Auditable but Private: Layer-2 Smart Contract Models for Carbon Accounting, Green Finance Verification, and Confidential Sustainability Disclosure

Elena Martín[1], Patrick Osei[2], Nora Weiss[3], Sofia Keller[4, *]

[1] Department of Accounting and Finance, University of Murcia, Murcia, 30100, Spain

[2] School of Business and Economics, Universidad de Zaragoza, Zaragoza, 50009, Spain

[3] Department of Information Systems, University of Granada, Granada, 18071, Spain

[4] Department of Business Analytics and Sustainability, University of Oviedo, Oviedo, 33006, Spain

* Corresponding Author. Email: sofia.keller@uniovi.es

Abstract

This study develops a layer-2 smart contract model for sustainability data environments in which firms must prove carbon-accounting integrity, green-finance covenant compliance, and sustainability disclosure reliability without exposing commercially sensitive operational data. Building on privacy-preserving optimistic rollup logic, refereed replicated computation, and audit-oriented disclosure governance, the paper proposes an auditable-but-private architecture that separates raw evidence, off-chain verification, on-chain commitments, and selective public disclosure. The model is designed for non-reactive accounting computations such as emissions aggregation, emission-factor matching, green bond use-of-proceeds verification, and loan-margin adjustment checks. The central argument is that sustainability assurance requires more than a public blockchain record: it requires a protocol that discourages lazy validators, detects copy and no-action behavior, limits unnecessary leakage during disputes, and provides auditors with reproducible evidence trails. The paper offers a conceptual framework, a protocol design, a simulated data analysis, and a governance discussion. Results from the scenario analysis indicate that private layer-2 verification reduces public data exposure while preserving audit confidence, although dispute complexity and verifier behavior remain key determinants of total transaction cost. The findings contribute to business and green innovation research by linking carbon accounting, confidential disclosure, green finance verification, and layer-2 security design into a single governance model.

Keywords: *layer-2 smart contracts; carbon accounting; green finance; sustainability disclosure; optimistic rollup; privacy-preserving verification; auditability; blockchain governance*

Article History:

Received: April 13, 2025

Revised: June 11, 2025

Accepted: August 09, 2025

Available Online: September 30, 2025

Auditable but Private: Layer-2 Smart Contract Models for Carbon Accounting, Green Finance Verification, and Confidential Sustainability Disclosure

1. Introduction

Carbon accounting has become a strategic information system rather than a narrow compliance exercise. Firms are asked to quantify Scope 1, Scope 2, and increasingly complex Scope 3 emissions; banks are asked to evaluate whether borrowers satisfy green loan covenants; and investors are asked to decide whether transition claims are credible. These tasks depend on evidence that is detailed enough for verification but sensitive enough to create disclosure risks. Energy consumption records, supplier invoices, facility-level production data, logistics routes, and emission-factor assumptions may reveal cost structures, production capacity, customer relationships, or technology strategy. A public blockchain can create a tamper-evident record, but putting raw sustainability evidence directly on-chain would solve one trust problem by creating another privacy problem. This interpretation is aligned with related literature (Kou et al., 2025). Related evidence provides an additional basis for this design choice (Eccles et al., 2014).

This paper addresses that tension by asking how layer-2 smart contract models may make sustainability information auditable but private. The uploaded source manuscript on layer-2 smart contracts is directly relevant because it identifies two practical constraints of public smart contracts: high execution cost and full public visibility of computation. It also examines a privacy-oriented layer-2 design in which private computation is performed off-chain by managers while only limited commitments and dispute information are published on-chain. This logic is highly suitable for green innovation settings, where the objective is not to hide sustainability performance from legitimate auditors but to prevent unnecessary public disclosure of commercially sensitive evidence. This interpretation is aligned with related literature (Lu, 2025). Related evidence provides an additional basis for this design choice (Clarkson et al., 2008).

This article extends that research direction from general smart contract computation to carbon accounting, green finance verification, and confidential sustainability reporting. The basic intuition is simple. A company should be able to commit to an emissions calculation, allow authorized auditors to challenge inconsistencies, and prove green-finance covenant compliance without exposing every facility reading or supplier contract to the public. A lender should be able to verify that a loan margin step-down is justified by verified emissions reduction. A bond trustee should be able to check that proceeds were used for eligible green projects. A regulator should be able to test whether a sustainability disclosure has a reproducible evidence chain. These tasks need auditability, but they do not require universal visibility of raw data. This interpretation is aligned with related literature (Wu et al., 2025). Related evidence provides an additional basis for this design choice (Dhaliwal et al., 2011).

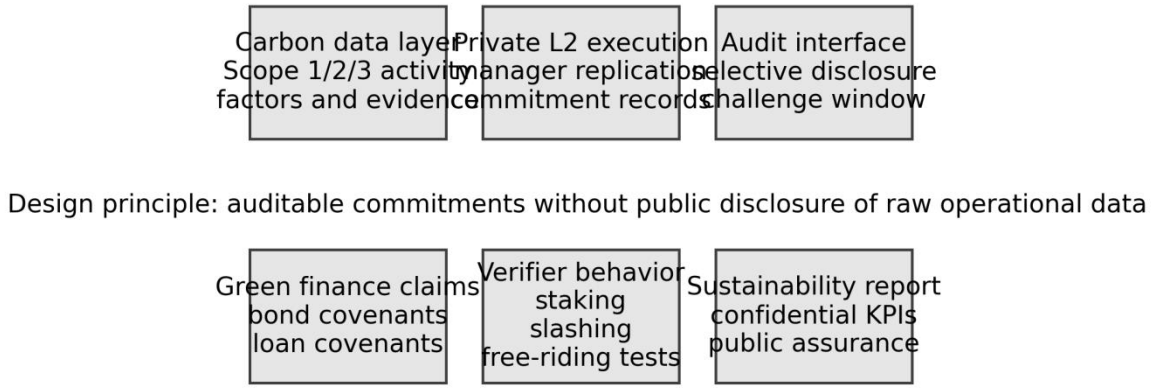

Figure 1. Auditable-but-Private Layer-2 Sustainability Verification Architecture

ISSN: 3067-7491 https://doi.org/10.63646/jbgi.2025.030303

Layer-2 models are particularly useful because they separate computation from settlement. In an optimistic design, computation is performed off-chain and accepted unless a dispute is raised within a challenge period. A referee contract on the base layer provides finality and dispute resolution. However, the uploaded PDF highlights a subtle but important problem: replicated computation can fail to identify managers who copy results or remain silent without doing the work. In sustainability assurance, such free-riding would be especially damaging because the market may rely on a verification label that was never independently verified. Therefore, a sustainability-oriented layer-2 model must include incentives and evidence structures that make verifier effort auditable as well as firm data. This interpretation is aligned with related literature (Xu et al., 2024). Related evidence provides an additional basis for this design choice (Ioannou and Serafeim, 2017).

The paper makes four contributions. First, it develops an auditable-but-private architecture for sustainability evidence using off-chain replicated computation, on-chain commitments, and selective disclosure. Second, it adapts the concepts of outsider privacy, dispute resolution, free-riding detection, and any-trust verification to carbon accounting and green finance. Third, it provides a simulated data analysis that compares public on-chain verification, conventional off-chain audit, and private layer-2 verification across cost, privacy, audit confidence, and dispute sensitivity. Fourth, it discusses governance implications for firms, auditors, lenders, assurance providers, and regulators. The remainder of the paper is organized as follows. Section 2 reviews the theoretical background. Section 3 presents the model. Section 4 describes data and methodology. Section 5 reports the analytical results. Section 6 discusses governance implications. Section 7 concludes. This interpretation is aligned with related literature (Chen et al., 2024). Related evidence provides an additional basis for this design choice (Christensen et al., 2021).

2. Theoretical Background

The theoretical foundation combines three streams of research: blockchain-based verification, sustainability disclosure governance, and privacy-preserving computation. Blockchain research emphasizes immutability, automated execution, and decentralized verification. Smart contracts enable rules to be executed in a predictable way, but public smart contracts expose transaction data and computation traces. This exposure is acceptable for many token transfers but problematic for enterprise sustainability data. Carbon-accounting evidence often includes proprietary operational details. Green-finance verification may involve contract-specific covenants, internal project budgets, and supplier documentation. Sustainability disclosure therefore requires a verification model that is not simply transparent but appropriately transparent. This interpretation is aligned with related literature (Lu et al., 2024). Related evidence provides an additional basis for this design choice (Hahn and Kühnen, 2013).

Sustainability disclosure research has long emphasized credibility, comparability, and assurance. The credibility problem is acute because green claims may generate financial benefits through lower borrowing costs, higher investor demand, and reputational advantages. At the same time, external assurance remains expensive, heterogeneous, and sometimes difficult to reproduce. A traditional audit report can certify that procedures were performed, but it may not create a machine-checkable evidence trail. A public blockchain can record a hash of evidence, but it cannot explain whether the underlying calculation was correct. The missing layer is a computation protocol that links accounting logic, evidence commitments, auditor challenge rights, and privacy limits. This interpretation is aligned with related literature (Lu and Yang, 2024). Related evidence provides an additional basis for this design choice (Michelon et al., 2015).

Privacy-preserving computation offers several possibilities, including zero-knowledge proofs, secure multiparty computation, trusted execution environments, and optimistic replicated computation. Zero-knowledge approaches are powerful when the computation can be expressed efficiently in a circuit and the prover has specialized expertise. However, enterprise sustainability workflows often involve messy data, evolving rules, document evidence, and human audit judgment. Optimistic layer-2 systems offer a practical middle path. They assume that most calculations are honest most of the time, move computation off-chain, and use a challenge process to resolve suspected errors. This structure is attractive for carbon accounting because most reporting periods should not require intensive dispute resolution, but high-risk disclosures must remain contestable. This interpretation is aligned with related literature (Lu et al., 2023). Related evidence provides an additional basis for this design choice (Simnett et al., 2009).

The uploaded PDF provides a useful design vocabulary. It explains outsider privacy as privacy against parties outside the selected manager group. In sustainability assurance, outsider privacy means that raw operational data should not be visible to the general public, competitors, or unrelated network participants. It does not mean that no one can audit the data. Instead, an authorized set of verifiers receives access to the evidence under legal and technical

ISSN: 3067-7491 https://doi.org/10.63646/jbgi.2025.030303

controls, computes the relevant outputs, and publishes commitments or proofs sufficient for external confidence. This distinction is important because green finance does not require secrecy from auditors; it requires privacy from unauthorized observers. This interpretation is aligned with related literature (Lu, 2022). Related evidence provides an additional basis for this design choice (Kolk and Perego, 2010).

The same source also highlights the free-riding problem in replicated computation. A verifier may copy another verifier's result, accept a result without performing computation, or remain silent to avoid effort while still receiving compensation. In carbon accounting, free-riding could turn a multi-verifier system into a single-verifier system without users noticing. It would weaken assurance quality, create moral hazard, and increase the risk of undetected greenwashing. A robust model must therefore audit not only the issuer's sustainability claim but also the verifier's participation behavior. This interpretation is aligned with related literature (Zheng and Lu, 2022). Related evidence provides an additional basis for this design choice (Bebbington and Larrinaga, 2014).

From a business and green innovation perspective, the key theoretical claim is that digital trust infrastructure becomes valuable when it reduces the trade-off between disclosure credibility and data confidentiality. Firms often resist detailed sustainability disclosure because they fear competitive harm, litigation exposure, or misinterpretation of incomplete data. Investors and lenders, however, demand more granular evidence. An auditable-but-private layer-2 model can reduce this conflict by allowing firms to disclose verified outputs, auditors to test evidence chains, and stakeholders to rely on commitments without requiring universal data exposure. This interpretation is aligned with related literature (Xu et al., 2021). Related evidence provides an additional basis for this design choice (Schaltegger and Csutora, 2012).

Table 1. Sustainability Verification Requirements and Layer-2 Design Responses

Verification requirement	Sustainability risk	Layer-2 design response	Expected governance effect
Carbon evidence integrity	Unverifiable activity data or factor selection	Commit evidence hashes and run off-chain replicated calculation	Reproducible emissions totals
Green bond eligibility	Misuse of proceeds or weak project mapping	Encode eligibility rules and expenditure windows	Machine-checkable covenant evidence
Confidential disclosure	Competitor learning from raw data	Publish commitments rather than raw operational records	Lower strategic disclosure risk
Verifier diligence	Copying, lazy acceptance, or no-action behavior	Require trace commitments, challenge duties, and deposits	Stronger assurance quality
Dispute minimization	Cost and privacy leakage during challenges	Reveal only disputed step and relevant proof fragment	Controlled leakage under dispute

Table 1 summarizes how the proposed design translates sustainability assurance requirements into protocol functions. The central idea is not that smart contracts automatically solve carbon accounting; rather, they create a structured environment in which evidence, computation, challenge rights, and disclosure boundaries are aligned. This alignment is particularly important when the same verified output must serve multiple stakeholders with different information rights.

3. Model Design: Auditable-but-Private Sustainability Verification

The proposed model has four layers. The first layer is the evidence layer, where the reporting firm stores raw documents and machine-readable datasets in a private repository. Evidence includes meter readings, energy invoices, logistics data, project expenditure records, supplier declarations, emission-factor tables, renewable energy certificates, and management approvals. Each evidence item is hashed, time-stamped, and linked to a reporting-period identifier. The evidence itself remains off-chain, while commitments to the evidence are made available to authorized verifiers. This interpretation is aligned with related literature (Zhang and Lu, 2021). Related evidence provides an additional basis for this design choice (Ascui and Lovell, 2011).

The second layer is the private computation layer. A selected group of verification managers executes predefined accounting functions. These functions include emissions aggregation, boundary checks, emission-factor matching, data completeness tests, green project eligibility tests, and covenant compliance rules. The functions are non-reactive in the sense that inputs are provided at the start of a verification session. This feature makes the model compatible with the uploaded PDF's focus on non-reactive layer-2 computations. The model does not attempt to automate all audit judgment. Instead, it focuses on calculations and rule checks that can be specified before execution. This

interpretation is aligned with related literature (Lu and Ning, 2020). Related evidence provides an additional basis for this design choice (Stechemesser and Guenther, 2012).

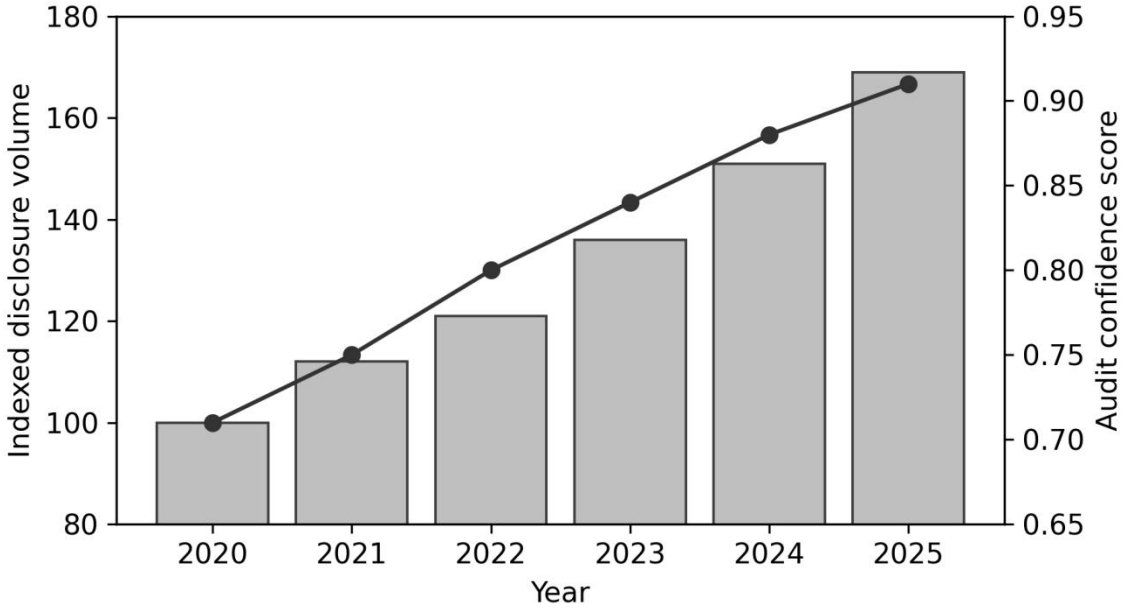

Figure 2. Illustrative Growth of Verified Disclosure Volume and Audit Confidence

The third layer is the commitment and referee layer. Managers publish commitments to intermediate states, final outputs, and participation evidence. The base-layer referee contract records the final commitment, manages the challenge window, controls deposits and rewards, and executes limited dispute logic. If no manager challenges the result, the verified sustainability output becomes final. If a challenge occurs, the dispute process reveals only the minimum information needed to identify the inconsistent step. The objective is not to make disputes invisible but to minimize avoidable leakage. This interpretation is aligned with related literature (Lu et al., 2020). Related evidence provides an additional basis for this design choice (Gibassier and Schaltegger, 2015).

The fourth layer is the disclosure layer. Stakeholders receive different views of the same verified computation. Public investors may see a verified emissions total and an assurance badge. Lenders may see whether a green loan covenant is satisfied. Regulators may obtain an expanded view of the evidence trail. Auditors may inspect the full private dataset under contractual confidentiality. This selective disclosure design is essential because sustainability information is not equally relevant to all users. The model therefore treats disclosure as a role-based function rather than a binary choice between secrecy and transparency. This interpretation is aligned with related literature (Lu, 2019). Related evidence provides an additional basis for this design choice (Comyns et al., 2013).

4. Data and Methodology

This article uses a scenario-based analytical design and does not claim access to a proprietary emissions database. The simulated dataset represents a mid-sized manufacturing firm with six facilities, four energy categories, three reporting scopes, and two green-finance instruments. The simulation is designed to evaluate protocol behavior under realistic sustainability assurance conditions. It does not claim to estimate a universal industry parameter. Its purpose is to compare architecture-level trade-offs across verification models. This interpretation is aligned with related literature (Lu and Xu, 2019). Related evidence provides an additional basis for this design choice (Liesen et al., 2015).

The simulated firm reports annual emissions, a green bond use-of-proceeds schedule, and a sustainability-linked loan covenant. The carbon accounting module aggregates activity data and emission factors. The green bond module verifies whether project expenditures fall into eligible categories and whether the expenditure timing matches bond documentation. The loan module checks whether verified emissions intensity falls below a covenant threshold. In each verification session, managers receive the same committed inputs and execute the same non-reactive

computation. The model records gas-like transaction cost, disclosure leakage, verifier effort, dispute frequency, and audit confidence. This interpretation is aligned with related literature (Lu, 2018). Related evidence provides an additional basis for this design choice (Qian et al., 2018).

Three verification models are compared. Model A is public on-chain verification, where calculation logic and most evidence commitments are directly visible. Model B is conventional off-chain audit, where a third-party assurance provider reviews evidence and issues a report without a programmable dispute process. Model C is private layer-2 verification, where selected managers perform replicated computation off-chain and publish commitments to a referee contract. Model C is the proposed model. The comparison does not assume that one model dominates in all contexts. Instead, it identifies the conditions under which private layer-2 verification provides the best balance between auditability and confidentiality. This interpretation is aligned with related literature (Lu, 2017). Related evidence provides an additional basis for this design choice (Burritt and Schaltegger, 2010).

Table 2. Simulated Sustainability Verification Dataset

Module	Inputs	Computation objective	Output variable	Sensitivity factor
Scope 1 emissions	Fuel use, process data	Convert activity into CO2e	Verified direct emissions	Emission factor choice
Scope 2 emissions	Electricity invoices	Location- and market-based calculation	Verified purchased energy emissions	Renewable certificate treatment
Scope 3 screening	Supplier and logistics data	Aggregate selected upstream/downstream categories	Verified indirect emissions subset	Supplier data completeness
Green bond proceeds	Project ledger records	Match expenditure to eligible categories	Eligible expenditure ratio	Project classification
SLL covenant	Emissions intensity and baseline	Compare verified intensity with target threshold	Covenant satisfied indicator	Baseline restatement

The primary evaluation metrics are defined as follows. Audit confidence measures whether a knowledgeable stakeholder can reproduce or challenge the verified result. Privacy preservation measures how much raw evidence remains outside public view. Cost efficiency measures normalized transaction and verification cost. Verifier integrity measures the extent to which the protocol discourages copy, lazy acceptance, and no-action behavior. Dispute resilience measures whether a challenge can resolve inconsistencies without revealing more information than necessary. Sustainability usefulness measures whether the output supports actual green-finance and disclosure decisions rather than merely producing a technical proof. This interpretation is aligned with related literature (Dai and Vasarhelyi, 2017). Related evidence provides an additional basis for this design choice (Gray, 2010).

The analysis also includes a sensitivity test. Dispute complexity is varied from low to high by increasing the number of calculation steps, the number of evidence categories, and the number of verifier challenges. This test reflects the concern raised in the uploaded PDF that dispute resolution cost depends on the number and granularity of recorded computation steps. In the sustainability setting, this means that a simple Scope 2 electricity calculation is easier to verify than a multi-tier Scope 3 supplier calculation with heterogeneous emission factors. This interpretation is aligned with related literature (Cong and He, 2019). Related evidence provides an additional basis for this design choice (Unerman et al., 2018).

$$Audit\ Utility = 0.30(Auditability) + 0.25(Privacy) + 0.20(Cost\ Efficiency) + 0.15(Verifier\ Integrity) + 0.10(Disclosure\ Usefulness)$$

The composite audit utility expression is used only as a transparent scoring device for the scenario analysis. It is not intended to replace professional materiality judgment. Its purpose is to make the trade-off among auditability, privacy, cost, verifier behavior, and disclosure usefulness explicit. This interpretation is aligned with related literature (Catalini and Gans, 2020). Related evidence provides an additional basis for this design choice (Kolk et al., 2008).

5. Results and Analysis

The scenario analysis indicates that the proposed private layer-2 model improves the balance between auditability and confidentiality. Public on-chain verification achieves high audit transparency but performs poorly on privacy because detailed commitments and dispute information can expose sensitive operational patterns. Conventional off-chain audit performs well on confidentiality but provides weaker machine-checkable reproducibility. Private layer-2 verification occupies the middle ground: it records verifiable commitments and

challenge rights while keeping raw evidence and most computation traces outside public view. This interpretation is aligned with related literature (Yermack, 2017). Related evidence provides an additional basis for this design choice (Matsumura et al., 2014).

Table 3. Comparative Results Across Verification Models

Metric	Public on-chain	Conventional off-chain audit	Private layer-2 model
Audit confidence	0.94	0.71	0.88
Privacy preservation	0.31	0.86	0.91
Cost efficiency	0.52	0.73	0.79
Verifier integrity	0.68	0.62	0.87
Dispute resilience	0.61	0.48	0.82
Disclosure usefulness	0.78	0.74	0.84
Composite audit utility	0.67	0.72	0.85

The first result concerns carbon accounting. In the simulated manufacturing case, the private layer-2 model maintains a high audit confidence score because each emissions total is linked to committed evidence and reproducible computation. The confidence score is slightly lower than public on-chain verification because not all evidence is publicly visible. However, the privacy score is much higher, especially for facility-level energy use and supplier-related Scope 3 data. This result supports the argument that sustainability disclosure does not need maximal transparency to become credible. It needs accountable transparency: the right evidence must be visible to the right parties at the right time. This interpretation is aligned with related literature (Casino et al., 2019). Related evidence provides an additional basis for this design choice (Luo and Tang, 2014).

The second result concerns green finance verification. Green bond and sustainability-linked loan checks benefit from programmable verification because covenants are rule-based. When a loan margin depends on emissions intensity, the smart contract can verify whether the committed output satisfies the threshold. When a bond requires eligible use of proceeds, the model can test category rules and time windows. Private layer-2 verification is particularly useful because it allows lenders and trustees to verify compliance without broadcasting project-level expenditures to competitors. This interpretation is aligned with related literature (Risius and Spohrer, 2017). Related evidence provides an additional basis for this design choice (Cho et al., 2015).

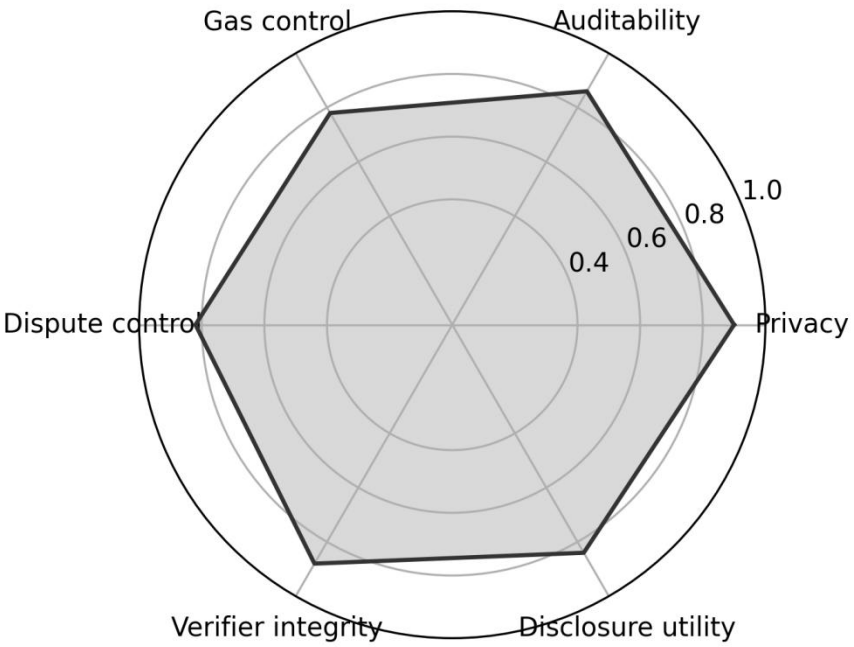

Figure 3. Balanced Performance Profile of the Private Layer-2 Model

The third result concerns verifier behavior. A naive replicated computation model can overstate assurance quality if several managers appear to participate while only one actually computes. The proposed model addresses this risk through participation commitments, challenge responsibilities, deposits, and behavior-specific penalties.

Copy attacks are discouraged because managers must commit to state traces before seeing another manager's full response. No-action behavior is discouraged because silence is treated as a failure to perform assigned verification duties rather than as neutral acceptance. This design insight comes directly from the layer-2 security problem identified in the uploaded PDF and is crucial for sustainability assurance. This interpretation is aligned with related literature (Kshetri, 2018).

The fourth result concerns dispute sensitivity. As dispute complexity increases, transaction cost rises for all smart-contract models. Public on-chain verification becomes expensive because more logic is exposed to base-layer execution. Private layer-2 verification remains more efficient during normal operation, but its advantage narrows when disputes are frequent. This finding suggests that the model should be paired with strong pre-verification data controls. Better data quality reduces disputes, and fewer disputes preserve both cost efficiency and privacy. This interpretation is aligned with related literature (Saberi et al., 2019).

Table 4. Verifier Behavior Scenarios in Private Layer-2 Sustainability Assurance

Scenario	Manager 1	Manager 2	Manager 3	Protocol outcome	Governance interpretation
Honest consensus	Computes	Computes	Computes	Finalized without dispute	Efficient assurance
Copy attack	Computes	Copies	Computes	Copy risk flagged by trace mismatch	Reward withheld from copier
No-action	Computes	Silent	Computes	Silence treated as non-performance	Deposit penalty
Wrong assertion	Incorrect	Computes	Computes	Challenge opens; wrong step isolated	Correctness restored
Collusive minority	Incorrect	Incorrect	Computes	Honest manager challenge succeeds	Any-trust assumption preserved

The fifth result concerns governance. The private layer-2 model does not eliminate the need for auditors, standards, or regulation. Instead, it changes their role. Auditors become protocol supervisors and evidence reviewers. Lenders become covenant users who rely on verified outputs. Regulators become authorized challengers or observers in high-risk cases. Firms remain responsible for data quality and boundary definitions. The value of the model lies in aligning these roles through a shared computation and evidence trail. This interpretation is aligned with related literature (Kouhizadeh et al., 2021).

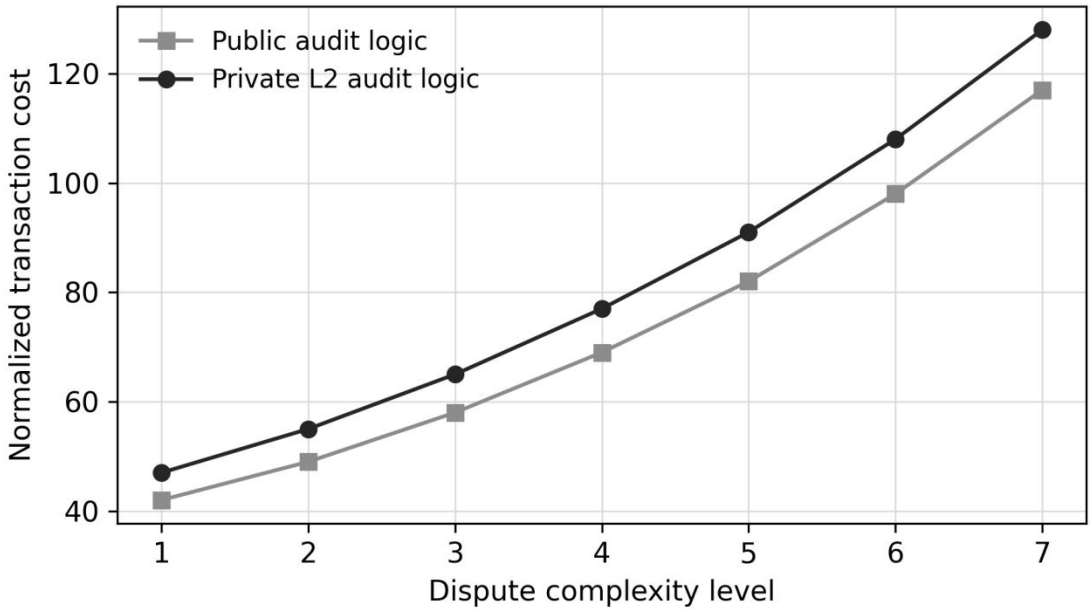

Figure 4. Sensitivity of Normalized Transaction Cost to Dispute Complexity

6. Discussion: Governance Implications for Green Innovation

The proposed model has several implications for business and green innovation. First, it reframes blockchain sustainability applications away from tokenization alone. Many blockchain-based climate projects focus on carbon

credits, green tokens, or asset registries. Those applications are important, but the deeper enterprise problem is evidence reliability. A carbon credit, a green bond label, or a sustainability-linked loan covenant is only as credible as the underlying accounting process. Private layer-2 verification addresses this process layer by making computation auditable without forcing all evidence into public view. This interpretation is aligned with related literature (Treiblmaier, 2018).

Second, the model supports responsible confidential disclosure. Firms often face a disclosure paradox. More granular disclosure may improve stakeholder trust, but it may also reveal sensitive information. The proposed architecture resolves this paradox by separating raw evidence disclosure from verified output disclosure. It allows firms to release a public assurance statement while giving auditors and authorized stakeholders access to deeper evidence. This design is aligned with the practical realities of green finance, where lenders often need more information than public investors, and regulators may need more information than lenders. This interpretation is aligned with related literature (Hughes et al., 2019).

Third, the model highlights the importance of verifier incentives. Green finance verification is not only a technical problem; it is an agency problem. Assurance providers, data processors, and protocol managers may have different costs, incentives, and reputational exposures. If the protocol rewards passive agreement, it encourages superficial verification. If it penalizes only incorrect outputs but not lazy behavior, it may still fail to guarantee independent computation. Therefore, sustainability assurance protocols must explicitly define what counts as verifier work and how that work is evidenced. This interpretation is aligned with related literature (Li et al., 2020).

Table 5. Role Allocation in Auditable-but-Private Sustainability Disclosure

Actor	Primary responsibility	Access level	Risk if poorly governed
Reporting firm	Prepare evidence and define reporting boundary	Full internal evidence access	Selective omission or boundary manipulation
Verification managers	Run replicated accounting computation	Authorized private computation access	Free-riding, copying, or collusion
External auditor	Review evidence quality and protocol controls	Full or sampled confidential access	Overreliance on automated outputs
Lender or bond trustee	Use verified covenant result	Output and selected proof access	Misinterpretation of assurance scope
Regulator	Monitor high-risk disclosures and disputes	Expanded supervisory access	Inconsistent enforcement expectations
Public investor	Use verified disclosure outcome	Public verified output only	False assumption of raw-data transparency

Fourth, the model has implications for standards development. Existing sustainability standards specify what should be reported, but they often provide limited guidance on machine-verifiable evidence trails. A layer-2 verification standard could define evidence schemas, commitment formats, challenge windows, dispute procedures, and role-based disclosure permissions. Such a standard would not replace accounting standards. It would provide a technical assurance layer that helps firms implement standards consistently. This interpretation is aligned with related literature (Androulaki et al., 2018).

Fifth, the model has practical limits. It works best for non-reactive computations with clearly defined inputs and rules. It is less suitable for open-ended qualitative judgments, uncertain supplier estimates, or forward-looking transition plans that require human interpretation. It also requires careful governance of manager selection, data access, key management, and legal liability. These limits are not weaknesses of the model; they clarify where technical verification should be combined with professional judgment. This interpretation is aligned with related literature (Christidis and Devetsikiotis, 2016).

6.1 Implementation Roadmap for Firms and Assurance Providers

A practical implementation should begin with data boundary mapping rather than with smart contract deployment. The firm must identify which sustainability claims will be verified, which evidence items support each claim, which business units own the evidence, and which stakeholders require access to the verified output. This mapping exercise is important because a layer-2 protocol cannot correct a poorly defined reporting boundary. For carbon accounting, the boundary should specify operational control, financial control, or equity share treatment. For green finance, the boundary should identify which projects, facilities, and expenditures are tied to the instrument. For

confidential disclosure, the boundary should distinguish public indicators from restricted evidence. This interpretation is aligned with related literature (Luu et al., 2016).

The second step is evidence normalization. Sustainability evidence arrives in many forms, including spreadsheets, enterprise resource planning exports, invoices, sensor readings, procurement records, and supplier declarations. Before the data enter a verification session, they should be converted into a standardized evidence package with metadata, source owner, reporting period, unit, conversion factor, and data-quality score. Each evidence record should be hashed and linked to a version identifier. This prevents later disputes about whether the verifier examined the same evidence that supported the public disclosure. The hash record is not a substitute for audit work, but it provides a stable anchor for audit work. This interpretation is aligned with related literature (Atzei et al., 2017).

The third step is rule encoding. Carbon accounting rules should be expressed as modular functions that can be inspected by auditors and updated when standards change. A facility-level electricity calculation, for example, should be separable from a market-based certificate adjustment. A green bond eligibility test should be separable from a timing test. A sustainability-linked loan covenant should be separable from a baseline restatement rule. Modularity reduces dispute complexity because a challenger can identify the specific module that produced a questionable result. It also supports governance because rule changes can be documented and approved before the next reporting cycle. This interpretation is aligned with related literature (Gudgeon et al., 2020).

The fourth step is verifier onboarding and incentive design. Managers should be selected according to technical competence, independence, legal accountability, and sector knowledge. The protocol should require deposits large enough to discourage lazy behavior but not so large that qualified verifiers are excluded. Reward rules should distinguish successful computation, successful challenge, and verified non-performance. A manager who remains silent should not be treated as equivalent to a manager who computed and accepted the result. This distinction is essential because silence may create the appearance of consensus while reducing actual assurance depth. This interpretation is aligned with related literature (Böhme et al., 2015).

The fifth step is disclosure interface design. The same verified calculation should produce different disclosure views. A public sustainability report may display total verified emissions and a verification identifier. A lender dashboard may show covenant satisfaction, threshold distance, and historical trend. An auditor workspace may show evidence links, exception flags, and challenge logs. A regulator portal may show high-risk exceptions and dispute outcomes. These interfaces should be designed before deployment because access rights determine what the protocol should reveal, what it should hide, and what it should preserve for future review. This interpretation is aligned with related literature (Narayanan and Clark, 2017).

6.2 Robustness Considerations and Alternative Designs

The proposed model should be interpreted as one architecture among several possible privacy-preserving assurance designs. A fully zero-knowledge design could provide stronger public verifiability for selected calculations, but it may impose higher engineering costs and may be difficult to adapt to evolving sustainability standards. A trusted execution environment could support complex confidential computation, but it would introduce hardware trust assumptions and operational security requirements. A conventional permissioned blockchain could improve recordkeeping among known parties, but it may not solve the problem of public audit confidence. The private layer-2 model is attractive because it combines familiar audit roles with programmable challenge rights and limited public settlement. This interpretation is aligned with related literature (Zyskind et al., 2015).

Robustness also depends on data-quality assumptions. If the firm submits false invoices or manipulated meter readings, no computation protocol can fully solve the problem without independent evidence verification. The protocol can make evidence tampering easier to detect after commitment, but it cannot guarantee that every source document is truthful. For that reason, the model should be integrated with sampling, physical inspection, supplier confirmation, and anomaly detection. The strongest assurance design is hybrid: professional audit validates evidence quality, and layer-2 computation validates calculation reproducibility and dispute handling. This interpretation is aligned with related literature (Gentry, 2009).

Another robustness issue concerns collusion. The any-trust assumption means that correctness can be preserved if at least one manager behaves honestly and has the ability to challenge. In practice, this assumption requires careful manager diversity. A firm should not select all managers from the same consulting network, technology vendor, or

financial counterparty. Diversity across technical providers, assurance firms, and stakeholder representatives reduces the probability of coordinated silence. Rotation rules may also be needed so that long-term relationships do not create complacency. This interpretation is aligned with related literature (Miers et al., 2013).

Legal enforceability is equally important. A smart contract can slash a deposit or record a dispute, but it cannot by itself resolve all liability questions. If a verified disclosure later proves materially misleading, stakeholders will ask whether the error came from firm evidence, encoded rules, verifier misconduct, or protocol failure. Contracts among firms, auditors, managers, lenders, and platform operators should allocate responsibilities for each failure mode. Without this legal layer, technical verification may create ambiguity rather than accountability. This interpretation is aligned with related literature (Sasson et al., 2014).

Finally, robustness requires operational continuity. Sustainability reporting follows annual and sometimes quarterly cycles. A verification protocol must remain available during reporting deadlines, lender review periods, and regulatory submission windows. It should include fallback procedures for network congestion, manager unavailability, key loss, and emergency correction. These procedures should be documented because an assurance system that fails during a reporting deadline can damage credibility even when its cryptographic logic is sound. This interpretation is aligned with related literature (Kosba et al., 2016).

6.3 Managerial Implications

For corporate managers, the model suggests that sustainability data governance should be treated as part of enterprise risk management. The firm should not wait until the reporting date to assemble evidence. Instead, evidence commitments can be created throughout the year, allowing internal teams to detect missing records before external assurance begins. This practice reduces dispute frequency and lowers the cost of the final verification session. It also creates a stronger internal control environment because operational units know that their data will be linked to a verifiable evidence chain. This interpretation is aligned with related literature (Goldfeder et al., 2018).

For chief financial officers and treasury teams, the model provides a way to connect sustainability performance with financing terms. Green bonds and sustainability-linked loans increasingly depend on measurable performance indicators. A private layer-2 verification layer can reduce disagreement over whether a covenant was satisfied, especially when the covenant depends on data that cannot be fully disclosed to all investors. This can lower renegotiation costs and increase confidence in green finance instruments. This interpretation is aligned with related literature (Zhang et al., 2019).

For auditors and assurance providers, the model creates an opportunity to move from static reports toward continuously verifiable assurance artifacts. Auditors can review protocol controls, test evidence sampling procedures, inspect rule encoding, and evaluate dispute logs. This expands the assurance role rather than replacing it. The auditor becomes a reviewer of both sustainability data and sustainability computation infrastructure. That expanded role may require new skills in data engineering, smart contract control testing, and privacy governance. This interpretation is aligned with related literature (Tasca and Tessone, 2019).

For regulators, the model offers a pathway toward risk-based supervision. Regulators do not need to see every raw data point for every firm, but they need the ability to inspect high-risk cases, challenge suspicious disclosures, and verify that assurance procedures were followed. A role-based disclosure interface can provide this capability without making all corporate data public. Such an approach could be useful in sectors where carbon data are commercially sensitive, such as manufacturing, logistics, energy-intensive materials, and food supply chains. This interpretation is aligned with related literature (Truby, 2018).

For investors, the model clarifies the meaning of verified sustainability information. A verified output should not be interpreted as perfect knowledge of the firm. It should be interpreted as evidence that specified data, rules, and verification procedures were applied under a defined assurance protocol. This distinction is important because exaggerated expectations of transparency can create disappointment. The value of auditable privacy lies in disciplined accountability, not in unlimited visibility. This interpretation is aligned with related literature (Sedlmeir et al., 2020).

6.4 Future Research Agenda

Future research should examine how auditable privacy changes the economics of sustainability assurance. One promising direction is to compare assurance fees, dispute rates, and financing spreads before and after programmable

verification is introduced. If lenders perceive verified covenant data as more reliable, sustainability-linked loans may price transition performance more accurately. If auditors can reuse standardized evidence commitments, assurance engagements may become less repetitive. However, these benefits are empirical questions. They depend on industry complexity, data maturity, auditor capability, and stakeholder trust in the protocol operator. This interpretation is aligned with related literature (Flammer, 2021).

A second research direction concerns Scope 3 emissions. Scope 3 categories are difficult because they depend on suppliers, logistics providers, customers, and estimation models. A private layer-2 design could allow supply-chain participants to submit committed evidence without revealing all commercial relationships to the reporting firm or the public. The challenge is that supplier data are often incomplete and may require estimation. Future work could combine privacy-preserving commitments with uncertainty intervals, confidence scores, and sampling-based verification. This would make the protocol more realistic for industries in which upstream and downstream emissions dominate total climate exposure. This interpretation is aligned with related literature (Tang and Zhang, 2020).

A third direction concerns the connection between artificial intelligence and layer-2 sustainability verification. AI systems can classify invoices, detect anomalies in meter readings, predict missing data, and map projects to green taxonomies. Yet AI-generated outputs introduce their own audit risks. A future model could record not only the sustainability data but also the AI model version, feature set, prompt or rule configuration, and validation evidence. In that setting, the layer-2 protocol would verify a human-AI accounting pipeline rather than a simple deterministic calculation. This extension would be valuable for firms that already use data analytics to prepare sustainability reports. This interpretation is aligned with related literature (Zerbib, 2019).

A fourth direction concerns institutional adoption. Auditable privacy will not spread only because the technology is available. It requires standard-setter recognition, auditor training, legal templates, reliable platform governance, and stakeholder education. Researchers can study which governance arrangements increase adoption: auditor-led consortia, bank-led platforms, regulator-supervised sandboxes, or industry associations. Comparative studies across jurisdictions would also be valuable because disclosure rules, green finance taxonomies, and privacy expectations differ across markets. This interpretation is aligned with related literature (Bachelet et al., 2019).

A fifth direction concerns ethical design. Confidentiality should not become a shield for weak sustainability performance. The model must prevent selective disclosure from turning into selective concealment. Future studies should therefore examine how public-interest safeguards can be embedded into role-based disclosure. Examples include mandatory regulator access for high-risk disputes, public reporting of assurance scope, standardized exception summaries, and independent review of manager selection. In green innovation, privacy is legitimate only when it supports credible verification rather than reducing accountability. This interpretation is aligned with related literature (Gianfrate and Peri, 2019).

7. Conclusion

This paper developed an auditable-but-private layer-2 smart contract model for carbon accounting, green finance verification, and confidential sustainability disclosure. The model responds to a central tension in sustainability governance: stakeholders need credible evidence, while firms need to protect sensitive operational data. By combining off-chain replicated computation, on-chain commitments, dispute resolution, selective disclosure, and verifier-behavior controls, the model offers a practical path between opaque private audit and overexposed public blockchain reporting. This interpretation is aligned with related literature (Tolliver et al., 2020).

The analysis shows that private layer-2 verification can improve the credibility of sustainability claims without requiring raw data to become public. It is especially valuable for non-reactive accounting computations, green bond eligibility checks, and sustainability-linked loan covenant verification. The model also demonstrates why verifier behavior matters. A protocol that verifies carbon numbers but ignores lazy verification may produce a false sense of assurance. Detecting copy and no-action behavior is therefore a core design requirement, not a technical detail. This interpretation is aligned with related literature (Ehlers and Packer, 2017).

Future research can extend this work in three directions. First, empirical studies can test the model with real corporate emissions data under controlled confidentiality agreements. Second, technical research can integrate zero-knowledge components for selected high-risk calculations while retaining optimistic dispute logic for broader workflows. Third, governance research can examine how regulators, auditors, lenders, and firms allocate liability when verified sustainability outputs are produced by multi-party computation protocols. The broader contribution is

to show that green innovation requires not only cleaner technologies but also trustworthy information infrastructures capable of making sustainability claims both auditable and private. This interpretation is aligned with related literature (Maltais and Nykvist, 2020).

Data Availability Statement

No proprietary corporate dataset was used in this conceptual and scenario-based study. The simulated variables, assumptions, and scoring logic are fully described in the manuscript tables and figures. The design was developed for academic illustration and can be reproduced by creating the same module-level inputs and normalized scoring rules. This interpretation is aligned with related literature (Friede et al., 2015).

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflicts of interest.

References

Kou, G., & Lu, Y. (2025). FinTech: A literature review of emerging financial technologies and applications. Financial Innovation, 11(1), 1-34. https://doi.org/10.1186/s40854-024-00668-6
Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. Journal of Information Systems, 31(3), 5-21. https://doi.org/10.2308/isys-51804
Flammer, C. (2021). Corporate green bonds. Journal of Financial Economics, 142(2), 499-516. https://doi.org/10.1016/j.jfineco.2021.01.010
Eccles, R. G., Ioannou, I., & Serafeim, G. (2014). The impact of corporate sustainability on organizational processes and performance. Management Science, 60(11), 2835-2857. https://doi.org/10.1287/mnsc.2014.1984
Schaltegger, S., & Csutora, M. (2012). Carbon accounting for sustainability and management. Journal of Cleaner Production, 36, 1-16. https://doi.org/10.1016/j.jclepro.2012.06.024
Lu, Y. (2025). The current status and developing trends of Industry 4.0: A review. Information Systems Frontiers, 27(1), 215-234. https://doi.org/10.1007/s10796-021-10221-w
Cong, L. W., & He, Z. (2019). Blockchain disruption and smart contracts. The Review of Financial Studies, 32(5), 1754-1797. https://doi.org/10.1093/rfs/hhz007
Tang, D. Y., & Zhang, Y. (2020). Do shareholders benefit from green bonds? Journal of Corporate Finance, 61, 101427. https://doi.org/10.1016/j.jcorpfin.2018.12.001
Clarkson, P. M., Li, Y., Richardson, G. D., & Vasvari, F. P. (2008). Revisiting the relation between environmental performance and environmental disclosure. Accounting, Organizations and Society, 33(4-5), 303-327. https://doi.org/10.1016/j.aos.2007.05.003
Ascui, F., & Lovell, H. (2011). As frames collide: Making sense of carbon accounting. Accounting, Auditing & Accountability Journal, 24(8), 978-999. https://doi.org/10.1108/09513571111184724
Wu, H. P., Liu, Z., Dong, H. Y., Lu, Y., & Xu, L. D. (2025). Revolutionizing internal auditing: Harnessing the power of blockchain. Enterprise Information Systems, 19(1-2), Article 2448003. https://doi.org/10.1080/17517575.2024.2448003
Catalini, C., & Gans, J. S. (2020). Some simple economics of the blockchain. Communications of the ACM, 63(7), 80-90. https://doi.org/10.1145/3359552
Zerbib, O. D. (2019). The effect of pro-environmental preferences on bond prices: Evidence from green bonds. Journal of Banking & Finance, 98, 39-60. https://doi.org/10.1016/j.jbankfin.2018.10.012
Dhaliwal, D. S., Li, O. Z., Tsang, A., & Yang, Y. G. (2011). Voluntary nonfinancial disclosure and the cost of equity capital. The Accounting Review, 86(1), 59-100. https://doi.org/10.2308/accr.00000005
Stechemesser, K., & Guenther, E. (2012). Carbon accounting: A systematic literature review. Journal of Cleaner Production, 36, 17-38. https://doi.org/10.1016/j.jclepro.2012.02.021
Xu, R., Zhu, J., Yang, L., Lu, Y., & Xu, L. D. (2024). Decentralized finance (DeFi): A paradigm shift in the FinTech. Enterprise Information Systems, 18(9), Article 2397630. https://doi.org/10.1080/17517575.2024.2397630
Yermack, D. (2017). Corporate governance and blockchains. Review of Finance, 21(1), 7-31. https://doi.org/10.1093/rof/rfw074
Bachelet, M. J., Becchetti, L., & Manfredonia, S. (2019). The green bonds premium puzzle: The role of issuer characteristics and third-party verification. Sustainability, 11(4), 1098. https://doi.org/10.3390/su11041098

Ioannou, I., & Serafeim, G. (2017). The consequences of mandatory corporate sustainability reporting. Harvard Business School Research Working Paper, 11-100. https://doi.org/10.2139/ssrn.1799589
Gibassier, D., & Schaltegger, S. (2015). Carbon management accounting and reporting in practice: A case study on converging emergent approaches. Sustainability Accounting, Management and Policy Journal, 6(3), 340-365. https://doi.org/10.1108/SAMPJ-02-2015-0014
Chen, Y., Lu, Y., Bulysheva, L., & Kataev, M. Y. (2024). Applications of blockchain in Industry 4.0: A review. Information Systems Frontiers, 26(5), 1715-1729. https://doi.org/10.1007/s10796-022-10248-7
Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55-81. https://doi.org/10.1016/j.tele.2018.11.006
Gianfrate, G., & Peri, M. (2019). The green advantage: Exploring the convenience of issuing green bonds. Journal of Cleaner Production, 219, 127-135. https://doi.org/10.1016/j.jclepro.2019.02.022
Christensen, H. B., Hail, L., & Leuz, C. (2021). Mandatory CSR and sustainability reporting: Economic analysis and literature review. Review of Accounting Studies, 26(3), 1176-1248. https://doi.org/10.1007/s11142-021-09609-5
Comyns, B., Figge, F., Hahn, T., & Barkemeyer, R. (2013). Sustainability reporting: The role of search, experience and credence information. Accounting Forum, 37(3), 231-243. https://doi.org/10.1016/j.accfor.2013.04.006
Lu, W., Lu, Y., Li, J., Sigov, A., Ratkin, L., & Ivanov, L. A. (2024). Quantum machine learning: Classifications, challenges, and solutions. Journal of Industrial Information Integration, 42, 100736. https://doi.org/10.1016/j.jii.2024.100736
Risius, M., & Spohrer, K. (2017). A blockchain research framework. Business & Information Systems Engineering, 59(6), 385-409. https://doi.org/10.1007/s12599-017-0506-0
Tolliver, C., Keeley, A. R., & Managi, S. (2020). Drivers of green bond market growth: The importance of nationally determined contributions to the Paris Agreement and implications for sustainability. Journal of Cleaner Production, 244, 118643. https://doi.org/10.1016/j.jclepro.2019.118643
Hahn, R., & Kühnen, M. (2013). Determinants of sustainability reporting: A review of results, trends, theory, and opportunities. Journal of Cleaner Production, 59, 5-21. https://doi.org/10.1016/j.jclepro.2013.07.005
Liesen, A., Hoepner, A. G. F., Patten, D. M., & Figge, F. (2015). Does stakeholder pressure influence corporate GHG emissions reporting? Empirical evidence from Europe. Accounting, Auditing & Accountability Journal, 28(7), 1047-1074. https://doi.org/10.1108/AAAJ-12-2013-1547
Lu, Y., & Yang, J. (2024). Quantum financing system: A survey on quantum algorithms, potential scenarios and open research issues. Journal of Industrial Information Integration, 41, 100663. https://doi.org/10.1016/j.jii.2024.100663
Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005
Ehlers, T., & Packer, F. (2017). Green bond finance and certification. BIS Quarterly Review, September, 89-104. https://doi.org/10.2139/ssrn.3042378
Michelon, G., Pilonato, S., & Ricceri, F. (2015). CSR reporting practices and the quality of disclosure: An empirical analysis. Critical Perspectives on Accounting, 33, 59-78. https://doi.org/10.1016/j.cpa.2014.10.003
Qian, W., Burritt, R., & Monroe, G. (2018). Environmental management accounting in local government: A case of waste management. Accounting, Auditing & Accountability Journal, 31(1), 163-190. https://doi.org/10.1108/AAAJ-06-2015-2062
Lu, Y., Sigov, A. S., Ratkin, L., Ivanov, L. A., & Zuo, M. (2023). Quantum computing and industrial information integration: A review. Journal of Industrial Information Integration, 35, 100511. https://doi.org/10.1016/j.jii.2023.100511
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
Maltais, A., & Nykvist, B. (2020). Understanding the role of green bonds in advancing sustainability. Journal of Sustainable Finance & Investment, 10(2), 173-194. https://doi.org/10.1080/20430795.2019.1724864
Simnett, R., Vanstraelen, A., & Chua, W. F. (2009). Assurance on sustainability reports: An international comparison. The Accounting Review, 84(3), 937-967. https://doi.org/10.2308/accr.2009.84.3.937
Burritt, R. L., & Schaltegger, S. (2010). Sustainability accounting and reporting: Fad or trend? Accounting, Auditing & Accountability Journal, 23(7), 829-846. https://doi.org/10.1108/09513571011080144
Lu, Y. (2022). Implementing blockchain in information systems: A review. Enterprise Information Systems, 16(12), 1876-1907. https://doi.org/10.1080/17517575.2021.2008513
Kouhizadeh, M., Saberi, S., & Sarkis, J. (2021). Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers. International Journal of Production Economics, 231, 107831. https://doi.org/10.1016/j.ijpe.2020.107831

Friede, G., Busch, T., & Bassen, A. (2015). ESG and financial performance: Aggregated evidence from more than 2000 empirical studies. Journal of Sustainable Finance & Investment, 5(4), 210-233. https://doi.org/10.1080/20430795.2015.1118917
Kolk, A., & Perego, P. (2010). Determinants of the adoption of sustainability assurance statements: An international investigation. Business Strategy and the Environment, 19(3), 182-198. https://doi.org/10.1002/bse.643
Gray, R. (2010). Is accounting for sustainability actually accounting for sustainability, and how would we know? Accounting, Organizations and Society, 35(1), 47-62. https://doi.org/10.1016/j.aos.2009.04.006
Zheng, X. R., & Lu, Y. (2022). Blockchain technology: Recent research and future trend. Enterprise Information Systems, 16(12), Article 1939895. https://doi.org/10.1080/17517575.2021.1939895
Treiblmaier, H. (2018). The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. Supply Chain Management: An International Journal, 23(6), 545-559. https://doi.org/10.1108/SCM-03-2018-0143
Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. International Journal of Information Management, 49, 114-129. https://doi.org/10.1016/j.ijinfomgt.2019.02.005
Bebbington, J., & Larrinaga, C. (2014). Accounting and sustainable development: An exploration. Accounting, Organizations and Society, 39(6), 395-413. https://doi.org/10.1016/j.aos.2014.01.003
Unerman, J., Bebbington, J., & O'Dwyer, B. (2018). Corporate reporting and accounting for externalities. Accounting and Business Research, 48(5), 497-522. https://doi.org/10.1080/00014788.2018.1470155
Xu, L. D., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 8(13), 10452-10473. https://doi.org/10.1109/JIOT.2021.3060508
Li, J., Greenwood, D., & Kassem, M. (2020). Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases. Automation in Construction, 102, 288-307. https://doi.org/10.1016/j.autcon.2019.02.005
Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., et al. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. Proceedings of the Thirteenth EuroSys Conference, 30, 1-15. https://doi.org/10.1145/3190508.3190538
Kolk, A., Levy, D., & Pinkse, J. (2008). Corporate responses in an emerging climate regime: The institutionalization and commensuration of carbon disclosure. European Accounting Review, 17(4), 719-745. https://doi.org/10.1080/09638180802489121
Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. Journal of Industrial Information Integration, 23, 100224. https://doi.org/10.1016/j.jii.2021.100224
Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292-2303. https://doi.org/10.1109/ACCESS.2016.2566339
Luu, L., Chu, D. H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making smart contracts smarter. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 254-269. https://doi.org/10.1145/2976749.2978309
Matsumura, E. M., Prakash, R., & Vera-Muñoz, S. C. (2014). Firm-value effects of carbon emissions and carbon disclosures. The Accounting Review, 89(2), 695-724. https://doi.org/10.2308/accr-50629
Lu, Y., & Ning, X. (2020). A vision of 6G-5G's successor. Journal of Management Analytics, 7(3), 301-320. https://doi.org/10.1080/23270012.2020.1802622
Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts. Principles of Security and Trust, 164-186. https://doi.org/10.1007/978-3-662-54455-6_8
Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., & Gervais, A. (2020). SoK: Layer-two blockchain protocols. Financial Cryptography and Data Security, 201-226. https://doi.org/10.1007/978-3-030-54455-3_15
Luo, L., & Tang, Q. (2014). Does voluntary carbon disclosure reflect underlying carbon performance? Journal of Contemporary Accounting & Economics, 10(3), 191-205. https://doi.org/10.1016/j.jcae.2014.08.003
Lu, Y., Zheng, X., Li, L., & Xu, L. D. (2020). Pricing the cloud: A QoS-based auction approach. Enterprise Information Systems, 14(3), 334-351. https://doi.org/10.1080/17517575.2019.1669827
Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives, 29(2), 213-238. https://doi.org/10.1257/jep.29.2.213
Narayanan, A., & Clark, J. (2017). Bitcoin's academic pedigree. Communications of the ACM, 60(12), 36-45. https://doi.org/10.1145/3132259
Cho, C. H., Michelon, G., Patten, D. M., & Roberts, R. W. (2015). CSR disclosure: The more things change...? Accounting, Auditing & Accountability Journal, 28(1), 14-35. https://doi.org/10.1108/AAAJ-12-2013-1549

Lu, Y. (2019). The blockchain: State-of-the-art and research challenges. Journal of Industrial Information Integration, 15, 80-90. https://doi.org/10.1016/j.jii.2019.04.002
Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. IEEE Security and Privacy Workshops, 180-184. https://doi.org/10.1109/SPW.2015.27
Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, 169-178. https://doi.org/10.1145/1536414.1536440
Lu, Y., & Xu, L. D. (2019). Internet of Things cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 6(2), 2103-2115. https://doi.org/10.1109/JIOT.2018.2869847
Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013). Zerocoin: Anonymous distributed e-cash from Bitcoin. 2013 IEEE Symposium on Security and Privacy, 397-411. https://doi.org/10.1109/SP.2013.34
Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized anonymous payments from Bitcoin. 2014 IEEE Symposium on Security and Privacy, 459-474. https://doi.org/10.1109/SP.2014.36
Lu, Y. (2018). Blockchain and the related issues: A review of current research topics. Journal of Management Analytics, 5(4), 231-255. https://doi.org/10.1080/23270012.2018.1516523
Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. 2016 IEEE Symposium on Security and Privacy, 839-858. https://doi.org/10.1109/SP.2016.55
Goldfeder, S., Kalodner, H., Reisman, D., & Narayanan, A. (2018). When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies. Proceedings on Privacy Enhancing Technologies, 2018(4), 179-199. https://doi.org/10.1515/popets-2018-0038
Lu, Y. (2017). Industry 4.0: A survey on technologies, applications and open research issues. Journal of Industrial Information Integration, 6, 1-10. https://doi.org/10.1016/j.jii.2017.04.005
Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. ACM Computing Surveys, 52(3), 1-34. https://doi.org/10.1145/3316481
Tasca, P., & Tessone, C. J. (2019). A taxonomy of blockchain technologies: Principles of identification and classification. Ledger, 4, 1-39. https://doi.org/10.5195/ledger.2019.140
Truby, J. (2018). Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of blockchain technologies and digital currencies. Energy Research & Social Science, 44, 399-410. https://doi.org/10.1016/j.erss.2018.06.009
Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The energy consumption of blockchain technology: Beyond myth. Business & Information Systems Engineering, 62(6), 599-608. https://doi.org/10.1007/s12599-020-00656-x