off-chain. Firstly, transparency can be narrowed by choosing the appropriate type of chain: public, permissionless blockchains strengthen public auditability but often at the cost of increased privacy exposure, whereas private, permissioned chains operate in a controlled environment where access and participation can be restricted, making it easier to implement data minimization requirements that limit processing to what is necessary. Secondly, identifiable information and continuous dynamic data can be stored off-chain, while the blockchain retains only hash values pointing to off-chain storage locations for integrity verification, and privacy-preserving techniques such as zero-knowledge proofs (ZKP) are used to demonstrate that an ESG claim or transaction is valid without revealing sensitive data [8, 9].

However, the limitations of these approaches mean that the conflict between transparency and data minimization can usually only be mitigated rather than fully resolved. Firstly, choosing permissioned chains can indeed narrow transparency through restricted access, but it shifts trust from public verifiability to internal governance control, which may weaken public trust and reintroduce risks that data could be altered through governance, permission and consensus arrangements. Secondly, moving personal information and dynamic data off-chain reintroduces centralized control, although ZKP can enhance privacy protection, it also increases system deployment cost, raising the governance and audit barriers [8, 9]. Overall, these designs reduce privacy leakage but may still support unnecessary data retention and monitoring, so they only conditionally improve compliance suitability rather than resolving the problem.

4.2 The Tension Between Data-Subject Rights and Immutability of blockchain

There is a direct conflict between data-subject rights and the immutability of blockchain. The GDPR provides data subjects the right to be forgotten (RTBF), but immutability and global replication are core features of blockchain, which make it fundamentally difficult for data subjects to protect on-chain personal data [8, 9]. This means once environmental or social data about identifiable persons are written on-chain, the extent to which data subjects can truly control subsequent uses remains a major compliance and trust risk. So, RTBF–immutability tension is a significant constraint when assessing blockchain suitability for ESG disclosure.

To address the tension between RTBF and immutability, existing research can be grouped into three main types of approaches. The most commonly proposed mitigation is hashing-out: personal data are stored off-chain, while the blockchain only keeps hash pointers to reference the off-chain record. Based on this framework, the literature proposes three execution mechanisms for RTBF. First, removing the personal data in the off-chain repository after an erasure request, so the on-chain hash pointer becomes functionally null and void. Second, hashing-out combined with encryption: destroying the private key, thereby breaking the link-ability between the on-chain pointer and the off-chain data. Third, storing the encrypted data on-chain and then claims erasure by deleting the encryption key [8, 9]. However, these mechanisms rely on a functional reinterpretation of erasure, and the legal applicability of inaccessibility remains contested because transaction traces remain on chain. In addition, hashing-out cannot guarantee non-identifiability in open-ledger settings: actors are often represented by hashes or public keys, and linkage analysis can still infer identities from network and transaction

patterns; this risk may increase over time as analytical methods and cryptographic attacks evolve [8-10].

The second type consists of redactable blockchain techniques, such as pruning, where old block data are deleted but block headers are retained. This may introduce trade-offs between security and verifiability, and in public blockchains it is impossible to guarantee that all nodes delete their full historical copies, so network-wide erasure cannot be assured. Another example is the use of chameleon hashes to modify block contents under authorized conditions, but this depends on a trusted third party or centralized authority, and is therefore criticized for undermining the very idea of decentralization; at the same time, legacy copies may still contain the deleted data, making it even more doubtful that GDPR-level erasure has been achieved, while weakening immutability also opens new attack surfaces for security threats [8, 9].

The third type is smart-contract-based governance of rights, which is linked to erasure mainly through functionally equivalent effects. Here, data-subject preferences about consent, withdrawal of consent, access control and restrictions on processing are translated into automatically executable rules. When a request is received, the system can block further access and subsequent processing by third parties, so that the data become “out of use” in functional terms. However, because smart contracts themselves are immutable, they can hardly roll back or delete past on-chain records, so this approach is closer to partial mitigation of Article 17 requirements than to strict erasure in the legal sense [8, 10].

Many existing proposals actually reinterpret the "erasure/correction" in the GDPR as making on-chain information unavailable, unlinkable or semantically invalid, but this is naturally not equivalent to the expectations of the GDPR regarding revocability and controller liability. Therefore, these mechanisms can only be regarded as risk mitigation rather than the complete elimination of potential conflicts.

4.3 Risks in Responsibility Allocation and Cross-Border Legal Applicability

The third risk is that it is difficult to clarify who is responsible for on-chain privacy impacts and which law applies, weakening accountability and effective remedies. Under the GDPR, personal data processing is expected to have an identifiable controller who bears compliance duties, while blockchain decentralization makes the responsibility allocation difficult [8, 9]. In practice, controllership is assessed in a functional way, even if parties assign responsibility by contract, controllers may be reappointed based on their actual influence. In particular, with case law expanding joint controllership, entities with limited involvement but that influence processing for their own purposes (such as platform operators, consortium members, and intermediaries providing crypto-asset wallets) may also be classified as joint controllers. Moreover, blockchain ecosystems are increasingly multi-layered (infrastructure, application, and intermediary actors). Application-layer entities may independently determine purposes, and multiple joint controllers may be responsible for different processing aspects, which makes the identification of responsible parties more complex [9]. This increases the difficulty of governance in multi-party ESG systems, especially when precise location and process data may be exploited for unauthorized purposes or identity inference [10].

Regarding legal applicability and cross-border governance, public-blockchain nodes may be globally distributed, and the network lacks clear geographic boundaries, which makes it difficult for controllers to identify where data will be replicated, and to ensure compliance with cross-border transfer requirements; even determining the applicable law and jurisdiction may become ambiguous when the physical location of controllers or key actors cannot be clearly identified [8, 9].

To address this risk, the literature broadly suggests combining organizational responsibility anchoring, contractual role allocation, and chain-type selection. First, regulatory guidance recommends identifying the controller at the start of the project and, where necessary, creating or appointing a specific legal entity to assume responsibility. It also recommends using GDPR Article 26 to establish joint-controller arrangements, allocate responsibilities, and set a single contact point for data subjects to support rights exercise and regulatory communication. However, because controllership is functional and fact-based, additional controllers or joint controllers may still be identified ex post under “factual control” and expanding case law; thus, Article 26 arrangements cannot fully stabilize responsibility boundaries over time [8, 9].

Second, some participants can be placed under processor contracts, for example by treating validation/execution-related parties as processors and using standard terms or entry conditions to define roles and obligations, thereby improving enforceability. Yet on public blockchains, nodes and miners are non-specific, unidentifiable, and constantly changing, so enforceable processor contracts or workable joint-control arrangements are often impractical; the absence of a single manager in decentralized systems also increases difficulties in enforcement and security responsibility [8, 9].

Third, some studies prefer permissioned blockchains to improve participant identifiability and geographic controllability, thereby reducing cross-border compliance uncertainty [8]. Nevertheless, even with a more controllable chain type, GDPR Articles 26 and 82 can still create a tension where parties with limited control may bear liability: data subjects may claim rights and remedies against any joint controller, followed by internal recourse among the parties. At the same time, proportional allocation of responsibility based on the level of involvement remains unclear, and too many responsible actors may form a complex “responsibility network” that reduces the accessibility and predictability of effective rights exercise [9].

Therefore, when evaluating ESG blockchain designs, it is necessary to continuously ask and document who bears ultimate responsibility for processing, how controller/joint-controller roles are allocated in governance, and what compliance pathway is used for cross-border flows of on-chain records; otherwise,

unclear responsibility boundaries can become a governance risk in themselves.

5. Risk Cluster C: Energy and Cost Risks of Blockchain as ESG Infrastructure

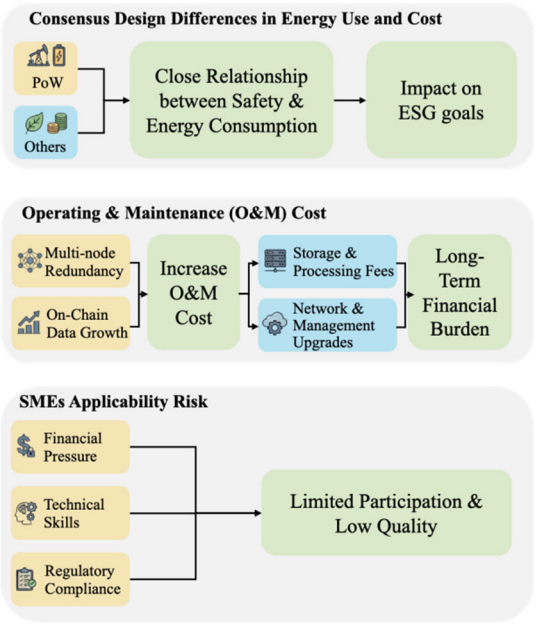

Figure 4. Energy and Cost Risks of Blockchain as ESG Infrastructure

5.1 Consensus Design Differences in Energy Use and Cost

Consensus mechanisms set the upper bound of energy use and cost in blockchain systems and therefore act as a key structural constraint in ESG infrastructure. Different consensus mechanisms achieve security, decentralization, and scalability through different ways, so the main sources of energy and cost depend on different drivers (computation intensity, communication overhead, node count, and hardware requirements), and these drivers scale at different rates as the network grows [12, 13].

The dominant Proof-of-Work (PoW) model relies on intensive computational competition, which requires sustained investment in electricity and hardware to maintain consensus, creating higher total cost of ownership (TCO) over long-term operation and potentially conflicting with sustainability goals [3, 11, 13]. This energy burden is not simply technical inefficiency but "energy-intensive by design": security is achieved by making attacks expensive, because an attacker typically needs around 25%–50% of total computing power to influence the system; moreover, miners' revenue comes from block rewards and transaction fees and is strongly driven by market price, so higher prices strengthen mining incentives and raise total energy use, making PoW energy resemble a fluctuating security budget rather than an IT operating cost that scales linearly with transaction demand [11, 12].

This also limits the claim that better technology automatically reduces energy: although efficiency improvements may lower unit cost in the short run, competition and difficulty adjustment can attract more hash power and raise difficulty, so long-run system-wide energy tends to be constrained by economic parameters such as electricity price, coin price, and reward structure unless these conditions change materially [11].

In addition, "energy per transaction" is often misapplied: PoW energy is mainly driven by the mining security race rather than transaction volume, so linear calculation using "energy consumption per transaction multiplied by global payment transaction volume" can overstate total energy. While scaling (e.g., larger blocks) does not necessarily increase mining energy in theory, larger blocks can worsen propagation delay and security risks and increase bandwidth and storage requirements for nodes, forcing a trade-off among throughput, security, and decentralization [11]. In an ESG infrastructure setting, attempts to reduce "unit write-in cost" through scaling may therefore shift costs from electricity to higher node thresholds and stronger governance centralization pressures.

Finally, other alternative consensus mechanisms cannot necessarily mean low cost. Proof of Stake (PoS) replaces energy-intensive computation, reducing energy but relying more on governance arrangements; it still depends on redundant validation and storage, so its energy and cost levels can remain higher than centralized databases. Meanwhile, cost pressure does not disappear but shifts from electricity and hardware to long-term capital lock-up (staking) and higher entry thresholds, where governance can be dominated by a small number of large validators. These barriers can reduce inclusiveness and governance credibility and increase compliance and audit costs. Proof-of-Authority (PoA) or Practical Byzantine Fault Tolerance (PBFT) does not need to tie voting power to scarce resources and can be more energy efficient, but PBFT-style communication costs rise quickly as the network grows. Meanwhile, high transaction per second (TPS) designs such as Delegated Proof-of-Stake (DPoS) are more centralized and may introduce security–governance costs such as delegate collusion [11-13].

Overall, consensus mechanism determines what "price" an organization pays for security; ignoring the binding relationship between security and energy consumption can lead to sharp cost increases when more participants are connected and the system scale expands, thereby affecting the environmental goals and economic feasibility of ESG projects.

5.2 Operating & Maintenance (O&M) Cost from Multi-Node Redundancy and On-Chain Data Growth

Even when more energy-efficient consensus mechanisms (i.e., non-PoW) are adopted, blockchain still has basic resource consumption: redundant replicated storage across multiple nodes to ensure verifiability and immutability. As blocks accumulate, scalability pressure rises and demands for storage and bandwidth increase [11, 12]. This pushes participants to higher-specification infrastructure and long-term operational work, such as maintenance and upgrades. Furthermore, transactions are processed in a replicated manner, which means that many

nodes repeatedly verify and execute the same transactions; therefore, the total cost of ownership (TCO) rise with the scale of the network. For large non-PoW networks, this natural redundancy may still make the blockchain more resource-intensive than centralized systems that rely on minimal redundancy (such as backups), thereby resulting in continuous power and O&M costs [11]. This risk is magnified in the ESG and supply chain environment. As time goes by, more stakeholders join in and shared data on the chain accumulates continuously. When the data volume grows, the scalability pressure rises accordingly, and the system has to increase investment in infrastructure like computing power, storage and bandwidth to maintain performance and stable operation [12].

Mitigations for redundancy and data growth (such as sharding, off-chain payment channels, and the use of sidechains) can improve throughput and scalability by reducing the number of nodes involved in certain operations or lowering the workload of transaction execution [11]. However, these methods introduce a stronger tendency towards centralization and rebalance among security, liveness and trust. Similarly, Layer-2 solutions (ZK-Rollups and Optimistic Rollups) can reduce energy use by offloading computation from Layer-1, but they often come with higher complexity, latency, and encryption overhead, raising implementation and operational capability requirements [13]. Overall, in ESG application scenarios, multi-node redundancy and continuous on-chain data expansion jointly increase storage, compute, bandwidth, and governance-related O&M costs, while scalability optimization unavoidably brings more complexity and trade-offs, creating key infrastructure and operational cost risks for blockchain ESG data governance.

5.3 SMEs Applicability Risk Driven by Cost and Capability Constraints

When blockchain is used as infrastructure for ESG data disclosure, and supply-chain traceability, small and medium-sized enterprises (SMEs) face feasibility and inclusiveness risks driven by resource constraints. Even if blockchain enhances traceability, verification, and tamper-resistance, SMEs may still find it difficult to continuously participate due to high costs, limited capabilities and coordination obstacles, which may lead to adoption gaps and weaken end-to-end disclosure coverage across supply chains [3].

Cost pressures are driven by the need for new hardware and software for continuous process data collection, which commonly requires additional devices. RFID and IoT are frequently proposed as enabling tools, increasing upfront capital expenditure and ongoing maintenance burdens [4]. Reducing consensus energy consumption (such as giving up PoW) does not eliminate cost issues: in large networks, multi-node redundancy (verification and replication) typically consumes more resources than “minimum redundancy” centralized systems, leading to structurally higher long-term cloud, operational, and scaling costs, thereby excluding cash-constrained small and medium-sized enterprises [11].

The requirements for capabilities and governance have further raised the barriers. Blockchain adoption requires clear organizational policies, and introduce new roles, responsibilities and professional capabilities. Limited internal knowledge and application ecosystems increase learning costs and reliance on external suppliers [4]. When traceability relies on the IoT and sensor networks, limited device computing and storage can reduce availability and operational stability, making it more difficult for SMEs to continuously collect data and interact on-chain [14]. Ecosystem coordination is equally crucial: blockchain-based supply chain governance requires stable data sharing rules and continuous collaboration. Inconsistent partner priorities and cultural differences increase communication costs and disrupt implementation, while the lack of successful cases adds uncertainty and experimental costs, which is more restrictive for SMEs [4].

These mechanisms imply three systematic outcomes. Firstly, the fact that SMEs do not participate concentrates on-chain ESG coverage among large firms, which reduces the completeness of information disclosure. Secondly, the reliance of SMEs on the standards and infrastructure set by leading enterprises has concentrated governance power, leading to conflicts with multi-party verification of ideals. Thirdly, immutability cannot prevent low-quality input; simplifying or outsourcing data collection under cost pressure may lock errors into continuous and traceable ledgers, increasing the costs of correction and interpretation and weakening the credibility of disclosure. Therefore, the suitability risk of SMEs cannot be eliminated through the optimization of a single technology. It requires training, financial support, and collaborative governance with cost-sharing arrangements to transform the transparency of blockchain into sustainable value.

6. Integrative evaluation

6.1 Suitability Definition and Evaluation Objective Setting

The blockchain-based ESG disclosure suitability assessment framework follows the logic of "threshold - trade-off – tiered conclusion". It clarifies the boundary between feasibility and applicability: feasibility refers to whether a solution can be designed and implemented, while applicability is defined as the ability of blockchain solutions to provide sustainable net benefits while keeping the remaining governance risks within an organization's tolerance range, compared to similar alternatives (such as centralized databases with access control and third-party safeguards).

Based on this definition, the framework applies structured assessment paths in eight sub-risks and transforms core blockchain commitments (immutability, traceability, and multi-party sharing) into testable decision-making criteria. This achievement serves as the reviewable and transferable basis for determining whether blockchain should be used as an ESG disclosure infrastructure.

6.2 Stage 1: Necessary condition threshold filtering

In the first stage of the framework, gatekeeper filters are adopted to test whether blockchain options meet the minimum pre-conditions for ESG disclosure. Immutability and traceability cannot guarantee the data authenticity, enforceable compliance or controllable privacy risks. If any requirements are lacking, continuing with the net income trade-off will lead to misleading conclusion and greenwashing. Thus, failure to pass any gatekeeper procedures will immediately result in "not suitable" decision and the assessment will be terminated before later stages.

6.2.1 Minimum Pre-conditions for Authenticity

G1 tests whether blockchain-based disclosure can meet the minimum verifiable standards for authenticity. The gatekeeper demands clear MRV boundaries and embedding points to independently verify the intervention, including corrective mechanisms.

This threshold has priority because immutability only reduces the probability of tampering after an event occurs, but it cannot replace the verification of the authenticity of the original information. Without institutional guarantees, on-chain records may freeze low-quality or strategic disclosures, create technical credibility illusions, and transform risk clustering A from a probabilistic issue into a structural outcome. The failure of G1 does not imply an increase in credibility, and thus rejects the applicability of blockchain as a disclosure infrastructure.

6.2.2 Enforceable Compliance and Accountability

G2 assesses whether compliance obligations and relief measures remain enforceable in a multi-party environment. The gatekeeper demands clear roles and responsibilities, data subject rights (access, correction, deletion or functionally equivalent paths), clear procedures and response time frames, as well as enforceable cross-border applicable laws, dispute resolution and enforcement scope arrangements.

The necessity of this threshold lies in the fact that the distributed collaborative structure of blockchain may blur responsibilities and complicate jurisdiction. If responsibility cannot be determined or remedial measures cannot be obtained, the risk of “unenforceable accountability and compliance” will become system-wide, undermining long-term sustainability. The failure of G2 indicates that compliance risks should directly lead to "inappropriate" conclusions.

6.2.3 Achievable Data Minimization

G3 assesses whether the transparency and replication of the blockchain comply with the data minimization principle under the ESG disclosure goals. The gatekeeper requires default off-chain storage of personal data, minimizes on-chain fields, and strictly limits visibility boundaries through access control, encryption, and selective disclosure.

The logical basis of this threshold lies in the fact that transparency and linkability increase the risk of inference and reidentification, while replication makes privacy leakage risk difficult to reverse. If the minimization architecture fails to meet the disclosure requirements, the conflict between transparency and minimization will become a persistent compliance obstacle. Therefore, the failure of G3 should also lead to an “inappropriate” conclusion.

Table 1. Gatekeeper checklist.

ID	Necessary condition	Operational criteria	Failure impact
G1	Credibility preconditions	Yes, if all: i. MRV method clear; ii. independent verification; iii. enforceable correction.	Non-verifiable authenticity; Only low-quality information on chain; Greenwashing.
G2	Enforceable compliance and accountability	Yes, if all: i. controller identifiable; ii. RTBF via equivalent path; iii. cross-border dispute resolution enforceable.	Remedies unreachable; Compliance risk spillover to participants.
G3	Data minimization achievable	Yes, if all: i. off-chain personal data; ii. minimized on-chain fields; iii. visibility only to necessary parties.	Privacy leakage.

6.3 Stage 2: Net-Benefit Trade-off Assessment

After passing through the gatekeeper, the assessment enters the net income trade-off module. The key point of comparison lies in whether blockchain can bring sustainable net benefits compared with similar alternatives in a specific information disclosure environment. The key test is whether the improvement in credibility and coordination exceeds the incremental costs brought by consensus design, redundant replication and data growth, as well as compliance and governance complexity, while the remaining risks remain within a controllable range.

6.3.1 Credibility and audit gains

T1 assesses the marginal improvement in the clarity and traceability of the evidence chain under multi-party sharing (like reconciliation, tracking, and evidence collection efficiency). The benefits depend on the institution: without MRV independent verification entry points, on-chain records may create an illusion of credibility and exacerbate greenwashing under reputation competition and regulatory pressure. Mitigation measures require embedding audit evidence points in the MRV and clarifying the chain of responsibility; residual risks still exist because on-chain control cannot replace source-level authenticity, and credibility is limited by assurance strength and governance implementation.

6.3.2 Consensus-driven energy–performance–governance trade-off

T2 assesses how consensus and scale selection affect throughput, confirmation efficiency, and governance structure. Higher frequency recording and cross-party coordination may improve, but the energy-performance-decentralization trade-off may introduce governance centralization and higher barriers to participation. As the number of nodes increases, throughput demands rise, the heterogeneity of participants increases, and rules become immature, especially when permission boundaries are not clear, risks will increase. Mitigation not only requires "more effective consensus design", but also clear chain and licensing strategies as well as governance controls (rotation, supervision, auditing). Residual risk reflects an increase in governance complexity and depends on organizational capabilities.

6.3.3 TCO risk from redundancy and on-chain data growth

T3 assesses the long-term total cost of ownership driven by multi-node redundancy and on-chain data growth. Replication and retention support availability and traceability verification, but storage, bandwidth, computing and O&M costs increase as the retention length and network scale grow. Risks particularly occur in high-frequency capture (such as in the IoT), long-term retention for traceability, and cross-border multi-node deployment. Hierarchical scalability and interoperability can shift the pressure to cross-layer coordination and governance costs. The main mitigation includes off-chain storage, on-chain summaries and data lifecycle management (retention/archiving). Residual risks exist because complexity is often transferred rather than eliminated.

6.3.4 Residual risks in privacy, responsibility, and cross-border governance

T4 regards privacy, accountability and jurisdiction as residual risk items. Off-chain storage, access control and selective disclosure reduce direct exposure, but on-chain transparency and linkability still exist risks of inference and reidentification. The multi-party setup blurs the boundaries of controllers and the chain of responsibility, and the distribution of cross-border nodes weakens the clarity and enforceability of the law. The risks of high data sensitivity, unstable sharing boundaries and scattered participants will increase. Mitigation measures include default off-chain personal data, minimized on-chain fields, selective disclosure to demonstrate compliance, and governance charters for liability and dispute resolution.

6.3.5 SME suitability and inclusiveness

T5 tests whether blockchain will make a significant barrier for SMEs to participate in the supply chain, thereby reducing coverage and the completeness of disclosure. Continuous IT deployment, key management, compliance response and operation set thresholds for capabilities and costs. Mitigation measures include tiered access (off-chain proof), shared services or hosted nodes, standardized interfaces, and support measures (training, subsidies, compliance assistance). Residual risks include the power asymmetry due to centralization and trusteeship, which shifts the burden from trust to platform dependence.

Table 2. Trade-off matrix.

ID	Assessment focus	Main risk	Risk triggers	Key mitigation design
T1	Credibility & audit gain	Technology-driven credibility illusion; greenwashing.	Many participants; regulatory stress; strong reputation competition.	Add audit evidence points into the MRV process.
T2	Consensus-driven trade-off	Centralization; participation barriers.	More nodes; higher participant heterogeneity.	Specify chain type; rotation, oversight, audit.
T3	Redundant operations & on-chain data growth	Higher TCO; increasing coordination cost.	High-frequency IoT capture; long retention data; multi-nodes network.	Off-chain storage; retention; explicit operations and governance capability design.
T4	Residual risks in privacy, accountability, and cross-border governance	Re-identification; reduced legal enforcement reach.	High data sensitivity; unclear sharing boundaries; many participants.	Default off-chain personal data; aggregation & minimization; selective disclosure.
T5	SMEs suitability & inclusiveness	Lower supply-chain coverage; weaken disclosure completeness.	High SME share in supply chain; weak digital capacity; high disclosure frequency.	Tiered access; subsidies, training, compliance support).

6.4 Stage 3: Tiered Decision Outcome

The third stage integrates the results of the first and second stages into three standardized results: suitable, conditional suitable and unsuitable, in order to balance the clarity and practicality of the norms. "Suitable" requires all gatekeepers to pass, and the trade-off assessment must prove that the credibility and audit benefits significantly outweigh the incremental costs and residual risks, and must not reduce disclosure completeness.

"Not suitable" applies when any gatekeeper fails, or when the gatekeepers pass but the trade-offs fail, such as the long-term TCO is unsustainable, untreatable and unabsorbable residual compliance risks, or inclusive losses that distort the integrity of disclosure.

"Conditional suitable" applies to cases where gatekeepers pass but the costs and residual risks remain high. It requires clear design and governance conditions to compress costs and residual risks within an acceptable range. For example, embedding audit evidence points into MRV to enhance credibility; utilize off-chain storage and minimization to reduce privacy externalities and enhance the enforceability of rights; apply lifecycle management and operational governance to control the long-term costs caused by redundancy and data growth; and adopt tiered access and support measures to reduce the exclusion of SMEs. Through the conditional checklist, the tiered output transforms the question of "whether to adopt blockchain" into governance and engineering requirements that conform to the risk cluster framework.

Table 3. Tiered Integrated Decision Table

Decision tier	Gatekeeper conditions (G1-G3)	Trade-off outcomes (T1–T5)
Suitable	G1=Yes; G2=Yes; G3=Yes	T1 credibility are verifiable; costs and residual risks from T2–T5 stay within a controllable range. T2 no unacceptable centralization spillover; T3 long-run TCO sustainable; T4 residual privacy/accountability/cross-border risks organizationally absorbable; T5 no significant loss in coverage. Total net benefit > 0.
Conditionally suitable	G1=Yes; G2=Yes; G3=Yes	Gatekeepers satisfied, but in the specific setting ≥1 of T2–T5 falls into a high-sensitivity / high-cost / high-residual-risk range. Net benefit depends on if additional governance adjustments can keep residual risks in an acceptable range.
Not suitable	Any gatekeeper fails	Trade-offs indicate non-sustainability: T3 long-run TCO not sustainable; T4 residual risk not absorbable in the target disclosure setting; T5 significant coverage loss and incomplete disclosure. Overall net benefit < 0.

7. Conclusion

This paper shows that blockchain is not a reliable and sustainable guarantee solution for ESG disclosure. Its benefits depend on the quality of off-chain data, enforceable data privacy strategies, as well as the energy cost feasibility of the selected architecture.

This review identified three core implementation risk clusters: (A) Biased MRVS and fragmented standards, which may freeze inaccurate data and increase greenwashing risk; (B) Privacy, data subject rights and cross-border accountability restrictions may weaken the enforceability of the law; (C) Energy usage, long-term TCO and inclusiveness risks may exclude SMEs and reduce the completeness of disclosure.

To translate these insights into practice, the paper proposes a "threshold - trade-offs - tiered decision" suitability framework: gatekeepers filter out cases that do not meet the minimum authenticity, compliance, and data minimization conditions; the trade-off module assesses whether the credibility benefits exceed the incremental costs and residual risks; tiered output (suitable/conditionally suitable/not suitable) links adoption decisions to clear governance and engineering conditions.

Overall, blockchain can improve ESG disclosure only under specific conditions. It typically requires a mixed arrangement with MRV control, safeguards, access control, and lifecycle cost management. Future research can enhance the framework by testing it in actual ESG disclosure projects and developing measurable metrics such as the MRV robustness, compliance execution, and long-term operating cost.

References

1. Simnett, R., A. Vanstraelen, and W.F. Chua, Assurance on Sustainability Reports: An International Comparison. The Accounting Review, 2009. 84(3): p. 937-967.
2. Lyon, T.P. and A.W. Montgomery, The Means and End of Greenwash. Organization & Environment, 2015. 28(2): p. 223-249. DOI: 10.1177/1086026615575332
3. Thanasi-Boçe, M. and J. Hoxha, Blockchain for Sustainable Development: A Systematic Review. Sustainability, 2025. 17(11). DOI: 10.3390/SU17114848
4. Saberi, S., et al., Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production

Research, 2018. 57(7): p. 2117-2135. DOI: 10.1080/00207543.2018.1533261

5. Patro, P.K., et al., Blockchain-based solution to enhance carbon footprint traceability, accounting, and offsetting in the passenger aviation industry. International Journal of Production Research, 2025: p. 1-34. DOI: 10.1080/00207543.2024.2441450
6. Almadadha, R., Blockchain Technology in Financial Accounting: Enhancing Transparency, Security, and ESG Reporting. Blockchains, 2024. 2(3): p. 312-333.
7. Belchior, R., et al., A Survey on Blockchain Interoperability: Past, Present, and Future Trends. ACM Computing Surveys, 2021. 54(8): p. 1-41.
8. Belen-Saglam, R., et al., A systematic literature review of the tension between the GDPR and public blockchain systems. Blockchain: Research and Applications, 2023. 4(2). DOI: 10.1016/J.BCRA.2023.100129
9. Zafar, A., Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways. Journal of Cybersecurity, 2025. 11(1).

   DOI:10.1093/CYBSEC/TYAF002
10. Hassan, M.U., M.H. Rehmani, and J. Chen, Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. Future Generation Computer Systems, 2019. 97: p. 512-529. DOI: 10.1016/j.future.2019.02.060
11. Sedlmeir, J., et al., The Energy Consumption of Blockchain Technology: Beyond Myth. Business & Information Systems Engineering, 2020. 62(6): p. 599-608. DOI: 10.1007/s12599-020-00656-x
12. Guo, H. and X. Yu, A survey on blockchain technology and its security. Blockchain: Research and Applications, 2022. 3(2).
13. Zimba, A., et al., A systematic literature review of blockchain technology and energy efficiency based on consensus mechanisms, architectural innovations, and sustainable solutions. Discover Analytics, 2025. 3(1). DOI: 10.1007/S44257-025-00041-6
14. Casino, F., T.K. Dasaklis, and C. Patsakis, A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 2019. 36: p. 55-81.